The current issue and full text archive of this journal is available on Emerald Insight at:
https://www.emerald.com/insight/2056-4961.htm



# Determining cybersecurity culture maturity and deriving verifiable improvement measures

Peter Dornheim and Ruediger Zarnekow
*Faculty for Economics and Management, Technische Universität Berlin, Berlin, Germany*

Received 1 July 2023
Revised 10 August 2023
20 August 2023
Accepted 13 September 2023

## Abstract

**Purpose** – The human factor is the most important defense asset against cyberattacks. To ensure that the human factor stays strong, a cybersecurity culture must be established and cultivated in a company to guide the attitudes and behaviors of employees. Many cybersecurity culture frameworks exist; however, their practical application is difficult. This paper aims to demonstrate how an established framework can be applied to determine and improve the cybersecurity culture of a company.

**Design/methodology/approach** – Two surveys were conducted within eight months in the internal IT department of a global software company to analyze the cybersecurity culture and the applied improvement measures. Both surveys comprised the same 23 questions to measure cybersecurity culture according to six dimensions: cybersecurity accountability, cybersecurity commitment, cybersecurity necessity and importance, cybersecurity policy effectiveness, information usage perception and management buy-in.

**Findings** – Results demonstrate that cybersecurity culture maturity can be determined and improved if accurate measures are derived from the results of the survey. The first survey showed potential for improving the dimensions of cybersecurity accountability, cybersecurity commitment and cybersecurity policy effectiveness, while the second survey proved that these dimensions have been improved.

**Originality/value** – This paper proves that practical application of cybersecurity culture frameworks is possible if they are appropriately tailored to a given organization. In this regard, scientific research and practical application combine to offer real value to researchers and cybersecurity executives.

**Keywords** Cybersecurity culture, Information security culture, Cybersecurity awareness, Information security awareness, Cybersecurity maturity

**Paper type** Research paper

## 1. Introduction

Each year, the number of cyberattacks increases, and attackers are developing increasingly effective methods to attack companies, steal and encrypt data, blackmail corporations or spy on various organizations. In response, companies are investing heavily in cybersecurity, i.e. cybersecurity budgets are increasing, new technologies are being implemented and the security of processes is being improved by implementing preventive, detective and corrective controls. Also, employees are regularly informed about cybersecurity threats and must undergo special training and simulated phishing campaigns.

© Peter Dornheim and Ruediger Zarnekow. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at http://creativecommons.org/licences/by/4.0/legalcode

Information & Computer Security
Vol. 32 No. 2, 2024
pp. 179-196
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-07-2023-0116

In 2022, cybersecurity spending (as part of corporate IT budgets) had the highest projected increase, and 69% of organizations planned to spend more on cybersecurity (ESG Research, 2022). This trend is not surprising because the average cost of a security breach has increased from $3.5m in 2006 to $9.4m in 2022, representing an increase of 170% in only 16 years (IBM Security and Ponemon Institute, 2022). Humans continue to be the primary cause of such security breaches. In fact, human behavior is responsible for 82% of security incidents (Verizon, 2022). Whether it is the use of stolen credentials, phishing, misuse of technology or simply a mistake, it is secondary. Humans play a predominant role in security incidents and breaches. Thus, it is necessary to address and improve human behavior and increase awareness regarding cyberthreats to reduce the number of incidents. These aspects can be subsumed under the term cybersecurity culture. Cybersecurity culture can demonstrably help minimize the risks of human vulnerability if it is well developed and established in an organization (da Veiga *et al.*, 2020).

However, one difficulty is measuring cybersecurity culture and identifying specific initiatives to realize improvements in such culture. Thus, many companies and institutions use common tools, such as annual cybersecurity awareness training and quarterly simulated phishing campaigns. These are also frequently used to satisfy appropriate audit requirements and provide data-driven reporting to the board of directors. However, they cannot be used to measure whether employee attitudes and behaviors are changing for the better. For this purpose, there are theoretically at least 48 cybersecurity culture frameworks available that define different focus points and contents (Nasir *et al.*, 2019). However, these frameworks are primarily scientific in nature and are difficult to apply in practice. Thus, there is a clear need to apply, test and evaluate such existing approaches and models for cybersecurity culture in organizations to prove (and improve) their effectiveness in practice (Uchendu *et al.*, 2021). This need, i.e. practical applicability, is satisfied in this work. A methodology is presented that surveys the maturity level of a cybersecurity culture in a scientific and comprehensible way. This paper also discusses which measures were implemented based on the surveyed maturity level and whether the implemented measures were effective. It is expected that the findings of this paper can be used by security executives to implement a practical and science-based cybersecurity culture maturity model in their organization. In addition, the model provides them with the possibility of verifying if their measures contribute to an improved cybersecurity culture.

Section 2 presents and assesses the related work regarding the practical applicability of cybersecurity culture frameworks. After that, Section 3 outlines the research method and provides a thorough explanation of how cybersecurity culture maturity was assessed and verifiable measures to improve the as-is maturity level were derived. Section 4 presents an analysis of the results. Section 5 concludes this paper and summarizes the findings, and Section 6 defines the limitations of this research and outlines future research areas.

## 2. Background and related work

This section explains the research question addressed in this paper. The current state of related research is then summarized.

### *2.1 Research question*

Based on previous cybersecurity culture studies and the research gap identified in the practical application of an effective cybersecurity culture framework, the following research question is considered in this paper:

*RQ1.* How can the maturity level of a cybersecurity culture be measured practically and how should the results be handled?

Thus, this paper focuses on a practical survey of the cybersecurity culture maturity level in a company. In addition, this study identifies which measures were initiated based on the surveyed maturity level and how these measures contributed to improving the cybersecurity culture of the company.

### *2.2 Related work*

Considerable research has been conducted in the area of cybersecurity policy compliance. In 2018, Moody *et al.* published a paper that reviews and compares 11 theories that have been used in previous information security behavior models. It includes a proposal for a unified model that integrates elements from the existing theories and is supported by preliminary empirical evidence. However, the authors state that further research is needed to determine its applicability to different types of cybersecurity behavior and policy violations (Moody *et al.*, 2018).

A meta-analysis conducted by Cram *et al.* in 2019 examined the literature on employee compliance with information security policies to identify key factors influencing this behavior. The study analyzed 95 empirical papers and classified 401 independent variables into 17 categories. The results indicate that the existing literature provides inconsistent findings. The authors recommend developing more refined theories and performing practical implementations of those theories to ensure effective security policy compliance initiatives (Cram *et al.*, 2019).

