Received 12 October 2023
Revised 13 January 2024
24 March 2024
Accepted 24 March 2024

Qualitative content analysis of actionable advice in information security policies – introducing the keyword loss of specificity metric

Elham Rostami and Fredrik Karlsson
School of Business, Informatics, Örebro University, Örebro, Sweden

Abstract

Purpose – This paper aims to investigate how congruent keywords are used in information security policies (ISPs) to pinpoint and guide clear actionable advice and suggest a metric for measuring the quality of keyword use in ISPs.

Design/methodology/approach – A qualitative content analysis of 15 ISPs from public agencies in Sweden was conducted with the aid of Orange Data Mining Software. The authors extracted 890 sentences from these ISPs that included one or more of the analyzed keywords. These sentences were analyzed using the new metric – keyword loss of specificity – to assess to what extent the selected keywords were used for pinpointing and guiding actionable advice. Thus, the authors classified the extracted sentences as either actionable advice or other information, depending on the type of information conveyed.

Findings – The results show a significant keyword loss of specificity in relation to pieces of actionable advice in ISPs provided by Swedish public agencies. About two-thirds of the sentences in which the analyzed keywords were used focused on information other than actionable advice. Such dual use of keywords reduces the possibility of pinpointing and communicating clear, actionable advice.

Research limitations/implications – The suggested metric provides a means to assess the quality of how keywords are used in ISPs for different purposes. The results show that more research is needed on how keywords are used in ISPs.

Practical implications – The authors recommended that ISP designers exercise caution when using keywords in ISPs and maintain coherency in their use of keywords. ISP designers can use the suggested metrics to assess the quality of actionable advice in their ISPs.

Originality/value – The keyword loss of specificity metric adds to the few quantitative metrics available to assess ISP quality. To the best of the authors' knowledge, applying this metric is a first attempt to measure the quality of actionable advice in ISPs.

Keywords Information security policy, Actionable advice, Policy design, Content analysis, Text analysis

Paper type Research paper

Information & Computer Security
Vol. 32 No. 4, 2024
pp. 492-508
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-10-2023-0187

1. Introduction

In today's digital world, organizations face an unprecedented level of information security threats from both external and internal sources that can lead to information security breaches. These breaches can cause severe damage to organizations' reputation, financial stability and even survival (Kör and Metin, 2021). Beyond organizational damage, such breaches can harm individuals (Culnan and Williams, 2009).

Although significant advances have been made in the technical controls that organisations implement, they are not enough to sustain a good information security posture. Both practitioner reports (PwC, 2018; Truesec, 2023) and research (Chatterjee *et al.*, 2019) have underscored the critical role of human behavior in information security. Employees often have access to sensitive information and information systems, that is, information assets, and they may cause damage to the organization intentionally or unintentionally. For example, an employee may intentionally leak information for personal gain or inadvertently share confidential information. Moreover, employees' actions may create opportunities for external threats to materialize, such as downloading a virus by clicking on a link in an e-mail. Human behavior has been consistently reported as a top-ranked information security threat over the last three decades (Loch *et al.*, 1992; Chowdhury *et al.*, 2019). Thus, it is natural that organizations take steps to guide employees' behavior by the use of formal controls.

One of the most important types of formal controls is the information security policy (ISP). ISP has been defined as "a document that states how an organization plans to protect its information assets from external and internal threats, operationalizes the implementation of security and provides guidelines for employee and management conduct" (Goel and Chengalur-Smith, 2010). ISPs can generally be defined at three levels. At the highest level, strategic ISPs contain top management's expression of the organization's overall direction, scope and tone for all information security efforts. At the middle level, operational ISPs provide procedures that employees must comply with in their daily work (Siponen and Vance, 2010). At the lowest level, technical ISPs are related to the security architecture of information systems (Whitman, 2008). This paper focuses on operational ISPs that intend to direct employee behavior.

Since operational ISPs are developed to support employees with their daily work, it is important that employees understand these ISPs and comply with them. However, employees' poor ISP compliance is a perennial problem for many organizations (Ponemon Institute LLC, 2020; PWC, 2014). Rostami (2023) asserted that ISP noncompliance could have at least two reasons: the employees' behavior and the ISP design. Consequently, employees should not always be blamed for noncompliance; the design of ISPs can also make complying with them difficult. Considering this point, several studies can be found that emphasize designing clear and understandable ISPs (e.g. Stahl *et al.*, 2012; Höne and Eloff, 2002; Lopes and Oliveira, 2015; Karlsson *et al.*, 2017). In addition, the ISO/IEC 27002 standard (ISO, 2022) and other regulations, such as European Union directives (Sundt, 2006), provide guidelines for ISP design. However, most of these guidelines provide high-level recommendations, such as what topics to address (ISO, 2022) and that ISPs should "give specific and actionable advice" (Stahl *et al.*, 2012).

Actionable advice provides instructions for employees about "what is allowed and what is not allowed regarding a specific work task" (Rostami *et al.*, 2023). These instructions can be associated with one or more consequences to sanction noncompliance. Karlsson *et al.* (2017) have stressed the importance of providing advice for employees' actions based on clear and congruent use of concepts. Still, not much guidance has been provided on how actionable advice should be worded to provide specific and congruent instructions to

employees. One exception is Diver (2021), who recommends style guidelines, for example, using specific keywords to ensure that pieces of actionable advice are "useable" for employees. As argued in a shorter version of this work previously presented at IFIP International Symposium on Human Aspects of Information Security and Assurance – HAISA 2023 (Rostami and Karlsson, 2023), there is also a lack of knowledge of how congruently such keywords are applied to give actionable advice. Against this backdrop, this paper aims to investigate how congruent keywords are used in ISPs to pinpoint and guide clear actionable advice and suggest a metric for measuring the quality of keyword use in ISPs. To this end, we develop a text analysis metric, keyword loss of specificity, which captures the relative frequency when a keyword is not used in line with a specific purpose, reducing the possibility of pinpointing and guiding a piece of actionable advice. We have used this metric to assess 15 ISPs from public agencies in Sweden, analyzing a total of 890 sentences that included a selected set of keywords (see Section 3.2 for details).

The remaining part of the paper is structured as follows. Section 2 discusses related research on ISP design and quality metrics. Section 3 presents the research method applied in this study. In Section 4, we present the results of our analysis. In Section 5, we discuss the findings and the implications for research and practice. We end this section by presenting the limitations and avenues for future research. Finally, in Section 6, we provide a short conclusion.

