A systematic literature review of how cybersecurity-related behavior has been assessed

Kristian Kannelønning and Sokratis K. Katsikas
Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway

Received 20 August 2022
Revised 23 October 2022
13 December 2022
Accepted 13 January 2023

Abstract

Purpose – Cybersecurity attacks on critical infrastructures, businesses and nations are rising and have reached the interest of mainstream media and the public's consciousness. Despite this increased awareness, humans are still considered the weakest link in the defense against an unknown attacker. Whatever the reason, naïve-, unintentional- or intentional behavior of a member of an organization, the result of an incident can have a considerable impact. A security policy with guidelines for best practices and rules should guide the behavior of the organization's members. However, this is often not the case. This paper aims to provide answers to how cybersecurity-related behavior is assessed.

Design/methodology/approach – Research questions were formulated, and a systematic literature review (SLR) was performed by following the recommendations of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses statement. The SLR initially identified 2,153 articles, and the paper reviews and reports on 26 articles.

Findings – The assessment of cybersecurity-related behavior can be classified into three components, namely, data collection, measurement scale and analysis. The findings show that subjective measurements from self-assessment questionnaires are the most frequently used method. Measurement scales are often composed based on existing literature and adapted by the researchers. Partial least square analysis is the most frequently used analysis technique. Even though useful insight and noteworthy findings regarding possible differences between manager and employee behavior have appeared in some publications, conclusive answers to whether such differences exist cannot be drawn.

Research limitations/implications – Research gaps have been identified, that indicate areas of interest for future work. These include the development and employment of methods for reducing subjectivity in the assessment of cybersecurity-related behavior.

Originality/value – To the best of the authors' knowledge, this is the first SLR on how cybersecurity-related behavior can be assessed. The SLR analyzes relevant publications and identifies current practices as well as their shortcomings, and outlines gaps that future research may bridge.

Keywords Cybersecurity, Human behavior, Assessment process

Paper type Literature review

This work was supported by the Research Council of Norway under Project nr 323131 "How to improve Cyber Security performance by researching human behavior and improve processes in an industrial environment" and Project nr 310105 "Norwegian Centre for Cyber Security in Critical Sectors (NORCICS)."

Information & Computer Security
Vol. 31 No. 4, 2023
pp. 463-477
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-08-2022-0139

1. Introduction

The importance of information systems (IS) security has increased because the number of unwanted incidents continues to rise in the last decades. Several avenues or paths can be taken by organizations to secure their IS. Technical solutions like whitelisting, firewalls and antivirus software enhance security, but research has shown that when people within the organization do not follow policies and guidelines these technical safeguards will be in vain.

1.1 Aims of the paper

Of the 26 articles included in this review, 10 used some variations of the phrase *humans are the weakest link in cybersecurity* in either the abstract or introduction. All articles cite multiple authors, accumulating a significant number of previous works, all claiming the same statement. One might agree with Kruger *et al.* (2020) that it is common knowledge that humans are the weakest link in information security.

Given the premise that humans are the weakest link and the acknowledgment that technology cannot be the single solution for security (McCormac *et al.*, 2017), research should investigate how organizations can assess the cybersecurity-related behavior of their employees. Identifying, evaluating and summarizing the methods and findings of all relevant literature resources addressing the issue, thereby systematizing the available knowledge and making it more accessible to researchers, while also identifying relevant research gaps, are the aims of this systematic literature review (SLR).

1.2 Background

Recent years have shown that cyberattacks are a global issue, such as the extensive power outage causing a blackout across Argentina and Uruguay in 2019 (Kilskar, 2020). In January 2018, nearly 3 million, or roughly 50% of the Norwegian population's medical records, were compromised by a cyberattack. Threats can vary from viruses, worms, trojan horses, denial of service, botnets, man-in-the-middle and zero-day ones (Pirbhulal *et al.*, 2021). The above-listed threats include technical terms with a distinctive flair and uniqueness that is hard to comprehend for employees without a technical background. Moreover, most information security issues are complicated and fully understanding them requires advanced technical knowledge.

With threats originating from internal and external sources, the need to communicate security measures from the management to the organization's members is of great importance (Sommestad *et al.*, 2014). Developing an organization's security policy is central to increasing knowledge and awareness. According to the ISO 27002:2022 standard, the information security policy sets out the organization's approach to managing its information security. It should contain statements concerning the following:

- Definition of information security;
- information security objectives or the framework for setting information security objectives;
- principles to guide all activities relating to information security;
- commitment to satisfy applicable requirements related to information security;
- commitment to continual improvement of the information security management system;
- assignment of responsibilities for information security management to defined roles; and
- procedures for handling exemptions and exceptions. (ISO, 2022)

The extent to which an employee is aware of and complies with information security policy defines the extent of their *information security awareness* (ISA). ISA is critical in mitigating the

risks associated with cybersecurity and is defined by two components, namely, *understanding* and *compliance*. *Compliance* is the employees' commitment to follow best-practice rules defined by the organization (Reeves *et al.*, 2020). Ajzen (1991) defines a person's *intention to comply* as the individual's motivation to perform a described behavior. The intention to comply captures the motivational factors that influence behavior. As a general rule, the stronger the effort, the willingness to perform a behavior, the more likely it will be performed.