An article from Paananen, published in 2020, reviews the development of cybersecurity policies by examining various literature sources. It also highlights the lack of consensus on the definition and function of those policies. Also, this review emphasizes the need for future research and especially practical applications to address issues in cybersecurity policy definitions and implementation methods, particularly focusing on organization-specific information security needs and the integration of contextual factors (Paananen *et al.*, 2020).

In the area of cybersecurity culture frameworks, a similar situation exists: In 2018, Glaspie *et al.* published a literature review that focused on cybersecurity culture within organizations, aiming to provide guidance. The study identifies factors that contribute to an organization's cybersecurity culture and develops a framework based on synthesized research. The findings are recommended to be used as a baseline to develop applicable cybersecurity programs in organizations (Glaspie and Karwowski, 2018).

Nasir *et al.* analyze in 2019 the dimensions of cybersecurity culture by reviewing 79 studies from 2000 to 2017. The findings indicate a lack of consensus on a standard set of dimensions for the cybersecurity culture concept, with overlapping dimensions found in the literature. The analysis explores factors that contribute to the variation in dimensions, including adopted theories, the objective of the study, type of organization and information security maturity level. The review highlights the need for further clarification, standardization and practical validation of cybersecurity culture dimensions (Nasir *et al.*, 2019).

But while there is extensive research in the theoretical area of cybersecurity policy compliance and cybersecurity culture frameworks, relatively little research can be found on the practical application of such frameworks.

The practical application of such frameworks was the subject of a recent study from Da Veiga *et al.* in 2020, which analyzed the differences between scientific and practical perspectives on cybersecurity culture. The industry perspective was adequately considered because 512 employees from multiple organizations participated in the survey and shared their views and

understanding. At the same time, the academic perspective was represented by 16 frequently cited frameworks for cybersecurity culture. The research findings have shown that academic interpretations of cybersecurity culture definitions and factors are much broader than their understanding in the industry. Therefore, the study advises implementing a practical methodology to assess the cybersecurity culture based on various input factors (da Veiga *et al.*, 2020).

In 2010, Da Veiga and Eloff presented a study that examined the practical applicability of a cybersecurity culture framework to an organization (da Veiga and Eloff, 2010). This paper presented the impact of triggers (information security component categories) on the cybersecurity behavior of employees in a South African company and the cybersecurity culture of the company. For this study, the participants filled out an 85-question survey, which is clearly too extensive for regular use in practical application. In addition, this study did not identify any way to measure how the survey results were used to improve the cybersecurity culture, and no follow-up survey was conducted to verify if the situation had changed over time.

In 2015, Da Veiga and Martins published a case study that was conducted over eight years at an international financial institution. The cybersecurity culture of this institution was assessed at four intervals, with a focus on training and awareness. In addition, this study provided empirical evidence to support the notion that a predefined questionnaire can be used to positively influence cybersecurity culture, identify gaps and implement recommendations (da Veiga and Martins, 2015a). However, the focus on training and awareness is very specific, and cyberthreats and threat actors have changed significantly since 2015.

In 2017, Parsons *et al.* validated the Human Aspects of Information Security Questionnaire (HAIS-Q), which measures knowledge, behavior, and attitudes in cybersecurity (Parsons *et al.*, 2017). This study involved two focus groups, i.e. 112 Australian university students and 505 Australian workers. The workers had to be at least 18 years old, spend at least 20% of their working hours on a computer, and work for a company that has implemented an information security policy. The HAIS-Q includes 63 questions that must be answered by the participants, and the researchers identified this high number of questions as a weakness in terms of practical application. In addition, rather than identifying measures that can be implemented to improve the existing cybersecurity culture, they stated that further research is required to identify such measures. Finally, the HAIS-Q can be considered outdated because it does not consider various modern technologies, e.g. cloud computing or the bring-your-own-device concept.

More recent studies have focused on other areas, or the underlying sample cannot be applied to companies. In 2022, Szczepaniuk conducted a study with a major focus on cybersecurity competencies, which are a part of cybersecurity culture, and how they can be improved (Szczepaniuk and Szczepaniuk, 2022). They analyzed the skills and knowledge of people relative to handling different cyberattacks, e.g. phishing, man-in-the-middle and distributed denial-of-service attacks.

In 2022, Witsenboer *et al.* measured cybersecurity behavior and skill; however, the target group did not fit the corporate context because the participants were elementary and high school students in The Netherlands (Witsenboer *et al.*, 2022). They found that teaching proper cybersecurity behavior is neglected; thus, the spontaneous behavior of elementary and high school students is not secure. Although this may be a very important area of study, the results do not help and cannot be applied in the corporate context.

In contrast, in 2021, Uchendu *et al.* published a study that summarizes the current practices and future requirements of developing a highly effective cybersecurity culture (Uchendu *et al.*, 2021). The study analyzed 58 research papers regarding cybersecurity culture published between 2010 and 2020. Their key findings are summarized as follows.

First, there is an urgent need for practitioners and researchers to collaborate more closely on approaches, frameworks, and metrics for cybersecurity culture because the transfer from theory to practical application is a significant gap in this field. Second, the surveys that have been conducted primarily represent a specific point in time, which does not allow for effective conclusions about the evolution of cybersecurity culture. In addition, they found that research into cybersecurity culture is not distributed evenly around the world, i.e. it is most prevalent in South Africa and generally lacking in the USA, the UK and Europe (Uchendu *et al.*, 2021).

Moreover, in 2020, Wiley *et al.* confirmed that cybersecurity culture plays an important role by connecting organizational culture and information security awareness. The confirmation is based on a quantitative survey that measures the level of organizational culture and information security awareness. The target group for the survey consisted of 508 employees in Australia. A major recommendation from this publication is that companies need to pay more attention to cybersecurity culture to increase their holistic cybersecurity maturity level (Wiley *et al.*, 2020).

## 3. Research method

The current study was conducted in survey form using a quantitative assessment technique. The population selected for the survey included the internal IT department employees of a global software institution. As of February 2022 (the date of the first survey), this IT department comprised 3,241 people. In October 2022 (the date of the second survey), the department comprised 4,196 people due to an organizational change. A comprehensive preparation of the surveys was required to obtain valid results and comply with the internal regulations of the company, e.g. the data privacy policies and the workers' council. The first survey was then executed, and several measures were defined and implemented based on the results. As a last step, the second survey was executed eight months later to verify whether the implemented measures yielded improvements in terms of the company's cybersecurity culture maturity.

