TU Delft

Delft University of Technology

# Sources of security risk information

## What do professionals rely on for their risk assessment?

de Wit, Johan; Pieters, Wolter; van Gelder, Pieter

**DOI**
10.1080/01972243.2025.2475311

**Publication date**
2025

**Document Version**
Final published version

**Published in**
Information Society

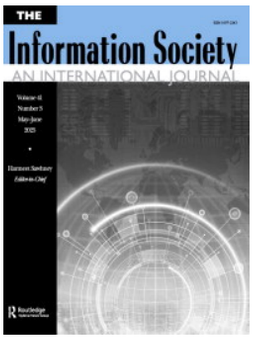
**Citation (APA)**
de Wit, J., Pieters, W., & van Gelder, P. (2025). Sources of security risk information: What do professionals rely on for their risk assessment? *Information Society*, *41*(3), 157-172. https://doi.org/10.1080/01972243.2025.2475311

**Important note**
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

**Copyright**
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

**Takedown policy**
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

*This work is downloaded from Delft University of Technology.*
*For technical reasons the number of authors shown on this cover page is limited to a maximum of 10.*



The Information Society
An International Journal

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/utis20

# Sources of security risk information: What do professionals rely on for their risk assessment?

Johan de Wit, Wolter Pieters & Pieter van Gelder

**To cite this article:** Johan de Wit, Wolter Pieters & Pieter van Gelder (2025) Sources of security risk information: What do professionals rely on for their risk assessment?, The Information Society, 41:3, 157-172, DOI: 10.1080/01972243.2025.2475311

**To link to this article:** https://doi.org/10.1080/01972243.2025.2475311

© 2025 The Author(s). Published with license by Taylor & Francis Group, LLC

Published online: 11 Apr 2025.

Submit your article to this journal

Article views: 157

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=utis20

THE INFORMATION SOCIETY
2025, VOL. 41, NO. 3, 157–172
https://doi.org/10.1080/01972243.2025.2475311

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

# Sources of security risk information: What do professionals rely on for their risk assessment?

Johan de Wit[a], Wolter Pieters[b] and Pieter van Gelder[a]

[a]Faculty of Technology, Policy, and Management, Delft Technical University, Delft, The Netherlands; [b]Behavioural Science Institute, Radboud University, Nijmegen, The Netherlands

**ABSTRACT**

Security risks, such as sabotage and cyberattacks, are an increasing threat to business and government processes. They originate from malicious human action, of which often exact historical information is lacking. Thus, the judgment and assessment of security professionals is the primary input for security risk management, a subjective probabilistic approach. In this study, we explore the information sources professionals, in both the physical and cybersecurity domain, use for this purpose, improving understanding of their daily praxis. Sources of security risk information are collected, their quality and trustworthiness is assessed, and their use is analyzed. Quality is assessed by experienced security practitioners applying the NATO system for intelligence evaluation, with source intention as additional criterion. Actual use is analyzed among security professionals. The results consist of a comparative ranking of both assessed quality and daily use of sources. Experts are ranked first for perceived quality and are also most relied upon in daily praxis, and individual/personal experience comes second. The additional criterion of source intention explained the lower level of use of information from science. This study provides the basis for enhancing security risk management by a more conscious selection of sources.

**ARTICLE HISTORY**
Received 8 May 2023
Accepted 28 February 2025

**KEYWORDS**
Information sources; NATO system; risk information; security assessment; trust

**JEL**
D810

## Introduction

Stating that predicting the future is impossible by definition is stating the obvious (Kahneman, Sibony, and Sunstein 2021). However, globally thousands of risk professionals do this on a daily basis. They manage risks, which are defined as "the effect of uncertainty on objectives" (ISO 2018). Forecasting potential future effects and predicting uncertainties, in other words predicting the risk future is part of their risk management processes and is usually labeled risk assessment (see Figure 1).

Security in society and organizations is heavily depending on this assessment, or in other words judgment, of these security professionals. It is, therefore, of the utmost importance to understand how these professionals form their opinion and judgment. Their predictive judgment is based on information available to them. Security breakdown in this work is considered to be initiated by malicious intent, a definition grounded in the physical security domain, but applicable to both physical and cyber security. Previous work of the authors found that security professionals felt that they had detailed information on security risk, on average, in half of their security risk assessments. They also felt that they almost always can assess and decide upon a security risk, even if they have no detailed information (de Wit, Pieters, and van Gelder 2024). These findings sparked follow-up research questions about the sources of this information.

This study is explorative and descriptive, driven by the curiosity to add to a deeper understanding of human security risk assessments. The research questions answered in this study are:

- What sources of security risk information are considered by practitioners?
- How reliable are these sources as perceived by these practitioners?

**CONTACT** Johan de Wit johan.de.wit@siemens.com Faculty of Technology, Policy and Management, Building 31, Jaffalaan 5, 2628 BX Delft, The Netherlands.

© 2025 The Author(s). Published with license by Taylor & Francis Group, LLC
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

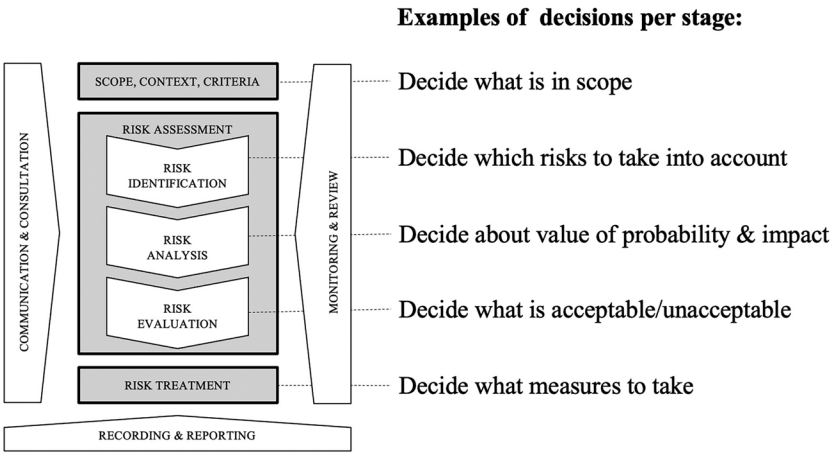



**Figure 1.** Risk management process according to ISO 31000 (NEN-ISO 2018) with examples of decisions per stage.

- Which sources are used in security risk assessment praxis?
- Are the most used sources also perceived as the most credible ones?
- Can we observe differences between security professionals based on their expertise (experience and knowledge)?

This study focusses on possible sources of security risk information, their perceived quality, and their level of use in security risk assessment by security practitioners, with both physical and cyber security backgrounds. First the possible sources of security risk information are collected in an expert consultation. This resulted in a list of 17 possible sources of security risk information. Second, the reliability, credibility and intention of these possible sources is assessed by a practitioners panel. This resulted in a source quality ranking which is considered a quality reference. Finally, by means of an online survey, a large group of security professionals is consulted on the use of these sources in their daily praxis. The individual expertise of the professionals is collected in the survey to explore if this influences their use of information sources. Previous work of the authors showed that more experienced security professionals value information to a lesser extent in their security risk assessment than less experienced practitioners (de Wit, Pieters, and van Gelder 2024).

So far, to the best of our knowledge, no comparable research has been done in the security domain.

The next section will briefly detail the background of judgment, expertise, information sources, and their quality. The research and analysis methods are explained in the method section followed by a section presenting the results. The article ends with a discussion and conclusions section.

## Background

Risks might seem hard to assess but over time a substantial body of knowledge has been gathered on risks. Historical data makes it possible to form evidence-based predictions under the precondition of similar context and circumstances. Security risks, the topic of this article, deal with malicious human acts and actors (Möller 2012; Husak et al. 2019; Krisper, Dobaj, and Macher 2020). With these acts in various ways trying to be unpredictable, be concealed, and evade existing risk controls, we have a large variety and constantly evolving number of modus operandi (Talbot and Jakeman 2011; Deb, Lerman, and Ferrara 2018). In combination with an almost unlimited variety of situations and context, in both location and time, security risks are hard to predict on solid data (Stanovich and West 2000; Oppelaar and Wittebrood 2006; de Meij 2010). Often there is limited historical data on specific security risks and/or a different context might not be conducive for the use of this data. In the domain under study, therefore, expert judgment is the predominant basis for security risk assessments (Talbot and Jakeman 2011; Möller 2012; Powell et al. 2019; Krisper, Dobaj, and Macher 2020).

To manage risks in a structured manner, over time risk management processes have been developed (Bojanc and Jerman-Blažič 2008). Various domains dealing with risks developed specific processes, which, however, all have similar sequence of steps. The assessment of risks is a part of these processes and consists of three consecutive steps: risk identification, risk analysis, and risk evaluation (Alhawari et al. 2012; ISO 2018; ISO/IEC 2020, 2022).