Several frameworks or theories can be applied to research human behavior. For cybersecurity, behavior can be viewed through lenses and theories borrowed from disciplines such as criminology (e.g. deterrence theory), psychology (e.g. theory of planned behavior) and health psychology (e.g. protection motivation theory) (Moody *et al.*, 2018; Herath and Rao, 2009). The most commonly used models in the context of cybersecurity are the general deterrence theory, the theory of planned behavior and the protection motivation theory (Alassaf and Alkhalifah, 2021).

Staff's attitude and awareness can pose a security problem. In those settings, it is relevant to consider why the situation exists and what can be done about it. In many cases, a key reason will be the limited extent to which security is understood, accepted and practiced across the organization (Furnell and Thomson, 2009). As a mitigating step toward compliance, decision-makers will need guidance on achieving compliance and discouraging misuse when developing information security policies (Sommestad *et al.*, 2014). Therefore, the ability to assess behavior is a prerequisite for decision-makers in their quest to develop the organizations' information security policies. The development and responsibility for implementing policies lie within the purview of management (Höne and Eloff, 2002). Accordingly, understanding the differences in cybersecurity-related behavior between management and employees will benefit the development of more secure organizations.

1.3 Structure of the paper

The rest of this paper is organized as follows: Section 2 describes the methodology for conducting the SLR; the research questions; the record search process; and the assessment criteria. In Section 3, the results and the findings are presented. A discussion of the findings is presented in Section 4. Section 5 summarizes our conclusions and outlines directions for future research.

2. Method

This section discusses the fundamental stages of conducting an SLR. The SLR constructs are obtained by following the recommendations of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses statement (Page *et al.*, 2021) and (Fink, 2019; Weidt and Silva, 2016).

The foremost step is to investigate if a similar review has already been conducted. Searching for and studying other reviews help refine both research questions and search strings. The search did not discover any similar reviews. Keywords, search strings and research questions were collected and categorized in a literature index tool and used to optimize search strings and verify that this review's chosen research questions are relevant and valuable to the body of knowledge.

A research review is explicit about the research questions, search strategy, inclusion and exclusion criteria, data extraction method and steps taken for analysis. Research reviews are, unlike subjective reviews, comprehensible and easily reproducible (Fink, 2019). The remainder of this section elaborates on the components of the performed SLR.

2.1 Research questions

The idea of such review studies is to broaden and get a deeper understanding of where the edge of current knowledge resides. The research questions should be broad enough to include relevant literature and be precise enough to guide the review (Fink, 2019). Research questions

are tailored to a topic and to a context; in this instance, in the context of the human aspect of cybersecurity. Specifically, how can we assess behavior adhering to rules or policies of an organization in a cybersecurity context? Accordingly, our main research question is:

RQ1. How is cybersecurity-related behavior assessed?

Such behavior may be affected by an individual's position within the organization. Considering the leading role that the management is expected to have in improving the cybersecurity culture in an organization, exploring possible behavioral differences between management and employees is also significant. Accordingly, a secondary research question is:

RQ2. Are there differences between manager and employee behavior in a cybersecurity context?

2.2 Record searching process

Various search strings were used in this SLR, depending on the database. The keywords were kept unchanged, but the syntax of each database differs; hence, the search strings have minor differences. This study includes the following databases: Scopus, IEEE, Springer, Engineering Village, ScienceDirect and ACM. In some form of syntax, the keywords (exact and stemmed words) were used: Cyber, Security, Information, policy, compliance, measure, behavior. As an example, the following is the search used in Scopus: TITLE-ABS-KEY ((information AND security AND policy OR information AND security AND compliance OR policy AND compliance) AND (information AND security AND behavior)) AND PUBYEAR > 2001. To increase the precision of the searches, title, abstract and keywords were used as a limiter in all the databases.

2.3 Assessment criteria

This section describes the screening methodology and eligibility criteria used in this study. First, duplicates were removed based on each entry's digital object identifier (DOI). No unique tool other than a spreadsheet was used to deploy the removal. In cases where an entry from the database did not include a DOI, a manual search and removal process was performed using the title, author, year or similar information that could identify the unique attributes of the entry. Second, inclusion and exclusion criteria were applied. For this study, the following criteria are defined:

(1) Exclusion criteria
   - studies from organization reports, guidelines, technical opinion reports;
   - research design – exclude reviews, editorials and testimonials, as using secondary data (data from other reviews, etc.) would make this review a tertiary one; and
   - nonresearch literature.

(2) Inclusion criteria
   - written in English;
   - published in 2001–2022;
   - original studies using theoretical or empirical data; and
   - studies published in Journals, Conference Proceedings and books/book sections.

2.4 Analysis of included articles

The result presented in this review is based on the abstraction of data from the articles. The descriptive synthesized results are based on the reviewers' experience and the quality and content

of the available literature (Fink, 2019). All results are based on an abstraction of data except for those in Section 3.3.4, where the NVIVO software was used to uncover the most frequently used words from a compiled text of all analysis sections from each and every article in the review.

3. Results

3.1 Identification, screening, eligibility and inclusion mechanism

This research returned 2,153 records. The first step before any analysis is to remove any duplicates. After removing duplicates, a total of 1,611 unique records remained. Following the recommendation from Weidt and Silva (2016), the first analysis step is screening by title and abstract. A total of 1,517 records were found to be irrelevant for this review, leaving 94 articles for additional screening. The (optional) second screening, depending on the number of articles, involves an analysis of each article's introduction and conclusion. For this study, an analysis of the method section was also included in the second screening step. This narrowed the number down to 28, where another 2 articles were excluded because of the lack of empirical data and irrelevance to the topic being reviewed, leaving the total number of 26 articles for complete text analysis. Figure 1, adapted from Page *et al.* (2021) depicts the screening process.

