Cybersecurity management system of large enterprises: Probabilistic behavioural model

Radek Svadlenka[1]

[1] *Prague University of Economics and Business, Faculty of Management, Department of Exact Methods, Czech Republic, ORCID: 0009-0006-2800-9383, xsvar05@vse.cz.*

Abstract: *This article presents an in-depth examination of the behaviours of large enterprises in managing information security, aiming to develop a model that illustrates the relationships between various cybersecurity variables. Conducted between 2022 and the first half of 2023, the study involved 52 significant organizations in the Czech Republic, offering insights applicable across the European Union. Amidst rising cyber threats, the research evaluates the current cybersecurity landscape within commercial and public institutions, analysing vulnerabilities, defence strategies, and compliance across different sectors. Utilizing interviews with security and IT managers, the study employs frameworks and methodologies including the Center for Internet Security controls and Bloom's taxonomy, to propose a probabilistic model that clarifies the marginal and conditional probabilities of cybersecurity variables. This model aims to support EU regulatory bodies and organizations specializing in cybersecurity services and training. Additionally, the study explores the impact of top management's cybersecurity education on organizational security levels and the economic aspects of information security management. Despite limitations related to sample size and potential respondent bias, this research contributes to the cybersecurity discourse by offering a comprehensive model that facilitates understanding of the complex interplay of factors affecting information security management in large organizations.*

Keywords: *Cyber security, security awareness, security self-assessment, cybersecurity posture, mutual information, probability distribution.*

JEL Classification: *O3.*

APA Style Citation: Svadlenka, R. (2025). Cybersecurity management system of large enterprises: Probabilistic behavioural model. *E&M Economics and Management*, *28*(1), 221–237. https://doi.org/10.15240/tul/001/2025-1-014

Introduction

The primary objective of this article is to evaluate the behaviour of large enterprises in the domain of information security management and, based on the information gathered, to develop a model reflecting the relationships between the studied variables. The secondary objectives include an analysis of the state of cybersecurity in commercial organizations and public institutions, with a breakdown into individual sectors. The research was conducted during the year 2022 and the first half of 2023, involving 52 significant organizations in the Czech Republic. However, the findings are applicable to most European Union countries.

In the ever-evolving digital age, cybersecurity stands as a critical pillar in the operational integrity and resilience of modern organizations. According to a report by Sophos (2023), the frequency and complexity of cyber-attacks have been increasing, underscoring a pressing need for robust cybersecurity measures. One of the paramount challenges in cybersecurity is the complexity of modern IT infrastructures, which are often expansive and interconnected, making them more vulnerable to attacks.

Human factors, including employee behaviour, add another layer of complexity. National Cyber and Information Security Agency (2023) highlights that inadvertent employee errors or deliberate actions can significantly compromise an organization's cybersecurity. Furthermore, navigating the legal and regulatory landscape, such as compliance with the General Data Protection Regulation (European Parliament and the Council, 2016b) and the Act on cybersecurity 181/2014 Coll. (National Cyber and Information Security Agency, 2014), adds to the complexity of cybersecurity management.

The main results of this article are supported by data collected during the interviews with security and IT managers. However, we start by examining the current state of knowledge in the researched area, particularly concerning the legal framework in cybersecurity. In addition, we will briefly focus on the current obligations and challenges faced by managers responsible for security within an organization. We will also touch upon some tools that can be utilized in managing cybersecurity in an organization. In the next part of the article, we will guide the reader through the techniques we have decided to use for data collection in our research. The ethical aspect of the research, which was crucial for the effective collection of relevant data considering the studied area, cannot be overlooked. In the following part of the article, we will present the used analytical procedures based on information theory and probability theory. The outputs, conclusions, discussions, and recommendations are then interpreted in the final part of the paper.

This work is based on unique and also very sensitive data, the collection of which was time-consuming. The techniques and procedures used to calculate the model are known from other fields, however, their application to the field of cyber security is an innovative approach for this area.

1. Theoretical background

The role of a manager responsible for the state of cyber security in an organization, typically a chief information security officer (CISO), is currently challenging. On the one hand, the risk associated with dealing with cyber incidents is constantly growing, and the demands for ensuring adequate protection are increasing. However, on the other hand, the resources that would fulfill the security requirements are limited. The main task of the CISO is to ensure the effective protection of the organization against cyberspace threats, however, the necessary resources are usually approved at the level of top management or owners of the organization. However, the willingness of stakeholders to invest in cyber security is influenced by several factors, including their subjective approach to risk. Švadlenka (2021) already pointed out the fact that support from top management or organization owners in the application of cyber security is one of the factors that influence the amount of resources released to this area, and therefore also the overall level of cyber security of the company.

1.1 Security legislation

In the Czech Republic, cyber security is regulated by the Act on cybersecurity, which is managed by the National Office for Cyber and Information Security (Doucek et al., 2019). To ensure information security at the required level, especially in the area of providing critical services for the company, in 2014, the legislative framework defined by Act No. 181/2014 Coll. on cybersecurity and its implementation documentation (National Cyber and Information Security Agency, 2014) was adopted in the Czech Republic. According to this standard, regulated entities have a number of obligations to implement technical and organizational measures, including the necessary security documentation. The development of legislation in the field of cyber security at the international level has not been left behind either. In 2016, Directive 2016/1148, the so-called NIS (European Parliament and the Council, 2016a), entered into force on measures to ensure a high level of security of networks and information systems in the European Union, which stipulated that the member states should bring their national legislation into line with this standard at the latest. As part of the harmonization of European law, Directive 2016/1148 was transposed into the Czech Act on cybersecurity in 2017, which undoubtedly brought new requirements for the organizations concerned. In 2016, with effect from May 25, 2018, Regulation 2016/679 (European Parliament and the Council, 2016b) on the protection of natural persons in connection with the processing of personal data and on the free movement of such data entered into force, which requires the application of many other measures by entities subject to this

standard. Obligations arising from the aforementioned legislative measures are controlled by the relevant state authorities, and non-compliance with the standard may be the cause of a sanction. The latest addition to the field of legislative measures is Directive 2022/2555 (European Parliament and the Council, 2022) on measures to ensure a high standard level of cyber security in the European Union, the so-called NIS2 Directive, which was published in the Official Journal of the European Union on December 27, 2022.

1.2 Security self-assessment

Cybersecurity management in an organization is associated with a process of continuous improvement. However, if we want to improve the sub-components of security, it is necessary to measure them over time and continuously check results (International Organization for Standardization, 2022). Risk analysis is a fundamental tool for working with risks for regulated entities according to the Act on cybersecurity 181/2014 Coll. (National Cyber and Information Security Agency, 2014). However, its implementation and maintenance in the organization's environment require specific knowledge and experience or considerable financial resources for outsourcing these services. However, organizations outside of regulation often cannot or do not want to afford this. This absence results from intuitive security management, which in larger organizations with a complex IT system leads to inefficient cyber security management. An alternative approach for managing Security in an organization can be security self-assessment. Security self-assessment is an essential process for organizations striving to maintain adequate cyber security. By conducting a self-assessment, organizations can gain a comprehensive understanding of their security posture, identify potential vulnerabilities, and prioritize their efforts to address them. In addition, security self-assessments can help organizations meet the regulatory requirements and standards outlined in the previous chapter.