### *3.1 Preparation of cybersecurity culture survey*

First, a company must determine which cybersecurity culture framework will be implemented in its organization. As mentioned in Section 1, many frameworks with different dimensions and different areas of focus are available. The framework designed by Da Veiga *et al.* was used in this study (and in its practical application in the company). This framework was initially introduced in 2002 and has been continually developed, adapted to emerging research results and verified continuously (da Veiga and Eloff, 2010; da Veiga, 2018; da Veiga and Martins, 2015b, Martins and Eloff, 2002; Veiga and Eloff, 2007). The most recent adoption was the introduction of the IPCA [1], which defines six dimensions to validate how employees perceive information protection from a cybersecurity perspective (da Veiga and Martins, 2015b). Table 1 presents the six IPCA dimensions (including one additional dimension for metaquestions).

The two surveys conducted as part of this study are based on the IPCA dimensions, as these can be seen as an evolution of the original ISCA questionnaire (da Veiga and Martins, 2015b). In its original version, the ISCA contained 73 statements and the IPCA contained 55 statements that must be answered (i.e. confirmed or rejected) by the participants (da Veiga, 2018; da Veiga and Martins, 2015b). This was planned as a voluntary survey; hence, it was expected that most participants would not spend a lot of time on the survey. Thus, the number of statements was reduced to 23 items. As outlined by the survey researchers, at least three questions per dimension were retained to measure each dimension effectively (da Veiga and Martins, 2015b). The questions in the survey were selected based on prioritization

| ID | Dimension | Description |
|---|---|---|
| 0) | Metaquestions | General Questions to analyze the given feedback |
| 1) | Cybersecurity accountability | Individual accountability to compliance and the requirements for cybersecurity training |
| 2) | Cybersecurity commitment | The perception on the commitment from an organizational, divisional and employee perspective regarding the protection of information and implementation of cybersecurity controls |
| 3) | Cybersecurity necessity and importance | Cybersecurity necessity is established by focusing on specific concepts such as people, time, money and the impact of changes |
| 4) | Cybersecurity policy effectiveness | The effectiveness of the cybersecurity policy and the communication thereof is established |
| 5) | Information usage perception | The perception on cybersecurity and privacy usage requirements |
| 6) | Management buy-in | The perception on management buy-in towards cybersecurity and the importance attached to the concept by senior managers and executives. The concept of management adherence to the cybersecurity policy is also established |

**Source:** da Veiga and Martins (2015b)

**Table 1.**
IPCA Dimensions of cybersecurity culture assessment

within the central cybersecurity team and can be found in Appendix 1. It must be mentioned that certain meta-information (such as region and department) is not queried, as this was automatically collected by the survey tool used. The total processing time required to answer the survey was calculated to be less than 5 min to reduce the risk of participants aborting the process.

Based on IPCA researchers, each statement can be assessed by the participants on a five-point Likert scale (strongly disagree, disagree, unsure, agree and strongly agree). By assigning a maturity level to each option, a dimension-specific and generic as-is maturity level could be derived. Before administering the survey, the responsible leadership team agreed on the target maturity level. For this, a reference to the CMMI [2] or the cybersecurity framework of the National Institute of Standards and Technology can be used. A level of 4.5 was defined as the target for the maturity of the cybersecurity culture, which means that on average, all participants must agree or strongly agree with the given statements.

### *3.2 Initial survey to identify as-is maturity*

The first step in the execution process was the announcement of the cybersecurity culture survey to relevant departments within the company. These are at least the workers' council and the data privacy department, depending on the geographical location and company guidelines. As no personal data were collected, the survey was executed in a voluntary and anonymous mode, and there are no inferences to performance or behavioral control; the approval was given in that specific case without any further requirements.

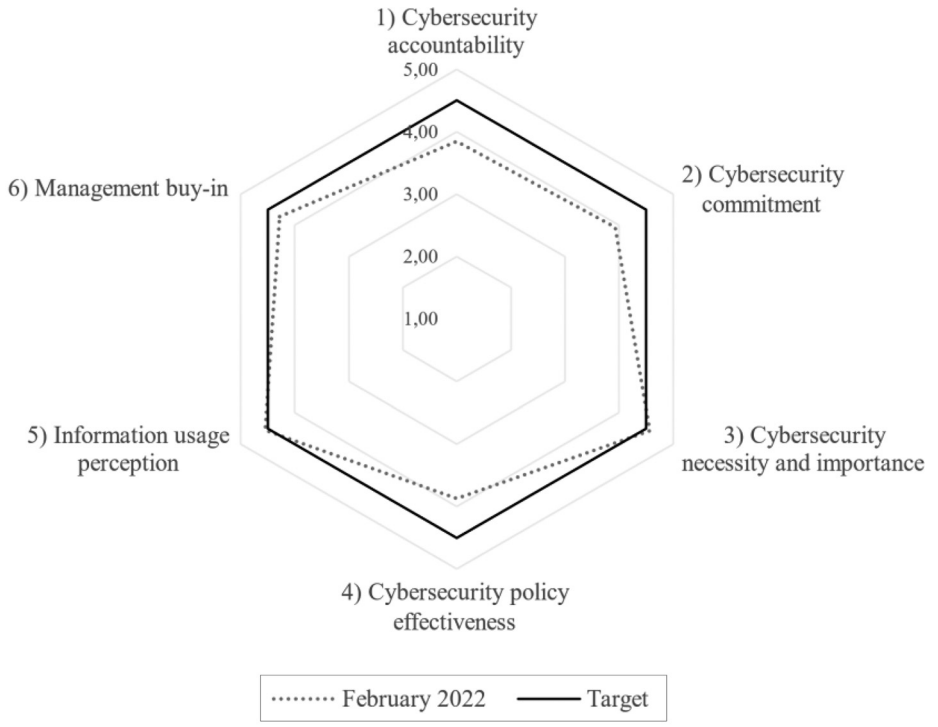
The second step involves selecting a technical solution capable of conducting and providing adequate reporting. SAP Qualtrics was selected because it fulfilled all requirements and was already available in the company (SAP Qualtrics, 2023). As the target population of the survey was the IT department, the CIO [3] as well as the cybersecurity leader announced the upcoming survey in an all-hands call and motivated the workforce to

participate. After that, an official email was sent out to all 3,241 IT employees, asking them to voluntarily participate in the cybersecurity culture survey. After one week, a reminder letter was sent. Seven days later, the survey was closed, and the results were evaluated.