3.2 Trend and classification of included studies

Of the 26 selected articles, 19 were published in journals, and the remaining 7 in conferences, or 73% and 27%, respectively (see Figure 2). The figure also demonstrates the increased interest in the subject in the past two years.

3.3 Findings

3.3.1 How is cybersecurity-related behavior assessed? Of the selected 26 articles in this review, 24 or 92% provide insight into how cybersecurity-related behavior is assessed. A three-step process emerges as the way to assess such behavior: First, information from subjects needs to be collected. This is referred to as *data collection*. Second, a measurement scale is deployed to ensure that the data collected is relevant and encompasses the research topic. The final step is the data analysis.

3.3.2 Data collection. Two forms of data can be collected, qualitative or quantitative. Both of these types of data can be subjective or objective; neither is exclusive to the other. The most common way to collect subjective data is using a questionnaire with questions whose answers fit into a five- or seven-point Likert scale. Within a survey, questions may be asked that are subjective, biased or misleading when viewed alone, but the results can easily be used quantitatively (O'Brien, 1999). With the ubiquity of qualitative data, the interest in quantifying and being able to assign "good" numerical values and make the data susceptible to more meaningful analysis has been a topic for research since the first methods for quantification first began to appear around 1940 (Young, 1981).

Subjective data can lead to inaccurate or skewed results. In contrast, *objective data* are free from the subject's opinions. This can be, for example, the number of attacks prevented or the number of employees clicking the link in a phishing campaign (Black *et al.*, 2008).

The SLR revealed six types of data collection methods, namely, self-assessment questionnaire (SAQ); interview; vignette; experiment with vignettes; affective computing and sentiment analysis; and clicking data from a phishing campaign. An overview of all articles and the data collection method used in each is presented in Table 1.

The most prominent form of data collection is self-assessment (SA). This subjective data collection method is defined by Boekaerts (1991) as a form of appraisal that compares one's behavioral outcomes to an internal or external standard. In total, 22 of the 24 articles used SA as the primary data collection method. The most common way to collect data is through

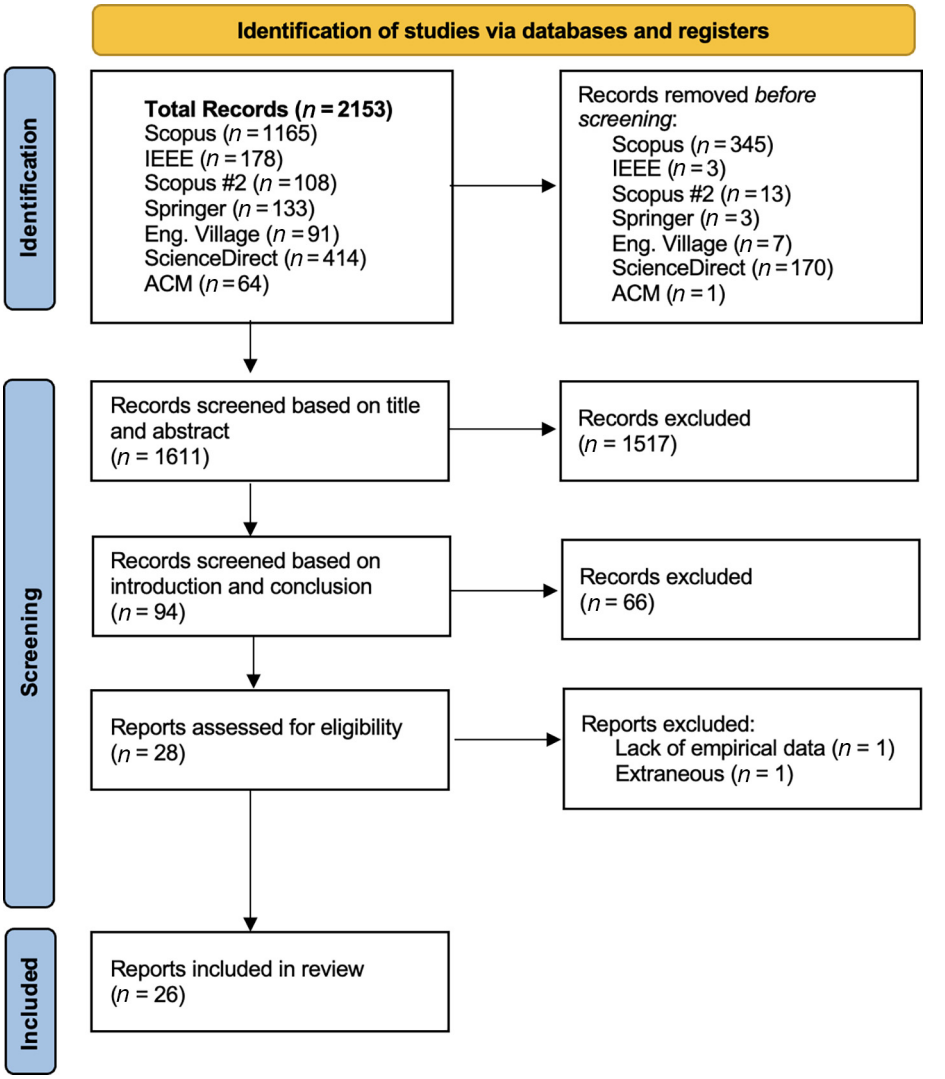

Figure 1.
The SLR screening process

a questionnaire (SAQ). A total of 17 or 71% of the articles used an SAQ as their sole method for data collection.

