Evaluating insider threat indicators and mitigation measures: a Delphi study

April 2022

Researchers:
PhD-candidate Mathias Reveraert, University of Antwerp
Professor Tom Sauer, University of Antwerp

Universiteit Antwerpen

Research Group International Politics University of Antwerp

This research was supported by

Table of Contents

List of tables and figures

Tables

Figures

Executive summary

The study resulted in a catalogue of possible insider threat mitigation measures that organizations can chose from to develop their tailor-made insider threat mitigation policy:

In the **recruitment stage**, recommended practices relate to screening background information of applicants (e.g. verifying CV, credentials, identity and criminal record) whereby organizations need to take screening seriously instead of carrying it out pro-forma, but also need to apply a risk-based approach (i.e. adjust screening depending on the position).
In the **organizational socialization stage**, the panel recommends organizations to apply the Aristotelian method, characterized by precept (e.g. a code of conduct), habit (e.g. a strong security culture) and demonstration (e.g. lead by example) to inform (new) employees on the organizational culture, as well as to have a general supportive attitude towards employees while simultaneously being strict but fair when it comes to violations of the code of conduct.
In the **observation stage**, the panel considers internal whistleblowing to be more effective than artificial intelligence tools to observe red flags of insider threat, although it does not completely disregard technology given that (alarms on) electronic access systems and endpoint security tools are recommended to guard the principle of least privilege (i.e. ensures that employees solely have access to the information needed to perform their job).
In the **investigation stage**, the panel advises organizations to have a formal investigation policy that outlines who conducts the investigation and how the investigation proceeds, but does not recommend to formally outline in policies and procedures what behavior would trigger the investigation process.
In the **anticipation stage**, it is noteworthy that the panel rather showed which practices are not recommended to pre-empt imminent insider threats (e.g. positive incentives to seek resolution before an incident develops, deterrence practices, and awareness-raising initiatives) than which practices are useful.
In the **damage limitation** and **reconstruction stage**, both preparatory practices (e.g. a business continuity plan and an event notification tree) and reactive practices (e.g. collecting evidence, identifying and changing compromised processes and conducting a post-incident analysis) are suggested by the panel to react to an insider threat incident, as well as practices related to internal and external incident communication.
In the **deliberation stage**, the panel recommends to have a fair and consistent disciplinary system that respects the rights of the offender, to focus on acts and not on people, to discuss different options with relevant stakeholders to develop a plan, to review access permissions and to make sure other employees know appropriate measures are taken.
In the **termination stage**, some exit procedures recommended by the panel are straightforward (e.g. the development, consistent application and regular update of termination procedures), whereas others resemble practices suggested in the insider threat literature (e.g. reclaiming equipment from the terminated employee, revoking virtual and physical access or conducting an exit interview).
Regarding **mismanagement,** practices that the panel recommends to deal with false positives (i.e. to insiders that are wrongly accused of being responsible for an incident) concern both practices aimed at restoring the relation with the wrongly accused insider (e.g. full rehabilitation or welfare/psychological support) and practices targeted at preventing the reoccurrence of similar false positives (e.g. reviewing the indicators and/or the reporting route that led to the false assessment and awareness of possible repercussions).
To conclude, the desirability of a **formal insider threat mitigation team** should depend on the size and type of the organization, should not necessarily be a distinct team but can equally reside in an already existing team and should cooperate with other relevant stakeholders like co-workers, line management and social partners.

Summary of the findings

This report elaborates on the results of a three-round Delphi study on insider threat mitigation. The goal of the study was to discover potential 'red flags' (i.e. indicators of insider threat incidents) and good practices on insider threat mitigation. The objective consisted of transforming the theoretical insider threat mitigation framework that was developed on the basis of the literature (Reveraert & Sauer, 2022a) into a framework with practical usability. The study employed the Delphi technique to iteratively compare and contrast the opinions of insider threat experts. A multidisciplinary panel of 25 international experts completed three rounds of online questionnaires on the 9 stages of the insider threat mitigation framework, namely recruitment (I), organizational socialization (II), observation (III), investigation (IV), anticipation (V), damage limitation (VI), reconstruction (VII), deliberation (VIII) and termination (IX). The panelists were also questioned on the possibility of mismanagement (X), on the desirability to establish a formal insider threat mitigation team (XI) and on their evaluation of the present Delphi study (XII).