As outlined in Figure 1, the major findings were related to two areas: First, the results of the initial survey showed that two out of the six dimensions had already exceeded the target maturity level of 4.5. The dimensions of information usage perception and cybersecurity necessity and importance seem to be well established in the IT department (the dimension of management buy-in is already at a good score with a maturity level above 4.0). Conversely, the dimensions of cybersecurity accountability, cybersecurity commitment and cybersecurity policy effectiveness scored a maturity level smaller than 4.0, indicating that these dimensions require a special focus.

Table 2 summarizes the detailed numeric maturity levels for each dimension. Overall, an initial cybersecurity culture maturity level of 4.17 was determined.

Section 4 presents and discusses more detailed results of the initial survey, such as the number of participants, age, and region distribution. The results of this initial survey are also compared with the results of the second survey, which took place after implementing the improvement measures. The procedure presented in Sections 3.1 and 3.3 already answered the first part of the research question, namely, "How can the maturity level of a cybersecurity culture be measured practically?."




**Source:** Created by authors

**Figure 1.**
Graphical results of initial survey and target maturity level

*3.3 Definition of verifiable actions*

Once the weak dimensions are identified, it is necessary to define measures to improve them. Here, there is no universal optimization process or method; thus, all weak dimensions must be considered in a focused manner. Table 3 presents an overview of improvement measures, which are described in detail in the following.

The cybersecurity accountability dimension covers individual accountability for compliance and cybersecurity training requirements. It measures whether the participants identify a need for additional cybersecurity training and if this topic should be part of the company's skill development plan. In addition, the cybersecurity commitment dimension analyzes whether employees support consequence management if cybersecurity policies or controls are violated. A poor result in this dimension means that people do not identify a need to improve their cybersecurity skills, which could also mean that the company does not appreciate that. In addition, it is likely that employees view cybersecurity violations as a trivial matter rather than a major problem, which may not impact individuals.

A management information campaign was planned as an initial improvement measure. The goal of this campaign was to convince managers that cybersecurity is an important asset for the company. It was assumed that the communication and support from a direct line manager would have a more meaningful impact on behavior of individuals than a centrally managed cybersecurity campaign. If managers communicate to their employees that cybersecurity is a skill set that is appreciated by the entire company, the gap between a central security team and individual development and operations teams can be closed. The line managers are also responsible for motivating their team members to participate in

**Table 2.**
Numeric results of initial survey

| ID | Dimension | Feb 2022 |
|---|---|---|
| 1) | Cybersecurity accountability | 3.84 |
| 2) | Cybersecurity commitment | 3.93 |
| 3) | Cybersecurity necessity and importance | 4.57 |
| 4) | Cybersecurity policy effectiveness | 3.87 |
| 5) | Information usage perception | 4.55 |
| 6) | Management buy-in | 4.28 |
| | Overall | 4.17 |

**Source:** Created by authors

**Table 3.**
Implemented improvement measures by dimension

| ID | Dimension | Improvement measure |
|---|---|---|
| 1) | Cybersecurity accountability | • Initiate management information<br>• Establish consequence management |
| 2) | Cybersecurity commitment | • Provide attacker insights<br>• Promote security champions |
| 4) | Cybersecurity policy effectiveness | • Perform tech-specific information sessions<br>• Provide consulting hours |

**Source:** Created by authors

specific cybersecurity training sessions. The management information campaign was executed through various emails (e.g. monthly human resource updates and cybersecurity newsletters) and dedicated consulting sessions with line managers. In addition, the line managers were pre-informed that a consequence management system will be defined and applied in the future if people violate the established cybersecurity rules and that it is important to convey this information to all employees.

The establishment of consequence management is the second activity to improve the score for the cybersecurity accountability domain. This study was conducted within the framework of a multinational company; thus, several local laws and human resource guidelines must be considered. In addition, multiple worker council committees and the data privacy department must be involved to implement and establish stable and sustainable consequence management. It should be noted that the implementation of this improvement measure was not successful because too many alignments were required among the identified stakeholders. Nonetheless, the goal of this activity was to form an agreement regarding a consequence catalog that defines violations of cybersecurity rules in various stages. A minor violation (e.g. becoming a victim of a simulated phishing attack for the first time) would result in the assignment of a voluntary phishing awareness training. A medium violation (e.g. attempting to install prohibited software) would lead to a meeting with the vice president of the corresponding area, at which the person concerned has to explain why he/she acted against the policy. A serious violation (e.g. operating a BitTorrent server in the company's datacenter) would result in an official warning and a corresponding note in the employee's record. Although this measure has not yet been fully implemented, work is continuing to introduce it in an adapted form.

The cybersecurity commitment dimension covers the perceptions of commitment from an organizational, divisional and employee perspective regarding the protection of information and implementation of cybersecurity controls. If this dimension has a low maturity level, it can be equated with ineffective cybersecurity awareness initiatives, unclear communication of expectations regarding the cybersecurity behaviors of individuals and a low priority for cybersecurity topics in terms of budget and staff allocation. To improve the cybersecurity commitment dimension, it is necessary to increase awareness and provide sufficient resources in terms of staff and budget for the respective teams so that they can satisfy the cybersecurity requirements. Here, there was already more than sufficient formal cybersecurity training in the organization, including yearly mandatory training sessions, simulated phishing campaigns and cybersecurity newsletters. Thus, it was determined that the perspectives needed to change.

As a result, several technical workshops were offered to demonstrate to employees how easy it is (even for non-cybersecurity experts) to launch a phishing attack against the company. Here, it was demonstrated how quickly Kali Linux can be downloaded and installed and how easy it is to run a phishing toolkit. This included cloning the company website, registering a fake domain and launching an email attack on multiple employees. These workshops were mostly for employees, but managers and executives were also made aware of these types of cyberattacks.

A second improvement activity would be to increase the allocation of cybersecurity resources to the teams; however, this must be balanced with the available budgets. The security champions concept was promoted in the company to not overstretch the budgets. A security champion is a member of a development or operations team but is also connected to the cybersecurity team. This benefits both sides because development teams receive cybersecurity information very quickly and always have a point of contact to address cybersecurity challenges. In turn, the cybersecurity team can build a network of cybersecurity experts, share information with them and provide specialized training, which

facilitates improving the company's cybersecurity coverage. Regular biweekly meetings with a fixed agenda were scheduled to establish the operational model of the security champions.