Of the remaining five articles with results stemming from subjective data, two used vignettes in combination with a regular SAQ. Vignettes are hypothetical scenarios in which the subject reads and forms an opinion based on the information. Barlow *et al.* (2013) performed a factorial survey method (FSM) experiment with vignettes by using randomly manipulated elements into sentences in the scenarios instead of static text. Both regular questionnaires and vignettes use the same Likert scale.

The average number of respondents in the included papers is n = 356, with 52% males and 48% females. The most common way to deploy the SAQ is through online Web

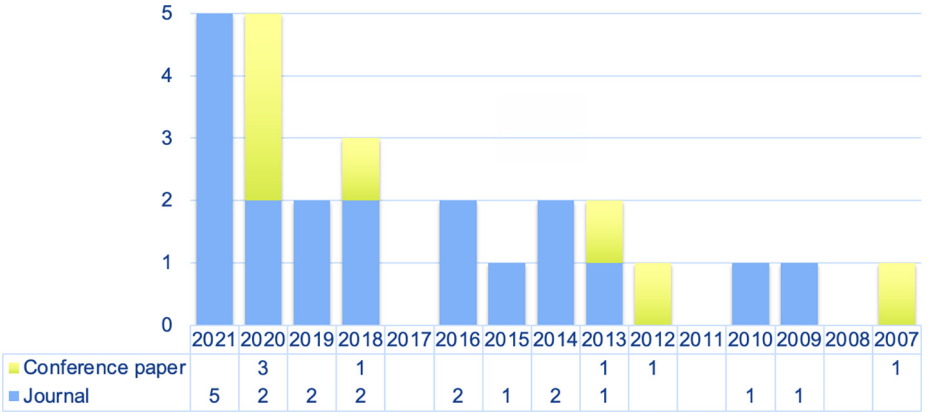

Figure 2. Trend and classification of included studies

platforms, e.g. a by-invitation-only webpage at a market research company. Pen and paper were only used twice. Market research companies and management distribution are the two most used recruitment strategies. The two methods are used in 73% of the papers, or 84% of the time, if articles that did not specify recruitment are excluded.

Two studies used interviews to collect information: one used interviews with an SAQ, and the other used interviews as the sole input. Interviews provide in-depth information and are suitable for uncovering the "how" and "why" of critical events as well as the insights reflecting the participants' relativist perspectives (Yin, 2018).

Only two studies used objective, quantitative data: Kruger *et al.* (2020) used affective computing and sentiment analysis. With the help of a deep learning neural network, the study accurately classified opinions as positive, neutral or negative based on facial expressions. Jalali *et al.* (2020) used a phishing campaign in conjunction with an SAQ to investigate whether there were any differences between intention to comply and actual compliance.

3.3.3 Measurement scale. A measurement scale ensures that the collected data encompass a topic or subject and do not miss any crucial facets. The role of a measurement scale is to ensure that the data collected is holistic and reproducible. Researchers can use predefined scales developed by others or self-developed ones. Those of the reviewed articles that use the latter form of scale are often not fully transparent about the content of the scale.

This SLR shows that 13 of the 22 articles that used a measurement scale used an unspecified scale. The most frequently (in seven papers) used specified scale is the Human Aspect of Information Security Questionnaire (HAIS-Q), developed by Parsons *et al.* (2014). When used in conjunction with other scales, HAIS-Q is often the most prominent.

Several pitfalls exist and must be considered when researchers select their measurement scale. If choosing to develop an unspecified scale, as found to be the most deployed alternative in this SLR, length, wording, familiarity with the topic, natural sequence of time and questions in a logical order are some of the topics that researchers should be mindful of (Fink, 2015). Especially the length of the questionnaire is significant; how much time do the respondents have to spend answering the survey? Another critical element when designing a measurement scale instead of using an existing one is validity and reliability. Proper pilot testing is required when choosing not to use an already-validated survey (Fink, 2015).

The HAIS-Q is designed to measure information security awareness related to information security in the workplace (McCormac *et al.*, 2017). The Knowledge, Attitude and Behavior (KAB)