(I) Recruitment

Red flags

The panel considers falsifications of background information, low integrity, addictions (to drugs, alcohol, gambling), affinity with extremist ideology/organizations, an unresponsive attitude during the recruitment process and negative advice from either government authorities or references all factors that may point to insider threat. On the other hand, previous employment for a competitor, job-hopping, discrepancies between educational and career path and mental and physical health issues are all examples of factors that were much less perceived as a red flag of insider threat. A bit to our surprise, the panel gave little attention to the applicant's motivation to work for the organization. Likewise, apart from addictions, low priority is given to the applicant's personal problems, even though both in the literature (Shaw & Sellers, 2015; Noonan, 2018) and in our survey on insider threat awareness and behavior (Reveraert & Sauer, 2021b) it is shown that personal problems can be a possible breeding ground of insider threats.

Good practices

The good practice to detect red flags during recruitment that the panel unanimously agreed upon is taking screening seriously instead of carrying it out pro-forma. Recommended screening practices correspond with recommendations found in the insider threat literature, like adopting a risk-based approach (Bishop et. al.,2009; Bishop et al., 2010; George et. al., 2019; Probst et. al., 2010) and verifying curriculum vitae, credentials, identity and criminal record (BaMaung et. al., 2018; Power & Forte, 2006). Transparency about the screening process, as well as training and awareness of recruiters, is also suggested by the panel. Reference checks with professional references are more popular than checks with social network references (i.e. family and friends). In line with earlier results about red flags during recruitment, the panel nuances the importance of the applicant's private life and possible personal problems, given that less than half of the panelists recommends to ask non work-related questions during the recruitment process.

Difficulties

Although background information screening of the applicant is important, the majority of the panel believes that lack of access to information and unclarity about the accuracy of the information provided by the applicant or his or her references hinders the detection of red flags during recruitment. In addition to this information deficit, resource limitations and positive or negative biases of recruiters are put forward by the panel as constraining the detection of red flags during recruitment. Issues that put relatively less strain on the detection of red flags during recruitment are the fact that the hiring process becomes too time-intensive or the fact that the candidate might feel some discomfort about the questions.

(II) Organizational socialization

To inform (new) insiders about the organizational norms corresponding to the organizational culture, the panel mainly recommends organizations to apply the Aristotelian method characterized by precept (e.g. a code of conduct in which expectations regarding both appropriate and inappropriate conduct are explained), by habit (e.g. a strong security culture) and by demonstration (e.g. lead by example by senior leadership and middle management). Organizations are also encouraged to have a supportive attitude towards (new) insiders (e.g. foster a spirit of belonging and show care when needed) while simultaneously being strict but fair when it comes to violations of the code of conduct. Moreover, it is noteworthy that positive reinforcement scores significantly better than negative reinforcement, and that except for *recurrent* company-wide awareness campaigns on the code of conduct, instruments to communicate the expectations outlined in the code of conduct (e.g. the use of intranet, newsletters, email campaigns, posters and screen savers) receive a relatively low rating from the panel. Furthermore, it is notable that informal communication between insiders and line managers is considered more important than formal communication about the expected behavior. The panel has also more confidence in evaluations conducted by management than in peer- or self-evaluations. To conclude, the panel rates the usefulness of team building events and gamification relatively low, not considering it appropriate practices of organizational socialization.