The risk professionals dealing with this task need to inform themselves about possible current and future threats, and analyze and evaluate these (Mandel

and Irwin 2021). The latter steps are usually performed on the, broadly accepted, two main components of risks: likelihood (expressing uncertainty) and impact (expressing effect). However theoretically impossible, as stated in the first line of the introduction, they do their best to be prepared for possible, unpredictable, future events.

In this sense risk management seems to be closely related to forecasting. Forecasting is defined as: intelligence work or guessing about the future (Tetlock and Gardner 2016). The term forecasting might give the impression of quantitative or scientific methods and processes, like weather forecasting, however, good predictions are based on how you think and not on what your know (Tetlock and Gardner 2016). In other words: good forecasting is tied to the quality of available information and, more importantly, how this information is processed.

How individuals process information to reach a judgment has been extensively studied over time in the domain of expert judgment (Einhorn 1974; Cooke 1991; Meyer and Booker 2001; Skjong and Wentworth 2001; Cooke and Goossens 2008; Ryan et al. 2012). These studies primarily focus on (determining) the expertise of experts and the accuracy of their judgments. Expert judgment is considered to be a degree of expert's belief, based on tacit knowledge and expertise (Fischbein and Ajzen 1975; Cooke 1991; Ajzen 2011). This tacit knowledge should be an important element of knowledge management, as it could create a competitive advantage for organizations (Johannessen, Olaisen, and Olsen 2001). The related field of Naturalistic Decision Making (NDM) focusses primarily on expertise of practitioners. NDM studies the, often not conscious, process of assessment and decision making by practitioners (Klein 1993, 1997, 2008; Lipshitz and Strauss 1997; Lipshitz et al. 2001; Pliske and Klein 2003; Hoffman and Klein 2017; Gore and Ward 2018; Markman 2018; Roberts and Cole 2018). In NDM perspective, practitioners form their assessment based on recognition of cues. These cues trigger recollection of both memories and knowledge of the individual practitioner. These in turn allow the practitioner to perform a mental simulation and assess/compare the real-life situation with the simulation. Information is considered to generate so called message cues (Trumbo and McComas 2003). In other words, information is one of the possible cues triggering the process of NDM in an agent. This field of study, predominantly empirical and exploratory, focuses on real-life praxis. It turned out to be very much in line with the renowned, more theoretical, laboratory research in the field of heuristics and biases, much to the surprise of its two "godfathers": Gary Klein and Daniel Kahneman (Kahneman and Klein 2009). For example: the recognition of cues (the cornerstone of NDM) seems to be closely related to the availability heuristic (the most prevalent heuristic in the domain of heuristics and biases).

A large body of research demonstrated that judgements in general are based on the information that is most accessible to the agent at the time of the judgment (e.g. Citroen 2011). Information in the present article is taken to be "knowledge obtained from investigation, study or instruction," as defined by Merriam–Webster[1]. In real life, agents rarely try to retrieve all the available information, but process (just) enough information that comes to mind to form a judgment with subjective certainty (Schwarz and Vaughn 2002). In our current society information is available in abundance, agents need to both consider information that is available to them, and select information that is of use in the given context (Weber 1987). Information selection is often based on the perceived reliability of the source of information (Hertzum et al. 2002; Viljanen 2005). Other scholars have identified the strong relation between knowledge/information management and risk management (Alhawari et al. 2012). This study focusses on characteristics of security risk information and especially its origin: the sources of information.

The quality of information is considered to be depending on two components: the quality of the content, and the quality of the source. Sources can be classified based on characteristics such as: content, origin/reputation, and recognition (Dongo, Cardinale, and Aguilera 2019), or more granular ones such as: accurate, trustworthy, accessible, ease of use, free, active/updated, comprehensive, and familiar (Kim and Sin 2011). These characteristics can be grouped in two overarching categories: the source quality and source accessibility (O'Reilly III 1982). In their study Kim and Sin found that the former is considered more important by their participants, but, their behavior showed otherwise (Kim and Sin 2011) as O'Reilly and Hertzum also concluded earlier (O'Reilly III 1982; Hertzum et al. 2002).

Analyzing and classifying information and information sources is of vital importance in the security domain (Gal-Or and Ghose 2005; Johnson 2010; Powell et al. 2019). Especially in the security intelligence community, where specialized tools and methods are developed and applied to classify information and information sources (Korkisch 2010; Seagle 2015; Powell et al. 2019). In this domain the quality of information is also predominantly evaluated based on

both the reliability of the content and the source, applying the international and broadly accepted evaluation criteria known as the Admiralty Code or NATO system (see Table 1). The NATO system classifies the reliability of sources based on: authenticity, trustworthiness and competency. The reliability assessment of sources results in a classification on a reliability scale as presented in Table 1. In using the NATO system, the authenticity, trustworthiness and competency of individual sources, is evaluated against past experience with these sources. Note that the first five categories of the scale are ordinal and the sixth represents the inability to categorize the information.

The NATO system is not free of debate. Overtime several scholars have presented shortcomings and recommendations to improve this NATO system. Applying this system and assessing information and information sources remains largely a human, and thus subjective, task with all its limitations and possible flaws (Capet and Delavallade 2014; Icard 2019, 2023). The system evaluates the information and the source of information separately. However, a source might be considered reliable for information in a certain context but might not be in another situation (as will also be discussed later in this section). With the separation the assessment of the information and the source of this information, this contextual relationship might be disregarded (Capet and Delavallade 2014)

**Table 1.** Outline of the Admiralty Code or NATO system (Powell et al. 2019).

| Source Reliability | Description |
|---|---|
| A – Completely reliable | No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability |
| B – Usually reliable | Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time |
| C – Fairly reliable | Doubt of authenticity, trustworthiness, or competency but has provided valid information in the past |
| D – Not usually reliable | Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past |
| E – Unreliable | Lacking in authenticity, trustworthiness, and competency; history of invalid information |
| F – Reliability cannot be judged | No basis exists for evaluating the reliability of the source |
| **Information Credibility** | **Description** |
| 1 – Completely credible | Logical, consistent with other relevant information, confirmed by independent sources |
| 2 – Probably true | Logical, consistent with other relevant information, not confirmed |
| 3 – Possibly true | Reasonably logical, agrees with some relevant information, not confirmed |
| 4 – Doubtful | Not logical but possible, no other information on the subject, not confirmed |
| 5 – Improbable | Not logical, contradicted by other relevant information |
| 6 – Truth cannot be judged | The validity of the information cannot be determined |

The scale used in the NATO system is also subject of debate. The current scale is considered evaluative and does not allow for a more objective, descriptive perspective on information (Icard 2023). An assessor should be allowed to clearly segregate facts from interpretations. Icard (2023) proposed a 3 × 3 matrix where information is classified as: true, indeterminate or false. The source can be classified as honest, imprecise or dishonest. Other studies conclude that assessors tend to group the NATO system's scale of six classifications in three groups, positive: upper three classifications, negative: bottom two and neutral: the one between (Mandel et al. 2023).

As the "original" NATO system is well known and accepted in the security community it is applied in this study. However, in this article a novel addition is proposed based on theories on trust. The characteristics of the NATO system on source reliability all relate to the notion of trustworthiness. Trust is the attitude that one takes to the trustworthiness of a source (Viljanen 2005). "Trust is of central importance because quality is a perceived property and, thus, assessing the quality of an information source is essentially a matter of establishing to what extent one is willing to place trust in it" (Hertzum 2002, 1).

The trustworthiness of a source, whether a source is worthy of confidence, is context dependent (Viljanen 2005; O'Hara 2012; Bennett 2020). A source might be very competent, and thus trusted, in one domain, but might be incompetent in others. Whether a source is worthy of acceptance and original and can therefore be considered real or genuine or in other words authentic (Van Leeuwen 2001; Lehman et al. 2019), depends on reputation, recognition or credentials attributed to the source. These are characteristics for assured reliance, or trust, in a source.

Trust is usually not solely based on facts and evidence. McAllister defines two types of trust: cognitive trust, based on evidence and knowledge (trusting with the head), and affective trust, based on emotional ties with others (trusting with the heart) (McAllister 1995). The latter relates to familiarity with the source (Denize and Young 2007). Source familiarity allows for easier and more precise determinable trustworthiness (Hertzum 2002). Non-familiar sources of information are treated with more caution (Hertzum et al. 2002). The NATO system does not explicitly refer to these phenomena. They will, however, be of value to explain the perceived source reliability in the discussion and conclusions section.

In available literature about trust another property of trust is deemed important. Besides the perceived competence of the source the perceived intent or agency of the source is essential for the trustworthiness of the source (Hawley 2012; O'Hara 2012). Sources of information may have diverging goals, intentions and incentives that can alter their trustworthiness. Even though sources might be considered competent, their information might be comprehensive, consistent, accurate and up to date, they still may be suspected of following an agenda that is not in line with the receiver of information (Hawley 2012). In this article source intention is interpreted as the sources apparent (or hidden) aspirations, goals, objectives or incentives. These might deviate from the assessors intentions.