The cybersecurity policy effectiveness dimension describes how established, known and understood the existing policies are and if changes are communicated effectively. A weakness in this dimension is seen as a gap in the communication of policies because, ideally, all employees should be aware of the existence, content and meaning of the corresponding policies. However, this does not appear to be the case. Thus, two measures were identified to improve communication regarding the policies.

The first measure required the content of the cybersecurity policies to be actively communicated to the central development and operations teams. In fact, the review and publication of cybersecurity policies was not a very mature process at the time because it was not known who would receive the information about new or updated policies by default. This information was distributed via email and wiki pages; however, there was no guarantee that all stakeholders would in fact receive this information. In addition, missing information inevitably leads to worse policies (because relevant feedback is not incorporated) and misunderstandings regarding the application and responsibilities. To operationalize this measure, multiple information sessions were scheduled with different teams to provide in-depth information regarding relevant cybersecurity policies for their area. Each information session comprised two parts. The first part provided a general overview of all policies and high-level processes, and the second part provided specific hardening guidelines and best practices for applied technologies (e.g. web development, database administration, operating system administration and mobile device management). In addition to these one-time efforts, regular quarterly touchpoints and Q&A sessions were scheduled with the respective teams. Redesigning the cybersecurity policy publishing process was not an option because the governance of this process belongs to a department outside of IT.

The second measure was the initiation of cybersecurity consulting hours. It is possible to request consulting services for cybersecurity-related questions (e.g. concrete implementation of cybersecurity policy requirements) using a simple booking system. The cybersecurity team was able to manage the workload by providing dedicated consulting hours in a fixed time slot. In addition, the development and operations teams were able to turn to a single point of contact for all cybersecurity issues and receive guidance on how to handle specific hardening guidelines or policy requirements. Depending on the availability of cybersecurity resources, the number of consulting hours offered per week may vary. However, during the ramp-up phase, three cybersecurity experts provided a total of 50–60 one-hour time slots per week, which could be booked using the company's intranet.

In total, five of six activities were initiated, tracked and ultimately implemented within approximately eight months to improve the company's cybersecurity culture maturity level.

### *3.4 Second survey to verify taken actions*

Eight months after the initial survey, a second survey was conducted to determine whether the implemented measures had resulted in an improvement in the respective dimensions. Here, the process was the same as that in the first survey. This survey was announced by the CIO and the cybersecurity leader, and all IT employees received an email that provided a link to the survey. The only change was that, at the end of the questionnaire, the specific improvement actions were listed, and the participants were asked if these actions had a perceived impact on the company's cybersecurity culture. The participants were able to confirm (positive impact), decline (negative impact) or skip (do not know) the measure.

In addition, compared with that in the first survey, the population in the second survey was higher because several teams joined the IT department due to restructuring, which resulted in a population of 4,196 employees. After two weeks, the second survey was closed, and the results were analyzed.

## 4. Analysis of results

In this section, the analysis of results is split into a brief statistical overview, the results obtained from the collected data, and a detailed evaluation of the specific dimensions and the corresponding improvement measures.

### *4.1 Statistical overview*

Prior to evaluating the first and second surveys, it was necessary to ensure that the results obtained from a subset of all respondents (sample size) could be applied to the total set of respondents (population). Here, a confidence level of >95% is recommended. As presented in Table 4, the number of participants for both surveys was sufficient to ensure a confidence level of >95%.

This means that the findings of both surveys are valid and could be generalized across the entire group of IT employees. It must be accepted that when conducting a two-step voluntary survey in a company, it is not possible to force the same number of people (or the same people) to participate in both surveys. However, the metadata indicate that both surveys are comparable in terms of the participants. Figure 2 shows the distribution by age.

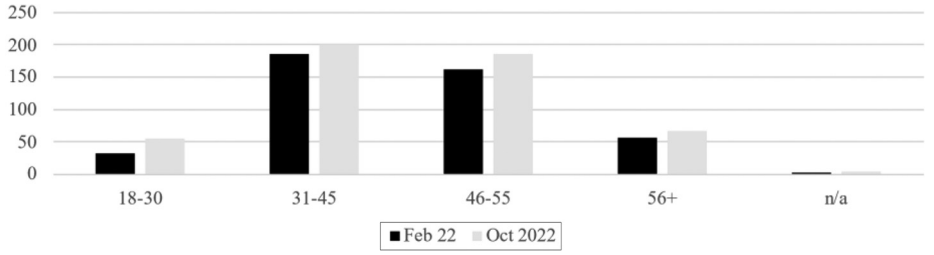
Based on the regions of the participants, it can be observed that ~50% come from Germany and approximately one-third come from the USA. As shown in Figure 3, the remaining participants are distributed between the Asia-Pacific region and Europe (excluding Germany).

Overall, the representation of the sample is sufficient (by size, age distribution and region distribution) to effectively reflect the IT organization.

| Survey | Feb 2022 | Oct 2022 |
|---|---|---|
| Population (IT employees) | 3,241 | 4,196 |
| Min. sample size for 95% confidence level (Krejcie and Morgan, 1970) | 346 | 354 |
| Responses obtained | 439 | 513 |

**Source:** Created by authors

**Table 4.** Number of survey participants




**Source:** Created by authors

**Figure 2.** Absolute distribution by participants age

*4.2 Data evaluation*

An unexpected finding in the first survey was that no single dimension had a truly poor maturity level. With dimension maturity levels ranging from 3.84 to 4.57, an average cybersecurity culture maturity level of 4.17 was calculated. After implementing the improvement measures and conducting the second survey, the overall maturity level was found to be 4.25, representing an increase of 1.9%. As shown in Figure 4, the degree of maturity improved in the identified dimensions.