Table 1.
Overview of reviewed articles

Author	Title	Data collection	Measurement scale
Pollini *et al.* (2021)	Leveraging human factors in cybersecurity: An integrated methodological approach	SAQ + Interview	HAIS-Q
Reeves *et al.* (2020)	Whose risk is it anyway: How do risk perception and organizational commitment affect employee information security awareness?	SAQ	(HAIS-Q)/Three-Component Organizational Commitment Questionnaire (3C-OCQ)/The Perception of Personal-Risk for InfoSec Threats Scale (PPRITS)/Psychometric Paradigm of InfoSec Threats Scale (PPITS)
McCormac *et al.* (2016)	Individual differences and Information Security Awareness	SAQ	HAIS-Q/The Big Five inventory (BFI)/ The Risk Averseness Scale
Barlow *et al.* (2013)	Don't make excuses! Discouraging neutralization to reduce IT policy violation	Experiment with vignettes	Self-developed scale
Merhi and Ahluwalia (2019)	Examining the impact of deterrence factors and norms on resistance to Information Systems Security	SAQ	Self-developed scale
Parsons *et al.* (2014)	Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)	SAQ	HAIS-Q
Parsons *et al.* (2015)	The influence of organizational information security culture on information security decision making	SAQ	HAIS-Q
Li *et al.* (2019)	Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior	SAQ	Self-developed scale
Cindana and Ruldeviyani (2018)	Measuring info sec awareness on employee using HAIS-Q case study at XYZ firm	SAQ	HAIS-Q
Niemimaa *et al.* (2013)	Interpreting information security policy outcomes: A frames of reference perspective	Self-assessment interview	Self-developed scale
Al-Omari *et al.* (2012)	Security policy compliance: User acceptance perspective	SAQ	Self-developed scale
Kruger *et al.* (2020)	Acquiring sentiment towards information security policies through affective computing	Affective computing and Sentiment analysis – AI	
Gangire *et al.* (2020)	Information security behavior: Development of a measurement instrument based on the self-determination theory	SAQ	HAIS-Q/SDT (ISCBMSDT)

(*continued*)

Author	Title	Data collection	Measurement scale
Goo *et al.* (2014)	A path to successful management of employee security compliance: An empirical study of information security climate	SAQ	Self-developed scale
Liu *et al.* (2020)	Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment	SAQ	Self-developed scale
Kurowski (2019)	Response biases in policy compliance research	SAQ + Self-assessment on vignettes	Self-reporting policy compliance (SRPC) scale, along with the Marlow–Crowne social desirability (MC-SDB) scale
Guhr *et al.* (2018)	The impact of leadership on employees' intended information security behavior: An examination of the full-range leadership theory	SAQ	Multifactor Leadership Questionnaire (MLQ) form 5X-Short
Jalali *et al.* (2020)	Why employees (still) click on phishing links: Investigation in hospitals	SAQ + Clicking data – Phishing campaign	Self-developed scale
Ameen *et al.* (2021)	Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce	SAQ	Self-developed scale
Chen *et al.* (2021a)	Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model	SAQ + Self-assessment on vignettes	Self-developed scale
Y. Chen *et al.* (2021b)	Voluntary and instrumental information security policy compliance: An integrated view of prosocial motivation, self-regulation and deterrence	SAQ	Self-developed scale

Table 1.

model is at the center of HAIS-Q. The hypothesis is that when computer users gain more knowledge, their attitude toward policies will improve, translating into more risk-averse behavior (Pollini *et al.*, 2021). The HAIS-Q comprises 63 questions covering 7 focus areas (internet use, email use, social networking site use, password management, incident reporting, information handling and mobile computing). Each focus area is divided into equal parts for KAB, resulting in 21 questions for each KAB element divided by the seven focus areas. For a detailed overview of the other scales used in conjunction with HAIS-Q, see the last column in Table 1.

The KAB model that underpins HAIS-Q has been criticized by researchers when used in, e.g. health and climate research. Both Parsons *et al.* (2014) and McCormac *et al.* (2016) cite McGuire (1969) who suggest that the problem is not with the model itself but with how it is applied. Parsons *et al.* (2014) highlight essential differences between environmental and health studies and the field of information security. Much ambiguity and unclear or contradictory information exist in the two former topics, while most organizations have an information security policy, either written or informal, indicating what is expected from employees (Parsons *et al.*, 2014). Barlow *et al.* (2013) advocate using scenarios instead of direct questions, like in HAIS-Q, because it is difficult to assess actual deviant behavior by observation or direct questioning.

Another critique of the HAIS-Q is the length of the questionnaire. With 63 questions, respondents might lose interest, be inattentive to the questions and sometimes give false answers (Velki *et al.*, 2019). On the contrary, Parsons *et al.* (2017) show that the HAIS-Q questionnaire is a reliable and validated measurement scale and accommodates some of the concerns raised by Fink (2015).

Pollini *et al.* (2021) advise that, when using one, the questionnaire only considers the individual level and may not capture a holistic and accurate measurement of the organizations. Therefore, in their study, HAIS-Q questionnaires were deployed at the individual level, and interviews were used to assess the organizational level.

3.3.4 Analysis. To uncover how the included articles had analyzed their results, NVIVO, a qualitative data analysis software, was used to identify the most frequently used words in each article. An accumulative document from each article's analysis section was analyzed in NVIVO. All articles use some sort of validation and statistical verification of the collected data. The use of word count provides both a structured presentation and an unbiased account of how often keywords affiliated with the technical part of the analysis are used. The result from NVIVO shows that partial least square (PLS) is the most frequently used method. Herman Wold first coined PLS in 1975; it can be preferable in cases where constructs are measured primarily by formative indicators, e.g. managerial research, or when the sample size is small (Haenlein and Kaplan, 2004). This result is also in line with the finding in Kurowski (2019): "Most of policy compliance research uses partial least squares, regression modeling or correlation analyses."