To achieve thorough and consistent assessments, organizations should employ a systematic approach that incorporates the use of established frameworks and standards. Some of the most commonly used frameworks include the NIST Cybersecurity Framework (National Institute of Standards and Technology, 2023), ISO/IEC 27001 (International Organization for Standardization, 2022), the Cyber Security Evaluation Tool developed by Cybersecurity & Infrastructure Security Agency (2024), and CIS controls (Center for Internet Security, 2022). These frameworks provide a structured methodology for assessment and help ensure that all relevant areas are covered. Utilizing these frameworks enables organizations to systematically identify vulnerabilities, assess risks, and implement appropriate control mechanisms. For instance, the NIST Cybersecurity Framework focuses on five key areas: identify, protect, detect, respond, and recover. These areas cover the entire security management lifecycle and assist organizations in comprehensively evaluating their security posture (Scarfone et al., 2008).

The CIS critical security controls are a set of 18 best practices that organizations can use to improve their cybersecurity posture. These controls are organized into three categories: basic, foundational, and organizational. The basic controls are the most critical, and failure to implement them can result in the most significant security risks. The foundational controls provide additional protections, while the organizational controls help ensure that the security measures are appropriately integrated into the organization's overall structure and culture. The CIS controls cover a range of security measures, including hardware and software security, network security, access control, and incident response. They are designed to be flexible and adaptable to different organizations' needs and resources. CIS controls are an essential tool for organizations to protect their digital assets from cyber threats. With the increasing frequency and sophistication of cyber-attacks, implementing these controls can help reduce the risk of a security breach and minimize the damage if one occurs. CIS controls are designed to apply to organizations of all sizes and industries, making them a valuable resource for businesses, government agencies, and non-profit organizations (Center for Internet Security, 2022).

1.3 Security awareness of top managers and user experience

Security awareness is critical to ensuring the protection of an organization's information assets. While many factors contribute to an organization's overall security posture, the awareness and actions of senior management can

have a significant impact. Senior management plays a crucial role in setting the tone for an organization's security culture. Their attitudes and actions toward security can significantly impact the rest of the organization. If top management prioritizes security, the rest of the organization is more likely to follow suit. Studies have shown that a lack of security awareness among top management can lead to a higher risk of security breaches (Kajava et al., 2007).

However, according to (Švadlenka, 2022), the top manager in the organization performs two different roles from the point of view of security. The first is as a regular user of the organization's ICT services with the risks described above. At the same time, however, it significantly affects the amount of resources flowing into the organization's security measures. For this reason, the information security management system, according to the ISO standard (International Organization for Standardization, 2022), forces top management's involvement in the implementation process. Likewise, Decree No. 82/2018 Coll. (National Cyber and Information Security Agency, 2018) on Security Measures requires the participation of a senior manager (or a person authorized by him) in the meetings of the organization's Cyber Security Committee. However, current legislation no longer establishes any other specific requirements for top management education. The new NIS2 directive already mentions this obligation in Article 20: "Member states shall ensure that the members of the management bodies of essential and important entities are required to follow the training, and shall encourage essential and important entities to offer similar training to their employees regularly, so that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity" (European Parliament and the Council, 2022). However, the question is, in what form will this provision be reflected in the national legislation? One of the possible approaches to monitor and evaluate results in the area of awareness is Bloom's taxonomy (Armstrong, 2010).

Following part of the article introduces the problematics of the intersection of user experience and cybersecurity measures, highlighting the challenges and solutions in balancing security requirements with user convenience. It underscores the significance of user-centric approaches in cybersecurity to enhance both protection and user satisfaction. In the digital era, cybersecurity is paramount for safeguarding data and ensuring privacy. However, stringent security measures often impede user experience, leading to resistance or non-compliance among users. User experience plays a pivotal role in the effectiveness of cybersecurity measures. A study by NIST (National Institute of Standards and Technology) emphasizes that user-friendly security solutions are more likely to be adopted and adhered to by end-users (Grassi et al., 2017). This is echoed by Acquisti et al. (2018), who argue that the complexity of security mechanisms often leads to user frustration and, consequently, weaker security adherence. The primary challenge lies in designing cybersecurity measures that are both secure and user-friendly. Renaud and Zimmermann (2020) highlight that overly complex passwords and frequent authentication requests can lead to "security fatigue."

2. Research methodology

2.1 Data description

To reach the objectives, set out in the introduction, it was necessary to use the processes of conceptualization and operationalization to correctly project the observed phenomena into measurable data. The next task was to define the research sample so that the data obtained would be relevant, minimally subjective, and representative of the domain under study. Finally, we had to decide how to collect the data to maximize the number of responses and address the ethical aspect of the research, which is absolutely critical in the field of cybersecurity.

The complexity of managing cybersecurity increases with the size and complexity of the system in which it is operated. For this reason, we decided to focus on the segment of the largest organizations in the Czech Republic, aiming to obtain data from respondents from both the public and commercial sectors. As a minimum threshold for the research sample, we set 250 employees, which corresponds to the category of a large enterprise according to the terminology of the European Commission's recommendations from 2003 (European Commission, 2003). According to the Czech Statistical Office, as of December 31, 2022 (Czech Statistical Office, 2023), there were 2,411 such organizations, approximately 300

of which are currently regulated by the Act on cybersecurity 181/2014 Coll. (National Cyber and Information Security Agency, 2014).

A total of 60 organizations from various fields were approached to obtain data from at least fifty respondents. We chose to collect data through questionnaire surveys combined with controlled expert interviews. The questionnaires regarding security were directed at the organizations' information security management staff, typically CISOs. Eventually, we managed to obtain data from 52 respondents, 32 of whom are regulated under the Act on cybersecurity. As of December 31, 2022, 414 entities were regulated in the Czech Republic under the Act on cybersecurity. (National Cyber and Information Security Agency, 2023). In total, 30 organizations fall into the public sector and 22 into the commercial segment. The second questionnaire focused on user satisfaction with the organization's security policy. This was addressed to regular IT users from various departments of the organizations in the research sample after consultation with the individual entities. The final phase of data collection was conducted through structured expert interviews with representatives of security and IT departments. A total of 65 respondents from large enterprises helped us uncover the context of organizations from a security management perspective, including specific information not covered by survey research. The structure and number of respondents, including the data collection methods used, are shown in Tab. 1.

Tab. 1: Respondent's position and methods used

Method	Respondent's position	Company size (No. of employees)	No. of respondents
Questionnaire 1	CISO	Large (>249)	52
Questionnaire 2	User	Large (>249)	285
Structured interview	IT/security manager	Large (>249)	28
Structured interview	IT director	Large (>249)	23
Structured interview	CISO	Large (>249)	14

Source: own

During the data collection, we placed the utmost emphasis on the ethical aspect of the research, as the provided data are confidential, and a leak could endanger the security of the organizations involved in the research. Therefore, anonymization and aggregation of all provided information is an absolute necessity. Due to the relatively small research sample, we decided to use a heuristic analysis supported by selected methods of probability theory and information theory instead of conventional statistical methods. The data collection took place in the second half of 2022 and the first half of 2023 in the Czech Republic. The obtained data were processed using Microsoft Excel tools and R statistical software.