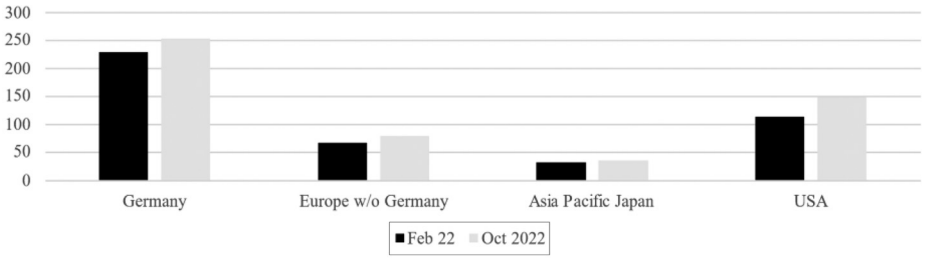



**Figure 3.**
Absolute distribution by participants region

**Source:** Created by authors

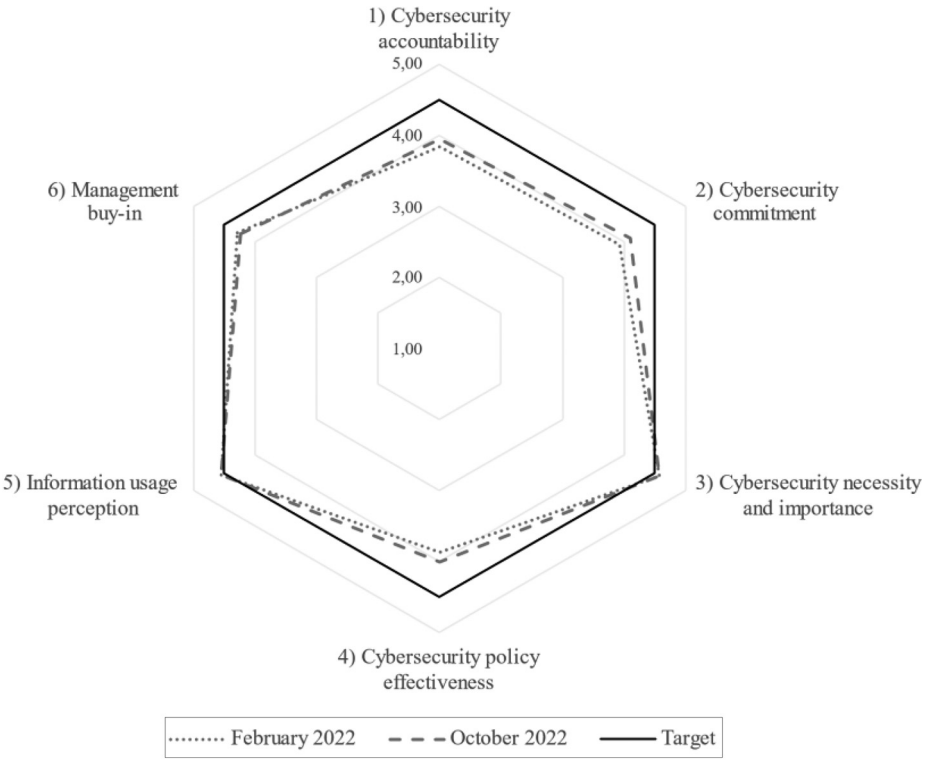



**Figure 4.**
Graphical results of both surveys and target maturity level

**Source:** Created by authors

Table 5 summarizes the detailed maturity level for each domain and the impact of the improvement measures. It is also clear that the level of maturity is stagnating or even declining in areas where no targeted measures have been implemented.

A margin of error of 3.0% for the February survey and 2.2% for the October survey was calculated. While the overall result shows an improvement of 1.9% (which would be in the error margin), the results for the dimensions that were addressed by improvement measures how a higher positive change: The average improvement in the dimensions of cybersecurity accountability, cybersecurity commitment and cybersecurity policy effectiveness is 4.1%, which can therefore be considered significant.

*4.3 Detailed evaluation of data*

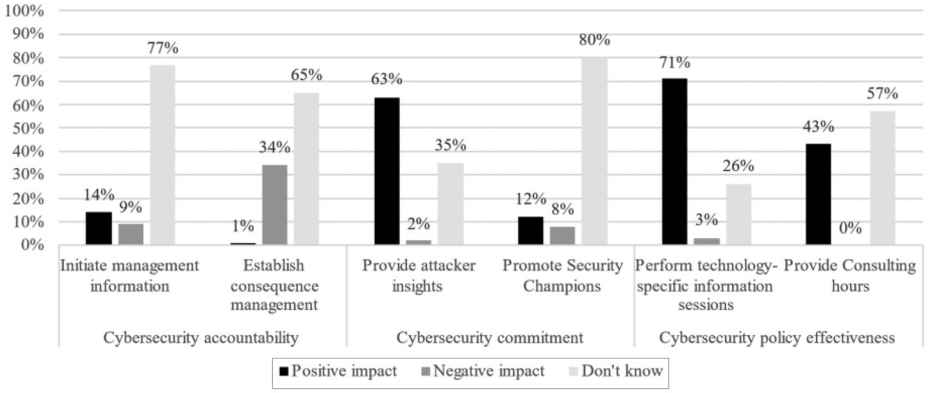
This section focuses on the dimensions targeted in the improvement measures. The stagnation or decline of the maturity level of other dimensions is discussed in the conclusion. Based on the participants' feedback regarding specific improvement measures, it is clear which measures were perceived by the employees as having a positive impact and which measures may not have had much impact (Figure 5).

Starting with the cybersecurity accountability dimension, the results show that this dimension was improved by 2.9% from a maturity score of 3.84 to 3.95. Nevertheless, compared to the other two dimensions (cybersecurity commitment and cybersecurity policy

| ID | Dimension | Feb 2022 | Oct 2022 | Change | Focused Dimensions |
|---|---|---|---|---|---|
| 1) | Cybersec. accountability | 3.84 | 3.95 | +2.9% | +2.9% |
| 2) | Cybersec. commitment | 3.93 | 4.10 | +4.3% | +4.3% |
| 3) | Cybersec. necessity and importance | 4.57 | 4.58 | +0.2% | |
| 4) | Cybersec. policy effectiveness | 3.87 | 4.07 | +5.2% | +5.2% |
| 5) | Information usage perception | 4.55 | 4.54 | −0.2% | |
| 6) | Management buy-in | 4.28 | 4.23 | −1.2% | |
| | Overall average | 4.17 | 4.25 | +1.9% | +4.1% |

**Source:** Created by authors

**Table 5.** Summarized results of both surveys




**Source:** Created by authors

**Figure 5.** Participants feedback on perceived impact of improvement measures

effectiveness), the feedback of the participants regarding the implemented measures is rather poor. The perceived positive impact of the information sessions for managers was confirmed only by 14% of the participants. More than three-quarters (77%) were not sure about the impact of the measure, which probably means that they have not noticed any effect. The fact that fewer managers than employees responded to the survey could potentially be the cause. As the measure of consequence management could not be finally implemented, it is also no surprise that the perceived positive impact was not confirmed by the participants. Most of them (65%) have either not noticed or cannot recall the measure. It is assumed that 34% of the participants who stated that consequence management had no positive impact are unaware of the implementation gap of this measure.