While the competence of a source is often stable over time or might show gradual changes, intentions of sources, on the other hand, can be very volatile and might even change overnight (for example due to bribery, extorsion or other external pressure). Specifically, evaluating source intention as part of classification of information can be considered of vital importance. In the original NATO code source intention might be considered a component of source reliability and assessed together with competence. Due to the specific importance of intent in the literature on trust and trustworthiness and the volatile character of source intention, a separate assessment of source intention is proposed. To enhance the quality of the NATO system, to classify information and information sources, a novel, additional, classification scale for source intention is proposed. This novel scale (see Table 2) is set up, tested, and evaluated in this study by a practitioners panel.

Other scholars identified this characteristic in perceived diverging goals and intentions in risk communication by industry and governmental risk communicators. Although these sources are considered competent their information is considered less trustworthy because of a potential divergent agenda. Industry is perceived to follow commercial incentives and governments try to accomplish policy goals. Due to these possibly expected diverging intentions, these sources are typically considered less trustworthy (Fessenden-Raden, Fitchen, and Heath 1987; McCallum, Hammond, and Covello 1991; Slovic, Flynn, and Layman 1991; Trumbo and McComas 2003).

The third novel classification criterion is added to the two existing quality criteria of the NATO system (see Figure 2). This study primarily focusses on these quality criteria as perceived by security practitioners.

The assessment of security risks is predominantly based on expert judgment. This judgment in turn is based on security risk information available to the agent at the time of the assessment. The quality of this information is, obviously, influencing the security risk assessment. This study seeks to evaluate this quality by focusing on the (perceived) quality of the source of information. To be able to assess the quality of information, the NATO system offers a solid and well accepted base. As the intention of the source of information is not explicitly assessed in the NATO system, for the study as presented in this article, the

**Table 2.** Proposed addition to the NATO code for classification of source intention.

| Source intention | Description |
|---|---|
| I – Completely shared intentions | No doubt of source intention or aspiration, goals and objectives are in line; has a history of shared intentions |
| II – Usually shared intentions | Minor doubt about source intention or aspiration, goals and objectives are in line; has a history of shared intentions most of the time |
| III – Fairly shared intentions | Doubt of source intention or aspiration, goals and objectives might be in line; had shared intentions in the past |
| IV – Not usually shared intentions | Significant doubt about source intention or aspiration, goals and objectives might not be in line; had shared intentions in the past |
| V – No shared intentions | Lacking in transparency of source intention; goals and objectives might not be in line; had different intentions in the past |
| VI – Intention cannot be judged | No basis exists for evaluating the intention of the source |

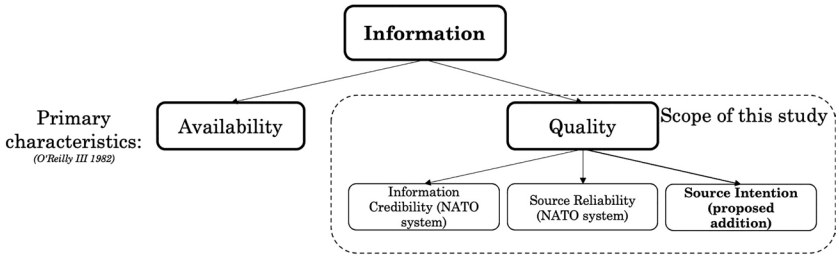



**Figure 2.** Characteristics of information and information sources.

additional classification scale, and assessment of, source intention is added to the study.

## Method

To explore the perceived trustworthiness and use of various information sources of security risk information, practitioners from both the physical and cyber-security domain were consulted. Different groups of practitioners participated in:

1. a small brainstorm session to identify the most prominent possible sources of information,
2. a panel consultation to rank the source quality,
3. a large-scale survey amongst security professionals to explore the use of these sources of information.

The quality ranking of the panel consultation will be compared to the real-life use of information sources.

First a list of possible sources of risk information is composed during a brainstorm session with the senior members ($n = 8$) of a security council in 2020. This predefined list of possible sources of security risk information consists of 17 predefined sources:

- Peers (people in your network with the same role),
- Experts (knowledgeable people recognized in the field),
- Expert communities,
- Higher management,
- Colleagues,
- Internal intelligence,
- External intelligence (government),
- External intelligence (commercial),
- Public sources like media,
- Social media sources,
- Government or government agencies,
- Consultants/consulting organizations,
- Science/scientific publications,
- Supplier organizations,
- Personal experience,
- Personal training/education,
- My "gut feeling".

This is considered a comprehensive list, but, in the next phase of this study the practitioners panel is offered the opportunity to add possibly missing sources. In the results section these possible additional sources are presented and discussed. This comprehensive list is used as primary input for the panel consultation resulting in a quality ranking of information and the survey to explore the real-life use of security risk information sources.

For the ranking of the quality of these preidentified sources a practitioners panel is formed by bringing together experienced respondents who indicated in response to a previous survey that they were willing to participate in follow-up research. This panel consisted of 18 experienced security practitioners from both the physical and security domain: on average 28 years of security experience, 83% followed specific security trainings, education level: associate's degree 11%, bachelor's degree 22%, master's/PhD degree 67%. Table 3 shows the professional position of the panelists.

In an online consultation the members of this practitioners panel are invited to rate the source reliability, information credibility, and source intention of each of the predefined sources (see Tables 1 and 2). The analysis of this consultation results in a quality ranking of the security risk information sources which is considered a quality reference. These results were compiled in July 2022.

In order to rank the perceived source quality based on these three criteria, a method for studying multiple-criteria decision making (MCDM) is selected. In this study the Technique for Order Performance by Similarity to Ideal Solution (TOPSIS) analysis is applied (a variation of the Analytical Hierarchy Process technique, AHP). The purpose of AHP is to capture the experts knowledge. AHP uses exact values to express a decision maker's opinion in a comparison of alternatives (Hota, Sharma, and Pavani 2014). TOPSIS is one of the most classical, compensatory, MCDM methods originally developed by Wang and Lee (Wang and Lee 2007). The concept here is to find the alternatives with the closest distance to the positive ideal solution ($d_i^*$) and the farthest distance to the negative ideal solution ($d_i^-$). Ranking takes place on the closeness coefficient ($CC_i = d_i^*/(d_i^- + d_i^*)$).

**Table 3.** Professional environment of the practitioners panel.

| My working environment is best described as: | *N* |
|---|---|
| Government/government agency: responsible security role | 3 |
| Government/government agency: advisory security role | 1 |
| Private organization: responsible security role | 3 |
| Private organization: advisory security role | 6 |
| Private organization: security supplier | 2 |
| Research/education | 2 |
| Other: "a variety of the above" | 1 |

As the assessment of security risk information entails various imprecise and non-numerical criteria, fuzzy logic is added to the TOPSIS method. Fuzzy Technique for Order Preference by Similarity to Ideal Solution (FTOPSIS) is a MCDM method specifically developed for ordering based on non-numerical criteria that can be fuzzified using fuzzy logic (Sevkli et al. 2010; Nădăban, Dzitac, and Dzitac 2016; Salih et al. 2019). "Fuzzy logic can deal with information arising from computational perception and cognition, that is, uncertain, imprecise, vague, partially true, or without sharp boundaries. Fuzzy logic allows for the inclusion of vague human assessments in computing problems" (Singh et al. 2013, 1). The subsequent steps of this method are presented in Figure 3.

The decision problem to be solved with Fuzzy TOPSIS is defined as follows: which possible source of security risk information is considered most trustworthy based on the criteria: source reliability, information credibility, and source intention?

The overall perceived quality ranking resulting from the FTOPSIS method will be used, as a quality reference, to compare the results of the main survey presented in this study on the use of sources in daily praxis.

In the third part of this study the third research question is addressed: Which sources are used in security risk assessment praxis? The exploratory results of the main survey are retrieved online between September 2020 and February 2021. Participation in the survey is promoted in both the IT and physical security professional community. It is promoted *via* LinkedIn and Twitter, both in general and in special interest groups like Security Management, ASIS Europe and ASIS International, as well as on Dutch cybersecurity platform. Second, a direct email campaign is launched targeting the existing professional network of the researchers. Third, the survey is promoted *via* the Information Security Forum world conference: Digital 2020 (cybersecurity domain) and ASIS Europe 2021 conference (physical security domain). The sample of respondents ($n = 174$) is regarded a convenience sample. About one third of the respondents have a general risk/management background, two thirds followed specific security trainings/education of which physical vs IT/cybersecurity is evenly divided.

This survey is set up with Qualtrics survey software. The survey consists of a question to explore the use of possible sources of risk information. The respondents are asked, for each individual source, to indicate the level of use in their security risk assessments by rating the importance *via* a three-point Likert scale is offered: very important, moderately important, and not important.