An important question in the research was the decision on how to quantify the level of security in an organization. These data are not publicly available due to their sensitive nature, and each company approaches the issue differently. In organizations where an information security management system is implemented, a qualitative risk analysis is usually carried out. However, this analysis is not quantitatively comparable to the risk analysis of another entity, even though it follows a similar methodology. There is a lack of information on how an organization stands in terms of cybersecurity protection compared to similar entities in the market. For this reason, we decided to use the CIS controls guidelines for this purpose, which cover key elements of organizational security across eighteen domains. Given the research sample, oriented exclusively towards large organizations, we could utilize the full complexity of measures in the organizational mode. In creating the questionnaire, we formulated a question for each measure from the eighteen domains with the response options "applied" or "not applied," without the possibility of not responding. Of course,

the reader can argue that often, an organization has partially addressed measures, and this objection is relevant. However, when collecting data, we had to consider the time it took to complete more than 160 questions. Increasing the complexity of the questionnaire would then have a significant impact on its return rate. The data obtained were evaluated on a scale of 0–100% according to the number of measures applied for each domain, and the arithmetic mean was calculated across domains. Any organization can follow this approach and compare the results with reference values according to individual sectors. For the purposes of further work, let's label this variable as *T*. Then *T* takes on the values, we have chosen as follows: very low (the value is from the interval [38;56]), low ((56;67]), medium ((67;75]), high ((75;85]), and very high ((85;99]).

The second variable monitored in our research is the level of knowledge of decision-makers in the field of cybersecurity. For this purpose, we decided to utilize Bloom's taxonomy model and its cognitive domain. The first level of Bloom's taxonomy is the knowledge level, where learners are expected to recall information and facts. At this level, students are required to demonstrate their ability to remember previously learned information (Anderson et al., 2001). The second level of Bloom's taxonomy is the comprehension level, where learners are expected to show their understanding of the material by explaining, summarizing, or paraphrasing information (Krathwohl, 2002). The third level is the application level, where learners are expected to use previously learned information to solve problems or complete tasks (Anderson et al., 2001). At this level, learners apply their knowledge to new situations, often with guidance or assistance from the teacher. The fourth level is the analysis level, where learners are expected to break down complex information into its constituent parts and identify the relationships among them (Krathwohl, 2002). The fifth level is the synthesis level, where learners are expected to combine parts of knowledge to create a new whole or produce something original (Anderson et al., 2001). This level involves higher-order thinking skills, such as creativity and problem-solving. The highest level of Bloom's taxonomy is the evaluation level, where learners are expected to judge the value, quality, or effectiveness of something based on a set of criteria (Krathwohl, 2002). We mapped similarly the knowledge level of the given managers on a scale of 0–4. Zero corresponds to no or minimal knowledge, while four indicates a high maturity of the manager with capabilities for critical evaluation and defense of solutions. In this case, we did not use the option of directly addressing these managers and their self-assessments, as the outputs could be subjectively biased. Instead, we decided to expand the original questionnaire and obtain evaluations from the employees responsible for security in the organization. The questionnaire accounted for the possibility of multiple decision-makers in the process of approving investments in security, each with a different influence. Let us denote this variable as *S*. Then *S* takes on the values very low, low, medium, high, and very high.

Analogously, we approached the third monitored variable, which is the willingness of decision-makers to educate themselves in the field of cybersecurity. Similar to the previous case, we utilized Bloom's taxonomy and its affective domain. According to the developers of the revised Bloom's taxonomy (Taba, 1965), the affective domain includes how we deal with things emotionally, such as feelings, values, appreciation, enthusiasm, motivations, and attitudes. There are five levels in the affective domain, moving through the lowest-order processes to the highest: receiving, responding, valuing, organizing, and characterizing. We mapped similarly the levels of willingness to educate on the various stages of the affective domain using a 0–4 point scale. Zero signifies a level where cybersecurity is completely outside the decision-maker's focus. In contrast, a score of four denotes a state where cybersecurity becomes a passion for the manager, who actively studies available security resources, influencing their behavior and decision-making. With this approach, they also positively affect other employees. Let's denote this variable as *W*. Then *W* takes on the values very low, low, medium, high, and very high.

Cybersecurity investment by large organizations is a critical aspect of their operational strategy, given the increasing prevalence and sophistication of cyber threats. These investments are not only a defensive measure but also a crucial part of maintaining business integrity and customer trust. The magnitude and allocation of these resources vary widely among organizations but are generally

substantial, reflecting the high stakes involved. As part of the research, we decided to evaluate the share of spent resources of the organization on the total expenses of the given company. This share then takes on values on a scale of 0–15%. Let us denote the variable volume of resources invested by organizations in cyber security as *V*. Then *V* takes on the values, we have chosen as follows: very low (the value is from the interval [0;0,5]), low ((0,5;1]), medium ((1;3]), high ((3;5]), and very high ((5;15]).

The goal of security management in an organization is a high level of resistance to threats combined with a positive user experience. With the help of the NIST standard (Grassi et al., 2017), we defined a set of questions aimed at IT users of the same organizations that provided us with the data for the first part of the research. On a scale of 0–3, respondents answered how they are influenced by the organization's security rules during their work. Zero corresponds to a very negative state of the user, in which he is frustrated by the set conditions that prevent or inhibit him from performing work activities. On the contrary, the three corresponds to the fact that the user perceives security as an integral part of his work, which is not limited by security rules. Let us denote the user experience variable as *U*. Then *U* takes on the values very negative, negative, positive, and very positive.

The last variable entering the research is the contextual variable, related to the legal regulation in the field of cyber security. Information on whether the organization is subject to regulation under Act 181/2014 Coll. (National Cyber and Information Security Agency, 2014) is not public. Let us denote this variable as *L*. Then *L* takes on just the two values regulated, and not regulated. All variables defined above are shown in Tab. 2.

Tab. 2: Variables characterizing organizations

Denotation	Variable	Number of values
T	Total security score of the organization	5
S	Security knowledge status of decision-makers	5
W	The willingness of decision-makers to educate themselves	5
V	The volume of resources invested in cybersecurity	5
U	User experience	4
L	Legislation	2

Source: own

2.2 Probability theory tools

Mutual information and Information measure of dependency

Mutual information is a concept from information theory that measures the amount of information we obtain about one random variable by observing another. The definition of mutual information *MI*(*X*;*Y*) between two random variables *X* and *Y* is given by:

$$MI(X;Y) = \sum_{x \in X} \sum_{y \in Y} p(x,y) \cdot \log\left(\frac{p(x,y)}{p(x) \cdot p(y)}\right) \quad (1)$$

where: $p(x,y)$ – the joint probability distribution function of *X* and *Y*; $p(x)$ and $p(y)$ – the marginal probability distribution functions of *X* and *Y*, respectively.

Equation (1) can also be seen as a measure of the divergence (known as a Kullback-Leibler divergence) between the joint distribution $p(x,y)$ and the product of the individual distributions $p(x) \cdot p(y)$. If *X* and *Y* are independent, i.e., $p(x,y) = p(x) \cdot p(y)$, then the mutual information is zero, indicating that knowing *X* provides no information about *Y* (Manning et al., 2008).