2. Related work

2.1 Information security policy and actionable advice

The content of ISPs can fulfill various roles, including providing general information or serving an educational purpose. Nevertheless, the primary objective of such policies is to guide employee behavior by offering actionable advice. Previous literature reviews on ISP research have shown that several studies address ISP design (Rostami *et al.*, 2020; Cram *et al.*, 2017). Several of these studies address the importance of writing clear, congruent and actionable advice for employees about how to handle information assets in a secure manner (e.g. Stahl *et al.*, 2012; Alshaikh *et al.*, 2015; Rostami *et al.*, 2020; Goel and Chengalur-Smith, 2010; Lopes and Oliveira, 2015; Doherty and Fulford, 2006; Karlsson *et al.*, 2017). However, these studies offer limited guidance on how to write instructions that cover the above-mentioned aspects. For example, Stahl *et al.* (2012) conducted critical discourse analysis on British National Health Service ISPs. Their study revealed a significant amount of ambiguity in these policies, especially concerning the ISPs' objectives and intended targets, as well as significant evidence of the use of jargon and unfamiliar language. Based on their findings, they provided a set of recommendations that should be considered when writing ISPs. They suggested that accessible language and terminology should be used and that specific, actionable advice and practical guidelines should be given to employees. However, the high-level recommendations presented by Stahl *et al.* (2012) lack enough elaboration to provide ISP designers with cues about what is an accessible language, what a piece of actionable advice consists of and how such a piece of advice should be written.

Also, using discourse analysis, Karlsson *et al.* (2017) investigated ISPs as a practical tool in employees' everyday work. They found that the investigated ISPs lacked internal congruence, making them difficult to use as a practical tool. As a result, they suggested eight quality criteria for ISPs, which can also provide guidance when writing ISPs. For example, it is advised that ISPs should provide "congruent guidelines for actions." Similar to Stahl *et al.* (2012), this is a high-level recommendation that lacks an explanation of how to write such a guideline. Still, in another of their criteria, they stress the importance of using a "clear and congruent conceptual framework" as the foundation for these guidelines. Thus, it

shows the importance of carefully choosing and applying concepts, such as keywords, when writing actionable advice.

Alshaikh *et al.* (2015) provided a comprehensive overview of the management practices of ISPs and developed a model for ISP design. They recommend easy-to-use language when making information security procedures explicit in ISPs. Building on Whitman (2004), Lopes and Oliveira (2015) state that ISPs should "define which users are authorized or not to use the system." Similarly, Doherty and Fulford (2006) argue that an ISP should include explicit steps to guide employees. However, none of these authors provide any guidance on how to use keywords when writing these pieces of actionable advice.

Based on existing research, Rostami *et al.* (2020) provide 14 requirements for developing software to support the design of ISPs. These requirements can also be considered characteristics of a high-quality ISP; a subset of them is related to writing actionable advice. First is the fundamental requirement that ISPs should include pieces of actionable advice. However, this requirement does not say anything about how such advice should be written. Still, three of the other requirements provide some input. In summary, the three additional requirements say that ISPs should be expressed using the employees' work practice language. Furthermore, a piece of actionable advice should be associated with clear responsibilities and consequences and be based on a clear set of concepts. Although the provided list of requirements is valuable and should be considered in designing ISPs, these requirements are defined at an abstract level.

Besides existing research, there exists practitioner-oriented literature that guides the design of ISPs (e.g. Diver, 2021; ISO, 2022; Landoll, 2017; NIST, 2006; Peltier, 2004; Smith, 2010). Although this type of literature places much focus on the structure of ISPs and topics to address (ISO, 2022), there exist guidelines about actionable advice. For example, Diver (2021) provides guidelines on how to word actionable advice to make it easy for employees to understand them. It is advisable to use concrete language and avoid abstract terminology that can be confusing. Negative statements such as "never" should be avoided, as they introduce shades of prohibition that may not be clear. Instead, the focus should be on presenting pieces of actionable advice that are clear, usable and unambiguous about actions that are allowed or disallowed, as well as any exceptions that apply. Diver (2021) further recommended using "must" instead of "shall" and "will," where "must" is intended, to avoid inconsistencies and prevent confusion between future tense and mandatory language.

In conclusion, research and practitioner-oriented literature highlight the importance of writing clear and comprehensive instructions for employees. However, while research studies offer valuable insights about shortcomings regarding these aspects of ISPs, they provide limited guidelines on how to write actionable advice beyond stressing the use of clear, accessible and congruent concepts and being explicit about the consequences of noncompliance with the actionable advice. Practitioner-oriented literature, to some extent, provides guidelines on how to write actionable advice, but without critically assessing how these guidelines are used. Thus, we have limited knowledge about how congruent keywords are applied to pinpoint and guide actionable advice.

2.2 Information security policy quality metrics

Existing research has provided few metrics – policy length (Alshaikh *et al.*, 2015; Höne and Eloff, 2002), breath, brevity and clarity (Goel and Chengalur-Smith, 2010) – to assess the quality of ISPs. In their model for ISP design, Alshaikh *et al.* (2015) stress that ISPs should not be too lengthy. They build on Höne and Eloff (2002), who argue that if ISPs are too lengthy, employees are likely to ignore them. A length metric is easy to use and can be operationalized in different ways. The most common implementations are word count or

page count analyses. However, length is a coarse, high-level metric that does not capture any aspects of the ISP content, and it does not address how keywords are used in ISP texts.

Goel and Chengalur-Smith (2010) have examined the existing ISP literature and defined three quantitative metrics – breadth, clarity and brevity – to assess the overall communicative effectiveness of ISPs. Breadth measures the level of comprehensiveness of the ISP, aligning with the suggestion put forth by Hong *et al.* (2006) that policies should be as comprehensive as possible. Goel and Chengalur-Smith (2010) use a master glossary as a starting point for measuring occurrences of information security terms; a higher degree of matches means a more comprehensive ISP. Brevity measures the repetitiveness of words in the ISP, and they argue that low repetitiveness eliminates redundancy, wordiness and jargon. Finally, clarity focuses on readability. Although using established metrics for text analysis (Flesch Reading Ease Score, Flesch–Kincaid Grade Level and the Gunning fog index), they conclude that such metrics do not account for readers' difficulties in absorbing the content. These three metrics are important as an analytical tool, and the measuring results should be considered when writing ISPs. However, these metrics do not focus on how pieces of actionable advice are worded or how keywords are used in these wordings.

3. Research method

The research approach taken in this study is qualitative content analysis (Assarroudi *et al.*, 2018). This research approach uses a systematic coding process to describe and interpret textual data, such as the one found in ISPs. According to Hsieh and Shannon (2005), there are three distinct approaches to qualitative content analysis: conventional, directed or summative. Key differences among these approaches center on how initial codes are developed. Conventional analysis derives categories from data during analysis, allowing for a richer understanding of a phenomenon. Directed analysis uses existing theory to develop the initial coding scheme, with the scheme being refined as analysis proceeds. Summative analysis approaches text as single words or specific content to interpret contextual meaning based on patterns. In this paper, the third approach was taken to identify patterns in ISPs. In the following, the data collection and analysis processes are presented, including the keyword loss of specificity metric.