To check whether the presented list is comprehensive the respondents are offered the opportunity to add additional information sources *via* an open box

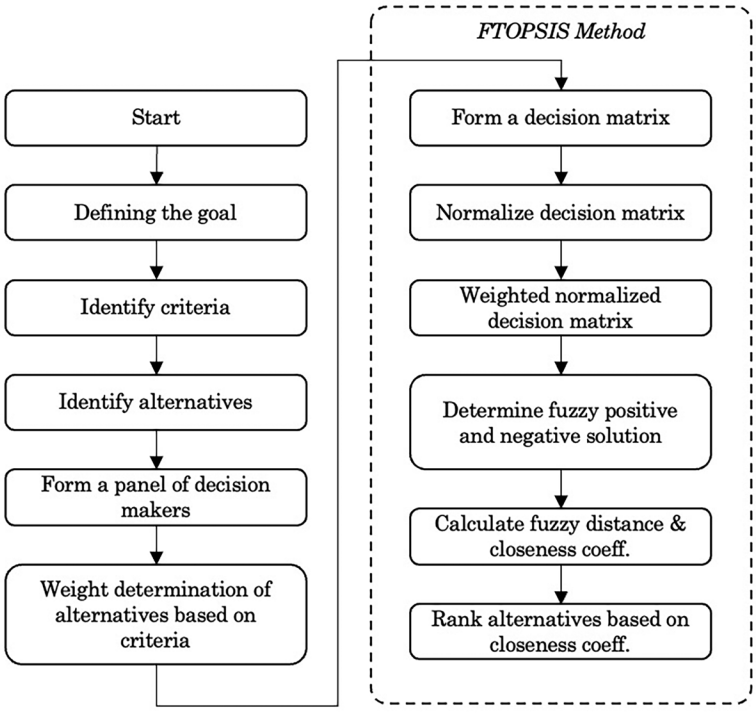



**Figure 3.** Steps of the Fuzzy TOPSIS method (Hota, Sharma, and Pavani 2014; Sevkli et al. 2010).

answer possibility. This question offers the respondents to add any possible missing source of security risk information. Based on the responses to this question the comprehensiveness and, thus, validity of the predefined list of information sources can be determined.

The predefined list is offered randomized to the respondents to avoid order bias (primacy, regency, contrast, and assimilation effects).

In the main survey the respondents are asked to express their expertise in a number of questions about individual characteristics. They are asked to indicate their age, number of years professional experience and number of years security experience. The current function of the respondents is asked including the number of years in this position. Finally they are asked to indicate their general education level (associate's degree, bachelor's degree or master's degree/PhD) and if any specific security trainings are completed. The possible influence of these characteristics on the use of information sources is explored.

Finally, the quality ranking of the information sources by the panel consultation is compared to the ranking of the use of sources resulting from the large-scale survey amongst security professionals.

## Results

First the results of the perceived source quality ranking by the practitioners panel consultation are presented. This panel of security practitioners ($n = 18$) analyzed the predefined list of information sources by assessing each source using the two criteria of the NATO system (see Table 1) and the additional criterion, source intention (see Table 2). Two of the panelists mentioned a potential additional source of information each:

1. "Books published by domain experts";
2. "Statistics relating to past events, frequency/impact".

The first is considered a part of a predefined source: experts. The second is interpreted as a kind of information that can have its origin in multiple sources. Historical information can be supplied by experts, intelligence communities, suppliers, expert communities, etc. and even can be regarded as arising from personal experience. In sum, both are considered already represented on the list and are, therefore, not interpreted as an additional source of information. As shown in Table 4 the answer: "N/A I do not consult this source" is selected six times. These are all selected by one single panelist. All the other panelists indicate they use all the predefined sources.

The results as presented in Table 4 corroborate with previous studies (Baker, McKendry, and Mace 1968; Samet 1975). The results of the security practitioners panel, as shown in Table 5, are analyzed using the FTOPSIS method. In this table, the values are obtained by applying the FTOPSIS method as detailed in the method section.

The results of Table 4 with the 17 alternatives and the three criteria are transferred to a decision matrix. This matrix is normalized and weighted resulting in a best and worst alternative (maximum vs minimum value) per criterion. For the criteria source reliability and information reliability the best (highest valued) alternative is experts. For the criterion source intention the best alternative is personal experience. The worst alternative for all three criteria is public sources like media. The last three columns in Table 5 reflect the ranking of the alternatives per criterion (1.000 is best, 0.000 is worst).

Based on these best and worst alternatives the Euclidian distance of each of the outcomes to the best and worst alternative is calculated ($d_i^*$ and $d_i^-$). Combing these leads to the closeness coefficient ($CC_i$) which can then be ordered into a final ranking.

Overall the source: experts, defined as knowledgeable people recognized in the field, is indicated to be the most trustworthy source of security risk information. They are considered to be the most reliable source, share completely credible information, but do not always share the same intentions (as they are ranked 4 on this criterion). Science/scientific publications, for example, are as a source considered reliable (rank 3) and this source shares equally credible information as the experts (rank 1), but on the other hand this source of information is perceived to not completely share the same intentions (rank 7).

The results show high perceived reliability of personal experience as a source of security risk information.

In the main online survey a larger group of security practitioners participated. They indicated on which sources they base their security risk assessments. This question is answered by 174 respondents (the answer options were not mandatory so some respondents did not assess each source). The respondents are offered the opportunity to add information sources to the 17 on the predefined list. Sixteen additional sources are mentioned in the open box answer possibility. In the left column of Table 6 these answers are presented (including occasional misspelling). In the right column the answers are interpreted. Except

**Table 4.** Classification results security practitioners panel from completely reliable (A) to completely unreliable (F), completely credible (1) to completely not credible (6), and completely shared intention (I) to completely unshared intention (VI), (numbers indicate the number of panelists assigning a certain rating).

| Predefined information sources | Source reliability | | | | | | | Information credibility | | | | | | | Source intention | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | A | B | C | D | E | F | n/a | 1 | 2 | 3 | 4 | 5 | 6 | n/a | 1 | 2 | 3 | 4 | 5 | 6 | n/a |
| Peers | 1 | 14 | 3 | – | – | – | – | 1 | 12 | 5 | – | – | – | – | 2 | 15 | 1 | – | – | – | – |
| Experts | 5 | 11 | 2 | – | – | – | – | 5 | 11 | 2 | – | – | – | – | 5 | 10 | 3 | – | – | – | – |
| Expert communities | 3 | 9 | 6 | – | – | – | – | 4 | 10 | 4 | – | – | – | – | 5 | 8 | 5 | – | – | – | – |
| Higher management | – | 5 | 9 | 4 | – | – | – | 1 | 7 | 6 | 3 | 1 | – | – | 1 | 11 | 3 | 3 | – | – | – |
| Colleagues | – | 7 | 10 | 1 | – | – | – | – | 6 | 12 | – | – | – | – | 3 | 11 | 4 | – | – | – | – |
| Internal intelligence | 4 | 10 | 4 | – | – | – | – | 5 | 9 | 4 | – | – | – | – | 5 | 9 | 4 | – | – | – | – |
| External intelligence (government) | 2 | 14 | 2 | – | – | – | – | 4 | 11 | 3 | – | – | – | – | 3 | 10 | 5 | – | – | – | – |
| External intelligence (commercial) | 1 | 11 | 5 | 1 | – | – | – | 2 | 9 | 6 | 1 | – | – | – | – | 7 | 9 | 2 | – | – | – |
| Public sources like media | – | 2 | 11 | 4 | 1 | – | – | – | 3 | 11 | 2 | 1 | 1 | – | – | 5 | 5 | 4 | 4 | – | – |
| Social media sources | – | 1 | 2 | 9 | 3 | 3 | – | – | – | 5 | 8 | 3 | 1 | 1 | – | 1 | 5 | 4 | 5 | 2 | 1 |
| Government or government agencies | 2 | 10 | 6 | – | – | – | – | 2 | 9 | 7 | – | – | – | – | 3 | 9 | 5 | 1 | – | – | – |
| Consultants/ consulting organizations | – | 7 | 10 | 1 | – | – | – | 1 | 7 | 9 | 1 | – | – | – | 2 | 5 | 10 | 1 | – | – | – |
| Science/scientific publications | 3 | 12 | 3 | – | – | – | – | 5 | 11 | 2 | – | – | – | – | 3 | 11 | 4 | – | – | – | – |
| Supplier organizations | – | 4 | 11 | 2 | 1 | – | – | – | 9 | 7 | 1 | – | – | 1 | – | 8 | 7 | 2 | – | – | 1 |
| Personal experience | 2 | 9 | 7 | – | – | – | – | 3 | 13 | 2 | – | – | – | – | 10 | 7 | 1 | – | – | – | – |
| Personal training/ education | – | 13 | 5 | – | – | – | – | 2 | 12 | 4 | – | – | – | – | 6 | 9 | 3 | – | – | – | – |
| My "gut feeling" | – | 6 | 12 | – | – | – | – | – | 8 | 9 | – | – | – | 1 | 6 | 7 | 3 | – | – | 1 | 1 |