(III) Observation during employment

Red flags

Factors that may point to insider threat concern both individual and organizational factors, with the majority relating to the former. The most obvious warning signals that were unanimously accepted by the panel are threatening employers or co-workers and receiving warnings from other employees, clients or third parties about the behavior of the insider. In line with the insider threat literature (BaMaung et. al., 2018; Gelles, 2016; Shaw & Sellers, 2015), the panel considers deviation from normal or baseline behavior an early warning of insider threat (e.g. unauthorized access attempts, unexplained wealth, changes in lifestyle), although the results show that not all deviant behavior is worrisome (e.g. changes in personal status like divorce, changes in online or social media behavior and changes in mental or physical health). Moreover, personality characteristics (e.g. not being very empathetic or introversion) were generally not regarded as a red flag. Concerning underlying reasons of insider threats, the panel rates disgruntlement with the organization relatively higher than personal strains (e.g. financial difficulties or unmet personal expectations) and personality disorders (e.g. narcissism), something that is in line with the results of our insider threat awareness and behavior survey (Reveraert & Sauer, 2021b). Regarding organizational factors, the presence of a culture of fear and silence and unexplained irregularities in the accountancy of the organization are considered to be factors that may stimulate insider threats, while other organizational factors (e.g. too heavy workloads or high levels of competitiveness) are not necessarily indicative of future insider threat incidents.

Good practices

The panel emphasizes the usefulness of the possibility of internal whistleblowing to observe red flags during employment, a practice also recommended in the insider threat literature (Bell et. al., 2019; Colwill, 2009; Mehan, 2016; UK Centre for the Protection of National Infrastructure, 2011; US National Insider Threat Task Force, 2016). Also other practices that the insider threat literature recommends, like the earlier mentioned risk-based approach and the principle of least privilege (Cole & Ring, 2006; International Atomic Energy Agency, 2008; Mehan, 2016) are recommended by the panel. Regarding technological factors, the panel recommends electronic access control and endpoint security tools to detect unauthorized access attempts, but the panel is reluctant to the use of artificial intelligence and machine learning tools to automatically detect deviant behavior. The latter is in contrast to the literature on insider threat, where artificial intelligence receives considerable attention (e.g. Brown et. al., 2013; Koutsouvelis et. al., 2020; Le & Zincir-Heywood, 2019).

Difficulties

One of the main difficulties to observe red flags is the fact that observation of red flags depends on the subjective interpretation of the observer, which implies that what may appear suspicious to one observer might be a positive sign to another observer. Moreover, similar to the recruitment stage reference is made by the panel to resource limitations as a factor constraining observation of red flags. Furthermore, a number of difficulties identified by the panel relate to good practices, whereby the panel either identifies reasons that complicate the implementation of these recommended practices or identifies a discrepancy between the recommended situation and the actual situation. Concerning the former, the panel for instance recommends to adopt a risk-based approach, but simultaneously recognizes that this implies unequal treatment of insiders that might on its turn lead to push back from unions/labor groups. Concerning the latter, the panel emphasizes the importance of a culture of reporting to observe red flags during employment, but simultaneously claims that whistleblowing is currently not culturally accepted, leading to an unwillingness to report. A similar discrepancy between the recommended situation and the actual situation is present with respect to tailor-made training for managers and staff to observe and report red flags, cultural acceptance of in-employment screening practices (e.g. electronic access control) and awareness of the insider threat problem among management, which are all recommended by the panel but are also believed to be currently absent.

(IV) Investigation

Most of the good practices suggested by the panel to investigate red flags observed during employment seem rather straight-forward, like respecting the (legal) rights of the suspect, knowing what employees ought to be doing and the provision of sufficient resources to conduct investigations. Furthermore, whereas the panel advises organizations to have a formal investigation policy that outlines who conducts the investigation and how the investigation proceeds (e.g. in relation to internal whistleblowing) and to be transparent on this process, it is to a lesser extent recommended to formally outline in policies and procedures what behavior would trigger the investigation process. Also temporary reassignment of the suspect to a less sensitive area during the investigation and involvement of external expertise on the investigation of potential insider threats is not recommended by the panel. A striking observation is that formal and informal conversations with the suspect are not specifically recommended. The same goes for the approval of formal investigation policies and procedures by social partners. Referring back to the identification of pushback from unions/labor groups as a significant difficulty to observe red flags, we assume that letting social partners approve formal investigation policies and procedures could help to reduce the push back from unions/labor groups.