3.1 Collecting information security policies

As an empirical starting point for our study, we obtained access to organization-wide ISPs from public agencies in Sweden. We choose to address public agencies since, according to the principle of public access to official records (SFS, 2009), documents such as ISPs stored, received and established at an agency are made public upon request if they are not classified as confidential. Since our focus is on actionable advice that is supposed to guide employees' behavior, we have collected operational ISPs. As discussed in the introduction, this type of policy dictates procedures that employees must adhere to in their daily tasks (Siponen and Vance, 2010). Thus, strategic and technical ISPs that define top management's view on information security (Baskerville and Siponen, 2002) and provide detailed information security configurations of information systems (Whitman, 2008), respectively, were not included. We used the principle of saturation (Strauss and Corbin, 1998) to decide how many ISPs to include in the analysis. In our case, saturation refers to the point when a stable pattern appeared in our analysis of extracted sentences from ISPs. In total, we have included 15 ISPs in this study. Although these ISPs all target employees, they differed in length; they ranged between 3 and 22 pages. In total, we analyzed 124 ISP pages of text (see Sections 3.4 and 3.5 for details on how sentences were extracted and analyzed).

3.2 Identifying the keywords

Our interest in how keywords are used in existing ISPs to pinpoint and guide actionable advice means that we are interested in analyzing specific parts of the ISPs. We are interested in sentences that include these keywords, that is, *possible* actionable advice. Thus, we need a relevant set of keywords to search and extract ISP sentences. As discussed in Section 2, the existing body of research does not provide clear guidance on how to design pieces of actionable advice that are direct, imperative and easily comprehensible. For example, the abstract guidelines provided by Karlsson *et al.* (2017) and Stahl *et al.* (2012) do not offer keywords on how to write actionable advice that employees must comply with in daily work. Therefore, we turned to practitioner-oriented literature and the guidelines offered by Diver (2021).

Drawing on Diver (2021), we selected the nine keywords presented in Table 1. The leftmost column contains our Swedish keywords, as the collected ISPs were in Swedish. The rightmost column presents the English translation. We have deliberately included keywords that Diver (2021) advises on using and against using to capture both aspects. As discussed in Section 2, Diver's (2021) advice against using "never" and for using "must" in place of "shall" and "will," where "must" is intended. To be inclusive, we have used synonyms for some of the Swedish keywords. The decision to include synonyms was based on our initial read of the ISPs. Thus, we included the words "ska" and "skall," which both mean shall, and "ej" and "inte," which both mean not.

3.3 Loss of keyword specificity metric

For keywords to be effective in ISPs, they should be used in line with their purpose. In the case of actionable advice, they should serve the purpose of helping employees pinpoint such pieces of advice and provide guidance on how employees are supposed to work with information assets. We developed the Loss of Keyword Specificity metrics to measure the quality of how keywords are used in the extracted sentences, where specificity is a measure of the quality of a keyword relating uniquely to a particular purpose. In our case, the particular purpose is about pinpointing and guiding actionable advice.

The development of the metrics was iterative and integrated into our content analysis of the ISPs. The development process started with trials to investigate one keyword (from Table 1) in one single ISP to find out how to extract potential actionable advice sentences (see Section 3.4), classify them based on how the keywords were used (see Section 3.5) and how to present the result. The last part required us to define what the results represented and what constituted its input. These definitions formed the embryo of our metrics. In

Swedish	English
Aldrig	Never
Behöver	Need
Bör	Should
Ej	Not
Förbjuden	Forbidden
Inte	Not
Måste	Must
Ska	Shall
Skall	Shall

Source: Created by authors

Table 1. Keywords used for extracting sentences in information security policies

subsequent iterations, more keywords and ISPs were gradually added. We used feedback from practitioners and scholars, for example, by presenting a shorter version of this work at HAISA 2023 (Rostami and Karlsson, 2023), to refine how to present the analysis, resulting in the loss of keyword specificity metrics.

The loss of keyword specificity for an individual keyword can be calculated as follows:

$$Keyword\ \ Loss\ \ of\ \ Specificity = 100 \times \frac{n_{not}}{n}$$

n = total number of occurrences of a keyword in the ISP; and

n_{not} = total number of occurrences where the keyword is *not* used in line with a defined purpose in the analyzed ISP.

To provide an overall assessment of an ISP, the use of individual keywords can be summarized as total keyword loss of specificity:

$$Total\ \ Keyword\ \ Loss\ \ of\ \ Specificity = \ 100 \times \frac{\sum_{i=1}^{kn} n_{not}}{N}$$

kn = total number of keywords; and

N = total number of occurrences of keywords in the analyzed ISPs.

3.4 Extracting sentences in each information security policy

As discussed above, we analyzed 124 pages of ISP text. We used the Orange Data Mining Software (Demsar *et al.*, 2013) to extract relevant sentences from the ISPs to increase efficiency and consistency in the research process. Orange is a powerful toolkit for machine learning, data mining and data visualization. Figure 1 shows the Orange software user