**Table 5.** Results of the FTOPSIS analysis, total results over the three criteria combined, in rank order based on the closeness coefficient CCi, followed by the results of each of the individual criteria: source reliability, information credibility, and source intention.

| Predefined information sources: | Total results: | | | | Source reliab. | | Inform. Cred. | | Source Intent. | |
|---|---|---|---|---|---|---|---|---|---|---|
| | $di^*$ | $di^-$ | $CC_i$ | Rank | $CC_i$ | Rank | $CC_i$ | Rank | $CC_i$ | Rank |
| Experts | 0.075 | 0.998 | 0.930 | **1** | 1.000 | 1 | 1.000 | 1 | 0.836 | 4 |
| Personal experience | 0.106 | 0.972 | 0.902 | **2** | 0.706 | 9 | 0.953 | 3 | 1.000 | 1 |
| Science/scientific publications | 0.134 | 0.937 | 0.875 | **3** | 0.906 | 3 | 1.000 | 1 | 0.768 | 7 |
| Internal intelligence | 0.156 | 0.925 | 0.856 | **4** | 0.883 | 4 | 0.907 | 5 | 0.802 | 5 |
| External intelligence (government) | 0.164 | 0.905 | 0.847 | **5** | 0.929 | 2 | 0.930 | 4 | 0.734 | 9 |
| Peers | 0.178 | 0.885 | 0.832 | **6** | 0.861 | 5 | 0.773 | 8 | 0.853 | 3 |
| Personal training/ education | 0.194 | 0.882 | 0.820 | **7** | 0.750 | 8 | 0.839 | 7 | 0.854 | 2 |
| Expert communities | 0.214 | 0.869 | 0.803 | **8** | 0.772 | 6 | 0.884 | 6 | 0.768 | 6 |
| Government or government agencies | 0.322 | 0.759 | 0.702 | **9** | 0.750 | 7 | 0.708 | 9 | 0.666 | 10 |
| Colleagues | 0.445 | 0.627 | 0.585 | **10** | 0.448 | 12 | 0.453 | 12 | 0.768 | 7 |
| External intelligence (commercial) | 0.465 | 0.609 | 0.567 | **11** | 0.683 | 10 | 0.663 | 10 | 0.420 | 14 |
| Consultants/consulting organizations | 0.555 | 0.521 | 0.484 | **12** | 0.448 | 12 | 0.514 | 11 | 0.488 | 13 |
| My "gut feeling" | 0.580 | 0.530 | 0.478 | **13** | 0.450 | 11 | 0.381 | 13 | 0.557 | 12 |
| Higher management | 0.650 | 0.434 | 0.400 | **14** | 0.227 | 15 | 0.335 | 15 | 0.563 | 11 |
| Supplier organizations | 0.759 | 0.330 | 0.303 | **15** | 0.183 | 16 | 0.379 | 14 | 0.331 | 15 |
| Social media sources | 1.911 | 0.815 | 0.299 | **16** | 0.326 | 14 | 0.310 | 16 | 0.266 | 16 |
| Public sources like media | 1.075 | 0.000 | 0.000 | **17** | 0.000 | 17 | 0.000 | 17 | 0.000 | 17 |

for one they all are considered to be already represented in the predefined list. The answer containing "lateral comparisons" is considered a valuable addition. It is interpreted as: *Risk information from other domains like safety, business continuity, etc.* As this additional source emerged as a result of the last survey it could not be included in further analysis. It is, however, a valuable additional source to be included in future research.

The results of the survey are presented in Table 7. The ranking of the use of the sources is based on a similar FTOPSIS analysis to allow a comparison with the perceived source quality ranking of the practitioners panel.

**Table 6.** Additional sources of security risk information as answered to the open box question.

| Open box answers | Answer is considered belonging to source |
|---|---|
| Networking | Communicating with peers (1), experts (2) and others (4, 5, 6, 7, 8, 12, 14) |
| Common sense | Personal experience (15) and gut feeling (17) |
| The business and incident metrics | Internal intelligence (6) |
| Literature self-reading on cyber security issues | Science/scientific publications (13) and personal training/ education(16) |
| Main focus: people who have dealt DIRECTLY, PERSONALLY with particular risk for long period | Peers (1) |
| Case studies | Science/scientific publications (13) and personal training/ education(16) |
| Lateral comparisons (different situations with partly matching characteristics) | **This is considered an additional source: other (related) domains** |
| Company experience (personal experience of others in company) | Colleagues (5) |
| Problem Management specialists… have we seen this before, can we learn from the past. | Peers (1), experts (2) |
| long term branch knowhow | Expert communities (3) |
| Events elsewhere in the world | This information is considered to be distributed *via* peers (1), experts (2), expert communities (3), public sources (9), government (11), consultants (12) or science (13) |
| Additional case-driven research; think-before-act; prepare for the worst instead of: "I've done it before so I think I can do it" | Science/scientific publications (13) |
| Each source of information misses the answer "don't know/not applicable" | Noted |
| Correct and detailed information on the subject of the risk assessment | Information to be retrieved from peers (1), experts (2) and others (4, 5, 6, 7, 8, 12, 14) |
| Others (anyone in the list below) who has dealt with same circumstances. Context is important, not two environments or circumstances are exactly the same. Hence difficult to rely on others. But I do welcome their viewpoints/ inputs and sharing of ideas. | Peers (1) |
| Intelligence from the sector. | Expert communities (3) |

The ranking of the quality of the information sources seems in line with the ranking of the use of sources. There are, however, a few differences. Information from peers seems to be used a little more (rank 4) than their quality (rank 6) might indicate. Information resulting from personal training/education is also used more (rank 5) while the quality is ranked 7 by the practitioners panel. Intelligence information from government shows the opposite result. The most remarkable difference between quality and use is the information source science and scientific publications. The panel ranked the quality of this source of information high (rank 3) but the use of this information source is stalling at rank 9.

In this survey the data on individual experience of the respondents is collected: their number of years professional experience and security experience, age, education level, and completed specific security trainings. A brief analysis of the influence of these characteristics on the use of information sources is performed.

Individual differences in age, education level, and completed security trainings did not show any significant influence on the use of the information sources. Professional and security experience did show significant effects on the use of some of the sources. More individual experience, based on number of years' experience, seems to reduce the use of commercial external intelligence following from the chi-square statistic alongside its degrees of freedom, sample size, and -value ($\chi^2$ (10, $n = 172$) = 18.3, $p$ = .047), public sources like media ($\chi^2$ (10, $n = 174$) = 22.5, $p$ = .013), and information offered by government/government agencies ($\chi^2$ (10, $n = 172$) = 21.6, $p$ = .017). On the other hand increasing experience, in number of years, seems to increase the reliance on personal experience ($\chi^2$ (10, $n = 173$) = 18.6, $p$ = .045) and gut feeling ($\chi^2$ (10, $n = 174$) = 22.8, $p$ = .011).

## Discussion and conclusions

The first research question of this study – What sources of security risk information are considered by practitioners? – led to a predefined list of 17 possible sources, compiled during a brainstorm session with senior experts ($n = 8$). This list is supported and not further supplemented during the panel consultation ($n = 18$). In the main survey ($n = 174$) one possible additional source is proposed: *Risk information from other domains like safety, business continuity, etc.*

**Table 7.** On what information source do you base your security risk assessment? Total results of the main survey, results of the FTOPSIS analysis, followed by the results of the practitioners panel (see also Table 5).