3.3.4.1 Are there differences between manager and employee intention and behavior in a cybersecurity context? Only five articles, or 19%, provide insight into the second research question. However, none provides a clear-cut response to this research question. There is a consensus in all five articles that organizational culture is a cornerstone for security and policy-compliant behavior (Reeves *et al.*, 2020; Hwang *et al.*, 2017; Alzahrani, 2021; Parsons *et al.*, 2015; Li *et al.*, 2019).

Among the articles, there is also a broad agreement that peers' behavior, the influence that peers have on our behavior, is vital for a positive cybersecurity outcome (Li *et al.*, 2019; Alzahrani, 2021; Hwang *et al.*, 2017). Peer- and policy-compliant behavior can only be achieved when the organization has a positive cybersecurity culture. The development of organizational culture often comes from the top management; hence, the development and continued improvement of culture will be assigned to management (Li *et al.*, 2019; Reeves

et al., 2020). One interesting finding in the context of developing or harnessing a security culture is that managers have a much lower information security awareness; Reeves *et al.* (2020) therefore recommend that future training should be targeted to management. This small paradox is at least something to dwell on, given that culture is built from the top.

All the articles provide reasons for noncompliance in their findings. In a hectic environment, employee workload has been shown to negatively impact compliance (Jalali *et al.*, 2020). Connected to workload are work goals. Security will draw the shortest straw when goals and security do not align. If security is viewed as a hindrance, noncompliant behavior will arise (Reeves *et al.*, 2020; Hwang *et al.*, 2017; Alzahrani, 2021; Parsons *et al.*, 2015). Also, when employees lack knowledge or have not been given sufficient information about the organization's security policies, compliant behavior will be impacted (Hwang *et al.*, 2017; Alzahrani, 2021; Parsons *et al.*, 2015; Li *et al.*, 2019).

4. Discussion

The findings of this SLR have shown that there is an overweight of subjective data collected to measure cybersecurity. Over 90% of the included articles use subjective data to measure behavior. Only one article relies solely on objective measurements. The availability and ease of use regarding subjective methods might be the reason. An interview can be done without much cost or planning, whereas using objective methods will require more resources, e.g. a phishing campaign.

However, the use of subjective data can lead to biased responses from the subjects. This bias can be problematic. According to Kurowski (2019), "For instance, survey reports of church attendance and rates of exercise are found to be double the actual frequency when self-reported." Almost all articles address the issue of biased measurement. Many refer to Podsakoff *et al.* (2003) and the recommendation therein to assure respondents that their identity will be kept anonymous. It seems like anonymization is an acceptable way to remove the risk of bias for several researchers. However, as Kurowski (2019) finds, there does exist bias in today's research. In his paper, to test for a biased response, two questionnaires were used, one using standard, straightforward compliance questions and one using vignettes, see Table 1. Kurowski (2019) found that generic questionnaires may capture biased policy compliance measures. If an individual reports policy compliance on the literature-based scale, it may mean any of the following: An individual is indeed compliant; an individual does not know the policy and does not act compliant; or an individual thinks they are compliant with the policy because they behave securely, but do not know the policy. This does not imply that existing research fails to measure policy compliance entirely, but it fails to measure it reliably (Kurowski, 2019).

Jalali *et al.* (2020) included objective and subjective measurements. They compared the employees' intention to comply with their actual compliance by examining whether the employees had clicked the link in the phishing campaign or not. They found no significant relationship between the intention to comply and the actual behavior. This result is not in line with previous studies that used self-reported data, a method that leaves room for socially desirable answers (Podsakoff *et al.*, 2003), or previous answers could influence later answers (Jalali, 2014).

Even the HAIS-Q, the single most used questionnaire, used seven times in this SLR, does not refrain from biased responses. Even though the questionnaire was validated and tested by Parsons *et al.* (2017), when researched to uncover biased responses by McCormac *et al.* (2017), showed that social desirability bias can be present. This means that further research is needed to exclude biased responses from HAIS-Q.

5. Conclusion

This SLR, which started with 2,153 unique articles and was reduced during several analysis steps to 26 articles, provides insights into the predefined research questions.

The main research question was:

RQ3. How is cybersecurity-related behavior assessed?

When excluding all preparational work before a study is performed, the assessment of behavior can be classified into three components: *data collection*, *measurement scale* and lastly, *analysis*. This research found that subjective data are collected to a much larger extent than objective data, in the context of cybersecurity, with online SAQ as the most prominent way to collect data. Measurement scales are often composed based on existing literature and adapted by the researchers. The most commonly used questionnaire is HAIS-Q, developed by Parsons *et al.* (2014). Finally, an analysis is performed to test for internal and external validation of the collected data. PLS analysis is the most frequent technique in selected articles. Although a clear path to assess behavior is uncovered, the proposed self-assessment method can produce biased data. Thus, future research should address the problem of objectively assessing cybersecurity-related behavior and the factors affecting it.

The second research question, i.e. whether there exist differences between manager and employee behavior, was not conclusively answered. Of the relatively small number of articles, several provide insights and noteworthy findings but not conclusive answers to this research question. In light of the significance of the matter for improving the cybersecurity culture in an organization, this constitutes another interesting research gap.