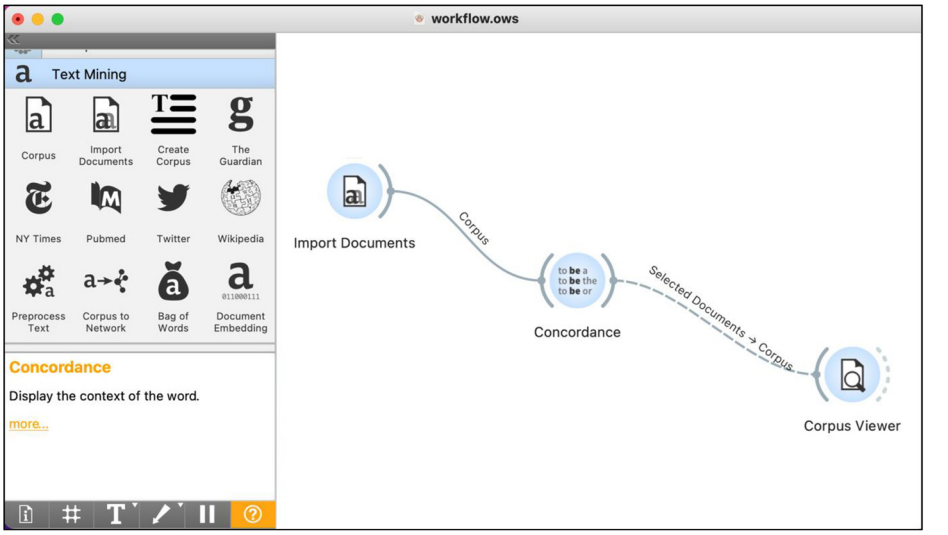


Figure 1.
The workflow for extracting sentences in Orange software

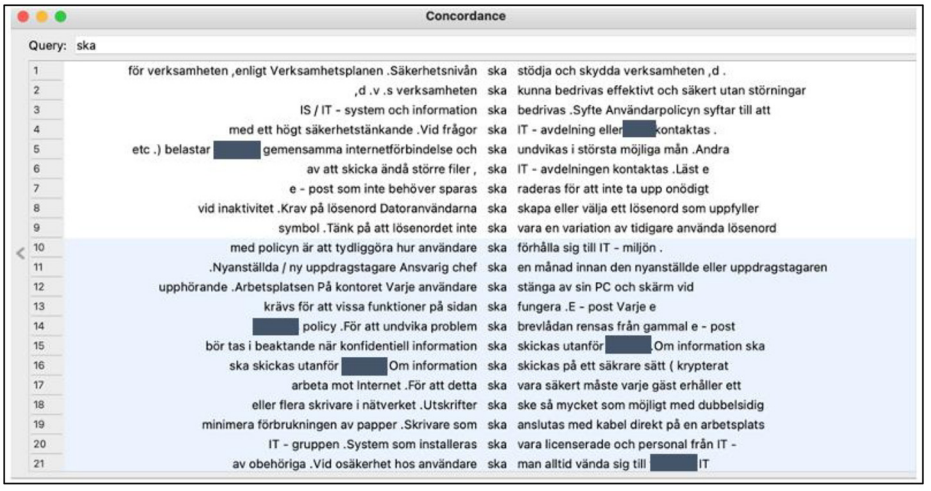
Source: Created by authors

interface and the workflow we created to extract sentences. As the workflow shows, a corpus, that is, a collection of authentic texts, in our case, the 15 ISPs, was migrated to the software through an Import Documents widget. A Concordance widget was connected to the Import Documents widget. Concordance is essentially a search engine tool used to examine the corpus, for example, to view words in context and extract information about frequency, range (how many different texts a word/phrase is used in), collocation and grammar. Finally, the Concordance widget was connected to a Corpus Viewer widget as an output of matching documents (in our case, the ISPs including our desired keywords).

This way of extracting sentences from the ISPs allowed us to make extraction decisions based on automated identification of the keywords rather than relying on manual searches. As shown in Figure 2, the concordance widget allowed us to identify sentences in the ISPs containing, for example, the keyword "ska" along with their surrounding contextual words. In the figure, we have masked minor parts of some sentences to avoid disclosing the public agencies. Concordance was applied nine times, which meant one search for each keyword. During each application, the ISPs containing the target keyword were selected and output to the Corpus viewer widget for further investigation. In total, 890 sentences (N) were extracted from the 15 ISPs, each sentence containing at least one of our predefined keywords.

3.5 Analyzing the extracted sentences

Upon identifying the sentences in each ISP, we proceeded to analyze them. The sentences were extracted from the corpus viewer and stored in an Excel sheet. The Excel sheet allowed us to write analytical memos about the ongoing analysis and connect these memos to individual sentences. The spreadsheet also made it possible to summarize how many times each keyword had occurred in each ISP (n). The sentences were divided between the authors, and the keyword analysis was done individually. After completing the individual analyses, we examined the challenges encountered during the analysis process, specifically focusing on the sentences that posed uncertainties in terms of categorization. Our analytical memos were used as input for this discussion. This discussion was conducted during a dedicated session and helped us to settle any inconsistencies. After the session, the individual analyses


Concordance

Query: ska

1	för verksamheten ,enligt Verksamhetsplanen .Säkerhetsnivån	ska	stödja och skydda verksamheten ,d .
2	,d .v .s verksamheten	ska	kunna bedrivas effektivt och säkert utan störningar
3	IS / IT - system och information	ska	bedrivas .Syfte Användarpolicyn syftar till att
4	med ett högt säkerhetstänkande .Vid frågor	ska	IT - avdelning eller [redacted] kontaktas .
5	etc .) belastar [redacted] gemensamma internetförbindelse och	ska	undvikas i största möjliga mån .Andra
6	av att skicka ändå större filer ,	ska	IT - avdelningen kontaktas .Läst e
7	e - post som inte behöver sparas	ska	raderas för att inte ta upp onödigt
8	vid inaktivitet .Krav på lösenord Datoranvändarna	ska	skapa eller välja ett lösenord som uppfyller
9	symbol .Tänk på att lösenordet inte	ska	vara en variation av tidigare använda lösenord
10	med policyn är att tydliggöra hur användare	ska	förhålla sig till IT - miljön .
11	.Nyanställda / ny uppdragstagare Ansvarig chef	ska	en månad innan den nyanställde eller uppdragstagaren
12	upphörande .Arbetsplatsen På kontoret Varje användare	ska	stänga av sin PC och skärm vid
13	krävs för att vissa funktioner på sidan	ska	fungera .E - post Varje e
14	[redacted] policy .För att undvika problem	ska	brevlådan rensas från gammal e - post
15	bör tas i beaktande när konfidentiell information	ska	skickas utanför [redacted] .Om information ska
16	ska skickas utanför [redacted] Om information	ska	skickas på ett säkrare sätt (krypterat
17	arbeta mot Internet .För att detta	ska	vara säkert måste varje gäst erhåller ett
18	eller flera skrivare i nätverket .Utskrifter	ska	ske så mycket som möjligt med dubbelsidig
19	minimera förbrukningen av papper .Skrivare som	ska	anslutas med kabel direkt på en arbetsplats
20	IT - gruppen .System som installeras	ska	vara licenserade och personal från IT -
21	av obehöriga .Vid osäkerhet hos användare	ska	man alltid vända sig till [redacted] IT

Figure 2.
The result of searching the keyword "ska" in Concordance widget

Source: Created by authors

were merged into one analysis, and the keyword loss of specificity and total keyword loss of specificity were calculated.

During the analysis, we categorized the extracted sentences as either actionable advice or other information, depending on the type of information conveyed. Thus, other information meant that the keywords were not used to provide actionable advice to employees (i.e. such a sentence was added to n_{not}). Categorizing the sentences was relatively straightforward, although it was not mechanical. If the sentence contained sufficient information to act upon without any ambiguity, it was categorized as clear actionable advice; otherwise, it was categorized as other information. Accordingly, other information represents both ambiguous instructions and sentences similar to actionable advice but written at an abstract level, indicating a general direction of the organization. For example, sentences such as "Passwords must not be given over the phone" or "read e-mail that does not need to be saved should be deleted in order not to take up unnecessary space on the server" were classified as actionable advice, as they provided specific directions for employees to follow. On the other hand, sentences such as "all staff must exercise caution when using e-mail" or "orders must be submitted to IT in good time for planning the implementation of the order" were classified as other information as they do not provide specific and clear instructions. The former sentence was considered vague because it lacked specificity on how to approach e-mails, while the latter was ambiguous since "good time" could be interpreted differently by employees. Meanwhile, sentences such as "the information in the [name of system] IT system sometimes concerns the personal circumstances of individual citizens, e.g. protected identity, and must therefore be carefully protected against unwanted changes as well as loss and disclosure" were also classified as other information because they provide an overall direction that is more suitable for strategic ISPs, despite including relevant keywords.