| Predefined information sources: | Very imp. % of resp. | Mod. imp. % of resp. | Not imp. % of resp. | *N* | Total results main survey $di^*$ | $di^-$ | $CC_i$ | Rank | Results panel $CC_i$ | Rank |
|---|---|---|---|---|---|---|---|---|---|---|
| Experts | 76.4 | 22.4 | 1.1 | 174 | 0.000 | 0.935 | 1.000 | **1** | 0.930 | 1 |
| Personal experience | 61.8 | 35.5 | 2.9 | 173 | 0.151 | 0.792 | 0.840 | **2** | 0.902 | 2 |
| Internal intelligence | 56.1 | 41.6 | 2.3 | 173 | 0.194 | 0.744 | 0.793 | **3** | 0.856 | 4 |
| Peers | 56.1 | 39.9 | 4.0 | 173 | 0.210 | 0.734 | 0.777 | **4** | 0.832 | 6 |
| Personal training/ education | 54.0 | 42.5 | 3.4 | 174 | 0.213 | 0.725 | 0.773 | **5** | 0.820 | 7 |
| Expert communities | 53.4 | 43.1 | 3.4 | 174 | 0.218 | 0.720 | 0.768 | **6** | 0.803 | 8 |
| External intelligence (government) | 50.0 | 45.3 | 4.7 | 172 | 0.273 | 0.670 | 0.710 | **7** | 0.847 | 5 |
| Government or government agencies | 44.2 | 51.7 | 4.1 | 172 | 0.313 | 0.621 | 0.665 | **8** | 0.702 | 9 |
| Science/scientific publications | 48.6 | 41.6 | 9.8 | 173 | 0.328 | 0.631 | 0.658 | **9** | 0.875 | 3 |
| Colleagues | 43.7 | 50.0 | 6.3 | 174 | 0.324 | 0.614 | 0.655 | **10** | 0.585 | 10 |
| External intelligence (commercial) | 35.5 | 54.1 | 10.5 | 172 | 0.444 | 0.498 | 0.528 | **11** | 0.567 | 11 |
| My "gut feeling" | 29.9 | 56.3 | 13.8 | 174 | 0.507 | 0.430 | 0.459 | **12** | 0.478 | 13 |
| Consultants/consulting organizations | 22.4 | 62.6 | 14.9 | 174 | 0.574 | 0.348 | 0.377 | **13** | 0.484 | 12 |
| Public sources like media | 19.5 | 60.9 | 19.5 | 174 | 0.646 | 0.280 | 0.302 | **14** | 0.000 | 17 |
| Higher management | 15.5 | 69.9 | 23.6 | 174 | 0.721 | 0.201 | 0.218 | **15** | 0.400 | 14 |
| Supplier organizations | 16.4 | 60.8 | 22.8 | 171 | 0.727 | 0.202 | 0.218 | **16** | 0.303 | 15 |
| Social media sources | 11.0 | 51.4 | 37.6 | 173 | 0.935 | 0.000 | 0.000 | **17** | 0.299 | 16 |

Future research might include this additional source of security risk information.

In the second part of this study a security practitioners panel ($n = 18$) assessed and classified the predefined list of security risk information sources. To answer the second research question – How reliable are these sources as perceived by these practitioners? – they assessed the sources by applying three criteria, as presented in Figure 2. The results, analyzed applying the MCDM FTOPSIS methodology, allowed a quality ranking of the predefined list of information sources. The results are presented in Table 5. This table shows the source quality ranking. The overall ranking in this table compared to the ranking of the individual criteria allows some interesting observations.

Experts are perceived to be the highest quality sources of information except for the fact that their intention (rank 4) seems not always to be in line with the intention of the panelists. More remarkable is the second highest ranking of "personal experience". The intention of the individuals is, as might be expected, completely in line. The credibility of information originating from personal experience is ranked third, the reliability of this source, on the other hand, is only ranked ninth. This overall second highest ranking of "personal experience" is in line with findings in previous work of the authors on confidence of security professionals in respect to their security risk assessments. Even if they are aware of incomplete security risk information they still have confidence in their assessments (de Wit, Pieters, and van Gelder 2024). The practitioners panel in this study, on the other hand, assign little credibility to their own gut feeling. Gut feeling is, however, knowing without knowing why (Kahneman, Sibony, and Sunstein 2021) and thus, can be considered a kind of experience (Klein 2008). The panelists seem to perceive gut feeling and experience as different sources of which the first is less trusted.

Science/scientific publications are ranked third, the information credibility of this source is regarded top ranked (equal to experts). The intention of science is ranked seventh. These results might indicate the perceived high quality of science but a limited alignment of intention which might be interpreted as a limited practical use. The ranking of the intention of the source "external intelligence (government)" is even lower at rank 9. This source is considered one of the most reliable, rank 2, their information credibility is ranked fourth.

Overall, the proposed additional criterion "source intention" seems to add interesting additional information on information sources that would not have been noticed with the original NATO system. This additional criterion seems to add value to a deeper assessment of sources and might be added in future evaluations.

This study does seem to confirm previous work in other domains that risk communication by government and industry is considered less trustworthy

(Fessenden-Raden, Fitchen, and Heath 1987; McCallum, Hammond, and Covello 1991; Slovic, Flynn, and Layman 1991; Trumbo and McComas 2003). Government sources rank relatively low on the perceived source quality list (rank 5 and 9) and industry even lower (rank 11, 12 and 15).

Table 7 shows the results of the main survey answering the third research question – Which sources are used in security risk assessment praxis? – of this study. These results, combined with the results of the quality ranking, allow answering the research question: Are the most used sources also perceived as the most credible ones?

The two rankings are, besides a few minor differences, similar. This indicates that the perceived high quality information sources, as assessed by the practitioners panel, are used and perceived as important for risk assessments in praxis, as indicated by the group of respondents. The most remarkable difference between the rankings is the source: science/scientific publications. It is perceived a high-quality source (rank 3 by the panel) but seems to be less used in daily praxis (rank 9 by the respondents). This might be explained by the additional proposed information quality criterion: source intention. The panelists assign a high source reliability to science/scientific publications (rank 3), the highest information credibility (rank 1 ex aequo with experts) but on source intention it is ranked at position seven. This means that there is at least some doubt on source intention or aspiration, goals, and objectives might be in line (but this is not certain). The results of the main survey seem to support this. The respondents indicate that they do not think this source is important for their daily practice. Without the proposed additional criterion on information quality: source intention, this could not properly be explained.

Familiarity, which is found important by other scholars as referred to in the background section (McAllister 1995; Hertzum et al. 2002; Denize and Young 2007; Redmiles, Kross, and Mazurek 2016) seems to be reflected in the results of this study. Information from peers who can be considered familiar, seems to be used a little more (rank 4) than their quality (rank 6) might indicate. This could also be a result of the influence of source availability (O'Reilly III 1982; Kim and Sin 2011) as information from peers can be expected to be easy available and accessible. Previous work by other scholars indicated that, although, the quality of information/information sources is indicated to be most important, in praxis the availability of information/information sources is driving behavior and the use of information (O'Reilly III 1982; Hertzum 2002; Kim and Sin 2011). Sources from within the own organization can also be considered familiar (Hertzum 2002). The source internal intelligence (4) ranks high; however, the other internal sources are ranked relatively low: colleagues (10), and higher management (14).

Interpersonal communication is found driving concern over risk more than mediated communication (Trumbo 1996; Kasperson et al. 2012). The top 5 ranking of the use of information sources (Table 7) show sources that can be interpreted as primarily interpersonal. These sources are found to amplify risk signals and, thus, can be expected to raise the risk perception of the security professionals.

Another factor influencing trust in a source is found to be credibility within a community (Kasperson et al. 2012). In this study and survey experts are defined as: knowledgeable people recognized in the field. In this study experts are ranked first in both the quality ranking and the ranking of use in daily praxis. These results seem to confirm the findings of Kasperson. Whom we trust is further based on a similarity in basic values rather than competence (Earle and Cvetkovich 1995). If we would translate "similarity in basic values" to "shared intentions", the proposed additional criterion "source intention" would, according to Earle and Cvetkovich, guide us to the top trusted sources. The last column of Table 5 shows the ranking of sources based on the source intention criterion. Top ranked are personal experience (1st) and personal training/education (2nd) which would indicate that the professionals foremost trust themselves. Previous research by the authors already showed a high level of confidence of the professionals even if they lack adequate information (de Wit, Pieters, and van Gelder 2024). Very close behind these personal sources are peers (3rd) and experts (4th). Both might be considered to have a "similarity in basis values" supporting the findings of other scholars.

The trustworthiness of risk communication by commercial organizations and government is found to be limited in other studies (Fessenden-Raden, Fitchen, and Heath 1987; McCallum, Hammond, and Covello 1991; Slovic, Flynn, and Layman 1991; Trumbo and McComas 2003). This study seems to confirm this. Commercial sources like external commercial intelligence (11th), consultants (12th), and supplier organizations (15th) are at the lower end of this ranking. They might contain too much marketing and are, therefore, considered less trustworthy (Redmiles, Kross, and Mazurek 2016). Government sources rank somewhat higher: external government intelligence (5th), government/government agencies

(9th). As other scholars concluded this lower perceived trustworthiness is primarily caused by deviating goals of both commercial and government risk information sources. The commercial and government sources indeed rank even lower on the source intention scale (last column of Table 5): commercial intelligence (14th), consultants (13th), supplier organizations (15th), external government intelligence (9th), government/government agencies (10th).

Finally the fifth research question – Can we observe differences between security professionals based on their expertise (experience and knowledge)? – is answered. The individual characteristics of the respondents seem to influence the use of a few of the information sources during their security risk assessments. A significant negative association is identified between experience, both professional and security, on use of the sources:

- commercial external intelligence ($p$ = .047),
- public sources like media ($p$ = .013),
- and government/government agencies ($p$ = .017)

More experienced professionals seem to value these sources less than unexperienced professionals. On the other hand significant positive associations are identified between experience and the sources:

- personal experience ($p$ = .045),
- gut feeling ($p$ = .011)

Note the difference in $p$ value that indicate a stronger significance.