(V) Anticipation

It is noteworthy that only four out of the in total 37 practices suggested by the panel in round 1 of this study were recommended by the panel, which is considerably less in comparison with the other stages. A possible explanation for the few recommended practices is the lack of contextualization of the insider threat situation presented to the panel. Contextualizing the question might therefore generate different results, with practices receiving a low rating from the panel possibly receiving a higher rating when discussed in relation to a specific scenario. The low number of recommended practices implies that the panel finds it easier to show which practices are not recommended to pre-empt imminent insider threats than which practices are useful. In this regard, it is noteworthy that relatively little importance is given to positive incentives to seek resolution before an incident develops (e.g. involvement of social/psychological support), deterrence practices, interaction with the suspect, and awareness-raising (either generally or in the direct environment of the suspect). Furthermore, apart from withdrawing the suspect's access, other measures taken to keep the suspect (temporarily) away from his or her position (e.g. suspension, offering the suspect time off the job, transferring the suspect internally or terminating the contract of the suspect) receive little attention from the panel.

(VI) Damage limitation & (VII) Reconstruction

Both preparatory (e.g. a business continuity plan and an event notification tree) and reactive practices (e.g. collecting and securing evidence, conducting a post-incident analysis and identifying and changing compromised processes) are suggested by the panel to react to an insider threat incident. Furthermore, the panel recommends organizations to minimize the damage to the organization's reputation by spending considerable attention to practices related to incident communication (e.g. develop internal- and external crisis communication plans and have trained staff in crisis communication). Transparency is less recommended in the aftermath of an insider threat incident, both internally and externally. Also interaction with the offender is not regarded as necessary.

(VIII) Deliberation

The total number of suggested practices with respect to the deliberation stage is relatively scarce with only 19 suggested practices. Nevertheless, almost half of them are recommended by the panel. More in particular, the panel recommends to have a fair & consistent disciplinary system whereby the rights of the offender are respected. Other practices include focusing on acts and not on people, discussing different options with relevant stakeholders to develop plan A/B/C, reviewing access permissions and making sure other employees know that appropriate measures are taken. Also noteworthy is the low priority given to questioning the offender by applying a hear and confront approach, which does not appear to be compatible with the generally accepted principle that an offender has the right to defend him- or herself. Similarly, the fact that almost two thirds of the panel believe that the severity of the impact of the incident should have an influence on the level of punishment is remarkable since according to the literature (Goold, 2002; Hawley, 2014; Ho & Katukoori, 2013; Elangovan & Shapiro, 1998; Morris & Moberg, 1994), the focus should not be on the impact but on the decision itself.

(IX) Termination

Some of the exit procedures outlined by the panel are straightforward, like the unanimous recommendation to comply with applicable laws and the development, consistent application and regular update of termination procedures. Also other recommendations resemble practices suggested in the insider threat literature, like reclaiming equipment from the terminated insider, revoking his or her virtual and physical access or conducting an exit interview (Beattie & BaMaung, 2015; Power & Forte, 2006; UK Centre for the Protection of National Infrastructure, 2019). Also documentation is important for the panel in the termination stage, both documenting terminations in general as well as documenting insider threat incidents that precede terminations. Again, both internal (e.g. debriefing with the terminated insider's social network) and external (e.g. sharing lessons learned with the broader community) transparency on the insider threat incident is not recommended by the panel. The same goes for post-monitoring social media and other open sources.

(X) Mismanagement of an insider threat case

The total number of suggested practices with respect to mismanagement is relatively scarce with only 16 suggested practices. That said, more than half of the practices are recommended by the panel. Practices are both aimed at restoring the relation with the wrongly accused insider (e.g. full rehabilitation and welfare/psychological support), and at preventing the reoccurrence of similar false positives (e.g. reviewing the indicators and/or the reporting route that led to the false assessment and awareness of possible repercussions). The panel considers offering the insider a public apology less appropriate than offering the insider a personal apology, but more appropriate than offering the insider a (financial) compensation.