4. Results

This section presents the analysis of the extracted ISP sentences and how the keywords are used. Table 1 presents an overview of each ISP's total keyword loss of specificity. The leftmost column lists the identifier of the ISP, while the second and third columns show the number of sentences classified as actionable advice and other information, respectively. The fourth column provides the total number of extracted sentences for each ISP. The last column presents total keyword loss of specificity, providing a comprehensive view of the distribution of the two categories of sentences in the entire data set.

As Table 2 shows, overall, 890 sentences were extracted from 15 ISPs that included at least one of our keywords, for example, "ska" (shall) and "måste" (must), that are suggested to guide actionable advice. However, as the results in the final row show, 66.9% of the sentences were other information. It means that the assessed keywords do not uniquely relate to actionable advice, as only 33.1% of the sentences were classified as actionable advice. Consequently, the assessed ISPs perform poorly from a design perspective, where keywords are to be used uniquely to help employees pinpoint actionable advice. When assessing the individual ISPs, it is only ISP 1 that stands out with a low total keyword loss of specificity (14.3%). In this ISP, the assessed keywords are used mainly to pinpoint and guide actionable advice.

There is a fairly significant gap to the next two ISPs (4 and 6), which have a total keyword loss of specificity of 42.9% and 37.8%, respectively. In total, we found only three ISPs where more than 50% of the extracted sentences were classified as actionable advice. In a majority of the assessed ISPs, there is a significant total keyword loss of specificity. In four of the ISPs (7, 8, 10 and 13), the total keyword loss of specificity is 85% or higher, which

ISP	Actionable advice	Other information	Total	Total keyword loss of specificity (%)
1	42	7	49	14.3
2	23	34	57	59.6
3	20	21	41	51.2
4	36	27	63	42.9
5	7	24	31	77.4
6	23	14	37	37.8
7	5	59	64	92.2
8	20	139	159	87.4
9	13	19	32	59.4
10	4	36	40	90.0
11	41	82	123	66.7
12	35	71	106	67.0
13	2	16	18	88.9
14	12	16	28	57.1
15	11	31	42	73.8
Sum	*294*	*596*	*890*	*66.9*

Source: Created by authors

Table 2. Total keyword loss of specificity

means, in these policies, the keywords are rarely used to pinpoint and guide actionable advice.

The analysis above provides an overview of the total keyword loss of specificity but it does not provide any details on how individual keywords have been used. To investigate the keyword loss of specificity for each keyword, we analyzed the number of times each keyword appeared in actionable advice and other information sentences. Tables 3 and 4

ISP	Aldrig (never)	Behöver (need)	Bör (should)	Ej (not)	Förbjuden (forbidden)	Inte (not)	Måste (must)	Ska (shall)	Skall (shall)
1	0	2	0	2	0	21	0	6	11
2	2	0	0	1	0	5	0	9	6
3	0	0	1	1	0	0	1	1	16
4	1	0	6	2	0	7	1	0	19
5	0	0	0	0	0	0	0	7	0
6	0	0	2	0	0	14	0	7	0
7	0	0	0	0	0	1	0	4	0
8	0	2	3	0	0	1	1	13	0
9	0	0	1	0	2	5	1	1	3
10	0	0	0	0	0	1	0	3	0
11	0	0	0	0	0	7	0	34	0
12	0	0	0	0	0	1	0	34	0
13	0	0	0	0	0	0	1	1	0
14	0	1	0	0	0	3	2	6	0
15	0	0	2	0	0	4	0	5	0
Sum	3	5	15	6	2	70	7	131	55
% of all AA	1.0%	1.7%	5.1%	2.0%	0.7%	23.8%	2.4%	44.6%	18.7%

Source: Created by authors

Table 3. Number of keywords for actionable advice

ISP	Aldrig (never)	Behöver (need)	Bör (should)	Ej (not)	Förbjuden (forbidden)	Inte (not)	Måste (must)	Ska (shall)	Skall (shall)
1	0	1	0	0	0	3	0	3	0
2	0	0	0	3	0	15	0	8	8
3	0	0	2	2	0	4	1	3	9
4	0	0	2	2	0	4	2	1	16
5	0	1	0	0	0	3	1	19	0
6	0	0	1	0	0	4	0	9	0
7	0	1	0	0	0	6	0	48	4
8	2	3	2	0	0	7	14	111	0
9	0	0	0	3	0	6	0	8	2
10	0	0	0	0	0	11	2	23	0
11	0	0	2	0	0	15	1	64	0
12	0	0	1	0	0	3	3	64	0
13	0	1	0	0	0	6	0	7	2
14	0	1	0	0	2	2	1	10	0
15	0	1	0	0	0	2	2	26	0
Sum	2	9	10	10	2	91	27	404	41
% of all OI	0.3%	1.5%	1.7%	1.7%	0.3%	15.3%	4.5%	67.8%	6.9%

Table 4.
Number of keywords for other information

Source: Created by authors

present the distribution of the keywords in actionable advice and other information sentences, respectively. Finally, Table 5 presents the keyword loss of specificity for each keyword.

Starting with the word frequencies and comparing Tables 3 and 4, it is evident that there is a degree of similarity in the patterns of keyword use. Notably, all analyzed keywords were used in both actionable advice and other information sentences. In addition, the keywords

ISP	Aldrig (never) (%)	Behöver (need) (%)	Bör (should) (%)	Ej (not) (%)	Förbjuden (forbidden) (%)	Inte (not) (%)	Måste (must) (%)	Ska (shall) (%)	Skall (shall)
1	–	33	–	–	–	12	–	33	0
2	0	–	–	25	–	25	–	47	57
3	–	–	67	67	–	100	50	75	36
4	0	–	25	50	–	46	67	100	46
5	–	100	–	–	–	100	100	73	–
6	–	–	33	–	–	22	–	56	–
7	–	100	–	–	–	86	–	92	100
8	100	60	40	–	–	87	93	90	–
9	–	–	0	100	0	55	0	89	40
10	–	–	–	–	–	92	100	88	–
11	–	–	0	–	–	68	100	65	–
12	–	–	100	–	–	75	100	65	–
13	–	100	–	–	–	100	0	88	100
14	–	50	–	–	100	40	33	62	–
15	–	100	0	–	–	33	100	84	–
Sum*	40	64	40	62	50	57	79	76	43

Table 5.
Keyword loss of specificity

Note: *Please note that the sum is calculated using the sums in Tables 3 and 4
Source: Created by authors

have been distributed with almost the same pattern in the two tables. Table 3 shows that out of the nine keywords analyzed, "inte" (not), "ska" (shall) and "skall" (shall) were used most frequently in actionable advice sentences. They were found in 23.8%, 44.6% and 18.7% of all these sentences and, in total, account for 87.1%. Furthermore, since "ska" (shall) and "skall" (shall) are synonyms, their frequencies can be combined, showing that they alone are found in 63.3% of the actionable advice sentences, while "måste" (must) is encountered only in 2.4% of these sentences. Among the rarely used keywords, we found "aldrig" (never) and "förbjuden" (forbidden) were used in only 1.0% and 0.7% of the actionable advice sentences.