To quantify the strength of influence between the above-mentioned variables, we computed mutual information for each pair of variables. To be precise: we do not know the actual probability distributions, we take the relative frequencies from the above-described

Tab. 3: Contingency table for variables *W* and *S*

	Variable *S*					$n_{.j}$
Variable *W*	8	1	0	0	0	9
	2	5	3	3	0	13
	0	2	2	2	0	6
	0	2	5	2	2	11
	0	0	1	2	10	13
$n_{i.}$	10	10	11	9	12	n = 52

Source: own

contingency tables (Tab. 3) as their estimates. So, Equation (1) for computation of an estimate of mutual information *MI*(*W*,*S*) between two considered variables *W* and *S* changes to:

$$MI(W;S) = \frac{1}{n}\sum_{i,j} n_{i,j} \cdot \log_2\left(n\frac{n_{i,j}}{n_{i.} \cdot n_{.j}}\right) \quad (2)$$

where: $n_{i,j}$ – the number appearing on the i^{th} row and j^{th} column in the contingency table; $n_{i.}$ and $n_{.j}$ are the corresponding row and column sums, respectively; n – a total sum in the contingency table, i.e., for Tab. 3, n = 52.

Let's remember a few basic characteristics of mutual information. It gauges the strength of the relationship between variables; the more connected they are, the greater their mutual information. Mutual information is non-negative (it is zero for independent variables). It is also always less than the Shannon entropy of either of the variables involved. Consequently, we frequently opt for its normalized form, commonly referred to as the information measure of dependence defined by the formula:

$$IMD\ (W,S) = \frac{MI\ (W,S)}{\min\left(H(n_{i.}), H(n_{.j})\right)} \quad (3)$$

where:

$$H(n_{i.}) = -\frac{1}{n}\sum_i n_{i.} \cdot \log_2\left(\frac{n_i}{n}\right),$$
$$H(n_{.j}) = -\frac{1}{n}\sum_j n_{.j} \cdot \log_2\left(\frac{n_{.j}}{n}\right). \quad (4)$$

The values of mutual information along with the information measure of dependence pertaining to the variables under examination are systematically arranged in Tab. 4, adhering to a descending sequence based on IMD. The highlighted figures represent those identified by experts as significant and necessitate accurate representation within the ensuing model.

Compositional probabilistic models

A six-dimensional probability distribution encompassing the variables in question is characterized by $2 \cdot 4 \cdot 5^4 - 1 = 4{,}999$ parameters (probabilities). The task of ascertaining this extensive number of parameters exceeds

Tab. 4: Values of information measures for pairs of variables

	WS	*ST*	*TU*	*WT*	*VU*	*VT*	*SU*	*WL*	*WU*	*WV*	*SV*	*SL*	*TL*	*UL*	*VL*
MI	0.924	0.737	0.450	0.485	0.416	0.377	0.301	0.132	0.266	0.265	0.241	0.096	0.090	0.043	0.040
IMD	0.407	0.319	0.227	0.213	0.209	0.169	0.152	0.135	0.134	0.119	0.108	0.098	0.092	0.044	0.041

Note: *W* – the willingness of decision-makers to educate themselves; *S* – security knowledge status of decision-makers; *T* – total security score of the organization; *U* – user experience; *V* – the volume of resources invested in cybersecurity; *L* – legislation.

Source: own

the expertise capacity of any expert. Consequently, this necessitates the consideration of a subset of distributions that are delineated by a reduced quantity of parameters.

A compositional model is conceptualized as a probability distribution formulated through the aggregation of its marginal distributions of lower dimensions, utilizing a composition operator (Jiroušek, 2011). The present analysis is restricted to graphical compositional models, wherein the marginal distributions are depicted through the cliques within a graph. By interpreting the pairs of variables highlighted in Tab. 4 as the edges of a graph in Fig. 1, the compositional models are construed as six-dimensional probability distributions characterized by the following properties:

$$\pi(L,S,T,U,V,W) = \pi(S,T,W) \rhd \\ \rhd \pi(T,U,V) \rhd \pi(L,S,W) = \pi(S,T,W) \cdot \\ \cdot \pi(U,V|T) \cdot \pi(L|S,W) \quad (5)$$

In our discourse, we employ only a few specific symbols. For a deeper understanding of compositional models see Jiroušek (2011). Consider a probability distribution π, defined for variables *r*. Let *s* be a proper subset of *r*, $\pi^{\downarrow s}$ denotes the marginal distribution of π, constricted to the variables *s*. Notice that the marginal distribution for an empty set, $\pi^{\downarrow \emptyset}$, equates to 1.

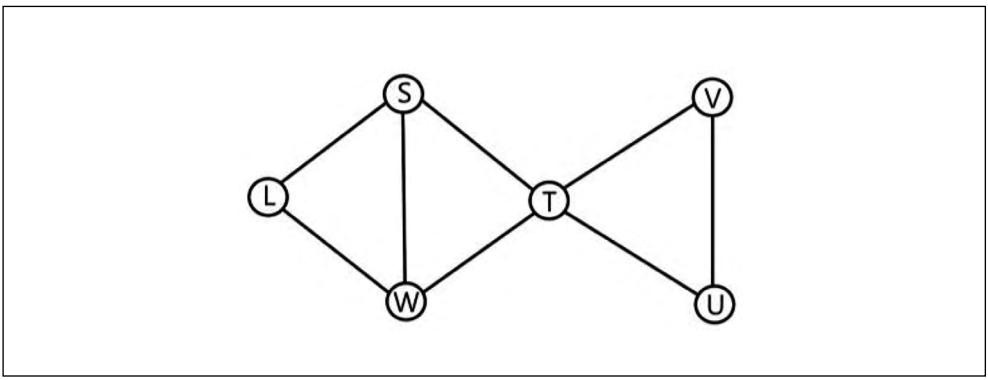

Fig. 1: Decomposable graph with three cliques: {*L,S,W*}, {*S,T,W*}, and {*T,U,V*}

Source: own

Consider distributions π and κ defined for variables *r* and *t*, respectively. The composition of these distributions into a more-dimensional distribution, denoted as $(\pi \rhd \kappa)$, yields a distribution defined for variables $r \cup t$. It is determined by:

$$(\pi \rhd \kappa) = \frac{\pi \cdot \kappa}{\kappa^{\downarrow r \cap t}} \quad (6)$$

If the right-hand-side formula in Equation (6) is defined. It is pertinent to note that the composition of two marginal distributions of a multi-dimensional probability distribution is always defined. As highlighted in Jiroušek (2011), the composition operator is non-commutative and non-associative. Consequently, to disambiguate expressions akin to those found in Equation (5), it is imperative to adhere to a left-to-right application of operators, barring explicit directives to alter this sequence through the use of parentheses.

Recall from graph theory that a simple graph with cliques $c_1, c_2, \ldots, c_k$ is said to be decomposable (or triangulated) if the cliques can be enumerated so that they meet the so-called running intersection property (RIP): $\forall i = 3,4, \ldots, k \; \exists \, j \; (1 \leq j < i)$: $c_i \cap (c_1 \cup \ldots \cup c_{i-1}) \subseteq c_j$.