(XI) Formal insider threat mitigation team

The majority of the panel recommends the creation of a formal insider threat mitigation team. However, this recommendation is put into perspective, with panelists indicating that the desirability of a formal insider threat mitigation team depends on the size and type of the organization, that the formal insider threat mitigation team should not necessarily be a distinct team but can equally reside in an already existing team and that the formal insider threat mitigation team should cooperate with other relevant stakeholders like co-workers, line management and social partners.

Acknowledgements

This report and the research behind it would not have been possible without the support of the expert panel that showed remarkable engagement to our study by completing our time-consuming questionnaires and sharing their insights on insider threat mitigation. Moreover, we would like to thank the sponsors of the research project on insider threats, namely Bel-V, Brussels Airport Company, Elia, Engie-Electrabel, the Federal Agency of Nuclear Control (FANC) and G4S. Also our colleagues from the University of Antwerp, in particular dr. Marlies Sas, Rikkert Horemans, Robin Vanderborght, Emmanuel Dockx, Zeger Verleye, Professor Jarl Kampen and Professor Kenneth Lasoen, have contributed to this research by providing feedback or by acting as test audience. To conclude, we are grateful for the insightful comments offered by Professor Genserik Reniers and Professor Emeritus Rona Beattie, members of the doctoral committee of this research project on insider threats.

1. Introduction

Funded by Bel-V, Brussels Airport Company, Elia, Engie-Electrabel, the Federal Agency of Nuclear Control (FANC) and G4S, the University of Antwerp initiated in February 2019 a doctoral project on 'insider threats'. An insider threat is interpreted here as the possibility that individuals who are or used to be trusted by the organization with the privilege of access to and/or knowledge about the organizational assets cause harm to the organization because they intentionally misuse this access or knowledge (Reveraert & Sauer, 2021a). The goal of the doctoral project is two-fold, namely on the one hand raising awareness on the insider threat problem, and on the other hand providing organizations with mitigation measures to better secure themselves against insider threats.

The research outlined in this report particularly concerns the second objective. It builds upon a theoretical insider threat mitigation framework established by Reveraert & Sauer (2022a), a conceptual model that consists of nine insider threat mitigation stages, namely recruitment, organizational socialization, observation, investigation, anticipation, damage limitation, reconstruction, deliberation and termination. The aim of the study is to take the first step towards transforming the conceptual model into an insider threat mitigation framework with practical usability. Its main goal is to discover (1) potential 'red flags' of insider threat incidents (i.e. factors that may point to insider threat), (2) good practices on insider threat mitigation throughout the employee life cycle (before, during and after employment), (3) actors responsible for insider threat mitigation and (4) difficulties related to insider threat mitigation.

To achieve this goal, the study employs the Delphi technique, "a widely used method of gathering group consensus from a panel of knowledgeable persons" (Stone Fish & Busby, 2005: 238) that is often used in the context of doctoral projects (Landeta, 2006; Skulmoski et. al., 2007). The three-round Delphi study iteratively compares and contrasts the opinions of prominent insider threat experts on the different steps of the theoretical framework. In concrete terms, a multidisciplinary panel of 25 experts in a field related to insider threats, like corporate security, counterintelligence, insider threat training, and so on, is asked to complete three rounds of online questionnaires. The questionnaire of round 1 concerns open-ended questions, whereby the different panelist individually brainstorm for important issues regarding the mitigation of insider threats. The questionnaire of round 2 outlines all important issues identified by the panel in round 1 and asks each expert to individually rate each issue. The questionnaire of round 3, to conclude, provides the panelists with a list of issues that received a high rating from the panel and asks each member of the panel to indicate whether he or she agrees or disagrees with the panel's decision to give that particular issue a high rating.

In what follows, the study will start with a brief outline of the theoretical insider threat mitigation framework of Reveraert & Sauer (2022a). After that, we will thoroughly describe the research design, elaborating on the different steps of our Delphi process. Subsequently, the center of attention will shift to the results of the study. The study will eventually be completed with a discussion and conclusion section.