Table 4 shows a similar pattern in other information sentences, with "inte" (not), "ska" (shall) and "skall" (shall) as the most frequently used keywords and "aldrig" (never) and "förbjuden" (forbidden) as the least frequently used. "Ska" (shall) and "skall" (shall) together appeared in 74.7% of other information sentences, and "inte" (not) appeared in 15.3% of these sentences. However, the keyword "måste" (must) appeared more frequently in other information sentences (4.5%) compared to actionable advice sentences (2.4%). An example of another information sentence including this keyword is: "All paper-based information of a sensitive nature must be handled carefully, even within the [name of the public agency's] premises." This sentence leaves room for ambiguity since multiple interpretations could be made regarding what constitutes "handling carefully."

Table 5 shows the calculated keyword loss of specificity for each keyword. The leftmost column presents the ISP identifier, and the remaining columns contain each keyword's loss of specificity. Not surprisingly, given the results in Table 1, all keywords show a significant loss of specificity, where "måste" (must) and "ska" (shall) are the most extreme ones. These two keywords have 79% and 76% loss of specificity, respectively. Thus, in terms of ISP design, it means these keywords rarely pinpoint actionable advice. In some ISPs, these keywords are used only to provide other information. For example, "måste" (must) is used entirely to provide other information in ISPs 5, 10, 11, 12 and 15. Still, returning to Table 4, we should acknowledge that, in some cases, the frequencies of these keywords are low, such as in ISP 15.

The keyword "ska" (shall) also has a high loss of specificity. Like the keyword "måste" (must), it is in most ISPs not used to provide guidance in Actionable advice. However, Table 4 reveals an interesting difference in frequency between these keywords. Several ISPs exhibit a notable frequency of the keyword "ska" (shall) in other information sentences, as seen in ISPs 7, 8, 11 and 12. The keyword was used 48, 111, 64 and 64 times, respectively. An example of another information sentence including this keyword is "all orders shall be approved by both the immediate manager and the IT manager before the assignment is carried out; however, the IT manager alone can approve the order within the framework of his powers." This sentence is ambiguous not only because the meaning of "framework of his powers" is unclear but also because it appears to be a general guideline for a strategic ISP.

5. Discussion

5.1 Implications for research practice

We make a methodological contribution to existing research on how to analyze ISPs. This contribution comes in two parts. First, we contribute with a new metric – keyword loss of specificity – to assess the quality of ISPs. This metric adds to the few existing quantitative metrics – policy length (Alshaikh *et al.*, 2015; Höne and Eloff, 2002), breath, brevity and clarity (Goel and Chengalur-Smith, 2010) – available to assess ISP quality. Our metric differs from these metrics because it focuses on how specific keywords are used compared to a particular purpose. In our case, we used it to assess the quality of how keywords were used to pinpoint and guide clear pieces of actionable advice. Thus, this metric could be used to assess how keywords are used for other purposes, such as highlighting consequences.

The keyword loss of specificity metric should not be viewed as a replacement for the other metrics. Instead, it should be viewed as a complement to help in the pursuit of designing high-quality ISPs. To see how these metrics complement each other, it is important to pinpoint their differences. The focus of the policy length metric differs from our metric. Policy length addresses the length of the entire ISP (Alshaikh *et al.*, 2015) and does not address individual sentences and the quality of actionable advice. Improving pieces of actionable advice that already exist in an ISP would probably have little impact on the overall length of the policy. Breath focuses on the comprehensiveness of the ISP and to what extent central concepts are covered (Goel and Chengalur-Smith, 2010). Thus, selected keywords may overlap with central concepts. However, while breath focuses on whether keywords/central concepts are used, keyword loss of specificity addresses how these keywords/central concepts are used in these sentences. Brevity measures the repetitiveness of words in ISPs (Goel and Chengalur-Smith, 2010). Our metric does not share this focus. Instead, keyword loss of specificity encourages repetitive use of certain keywords to make messages in actionable advice more coherent. Thus, one could expect that ISPs performing well concerning keyword loss of specificity, would perform worse when it comes to brevity on these keywords. However, such repetitiveness is not a sign of technical jargon. To some extent, keyword loss of specificity connotates with ease of understanding of ISP text, that is, clarity. However, Goel and Chengalur-Smith's (2010) operationalization of clarity focuses on approximating an entire ISP text's difficulty. Keyword loss of specificity addresses clarity in how keywords are used in relation to a specific purpose.

Second, we contribute with a set of steps on how to operationalize the keyword loss of specificity metric. We have given a detailed account in Section 3 of how we executed the analysis and shown in Section 4 how the data has been used. In addition, we have shown how to semi-automate the analysis using text analysis software. Of course, using text analysis software is not a requirement for assessing keyword loss of specificity in ISPs. Regardless of semi-automated or manual analyses, users of this metric should be aware that, depending on how many times a keyword is used in an ISP, the metric can be volatile; the lower the use frequency, the more volatile the results. Still, this is a problem shared with many other relative text analysis metrics.

We also make empirical contributions to existing research by using the keyword loss of specificity metric to assess ISPs from public agencies in Sweden; we provide details about ISPs covered to a limited extent in existing research. Although previous studies have revealed ambiguities in existing ISPs (e.g. Stahl *et al.*, 2012; Karlsson *et al.*, 2017), our empirical findings about the loss of keyword specificity and actionable advice were unexpected. The inclusion of operational ISPs led us to anticipate a greater proportion of actionable advice among the extracted sentences, that is, sentences where the keywords were used. However, our results indicate that, contrary to the prevailing emphasis in existing research on the importance of clear and understandable ISPs (e.g. Alshaikh *et al.*, 2015; Rostami *et al.*, 2020; Stahl *et al.*, 2012; Lopes and Oliveira, 2015), a majority of the ISPs assessed do not provide employees with unambiguous instructions on how to use and handle information assets securely. As shown in Table 2, in most of the analyzed sentences, keywords recommended to guide employees' actions were used to provide unclear instructions or more general information related to information security.