The cybersecurity commitment dimension improved by 4.3%, from a maturity score of 3.93 in the first survey to a maturity score of 4.10 in the second survey. In this dimension, the participants confirmed the positive impact of the initiated improvement measures, with 63% of the employees stating that gaining some attacker insights positively influenced their cybersecurity behavior. However, the number of participants who did not notice the measure remained high, at 35%. This result shows that it will probably pay off to promote this measure more to reach even more employees. The promotion of security champions has not been deemed successful, but the results may also indicate that this measure requires more marketing and time to be implemented throughout the organization. After approximately eight months, the majority of the staff (80%) had not even recognized this measure, and 8% were not convinced by it.

As the last dimension, the cybersecurity policy effectiveness was subject to several improvement measures. The maturity score increased from 3.87 to 4.07, representing a 5.2% increase. This dimension included the most successful improvement measure, with 71% of the participants agreeing that providing technology-specific information sessions (including a clear mapping of security requirements to their technologies) positively shapes the cybersecurity culture. In addition, providing security consulting hours by the central security team was also perceived positively by nearly half of the participants (43%). Even with these two measures, however, some participants were unaware of their implementation. Thus, 26% of the respondents stated they had not heard about the information sessions. The result for the consulting hours was even worse, with 57% of the participants unaware of this measure.

While two dimensions (cybersecurity necessity and importance and information usage perception) of the three dimensions – for which no dedicated improvement measures were implemented – did not show any significant changes, the dimension of management buy-in showed a considerable decrease of −1.2% from the maturity score of 4.28 to 4.23. It might therefore be possible that participants of the second survey rated the questions related to the management buy-in dimension (which are asking if managers lead by example, perceive cybersecurity as important and demonstrate commitment to cybersecurity) with a lower score because for them it seems that only technical/operational but no managerial improvements were implemented. That all these improvement measures required management buy-in in terms of resource approval, budget allocation, and prioritizing cybersecurity measures does not seem to have been transparent or perceived. Thus, this finding supports earlier research that a cybersecurity culture not only needs to be built and maintained but, very importantly, changes and activities communicated openly and clearly (Uchendu *et al.*, 2021; Alshaikh, 2020; Reegård *et al.*, 2019).

With the improvement measures outlined in Section 3 and the analysis of their impact described in Section 4, the second part of the research question can be answered, which is "how should the results [of a cybersecurity culture maturity survey] be handled?."

## 5. Conclusion

This paper demonstrated how a cybersecurity culture framework can be applied practically in a company and how the findings of a cybersecurity culture maturity survey should be handled. The results showed that such frameworks must be tailored to the given company and that different stakeholders must be considered when determining how corresponding surveys are conducted. In addition, this paper identified how to reflect the current cybersecurity culture, going far beyond the implementation of standard measures, e.g. simulated phishing campaigns or cybersecurity awareness sessions.

In this study, two surveys were executed, and the participants were able to provide feedback regarding the implemented measures. As a result, it was also possible to validate which specific measures yielded improvements to the cybersecurity culture maturity of the company. There were three measures that had a significant positive impact on the maturity level. First, providing insights into the daily work of hackers was very well perceived, and participants confirmed that this measure improved the cybersecurity culture. An equally positive effect was confirmed for the measure of technology-specific information sessions. Finally, providing security consulting hours was identified as a positive factor influencing the cybersecurity culture.

To give more clarity on the meaning when an employee rates the impact of a measure as "Don't know," this option should be changed or at least rephrased in future surveys. It must be possible to distinguish whether employees have not perceived a specific measure at all or whether it remains without effect despite perception or participation. In such a case, the impact of the measure could also be considered negative.

It is acknowledged that the maturity level improvement rates appear to be low, e.g. the percentage improvement value of all measures was only 1.9% with an absolute improvement of 0.08. However, a closer look at this result indicates that even an improvement rate of 4.1% was achieved if only the dimensions focused on by the targeted improvement measures were considered. If an average improvement of 4.1% per survey is assumed, the maximum maturity level of 5 is reached after five more surveys (which would take about 2–3 years).

Moreover, considering the declining dimensions, it is obvious that creating and maintaining a cybersecurity culture are ongoing tasks. The dimensions that are not addressed will decrease or stagnate over time. Thus, an effective cybersecurity culture program must be established, covering all related areas and stakeholders. In particular, this program should include communicating activities that are not directly visible to the entire workforce, such as the leadership approval of cybersecurity-related activities, as this demonstrates their active engagement and commitment.

As cyberthreats become increasingly sophisticated, it is strongly recommended that all companies consider the cybersecurity culture in their organizational setup and assign clear accountability to a cybersecurity executive to ensure a high level of maturity.

## 6. Limitations and future research

The methodology employed in this study cannot be applied to any company because different stakeholders and organizational characteristics must be considered to a greater or lesser extent depending on the given company. By tailoring validated cybersecurity culture frameworks, it must be accepted that the results cannot be compared in a one-to-one manner across organizational boundaries. In addition, it is acknowledged that if a voluntary survey on cybersecurity culture is conducted, employees with an interest in this area are likely to outnumber those with no interest in the subject. Moreover, there is evidence that there could

be a response bias in cybersecurity policy surveys (Kurowski, 2019). Thus, the results may be biased toward the positive.

This study identifies some areas for future research. One is the development and implementation of a cybersecurity consequence management catalog in organizations, and another is the format and content of cybersecurity management briefings. It must be studied how non-security managers can be convinced that cybersecurity plays a significant role and that they must empower their development and operations teams to work more closely with central security teams. Also, the mapping between the consent rate of the Likert scale and a maturity assessment in terms of CMMI must be analyzed, and an improved proposal must be developed. This is considered one of the most important topics because it is also expected to improve the perception of (a small) improvement rate. In addition, respondents who have already participated in a previous survey should be asked voluntarily for a reason if they change the rating of a question compared to the former survey. This allows a clear understanding of which measures the workforce actively perceived (and which may need better communication). Finally, to eliminate the potential bias, qualitative research like expert interviews or group discussions can be conducted to verify the survey results.