Future research should bridge the above research gaps, and studies should include employees and management from the same organization. This will require more planning and coordination than simply deploying a questionnaire online. Extra effort in anonymizing personal data must be in place because subjects come from the same organization. The uncertainty surrounding anonymization and the risk of biased responses concerning anonymization must be mitigated. This can be obtained by, e.g. using a hybrid method consisting of objective and subjective data collection, e.g. self-assessment questionnaires and phishing campaigns. Future research should collect holistic data within a market, country, segment or similar, as research into compliance is context-dependable (Jalali *et al.*, 2020).

References

Ajzen, I. (1991), "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, Vol. 50 No. 2, pp. 179-211.

Alassaf, M. and Alkhalifah, A. (2021), "Exploring the influence of direct and indirect factors on information security policy compliance: a systematic literature review", *IEEE Access*, Vol. 9, pp. 162687-162705.

Al-Omari, A., El-Gayar, O. and Deokar, A. (2012), "Security policy compliance: user acceptance perspective", *2012 45th HI International Conference on System Sciences*, *IEEE*, pp. 3317-3326.

Alzahrani, L. (2021), "Factors impacting users' compliance with information security policies: an empirical study", *International Journal of Advanced Computer Science and Applications*, Vol. 12 No. 10.

Ameen, N., Tarhini, A., Shah, M.H., Madichie, N., Paul, J. and Choudrie, J. (2021), "Keeping customers' data secure: a cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce", *Computers in Human Behavior*, Vol. 114, p. 106531, doi: 10.1016/j.chb.2020.106531.

Barlow, J.B., Warkentin, M., Ormond, D. and Dennis, A.R. (2013), "Don't make excuses! Discouraging neutralization to reduce IT policy violation", *Computers and Security*, Vol. 39, pp. 145-159, doi: 10.1016/j.cose.2013.05.006.

Black, P.E., Scarfone, K. and Souppaya, M. (2008), "Cyber security metrics and measures", *Wiley Handbook of Science and Technology for Homeland Security*, Wiley, NH, pp. 1-15.

Boekaerts, M. (1991), "Subjective competence, appraisals and self-assessment", *Learning and Instruction*, Vol. 1 No. 1, pp. 1-17, doi: 10.1016/0959-4752(91)90016-2.

Chen, Y., Galletta, D.F., Lowry, P.B., Luo, X., Moody, G.D. and Willison, R. (2021a), "Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model", *Information Systems Research*, Vol. 32 No. 3, pp. 1043-1065, doi: 10.1287/isre.2021.1014.

Chen, Y., Xia, W. and Cousins, K. (2021b), "Voluntary and instrumental information security policy compliance: an integrated view of prosocial motivation, self-regulation and deterrence", *Computers and Security*, Vol. 113, p. 102568, doi: 10.1016/j.cose.2021.102568.

Cindana, A. and Ruldeviyani, Y. (2018), "Measuring information security awareness on employee using HAIS-Q: case study at XYZ firm", *2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, pp. 289-294.

Fink, A. (2015), *How to Conduct Surveys: A Step-by-Step Guide*, Sage Publications, London.

Fink, A. (2019), *Conducting Research Literature Reviews: From the Internet to Paper*, Sage publications, London.

Furnell, S. and Thomson, K.L. (2009), "From culture to disobedience: recognising the varying user acceptance of IT security", *Computer Fraud and Security*, Vol. 2009 No. 2, pp. 5-10, doi: 10.1016/S1361-3723(09)70019-3.

Gangire, Y., Da Veiga, A. and Herselman, M. (2020), "Information security behavior: development of a measurement instrument based on the self-determination theory", *International Symposium on Human Aspects of Information Security and Assurance*, Springer, Cham, pp. 144-157.

Goo, J., Yim, M. and Kim, D.J. (2014), "A path to successful management of employee security compliance: an empirical study of information security climate", *IEEE Transactions on Professional Communication*, Vol. 57 No. 4, pp. 286-308, doi: 10.1109/TPC.2014.2374011.

Guhr, N., Lebek, B. and Breitner, M.H. (2018), "The impact of leadership on employees' intended information security behaviour: an examination of the full-range leadership theory", *Information Systems Journal*, Vol. 29 No. 2, pp. 340-362, doi: 10.1111/isj.12202.

Haenlein, M. and Kaplan, A.M. (2004), "A beginner's guide to partial least squares analysis", *Understanding Statistics*, Vol. 3 No. 4, pp. 283-297.

Herath, T. and Rao, H.R. (2009), "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106-125.

Höne, K. and Eloff, J.H.P. (2002), "Information security policy – what do international information security standards say?", *Computers and Security*, Vol. 21 No. 5, pp. 402-409, doi: 10.1016/S0167-4048(02)00504-7.

Hwang, I., Kim, D., Kim, T. and Kim, S. (2017), "Why not comply with information security? An empirical approach for the causes of non-compliance", *Online Information Review*, Vol. 41 No. 1, pp. 2-18.

International Standardization Organization (2022), "ISO/IEC 27002:2022, information security, cybersecurity and privacy protection – information security controls".

Jalali, M.S. (2014), "How individuals weigh their previous estimates to make a new estimate in the presence or absence of social influence", *International Social Computing, Behavioral-Cultural Modeling and Prediction*, Springer, Cham, pp. 67-74.

Jalali, M.S., Bruckes, M., Westmattelmann, D. and Schewe, G. (2020), "Why employees (still) click on phishing links: investigation in hospitals", *Journal of Medical Internet Research*, Vol. 22 No. 1, p. E16775, doi: 10.2196/16775.