We provide a more detailed assessment of actionable advice than the discourse analyses in Stahl *et al.* (2012) and Karlsson *et al.* (2017). These details allowed us to address a specific type of ambiguity, showing to what extent pieces of actionable advice written by ISP designers align with the recommended use of keywords. We found a high frequency of "ska" (shall) and "skall" (shall) in sentences classified as other information. As shown in Table 4, together, they were found in 74.7% of sentences classified as other information, although the

loss of specificity is higher for "ska" (shall) compared to "skall" (shall). Thus, we found that, in a majority of the sentences, the use of "ska" (shall) and "skall" (shall) contradicts the recommendation made by Diver (2021). This is a concern because employees rely on these documents to comprehend instructions about their job duties but may become further confused. Consequently, our results indicate an incongruent use of keywords in ISPs to highlight actionable advice, which increases the ambiguity of ISPs. These results are at odds with the importance of writing ISPs using clear and easy-to-understand language (Alshaikh *et al.*, 2015; Rostami *et al.*, 2020; Stahl *et al.*, 2012; Whitman, 2008; Wood, 1995).

Still, upon a closer examination of the analyzed ISP sentences, it becomes apparent that the *actual* actionable advice, that is, sentences that contain clear instructions to the employees, aligns with the recommendation about avoiding negative statements (Diver, 2021). As shown in Table 3, the analysis of actionable advice revealed a scarcity of negative statements such as "aldrig" (never) and "förbjuden" (forbidden). At the same time, our analysis of actionable advice shows that "ska" (shall) and "skall" (shall) have been used mostly instead of the recommended "måste" (must). On the face of it, this use contradicts Diver's (2021) recommendation. It is true that, similar to the English language, "måste" (must) is a stronger request in Swedish than "ska" (shall) and "skall" (shall). However, Höne and Eloff (2002) have previously argued about the importance of the ISP being consistent with the "organization's overall communication style." Consequently, considering the culture and the tone used in Swedish organizations and the point that these keywords convey strong advice in the Swedish language, the use of these keywords is understandable.

Finally, our findings show that none of the analyzed ISPs include high frequencies of all or a large share of the keywords. This is a positive finding because incorporating a variety of keywords such as "ska" (shall), "bör" (should), "behöver" (need) and "måste" (must) in a single ISP can contribute to ambiguity and uncertainty.

5.2 Implications for information security policy design practice

In the same way as researchers can use the keyword loss of specificity metric to assess the quality of ISPs, practitioners can use this metric to assess the quality of their ISPs. Consequently, ISP designers can use this metric to improve the quality of ISPs in their organizations. They can measure how much loss of specificity they have regarding a set of keywords. Of course, this set of keywords does not necessarily have to correspond to the one used in this paper. Instead, it is important to make a situational selection and consider the tone of the national and business language used in the organization. Still, when a set of keywords has been chosen to communicate actionable advice, it can be used to measure this quality aspect of the ISP.

As discussed above, our empirical results showed a significant loss in the specificity of keywords in the analyzed ISPs. Based on our findings, we suggest that ISP designers should be mindful of their word choices, particularly when crafting actionable advice containing obligation-conveying words such as "must." To ensure the advice is actionable, ISP designers should ensure that employees can act upon it without any interpretation. Furthermore, using keywords in a congruent manner within the ISP is paramount. To maintain a low level of keyword loss of specificity in actionable advice, the following practices are it is advisable:

- Reserve specific keywords for actionable advice and refrain from using this terminology in other information;
- Document the reserved keywords and their purpose separately to keep a track record of how this set of keywords is supposed to be used. Such a track record will ease the burden of staying congruent in how keywords are used when multiple actors contribute to an ISP and when changes are made over time; and

- Avoid using different synonyms or similar words when the level of obligation remains the same. In other words, if multiple sentences convey the same level of obligation, it is preferable to use the same keyword in all of them to avoid ambiguity and confusion.

5.3 Limitations and future research

As with any research, our study has limitations that should be considered in future research. The first limitation concerns the set of keywords that we have used as a starting point for the analysis. There appears to be no universal agreement on a set of keywords to use when writing actionable advice in ISPs. The set of keywords we have used is an operationalization of Diver (2021), but we do claim that our operationalization is the only possible one or that this set of keywords is comprehensive. For example, our results exclude sentences containing phrases such as "be careful" and "keep in mind." Including such phrases could provide a more comprehensive understanding of how actionable advice is constructed. Still, the scarcity of guidelines about using keywords points to a research gap. More research is needed to identify a set or sets of keywords for pinpointing and guiding actionable advice and to learn more about how employees view these keywords.

Second, our analysis is limited to Swedish-language ISPs and the Swedish organizational context. As discussed above, it is vital to acknowledge the importance of the tone used in different languages and national cultures. Thus, the results may vary when applied to ISPs written in other languages and countries. Therefore, we urge researchers in other countries to execute similar studies to learn more about using keywords in ISPs in different contexts.

Third, our operationalization of actionable advice as corresponding to one sentence is a limitation. Existing research does not provide any clear guidance on how to demarcate a piece of actionable advice in an ISP. Consequently, a piece of actionable advice could also be operationalized as a set of sentences that provide instruction to employees. Probably, such an operationalization calls for more advanced text analysis, for example, addressing the relationship between sentences. It could be the case that one sentence containing vague, actionable advice is clarified by a subsequent sentence. Future research should, therefore, investigate how actionable advice and other information sentences are positioned in relation to each other.

Fourth, we have not studied if, and in that case, how, the keyword loss of specificity metric contributes to improving ISPs in organizational settings. Consequently, future research should address the use of the metric in actual ISP design work. For example, such studies could study how information security managers use the metrics to improve the design of existing ISPs.

6. Conclusion

This study set out to investigate how congruent keywords are used in ISPs to pinpoint and guide clear actionable advice and suggest a metric for measuring the quality of keyword use in ISPs. To this end, we developed a text analysis metric, keyword loss of specificity, that captures the relative frequency when a keyword is not used in line with a specific purpose, in our case reducing the possibility of pinpointing and guiding a piece of actionable advice. We found a significant loss of keyword specificity in the 15 ISPs from public agencies in Sweden that we analyzed. It means that keywords recommended to be used when writing actionable advice are used for other purposes in these ISPs. As a result, such dual use of keywords reduces the possibility of pinpointing and communicating clear, actionable advice. Based on our empirical findings, we provide three pieces of advice to ISP designers

on how to work with keywords to maintain a low level of keyword loss of specificity and increase clarity when writing actionable advice in ISPs.

References

Alshaikh, M., Maynard, S.B., Ahmad, A. and Chang, S. (2015), "Information security policy: a management practice perspective", *Australasian Conference on Information Systems*.

Assarroudi, A., Heshmati Nabavi, F., Armat, M.R., Ebadi, A. and Vaismoradi, M. (2018), "Directed qualitative content analysis: the description and elaboration of its underpinning methods and data analysis process", *Journal of Research in Nursing*, Vol. 23 No. 1, pp. 42-55.