Probability distribution π for variables *r* is said to be decomposable if there exists a decomposable graph $G = (r, E)$ with cliques $c_1, c_2, \ldots, c_k$ such that $\pi = \pi^{\downarrow c1} \rhd \pi^{\downarrow c2} \rhd \ldots \rhd \pi^{\downarrow ck}$, if the ordering $c_1, c_2, \ldots, c_k$ meets RIP.

Note that it was shown that for decomposable distribution π, $\pi = \pi^{\downarrow c1} \rhd \pi^{\downarrow c2} \rhd \ldots \rhd \pi^{\downarrow ck}$ for all RIP orderings of the cliques

c_1, c_2, …, c_k (Jiroušek, 2011). When designing the required model, we will also employ the following statement.

Proposition. Let π be a decomposable distribution with the decomposable graph *G*, the cliques of which are c_1, c_2, …, c_k. Consider any probability distribution κ of variables $\bigcup_{j=1}^{k} cj \cdot \text{If } \pi^{\downarrow j} = \kappa^{\downarrow j}$ for all j = 1, ..., k, then $H(\kappa) \leq H(\pi)$.

Pairwise dependence corrections

As previously mentioned, experts have identified eight pairs of variables whose mutual dependencies are deemed crucial for reflection within the resultant model. Should the marginal probabilities of the model be directly inferred from the relative frequencies delineated in the contingency table (Tab. 3), it might lead to what is colloquially referred to within the machine learning domain as "overlearning." Such a predicament would render the model inept at accommodating scenarios that deviate from the explicitly observed data, for instance, certain combinations of values not previously encountered or recorded by the contributing experts (e.g., recall the variables *W* and *S* listed in Tab. 3, where the frequency of managers' very high willingness to learn combined with their medium level of cybersecurity knowledge is equal to 0, however, the existence of such a combination is possible). Nevertheless, these experts acknowledge the potential for such variable configurations to manifest in distinct organizational contexts. This recognition underscores the necessity to imbue the model with a certain degree of epistemic humility, thereby enabling it to accommodate a broader spectrum of possibilities without stringent reliance on the observed data alone. This approach necessitates the incorporation of a calculated measure of ignorance into the model to ensure its robustness and applicability across varying circumstances.

Tab. 5: Modification for contingency table for variables *W* and *S*

	Variable *S*					∑
Variable *W*	8 + ε	1 + ε	ε	ε	0	9 + 4ε
	2 + ε	5 + ε	3 + ε	3 + ε	ε	13 + 5ε
	ε	2 + ε	2 + ε	2 + ε	ε	6 + 5ε
	ε	2 + ε	5 + ε	2 + ε	2 + ε	11 + 5ε
	0	ε	1 + ε	2 + ε	10 + ε	13 + 4ε
∑	10 + 4ε	10 + 5ε	11 + 5ε	9 + 5ε	12 + 4ε	n = 52 + 23ε

Source: own

In the probability theory, the articulation of ignorance is conventionally achieved through a uniform distribution. Hence, to address the issue previously delineated, a minor alteration was applied to all eight contingency tables. To elucidate this methodology, we refer specifically to Tab. 3. Initially, a consultation with domain experts was conducted to ascertain the presence of zeroes within the contingency table that ought to be preserved within the model, thereby assessing the existence of any inherent logical relationships.

In examining the contingency table that maps the interrelation between variables *W* and *S*, the consensus among experts was that only zeroes positioned in the upper-right and lower-left boxes should be retained. Consequently, the task became to identify an appropriate positive value of ε, such that the modified contingency table (Tab. 5) would align with the expert panel's stipulations. To underpin the determination of an apt ε value, the calculation of mutual information and the measure of information dependence for various ε values was undertaken (detailed in Tab. 6). After a thorough review, the experts unanimously agreed on selecting ε = 0.15. Their rationale was twofold: a value exceeding 0.15 would lead to an excessive dilution of informative content, whereas lower ε values might disproportionately emphasize the data derived from organizations already included in the study.

Tab. 6: Decrease of IMD with increasing ε in Tab. 5

	ε										
	0.00	**0.05**	**0.10**	**0.15**	**0.20**	**0.25**	**0.30**	**0.35**	**0.40**	**0.45**	**0.50**
IMD	0.407	0.38	0.361	0.344	0.33	0.317	0.305	0.294	0.283	0.274	0.265
Δ (%)	0.000	6.400	11.200	15.300	19.900	22.100	25.100	27.800	303.000	32.600	34.700

Source: own

Iterative proportional fitting

The method under discussion was designed in 1940 (Deming & Stephan, 1940), albeit its convergence was substantiated at a later stage by (Csiszar, 1975). With the availability of the composition operator, the description of this procedure becomes straightforward.

Consider π_1, π_2, ..., π_k, as a series of probability distributions, each defined over a distinct group of variables c_1, c_2, …, c_k (the ordering is arbitrary). The initial phase of the procedure involves establishing a uniform probability distribution, denoted as κ_0, across the variables encompassed within the union of all c_j groups. The method consists of iterative calculating:

$$\kappa_i = \pi_{(i \bmod(k))} \rhd \kappa_{i-1} \tag{7}$$

To rephrase, we sequentially process distributions c_1, c_2, …, c_k, composing each with the outcome from its preceding step. Upon reaching the final distribution in the sequence c_k, the procedure recommences with c_1, persisting in this cyclical manner until achieving convergence to the stipulated level of precision. This approach is underpinned by findings from (Csiszar, 1975), which ascertain that the Shannon entropy of the eventual distribution, $H(\lim_{i\to\infty} \kappa i)$, is either equivalent to or surpasses the entropy of any given distribution π (defined for variables $\bigcup_{j=1}^{k} c_j$) that includes π_1, π_2, ..., π_k as its marginal distributions. In light of this, coupled with Proposition, it is deduced that a six-dimensional decomposable framework (Fig. 1), whose three-dimensional components are derived from two-dimensional distributions via the iterative proportional fitting process, constitutes the optimal entropy augmentation of all the chosen two-dimensional distributions.

3. Results and discussion

The previous section elucidated the development of a six-dimensional decomposable compositional model in a form given in Equation (5). This construction was supported by the analysis of mutual information, which guided the selection of a decomposable graph structure. To mitigate the potential for overlearning the corresponding two-dimensional contingency tables were slightly modified. The whole process culminated in the identification of maximal entropy distributions $\pi(S,T,W)$, $\pi(T,U,V)$, and $\pi(L,S,W)$, which collectively comprise the model $\pi(L,S,T,U,V,W)$. With the model thus defined in Equation (5), we are positioned to apply the computational techniques outlined in Bína et al. (2021) for the calculation of any marginal or conditional probabilities needed for inference processes.

3.1 Example 1

Let's look at how security regulation affects organizational behavior in terms of managers' willingness to learn, combined with the organization's overall level of security. The outputs from the model are shown in Figs. 2–3, where we have united the detailed probabilities into four quadrants for better clarity.

At first glance (highlighted in bold), the difference is visible in the upper left quadrant, i.e., for not regulated entities there is a significantly higher probability that managers with a low to medium willingness to educate themselves in the field of cyber security will make decisions in organizations with a low to medium level of security.

3.2 Example 2

We will proceed analogously in the following case. How does regulation in the field of cyber security affect the behavior of organizations with regard to the level of security combined with the amount of investment in their protection? Calculations from the model are shown in Figs. 4–5.