## Notes

1. Information Protection Culture Assessment
2. Capability Maturity Model Integration
3. Chief Information Officer

## References

Alshaikh, M. (2020), "Developing cybersecurity culture to influence employee behavior: a practice perspective", *Computers and Security*, Vol. 98.

Cram, W.A., D'Arcy, J. and Proudfoot, J. (2019), "Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance", *MIS Quarterly*, Vol. 43 No. 2, pp. 525-554.

da Veiga, A. (2018), "An approach to information security culture change combining adkar and the isca questionnaire to aid transition to the desired culture", *Information and Computer Security*, Vol. 26 No. 5, pp. 584-612.

da Veiga, A. and Eloff, J. (2010), "A framework and assessment instrument for information security culture", *Computers and Security*, Vol. 29 No. 2, pp. 196-207.

da Veiga, A. and Martins, N. (2015a), "Improving the information security culture through monitoring and implementation actions illustrated through a case study", *Computers and Security*, Vol. 49, pp. 162-176.

da Veiga, A. and Martins, N. (2015b), "Information security culture and information protection culture: a validated assessment instrument", *Computer Law and Security Review*, Vol. 31 No. 2, pp. 243-256.

da Veiga, A., Astakhova, L.V., Botha, A. and Herselman, M. (2020), "De ning organisational information security culture perspectives from academia and industry", *Computers and Security*, Vol. 92.

ESG Research (2022), "2022 Technology spending intentions survey".

Glaspie, H. and Karwowski, W. (2018), *'Human Factors in Information Security Culture: A Literature Revie'*, Springer International Publishing.

IBM Security and Ponemon Institute (2022), "Cost of a data breach report 2022".

Krejcie, R.V. and Morgan, D.W. (1970), "Determining sample size for research activities", *Educational and Psychological Measurement*, Vol. 30 No. 3, pp. 607-610.

Kurowski, S. (2019), "Response biases in policy compliance research", *Information and Computer Security*, Vol. 28 No. 3, pp. 445-465.

Martins, A. and Eloff, J. (2002), "Information security culture", *Security in the Information Society*, Vol. 86, pp. 203-214.

Moody, G.D., Siponen, M. and Pahnila, S. (2018), "Toward a uni ed model of information security policy compliance", *MIS Quarterly*, Vol. 42 No. 1, pp. 285-312.

Nasir, A., Arshah, R.A., Hamid, M.R.A. and Fahmy, S. (2019), "An analysis on the dimensions of information security culture concept: a review", *Journal of Information Security and Applications*, Vol. 44, pp. 12-22.

Reegård, K., Blackett, C. and Katta, V. (2019), "The concept of cybersecurity culture", *29th European Safety and Reliability Conference*, pp. 4036-4043.

Paananen, H., Lapke, M. and Siponen, M. (2020), "State of the art in information security policy development", *Computers and Security*, Vol. 88, pp. 101-108, available at: www.sciencedirect.com/science/article/pii/S0167404818313002

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. (2017), "The human aspects of information security questionnaire (hais-q): two further validation studies", *Computers and Security*, Vol. 66, pp. 40-51.

SAP Qualtrics (2023), "Qualtrics homepage", available at: www.qualtrics.com/

Szczepaniuk, E.K. and Szczepaniuk, H. (2022), "Analysis of cybersecurity competencies: recommendations for telecommunications policy", *Telecommunications Policy*, Vol. 46 No. 3.

Uchendu, B., Nurse, J.R., Bada, M. and Furnell, S. (2021), "Developing a cyber security culture: current practices and future needs", *Computers and Security*, Vol. 109.

Veiga, A.D. and Eloff, J.H.P. (2007), "An information security governance framework", *Information Systems Management*, Vol. 24 No. 4, pp. 361-372.

Verizon (2022), "Data breach investigations report 2022".

Wiley, A., McCormac, A. and Calic, D. (2020), "More than the individual: examining the relationship between culture and information security awareness", *Computers and Security*, Vol. 88.

Witsenboer, J.W.A., Sijtsma, K. and Scheele, F. (2022), "Measuring cyber secure behavior of elementary and high school students in The Netherlands", *Computers and Education*, Vol. 186.

**Corresponding author**
Peter Dornheim can be contacted at: peter.dornheim@campus.tu-berlin.de

## Appendix 1. Selected questions by dimensions

**Table A1.**
Selected questions by dimension

| Dimension | Statement |
|---|---|
| Meta | I am interested in cybersecurity |
| Meta | I believe I am an cybersecurity expert |
| Cybersecurity accountability | There is a need for additional training for cybersecurity controls (e.g., multi-factor authentication, cyber security frameworks, incident management) |
| Cybersecurity accountability | Cybersecurity should be part of my company development program |
| Cybersecurity accountability | Action (e.g., disciplinary procedure) should be taken if someone does not adhere to the cybersecurity policy (e.g. if they share passwords, give out confidential information or visit prohibited internet sites |
| Cybersecurity commitment | The company cybersecurity awareness initiatives are effective |
| Cybersecurity commitment | I understand what is expected of me when it comes to cybersecurity/secure behavior at the company |
| Cybersecurity commitment | My unit assigns enough people to cybersecurity |
| Cybersecurity commitment | My unit dedicates enough time to cybersecurity |
| Cybersecurity commitment | My unit encourages compliance to the cybersecurity policy |
| Cybersecurity necessity and Importance | I am aware of the cybersecurity aspects relating to my job function (e.g. how to choose a password or handle confidential information) |
| Cybersecurity necessity and Importance | It is necessary to commit time to cybersecurity |
| Cybersecurity necessity and Importance | Cybersecurity is necessary in my unit |
| Cybersecurity necessity and importance | I am aware of the impact and consequences that a breach of/neglecting security can have for the company |
| Cybersecurity policy effectiveness | The content of the cybersecurity policy was effectively communicated to me |
| Cybersecurity policy effectiveness | I am informed in a timely manner as to how cybersecurity changes will affect me |
| Cybersecurity policy effectiveness | The content of the cybersecurity policy is easy to understand |
| Information usage perception | The company has clear directives on how to protect sensitive/confidential employee information |
| Information usage perception | I believe that it is important to limit the collection and sharing of sensitive, personal information |
| Information usage perception | My colleagues and I take care when talking about confidential information in public places |
| Management buy-in | Managers lead by example when it comes to cybersecurity |
| Management buy-in | My colleagues demonstrate commitment to cybersecurity |
| Management buy-in | Cybersecurity is perceived as important by managers |

**Source:** da Veiga and Martins (2015b)