Kilskar, S.S. (2020), "Socio-technical perspectives on cyber security and definitions of digital transformation – a literature review", *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*, *Venice*.

Kruger, H., Du Toit, T., Drevin, L. and Maree, N. (2020), "Acquiring sentiment towards information security policies through affective computing", *2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, 25-27 Nov. 2020, pp. 1-6.

Kurowski, S. (2019), "Response biases in policy compliance research", *Information and Computer Security*, Vol. 28 No. 3, pp. 445-465, doi: 10.1108/ICS-02-2019-0025.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019), "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior", *International Journal of Information Management*, Vol. 45, pp. 13-24, doi: 10.1016/j.ijinfomgt.2018.10.017.

Liu, C., Wang, N. and Liang, H. (2020), "Motivating information security policy compliance: the critical role of supervisor-subordinate guanxi and organizational commitment", *International Journal of Information Management*, Vol. 54, p. 102152, doi: 10.1016/j.ijinfomgt.2020.102152.

McCormac, A., Calic, D., Butavicius, M.A., Parsons, K., Zwaans, T. and Pattinson, M.R. (2017), "A reliable measure of information security awareness and the identification of bias in responses", *Australian Journal of Information Systems*, Vol. 21.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M. (2016), "Individual differences and information security awareness", *Computers in Human Behavior*, Vol. 69, pp. 151-156, doi: 10.1016/j.chb.2016.11.065.

McGuire, W. (1969), *'The Nature of Attitudes and Attitude Change*, Vol. 3, Addison-Wesley, Reading.

Merhi, M. and Ahluwalia, P. (2019), "Examining the impact of deterrence factors and norms on resistance to information systems security", *Computers in Human Behavior*, Vol. 92, pp. 37-46, doi: 10.1016/j.chb.2018.10.031.

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

Niemimaa, M., Laaksonen, A.E. and Harnesk, D. (2013), "Interpreting information security policy outcomes: a frames of reference perspective", *2013 46th HI International Conference on System Sciences*, *IEEE*, pp. 4541-4550.

O'Brien, D.P. (1999), "Quantitative vs Subjective", *Business Measurements for Safety Performance*, CRC Press, Boca Raton, p. 51.

Page, M., McKenzie, J., Bossuyt, P., Boutron, I., Hoffmann, T., Mulrow, C., Shamseer, L., Tetzlaff, J., Akl, E., Brennan, S., Chou, R., Glanville, J., Grimshaw, J., Hróbjartsson, A., Lalu, M., Li, T., Loder, E., Mayo-Wilson, E., McDonald, S. and Moher, D. (2021), "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews", *Bmj*, Vol. 372, p. N71, doi: 10.1136/bmj.n71.

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.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)", *Computers and Security*, Vol. 42, pp. 165-176, doi: 10.1016/j.cose.2013.12.003.

Parsons, K.M., Young, E., Butavicius, M.A., McCormac, A., Pattinson, M.R. and Jerram, C. (2015), "The influence of organizational information security culture on information security decision making", *Journal of Cognitive Engineering and Decision Making*, Vol. 9 No. 2, pp. 117-129, doi: 10.1177/1555343415575152.

Pirbhulal, S., Gkioulos, V. and Katsikas, S. (2021), "A systematic literature review on RAMS analysis for critical infrastructures protection", *International Journal of Critical Infrastructure Protection*, Vol. 33, p. 100427.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y. and Podsakoff, N.P. (2003), "Common method biases in behavioral research: a critical review of the literature and recommended remedies", *Journal of Applied Psychology*, Vol. 88 No. 5, pp. 879-903.

Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F. and Guerri, D. (2021), "Leveraging human factors in cybersecurity: an integrated methodological approach", *Cognition, Technology and Work*, Vol. 24 No. 2, pp. 371-390, doi: 10.1007/s10111-021-00683-y.

Reeves, A., Parsons, K. and Calic, D. (2020), "Whose risk Is it anyway: how do risk perception and organisational commitment affect employee information security awareness?", *International Conference on Human-Computer Interaction*, Springer, Cham, pp. 232-249.

Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J. (2014), "Variables influencing information security policy compliance: a systematic review of quantitative studies", *Information Management and Computer Security*, Vol. 22 No. 1, pp. 42-75.

Velki, T., Mayer, A. and Norget, J. (2019), "Development of a new international behavioral-cognitive internet security questionnaire: preliminary results from Croatian and German samples", *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, *IEEE*, pp. 1209-1212.

Weidt, F. and Silva, R. (2016), "Systematic literature review in computer science-a practical 'guide", *Relatórios Técnicos Do DCC/UFJF*, Vol. 1 No. 8, doi: 10.13140/RG.2.2.35453.87524.

Yin, R.K. (2018), *Case Study Research and Applications*, 6th ed., Sage, London.

Young, F.W. (1981), "Quantitative analysis of qualitative data", *Psychometrika*, Vol. 46 No. 4, pp. 357-388, doi: 10.1007/BF02293796.

Further readings

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548.

Pahnila, S., Siponen, M. and Mahmood, A. (2007), "Employees' behavior towards IS security policy compliance", *2007 40th Annual HI International Conference on System Sciences (HICSS'07)*, *IEEE*, pp. 156b-156b.

Corresponding author

Sokratis K. Katsikas can be contacted at: sokratis.katsikas@ntnu.no