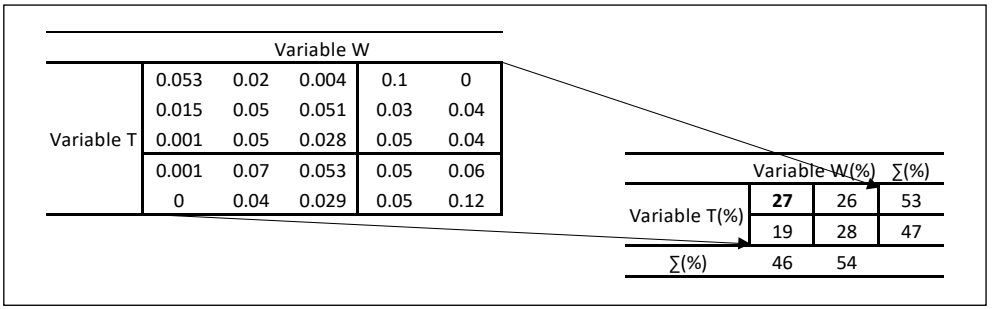

Fig. 2: **Conditional probability *T*&*W* under condition *L* (regulated)**

Source: own

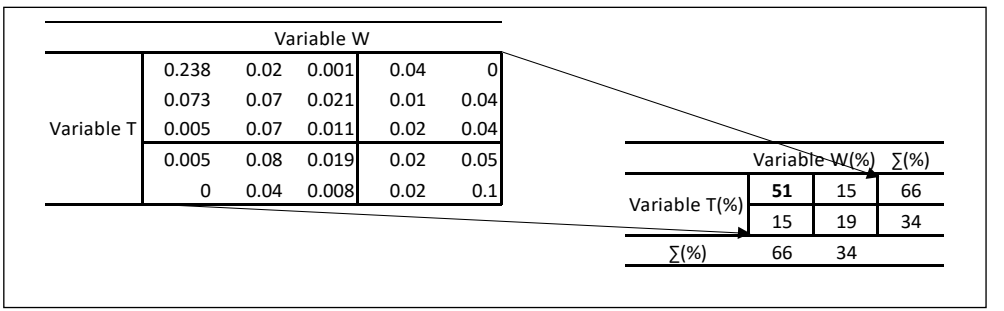

Fig. 3: **Conditional probability *T*&*W* under condition *L* (not regulated)**

Source: own

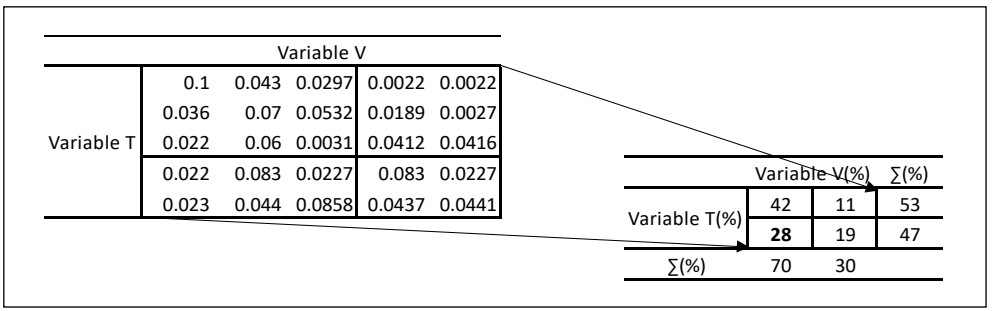

Fig. 4: **Conditional probability *T*&*V* under condition *L* (regulated)**

Source: own

In this case, regulation has a decidedly lower influence on the behavior of organizations than in the previous example. As can be seen from the values in the lower left quadrant of the tables (highlighted in bold), among regulated entities, organizations with higher levels of security are 8% more likely to invest lower to moderate amounts of resources in their protection.

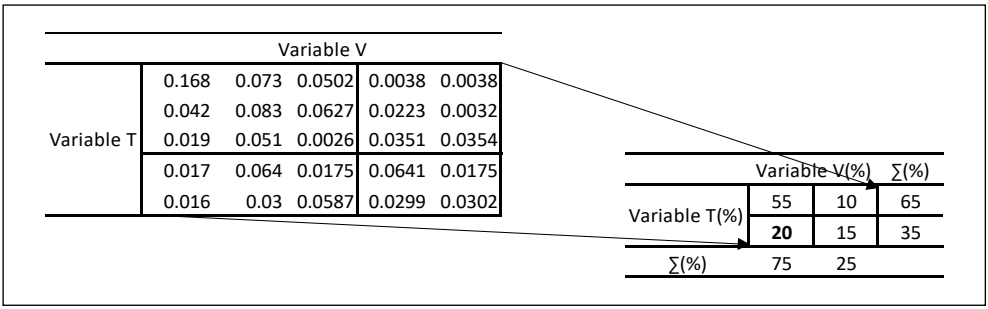

Fig. 5: **Conditional probability *T*&*V* under condition *L* (not regulated)**

Source: own

3.3 Example 3

In this case, we will address a situation where we compare the behavior of organizations with and without regulation based on the probability of occurrence of a combination of the organization's security level and user experience. Security practice is more inclined to the rule of decreasing user satisfaction with increasing

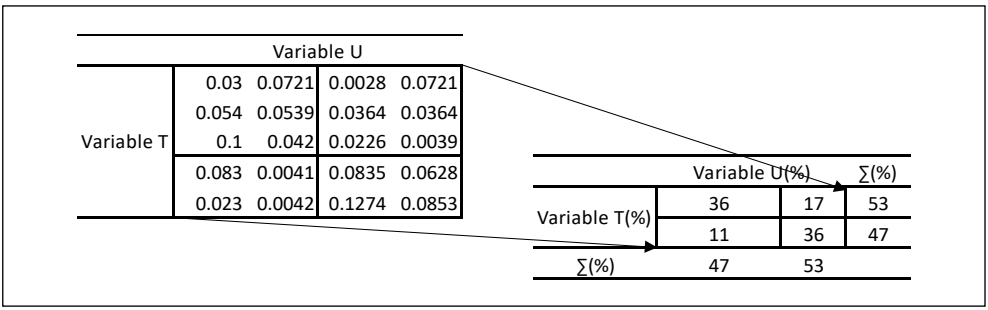

Fig. 6: **Conditional probability *T*&*U* under condition *L* (regulated)**

Source: own

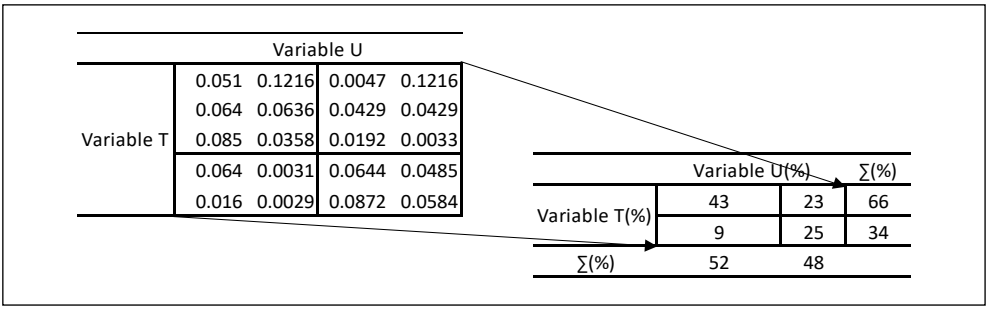

Fig. 7: **Conditional probability *T*&*U* under condition *L* (not regulated)**

Source: own

firm resistance to cyberspace threats. Let's look at Figs. 6–7 to see how the data processed in the model can be interpreted.