It seems that more experienced practitioners have more confidence in their own perception and judgment. Previous work of the authors of this study also identified the influence of experience on confidence and the need for additional information in security risk assessments. More experienced security professionals express higher levels of confidence, even if risk information is known to be incomplete. This indicates confidence in their own expertise. More experienced security professionals also indicated they have a lesser need for additional information in general than less experienced professionals when assessing security risks, even if the information is known to be incomplete (de Wit, Pieters, and van Gelder 2024). The results in this survey seem to confirm these findings, at least for some of the information sources

This study is exploratory and studying phenomena in the security domain that, to the best of our knowledge, have not been studied before. The exploratory nature of this research results in interesting findings that: (1) identify topics for future research in the academic domain, and (2) help the professional domain understanding their daily praxis and offers valuable insights for reflection. The findings of this study can improve professional security risk assessments by assigning weights to the sources delivering information with the highest perceived quality. Therefore this study offers a quality ranking of possible sources of information to the professional domain. The in this study applied enhanced NATO system additionally presents the professional community a tool for the assessment of their sources. Organizations and individuals providing risk information, on the other hand, can find valuable cues in this study to improve their quality. As the English philosopher and physician John Locke remarked over 300 years ago: "The improvement of understanding is for two ends: first, our own increase of knowledge; secondly, to enable us to deliver that knowledge to others." This article seeks to do both and hopes to encourage the academic as well as the professional security domain to translate the offered knowledge into improvement of selection and assessment of sources of security risk information.

## Note

1. https://www.merriam-webster.com/dictionary/information?src=search-dict-box (accessed February 16, 2025).

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## ORCID

Johan de Wit http://orcid.org/0000-0003-0958-3700
Wolter Pieters http://orcid.org/0000-0003-3985-4452
Pieter van Gelder http://orcid.org/0000-0002-0001-0351

## References

Ajzen, I. 2011. The theory of planned behaviour: Reactions and reflections (Editorial). *Psychology and Health* 26 (9):1113–27. doi:10.1080/08870446.2011.613995

Alhawari, S., L. Karadsheh, A. N. Talet, and E. Mansour. 2012. Knowledge-based risk management framework for information technology project. *International Journal of Information Management* 32 (1):50–65. doi:10.1016/j.ijinfomgt.2011.07.002

Baker, J. D., J. M. McKendry, and D. J. Mace. 1968. *Certitude judgments in an operational environment* (Technical

Research Note 200). Arlington, VA: US Army Behavioral Science Research Laboratory.
Bennett, M. 2020. Should I do as I'm told? Trust, experts, and COVID-19. *Kennedy Institute of Ethics Journal* 30 (3–4):243–63. doi:10.1353/ken.2020.0014
Bojanc, R., and B. Jerman-Blažič. 2008. An economic modelling approach to information security risk management. *International Journal of Information Management* 28 (5):413–22. doi:10.1016/j.ijinfomgt.2008.02.002
Capet, P., and T. Delavallade (eds.). 2014. *Information evaluation*. New York: Wiley Online Library.
Citroen, C. L. 2011. The role of information in strategic decision-making. *International Journal of Information Management* 31 (6):493–501. doi:10.1016/j.ijinfomgt.2011.02.005
Cooke, R. M. 1991. *Experts in uncertainty: Opinion and subjective probability in science*. New York: Oxford University Press.
Cooke, R. M., and L. L. H. J. Goossens. 2008. TU Delft expert judgment data base. *Reliability Engineering and System Safety* 93 (5):657–74. doi:10.1016/j.ress.2007.03.005
de Meij, C. 2010. *Subjectieve en objectieve veiligheid: Een overbrugbare kloof?* Master's thesis, Erasmus University Rotterdam.
de Wit, J., W. Pieters, and P. van Gelder. 2024. Bias and noise in security risk assessments, an empirical study on the information position and confidence of security professionals. *Security Journal* 37 (1):170–91. doi:10.1057/s41284-023-00373-6
Deb, A., K. Lerman, and E. Ferrara. 2018. Predicting cyber-events by leveraging hacker sentiment. *Information* 9 (11):280. doi:10.3390/info9110280
Denize, S., and L. Young. 2007. Concerning trust and information. *Industrial Marketing Management* 36 (7):968–82. doi:10.1016/j.indmarman.2007.06.004
Dongo, I., Y. Cardinale, and A. Aguilera. 2019. Credibility analysis for available information sources on the web: A review and a contribution. Paper presented at the 4th International Conference on System Reliability and Safety (ICSRS 2019), Rome, Italy.
Earle, T. C., and G. Cvetkovich. 1995. *Social trust: Toward a cosmopolitan society*. Westport, CT: Greenwood Publishing Group.
Einhorn, H. J. 1974. Expert judgment: Some necessary conditions and an example. *Journal of Applied Psychology* 59 (5):562–71. doi:10.1037/h0037164
Fessenden-Raden, J., J. M. Fitchen, and J. S. Heath. 1987. Providing risk information in communities: Factors influencing what is heard and accepted. *Science, Technology and Human Values* 12 (3/4):94–101.
Fischbein, M., and I. Ajzen. 1975. *Attitude intention and behaviour: An introduction to theory and research*. Reading, MA: Addison-Wesley.
Gal-Or, E., and A. Ghose. 2005. The economic incentives for sharing security information. *Information Systems Research* 16 (2):186–208. doi:10.1287/isre.1050.0053
Gore, J., and P. Ward. 2018. Naturalistic decision making under uncertainty: Theoretical and methodological developments – An introduction to the special section. *Journal of Applied Research in Memory and Cognition* 7 (1):33–4. doi:10.1016/j.jarmac.2017.12.006
Hawley, K. 2012. *Trust: A very short introduction*. New York: Oxford University Press.
Hertzum, M. 2002. The importance of trust in software engineers' assessment and choice of information sources. *Information and Organization* 12 (1):1–18. doi:10.1016/S1471-7727(01)00007-0
Hertzum, M., H. H. K. Andersen, V. Andersen, and C. B. Hansen. 2002. Trust in information sources: Seeking information from people, documents, and virtual agents. *Interacting with Computers* 14 (5):575–99. doi:10.1016/S0953-5438(02)00023-1
Hoffman, R. R., and G. L. Klein. 2017. Challenges and prospects for the paradigm of naturalistic decision making. *Journal of Cognitive Engineering and Decision Making* 11 (1):97–104. doi:10.1177/1555343416689646
Hota, H. S., L. K. Sharma, and S. Pavani. 2014. Fuzzy TOPSIS method applied for ranking of teacher in higher education. In *Intelligent computing, networking, and informatics*, eds. D.P. Mohapatra and S. Patnaik, 1225–32. Berlin: Springer.
Husak, M., J. Komarkova, E. Bou-Harb, and P. Celeda. 2019. Survey of attack projection, prediction, and forecasting in cyber security. *IEEE Communications Surveys and Tutorials* 21 (1):640–60. doi:10.1109/COMST.2018.2871866
Icard, B. 2019. Lying, deception and strategic omission: Definition and evaluation. Doctoral diss., Université Paris Sciences et Lettres.
Icard, B. 2023. Facts versus interpretations in intelligence: A descriptive taxonomy for information evaluation. *Intellectica* 78 (1):89–105.
ISO. 2018. ISO 31000. 2018. Risk management – Guidelines. Accessed February 16, 2025. https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en
ISO/IEC. 2020. ISO/IEC 27000 International standard information technology security techniques. https://www.iso.org/standard/iso-iec-27000-family
ISO/IEC. 2022. ISO/IEC 27005 Information security, cybersecurity and privacy protection—Guidance on managing information security risks. https://www.iso.org/standard/80585.html
Johannessen, J.-A., J. Olaisen, and B. Olsen. 2001. Mismanagement of tacit knowledge: The importance of tacit knowledge, the danger of information technology, and what to do about it. *International Journal of Information Management* 21 (1):3–20. doi:10.1016/S0268-4012(00)00047-5
Johnson, L. K. 2010. *The Oxford handbook of national security intelligence*. New York: Oxford University Press.
Kahneman, D., and G. Klein. 2009. Conditions for intuitive expertise: A failure to disagree. *The American Psychologist* 64 (6):515–26. doi:10.1037/a0016755
Kahneman, D., O. Sibony, and C. R. Sunstein. 2021. *Noise: A flaw in human judgment*. London: William Collins.
Kasperson, J. X., R. E. Kasperson, N. Pidgeon, and P. Slovic. 2012. The social amplification of risk: Assessing 15 years of research and theory. *Social contours of risk*, Vol. 1, eds. R. E. Kasperson and J. Kasperson, 217–45. London: Routledge.
Kim, K.-S., and S.-C. J. Sin. 2011. Selecting quality sources: Bridging the gap between the perception and use of information sources. *Journal of Information Science* 37 (2):178–88. doi:10.1177/0165551511400958
Klein, G. 1997. The recognition-primed decision (RPD) model: Looking back, looking forward. In *Naturalistic decision making*, eds. C.E. Zsambok and G. Klein, 285–92. New York: Psychology Press.