Baskerville, R. and Siponen, M. (2002), "An information security meta-policy for emergent organizations", *Logistics Information Management*, Vol. 15 Nos 5/6, pp. 337-346.

Chatterjee, S., Gao, X., Sarkar, S. and Uzmanoglu, C. (2019), "Reacting to the scope of a data breach: the differential role of fear and anger", *Journal of Business Research*, Vol. 101, pp. 183-193.

Chowdhury, N.H., Adam, M.T. and Skinner, G. (2019), "The impact of time pressure on cybersecurity behaviour: a systematic literature review", *Behaviour and Information Technology*, Vol. 38 No. 12, pp. 1290-1308.

Cram, W.A., Proudfoot, J.G. and D'arcy, J. (2017), "Organizational information security policies: a review and research framework", *European Journal of Information Systems*, Vol. 26 No. 6, pp. 605-641.

Culnan, M.J. and Williams, C.C. (2009), "How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches", *MIS Quarterly*, Vol. 33 No. 4, pp. 673-687.

Demsar, J., Curk, T., Erjavec, A., Gorup, C.R., Hocevar, T., Milutinovič, M., Možina, M., Polajnar, M., Toplak, M., Starič, A., Stajdohar, M., Umek, L., Agar, L.Z., Bontar, J.Z., Itnik, M.Z. and Zupan, B. (2013), "Orange: data mining toolbox in python", *Journal of Machine Learning Research*, Vol. 14.

Diver, S. (2021), *Information Security Policy – A Development Guide for Large and Small Companies*, *SANS Institute*, Rockville Pike.

Doherty, N. and Fulford, H. (2006), "Aligning the information security policy with the strategic information systems plan", *Computers and Security*, Vol. 25 No. 1, pp. 55-63.

Goel, S. and Chengalur-Smith, I.N. (2010), "Metrics for characterizing the form of security policies", *The Journal of Strategic Information Systems*, Vol. 19 No. 4, pp. 281-295.

Höne, K. and Eloff, J.H.P. (2002), "What makes an effective information security policy?", *Network Security*, Vol. 2002 No. 6, pp. 14-16.

Hong, K.-S., Chi, Y.-P., Chao, L.R. and Tang, J.-H. (2006), "An empirical study of information security policy on information security elevation in Taiwan", *Information Management and Computer Security*, Vol. 14 No. 2, pp. 104-115.

Hsieh, H.-F. and Shannon, S.E. (2005), "Three approaches to qualitative content analysis", *Qualitative Health Research*, Vol. 15 No. 9, pp. 1277-1288.

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

Karlsson, F., Hedström, K. and Goldkuhl, G. (2017), "Practice-based discourse analysis of information security policies", *Computers and Security*, Vol. 67, pp. 267-279.

Kör, B. and Metin, B. (2021), "Understanding human aspects for an effective information security management implementation", *International Journal of Applied Decision Sciences*, Vol. 14 No. 2, pp. 105-122.

Landoll, D.J. (2017), *Information Security Policies, Procedures, and Standards – A Practitioner's Reference*, Taylor and Francis, Boca Raton.

Loch, K.D., Carr, H.H. and Warkentin, M.E. (1992), "Threats to information systems: today's reality, yesterday's understanding", *MIS Quarterly*, Vol. 16 No. 2, pp. 173-186.

Lopes, I. and Oliveira, P. (2015), "Applying action research in the formulation of information security policies", in Rocha, A., Correia, A.M., Costanzo, S. and Reis, L.P. (Eds), *New Contributions in Information Systems and Technologies*, Springer, Cham, pp. 513-522.

Nist (2006), *Information Security Handbook: A Guide for Managers*, National Institute of Standards and Technology, Gaithersburg.

Peltier, T.R. (2004), *Information Security Policies and Procedures – a Practitioner's Reference*, Auerbach Publications, Boca Raton.

Ponemon Institute Llc (2020), "Cost of insider threats: global report", available at: www.ibm.com/downloads/cas/LQZ4RONE

Pwc (2014), *The Information Security Breaches Survey – Technical Report*, Department for Business, Innovation and Skills (BIS), London.

Pwc (2018), *The Global State of Information Security Survey 2018*, PriceWaterhouseCoopers, London.

Rostami, E. (2023), *Tailoring Information Security Policies–a Computerized Tool and a Design Theory*, Örebro universitet, Örebro.

Rostami, E. and Karlsson, F. (2023), "A qualitative content analysis of actionable advice in Swedish public agencies' information security policies", in Furnell, S. and Clarke, N. (Eds), Human Aspects of Information Security and Assurance – 17th IFIP WG 11.12 International Symposium, HAISA 2023, Kent, July 4–6, Proceedings. Springer, *Cham*, pp 157-168.

Rostami, E., Karlsson, F. and Gao, S. (2020), "Requirements for computerized tools to design information security policies", *Computers and Security*, Vol. 99, p. 102063.

Rostami, E., Karlsson, F. and Gao, S. (2023), "Policy components – a conceptual model for modularizing and tailoring of information security policies", *Information and Computer Security*, Vol. 31 No. 3,

Sfs (2009), "2009:400 Offentlighets – och sekretesslag. Justitiedepartementet, Stockholm".

Siponen, M. and Vance, A. (2010), "Neutralization: new insights into the problem of employee information systems security policy violations", *MIS Quarterly*, Vol. 34 No. 3, pp. 487-502.

Smith, C.R. (2010), *The Definitive Guide to Writing Effective Information Security Policies and Procedures*, Createspace, CA.

Stahl, B.C., Doherty, N.F. and Shaw, M. (2012), "Information security policies in the UK healthcare sector: a critical evaluation", *Information Systems Journal*, Vol. 22 No. 1, pp. 77-94.

Strauss, A.L. and Corbin, J.M. (1998), *Basics of Qualitative Research: techniques and Procedures for Developing Grounded Theory*, SAGE, Thousand Oaks, CA.

Sundt, C. (2006), "Information security and the law", *Information Security Technical Report*, Vol. 11 No. 1, pp. 2-9.

Truesec (2023), *Threat Intelligence Report 2023*, Truesec, Stockholm.

Whitman, M.E. (2004), "In defense of the realm: understanding threats to information security", *International Journal of Information Management*, Vol. 24 No. 1, pp. 43-57.

Whitman, M.E. (2008), "Security policy – from design to maintenance ", in Straub, D.W., Goodman, S. and Baskerville, R. (Eds) *Information Security – Policy, Processes, and Practices*, M E Sharpe, New York, NY, pp. 123-151.

Wood, C.C. (1995), "Writing InfoSec policies", *Computers and Security*, Vol. 14 No. 8, pp. 667-674.

Corresponding author
Fredrik Karlsson can be contacted at: fredrik.karlsson@oru.se