The model shows the biggest difference between regulated and unregulated subjects this time in the lower right quadrant, where there is a combination of high level of security and high user satisfaction. These outputs indicate that regulated entities are using new technologies supporting the automation and orchestration of some actions and are thus not burdensome for users.

Analogously, it is possible to use the model for any combination of variables *L*, *S*, *T*, *U*, *V*, *W*.

3.4 Reference model

The partial goal of this article was to perform an analysis of the state of cyber security in large enterprises. Based on the methodology described in previous part of the article, we compiled a graph (Fig. 8) of reference values for individual sectors. Each of the selected sectors is represented by at least four respondents working in the given area. For example, large educational institutions, typically universities, were included in the education category, the ICT category consists of organizations providing IT and cloud services and telecommunications operators, the services area is represented by sellers of goods, typically retail chains. In general, regulated industries fare better in terms of security than organizations that are not affected by legislation. Financial sector entities (e.g., banks) are the most protected, followed by healthcare organizations (e.g., large hospitals) and critical information infrastructure (CII) enterprises. The lowest security score achieved is associated with the media and educational institutions sector.

3.5 Discussion

Using the methods described, based on the 52 top security managers' knowledge and the data they used to characterize their organizations (52 large enterprises), we created a probabilistic model including a total of six variables related to cyber security. On the basis of this model, we are able to derive the marginal and conditional probabilities of all combinations of observed variables. Outputs from the model can serve the authorities regulating

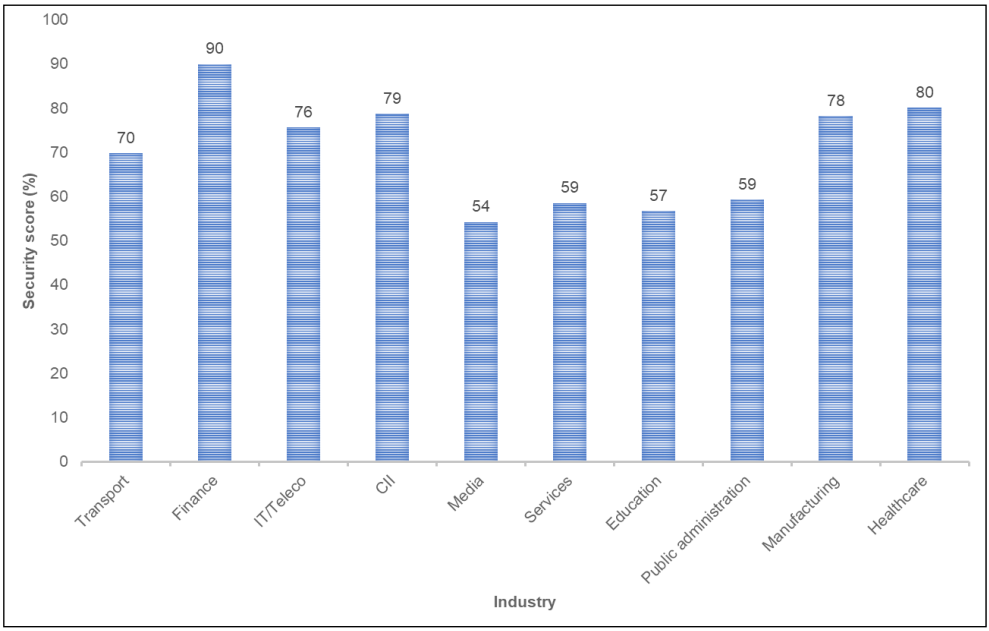

Fig. 8: Reference model for the overall security posture score

Source: own

cyber security conditions within the European Union. Union law in this area is governed by the form of harmonization, i.e., it carries the same elements of the transposed directives (European Parliament and the Council, 2016a). The knowledge contained in the model can also serve organizations that specialize in products and services in cyber security, including training centers. Conversely, the reference model of the state of cyber security by industry may interest managers responsible for security management in large organizations, who can compare their organization's security score with benchmarks using the CIS controls framework.

National Cyber and Information Security Agency is a reliable source of information in the field of cyber security for regulated as well as unregulated organizations in the Czech Republic. The situation is similar in other EU countries, including the umbrella organization European Union Agency for Cybersecurity (National Cyber and Information Security Agency, 2023). Every year, National Cyber and Information Security Agency publishes a report on the state of security in the Czech Republic (National Cyber and Information Security Agency, 2024) compiled based on a questionnaire survey of regulated entities according to the Act on cybersecurity 181/2014 Coll. (National Cyber and Information Security Agency, 2014). Our study expands the spectrum of information on domains that this report does not provide.

The results of our research confirm the conclusions of the authors (Kajava et al., 2007) that the education of top management in the area of cyber security is an important factor influencing the overall level of security of a given organization. However, our findings broaden the view of managers' willingness to educate themselves in cyber security. Example 1 demonstrates the fact that unregulated entities with a low to medium level of security are almost twice as likely to have top managers with a low to medium willingness to educate themselves in cyber security compared to entities that are regulated. This effect confirms that the current regulation motivates decision-makers to educate themselves in cyber security. Furthermore, research has shown that cyber security regulation, in general, helps enforce security rules in organizations. The research outputs are fully in line with the wording of the EU directive (European Parliament and the Council, 2022), which explicitly requires the education of top management in the field of cyber security. However, this directive will not be reflected in the Czech legislation until the second half of 2024.

Example 2 provides an economic perspective on information security management. Unregulated entities with high levels of security are less likely to invest low to moderate resources in security compared to regulated organizations. This result suggests that achieving a high level of security is possible with lower costs, however, regulation in the industry increases these costs. Example 3 discusses a comparison between the behavior of regulated and unregulated organizations in relation to cybersecurity and user experience. It highlights the trade-off where increased security often reduces user satisfaction. The analysis of data (from Figs. 6–7) shows the most significant difference in the lower right quadrant, where both high security levels and high user satisfaction coexist. This suggests that regulated organizations are adopting advanced technologies that automate and streamline certain security actions, minimizing the impact on users and improving overall satisfaction.

According to Leszczyna (2021), there is a whole range of methods and frameworks to measure the level of cybersecurity in an organization. Each method has its limits. For our work, we decided, like Lykou et al. (2018), to use the self-assessment method, which provides a reasonable degree of objectivity and is not expensive, unlike commercial analyses. The assessment methodology, including the framework used, can serve the responsible security manager as a simple tool to detect security vulnerabilities. The reference values shown in Fig. 8 can then be used for comparison with the result of the organization's security level in the listed fields.