Klein, G. 2008. Naturalistic decision making. *Human Factors* 50 (3):456–60. doi:10.1518/001872008X288385

Klein, G. A. 1993. A recognition-primed decision (RPD) model of rapid decision making. In *Decision making in action: Models and methods*, eds. G. A. Klein, J. Orasanu, R. Calderwood, and C. Zsambok, 138–47. Norwood, NJ: Ablex.

Korkisch, F. W. 2010. NATO gets better intelligence (Strategy Paper 1-2010). Vienna: Institute Für Aussen- and Sicherheitspolitik.

Krisper, M., J. Dobaj, and G. Macher. 2020. Assessing risk estimations for cyber-security using expert judgment. Paper presented at the European Conference on Software and Service Process Improvement, Düsseldorf, September.

Lehman, D. W., K. O'Connor, B. Kovács, and G. E. Newman. 2019. Authenticity. *Academy of Management Annals* 13 (1):1–42. doi:10.5465/annals.2017.0047

Lipshitz, R., G. Klein, J. Orasanu, and E. Salas. 2001. Taking stock of naturalistic decision making. *Journal of Behavioral Decision Making* 14 (5):331–52. doi:10.1002/bdm.381

Lipshitz, R., and O. Strauss. 1997. Coping with uncertainty: A naturalistic decision-making analysis. *Organizational Behavior and Human Decision Processes* 69 (2):149–63. doi:10.1006/obhd.1997.2679

Mandel, D. R., and D. Irwin. 2021. Uncertainty, intelligence, and national security decisionmaking. *International Journal of Intelligence and CounterIntelligence* 34 (3):558–82. doi:10.1080/08850607.2020.1809056

Mandel, D. R., D. Irwin, M. K. Dhami, and D. V. Budescu. 2023. Meta-informational cue inconsistency and judgment of information accuracy: Spotlight on intelligence analysis. *Journal of Behavioral Decision Making* 36 (3):E2307. doi:10.1002/bdm.2307

Markman, A. B. 2018. Combining the strengths of naturalistic and laboratory decision-making research to create integrative theories of choice. *Journal of Applied Research in Memory and Cognition* 7 (1):1–10. doi:10.1016/j.jarmac.2017.11.005

McAllister, D. J. 1995. Affect-and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal* 38 (1):24–59. doi:10.2307/256727

McCallum, D. B., S. L. Hammond, and V. T. Covello. 1991. Communicating about environmental risks: How the public uses and perceives information sources. *Health Education Quarterly* 18 (3):349–61. doi:10.1177/109019819101800307

Meyer, M. A., and J. M. Booker. 2001. *Eliciting and analyzing expert judgment: A practical guide*. Philadelphia, PA: SIAM.

Möller, N. 2012. The concepts of risk and safety. In *Handbook of risk theory: Epistemology, decision theory, ethics, and social implications of risk*, eds. S. Roeser, R. Hillerbrand, P. Sandin, and M. Peterson, 55–85. Berlin: Springer.

Nădăban, S., S. Dzitac, and I. Dzitac. 2016. Fuzzy TOPSIS: A general view. *Procedia Computer Science* 91:823–31. doi:10.1016/j.procs.2016.07.088

O'Hara, K. 2012. A general definition of trust. Accessed February 14, 2025. https://eprints.soton.ac.uk/341800/1/ohara_trust_working_paper_aug_2012.pdf

O'Reilly, C. A. 1982. Variations in decision makers' use of information sources: The impact of quality and accessibility of information. *Academy of Management Journal* 25 (4):756–71. doi:10.2307/256097

Oppelaar, J., and K. Wittebrood. 2006. *Angstige burgers? De determinanten van gevoelens van onveiligheid onderzocht*. The Hague: Sociaal en Cultureel Planbureau.

Pliske, R., and G. Klein. 2003. The naturalistic decision-making perspective. In *Emerging perspectives on judgement and decision research*, eds. S.L. Schneider and J. Shanteau, 559–85. Cambridge, UK: Cambridge University Press.

Powell, T., S. Oggero, J. Schook, and E. Westerveld. 2019. Dealing with uncertainty in hybrid Conflict: A novel approach and model for uncertainty quantification in intelligence analysis (NATO STO-MP-IST-190). Accessed February 14, 2025. https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/Forms/All%20MPs.aspx?RootFolder=/publications/STO%20Meeting%20Proceedings/STO%2DMP%2DIST%2D190&FolderCTID=0x0120D5200078F9E87043356C409A0D30823AFA16F602008CF184CAB7588E468F5E9FA364E05BA5&View=%7B72ED425F-C31F-451C-A545-41122BBA61A7%7D

Redmiles, E. M., S. Kross, and M. L. Mazurek. 2016. How I learned to be secure: A census-representative survey of security advice sources and behavior. In *CCS'16: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 666–77. New York: ACM.

Roberts, A. P. J., and J. C. Cole. 2018. Naturalistic decision making: Taking a (cognitive) step back to take two steps forward in understanding experience-based decisions. *Journal of Applied Research in Memory and Cognition* 7 (1):70–81. doi:10.1016/j.jarmac.2018.01.003

Ryan, J. J., T. A. Mazzuchi, D. J. Ryan, J. L. De la Cruz, and R. Cooke. 2012. Quantifying information security risks using expert judgment elicitation. *Computers and Operations Research* 39 (4):774–84. doi:10.1016/j.cor.2010.11.013

Salih, M. M., B. B. Zaidan, A. A. Zaidan, and M. A. Ahmed. 2019. Survey on fuzzy TOPSIS state-of-the-art between 2007 and 2017. *Computers and Operations Research* 104:207–27. doi:10.1016/j.cor.2018.12.019

Samet, M. G. 1975. Quantitative interpretation of two qualitative scales used to rate military intelligence. *Human Factors: The Journal of the Human Factors and Ergonomics Society* 17 (2):192–202. doi:10.1177/001872087501700210

Schwarz, N., and L. A. Vaughn. 2002. The availability heuristic revisited: Ease of recall and content of recall as distinct sources of information. In *Heuristics and biases: The psychology of intuitive judgment*, eds. T. Gilovich, D. Griffin, and D. Kahneman, 103–19. New York: Cambridge University Press.

Seagle, A. N. 2015. Intelligence sharing practices within NATO: An English school perspective. *International Journal of Intelligence and CounterIntelligence* 28 (3):557–77. doi:10.1080/08850607.2015.1022468

Sevkli, M., S. Zaim, A. Turkyilmaz, and M. Satir. 2010. An application of fuzzy Topsis method for supplier selection. Paper presented at the International Conference on Fuzzy Systems, Barcelona, July.

Singh, H., M. M. Gupta, T. Meitzler, Z.-G. Hou, K. K. Garg, A. M. G. Solo, and L. A. Zadeh. 2013. Real-life applications of fuzzy logic. *Advances in Fuzzy Systems* 2013 (1):1–3. doi:10.1155/2013/581879

Skjong, R., and B. H. Wentworth. 2001. Expert judgment and risk perception. Paper presented at the Eleventh

International Offshore and Polar Engineering Conference, Stavanger, Norway, June.
Slovic, P., J. H. Flynn, and M. Layman. 1991. Perceived risk, trust, and the politics of nuclear waste. *Science (New York, NY)* 254 (5038):1603–7. doi:10.1126/science.254.5038.1603
Stanovich, K. E., and R. F. West. 2000. Individual differences in reasoning: Implications for the rationality debate? *Behavioral and Brain Sciences* 23 (5):645–65. doi:10.1017/s0140525x00003435
Talbot, J., and M. Jakeman. 2011. *Security risk management body of knowledge*. New York: John Wiley.
Tetlock, P. E., and D. Gardner. 2016. *Superforecasting: The art and science of prediction*. New York: Random House.
Trumbo, C. W. 1996. Examining psychometrics and polarization in a single-risk case study. *Risk Analysis* 16 (3):429–38. doi:10.1111/j.1539-6924.1996.tb01477.x
Trumbo, C. W., and K. A. McComas. 2003. The function of credibility in information processing for risk perception. *Risk Analysis: An Official Publication of the Society for Risk Analysis* 23 (2):343–53. doi:10.1111/1539-6924.00313
Van Leeuwen, T. 2001. What is authenticity? *Discourse Studies* 3 (4):392–7. doi:10.1177/1461445601003004003
Viljanen, L. 2005. Towards an ontology of trust. Paper presented at the Second International Conference on Trust, Privacy and Security in Digital Business, Copenhagen, August.
Wang, Y.-J., and H.-S. Lee. 2007. Generalizing TOPSIS for fuzzy multiple-criteria group decision-making. *Computers and Mathematics with Applications* 53 (11):1762–72. doi:10.1016/j.camwa.2006.08.037
Weber, M. 1987. Decision making with incomplete information. *European Journal of Operational Research* 28 (1):44–57. doi:10.1016/0377-2217(87)90168-8