Our research is primarily based on data obtained from CISOs of 52 large companies operating in the Czech Republic. The relatively low number of respondents, despite all our modifications, to some extent limits the quality of the resulting model. Another factor that can affect the work output is the respondent's different subjective perception of the situation. Although we tried to be accurate, some degree of subjective bias on the part of the respondents is likely. In the contribution, among other things, we also address the resources spent on cyber security. However, it was unrealistic to obtain a specific figure on the financial costs. Therefore, we proposed this variable as the share of costs spent on cyber security in the total costs of the organization. The value of the organization's total costs, which

is different for organizations operating in different fields, can be misleading. However, the proposed probabilistic model provides a full set of combinations of observed variables. Examples 1–3 are just a taster for other combinations of selected parameters. In the future, it will certainly be interesting to enrich the research with the values found after the introduction of the new act on cyber security into the national legislation and to analyze the obtained data from the point of view of causality.

Conclusions

The central aim of this study was to scrutinize the strategic behaviors exhibited by major corporations within the realm of information security management. By collating and analyzing pertinent data, the research endeavored to construct a theoretical framework that elucidated the dynamics and interconnections among the variables under investigation. This endeavor sought not only to chart the landscape of information security practices among large enterprises at that time but also to contribute to the existing body of knowledge by offering a comprehensive model that encapsulated the intricate relationships between these key factors. Subsidiary objectives encompassed a thorough examination of the state of cybersecurity within both commercial entities and public sector organizations, segmented by specific industry sectors. This analytical endeavor aimed to delineate the cybersecurity landscape retrospectively, identifying prevalent vulnerabilities, defense mechanisms, and compliance levels within distinct sectors. Through this sector-specific analysis, the study intended to unveil patterns, challenges, and best practices in cybersecurity management, thereby facilitating targeted improvements and strategic planning for enhanced security measures across the board.

Acknowledgments: *Supported by grant number IG632060 based on the internal grant competition of the Prague University of Economics and Business.*

References:

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2018). Nudges for privacy and security. *ACM Computing Surveys*, *50*(3), 1–41. https://doi.org/10.1145/3054926

Anderson, L. W., Krathwohl, D. R., & Bloom, B. (2001). *A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives*. Pearson Education.

Armstrong, P. (2010). *Bloom's taxonomy*. Vanderbilt University. https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/

Bína, Vl., Jiroušek, R., & Kratochvíl, V. (2021). Foundations of compositional models: Inference. *International Journal of General Systems*, *50*(4), 409–433. https://doi.org/10.1080/03081079.2021.1895142

Center for Internet Security. (2022). *CIS critical security controls*. https://www.cisecurity.org/controls/v8

Csiszar, I. (1975). I-divergence geometry of probability distributions and minimization problems. *The Annals of Probability*, *3*(1). https://doi.org/10.1214/aop/1176996454

Cybersecurity & Infrastructure Security Agency. (2024). *The cyber security evaluation tool (CSET)*. https://www.cisa.gov/

Czech Statistical Office. (2023). *Timelines*. https://www.czso.cz/csu/czso/res_cr

Deming, W. E., & Stephan, F. F. (1940). On a least squares adjustment of a sampled frequency table when the expected marginal totals are known. *The Annals of Mathematical Statistics*, *11*(4), 427–444. https://doi.org/10.1214/aoms/1177731829

Doucek, P., Konečný, M., & Novák, L. (2019). *Řízení kybernetické bezpečnosti a bezpečnosti informací* [Cybersecurity and information security management]. Professional Publishing.

European Commission. (2003). *Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises*. In Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003H0361

European Parliament and the Council. (2016a). *Directives. Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016*. In Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148

European Parliament and the Council. (2016b). *Regulations. Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016*. In Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

European Parliament and the Council. (2022). *Directives. Directive (EU) 2022/2555 of the European Parliament and the Council of 14 December 2022. NIS 2 Directive*. In Official

Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1678405383409&from=EN

Grassi, P. A., Fenton, J. L., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2017). *Digital identity guidelines: Enrollment and identity proofing*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-63a

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 – Information security management systems – Requirements*. https://www.iso.org/standard/27001

Jiroušek, R. (2011). Foundations of compositional model theory. *International Journal of General Systems*, *40*(6), 623–678. https://doi.org/10.1080/03081079.2011.562627

Kajava, J., Anttila, J., Varonen, R., Savola, R., & Röning, J. (2007). Senior executives commitment to information security – From motivation to responsibility. In *Computational intelligence and security* (pp. 833–838). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-74377-4_87

Krathwohl, D. R. (2002). A revision of Bloom's taxonomy: An overview. *Theory Into Practice*, *41*(4), 212–218. https://doi.org/10.1207/s15430421tip4104_2

Leszczyna, R. (2021). Review of cybersecurity assessment methods: Applicability perspective. *Computers & Security*, *108*, 102376. https://doi.org/10.1016/j.cose.2021.102376

Lykou, G., Anagnostopoulou, A., Stergiopoulos, G., & Gritzalis, D. (2019). Cybersecurity self-assessment tools: Evaluating the importance for securing industrial control systems in critical infrastructures. In *Critical information infrastructures security* (pp. 129–142). Springer International Publishing. https://doi.org/10.1007/978-3-030-05849-4_10

Manning, C. D., Raghavan, P., & Schütze, H. (2008). *Introduction to information retrieval*. Cambridge University Press. https://doi.org/10.1017/cbo9780511809071

National Cyber and Information Security Agency. (2014). *Act on cybersecurity 181/2014 Coll*. In Collection of Laws, Czech Republic.

National Cyber and Information Security Agency. (2018). *Decree No. 82/2018 Coll. on security measures, cybersecurity incidents, reactive measures, cybersecurity reporting requirements, and data disposal (The cybersecurity decree)*. In Collection of Laws, Czech Republic.

National Cyber and Information Security Agency. (2023). *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022* [Report on the state of cybersecurity in the Czech Republic for 2022]. https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf

National Cyber and Information Security Agency. (2024). *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2023* [Report on the state of cybersecurity in the Czech Republic for 2023]. https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2023.pdf

National Institute of Standards and Technology. (2023). *NIST*. https://www.nist.gov/

Renaud, K., & Zimmermann, V. (2020). How to nudge in cyber security. *Network Security*, *2020*(11), 20. https://doi.org/10.1016/s1353-4858(20)30132-x

Scarfone, K. A., Souppaya, M. P., Cody, A., & Orebaugh, A. D. (2008). *Technical guide to information security testing and assessment*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-115

Sophos. (2023). *Sophos 2023 threat report*. https://assets.sophos.com/X24WTUEQ/at/b5n9ntjqmbkb8fg5rn25g4fc/sophos-2023-threat-report.pdf

Švadlenka, R. (2021). Risk in organisational decision-making: Successful implementation of cryptographic tools. In *Proceedings of the 14th International Scientific Conference COMPETITION FMSCICON2020* (pp. 30–42). Prague University of Economics and Business.

Švadlenka, R. (2022). Security as an indispensable condition for competitiveness. In *Proceedings of International Scientific Conference COMPETITION* (pp. 216–226). College of Polytechnics Jihlava. https://konference.vspj.cz/download?hash=1ff5cf771da0cbcb84c4a166e618745a7c2dcbb7

Taba, H., Krathwohl, D. R., Bloom, B. S., & Macia, B. B. (1965). Taxonomy of educational goals. Handbook II: Affective domain. *Journal of Teacher Education*, *16*(2), 254–255. https://doi.org/10.1177/002248716501600228