2. Insider threat mitigation framework

This study draws upon Reveraert & Sauer's (2021a) interpretation of the insider threat problem. An insider is interpreted as an individual that is or used to be trusted by the organization with access to the organizational assets. In an attempt to manage insider access, organizations establish guidelines regarding the appropriate use of the insider access (i.e. organizational norms), and expect that insiders will handle the insider access received from their organization in an appropriate way (Neumann, 2010; Reason, 1998; Von Solms & Von Solms, 2004). Still, the possibility exists that insiders deviate from these organizational norms and misuse their insider access.

In other words, organizations are vulnerable to insider misconduct, which can either be unintentional due to a lack of competency (i.e. insider hazards) or intentional due to a lack of trustworthiness (i.e. insider threats) (Reveraert & Sauer, 2021a). While competency relates to whether the insider *can* adhere to the behavioral expectations of the organization, trustworthiness relates to whether the insider *wants to* adhere to them (Colquitt et. al., 2007; Elangovan & Shapiro, 1998; Hawley, 2014; McKnight & Chervany, 2001). Building on Reveraert & Sauer's distinction between insider hazards and insider threats, only intentional misuse of privileged access or knowledge by insiders, whether or not with the intention to inflict harm, is interpreted as an insider threat. As a result, members of the expert panel are explicitly informed that the scope of this Delphi study is **limited to intentional misconduct, leaving aside incidents resulting from insiders that unintentionally or accidentally misconduct**[1].

The aim of organizations is to mitigate insider threats. Therefore, Reveraert & Sauer (2022a) established on the basis of the literature a theoretical insider threat mitigation framework that outlines the different steps that should be followed when confronted with an insider threat. This conceptual model for insider threat mitigation consists of 9 stages, namely recruitment, organizational socialization, observation, investigation, anticipation, damage limitation, reconstruction, deliberation and finally termination.

In the *recruitment stage* (I), the goal of the organization is to evaluate the trustworthiness of potential future insiders to confirm that only trustworthy candidates are recruited. More specifically, the organization should perform pre-employment screenings to ensure that new recruits are trustworthy (Afolabi, 2017; Eoyang, 1994; Klotz et. al., 2013; Waltz, 2003), possibly supplemented with vetting by government authorities (Afolabi, 2017; Van Laethem, 2005). Competent candidates of which the trustworthiness is perceived to be below the satisfactory level are rejected, while those above the threshold can join the organization.

Insider threat mitigation is however more than just performing pre-employment screening. After the insider has joined the organization, the organization should socialize the insider, entering the *organizational socialization stage* (II). The main goal of the organization is to consolidate the insider's trustworthiness above the desirable threshold by not only informing (new) insiders on the organizational norms corresponding to the organizational culture, but also persuading them to adhere to these organizational norms. Insiders can be extrinsically motivated via positive and negative sanctions, or intrinsically motivated, accepting or internalizing the norm as the appropriate way to

[1] An example of unintentional misconduct is an employee that spreads sensitive information to unauthorized individuals by accidentally hitting 'reply all' instead of 'reply' (Probst et. al., 2010).

conduct and automatically complying with it without the need of sanctions (Pfleeger et. al., 2014; Siponen & Kajava, 1998; Siponen, 2000; Von Solms & Von Solms, 2004).

Apart from assimilating its insiders to the organizational culture, the organization should remain vigilant for signals that might indicate a decline in insider trustworthiness (Costa et. al. 2014; Gelles, 2016; Greitzer et. al., 2012; Greitzer et al, 2016; Ho et. al., 2018). Such vigilance relates to the *observation stage* (III). Here, the goal of the organization is to observe 'red flags', or potential early warning signals of insider threat. After becoming aware of a potential red flag, the organization has to assess whether it concerns misinformation that can be closed without further action (Gelles, 2016), or whether the signal is worth to investigate in more detail.

If the organization interprets the red flag as a signal that is worth to investigate in more detail, the organization has to check the validity of the red flag (Steneck, 1994). This happens in the *investigation stage* (IV), where the organization starts an investigation to discover whether the red flag is indeed an early warning that requires immediate counteraction. The organization should not conduct the investigation from a police/judicial perspective by looking for evidence of already committed misconduct (i.e. what happened?), but should rather use an intelligence approach (i.e. what will likely happen?) whereby the raw information that was observed in the previous stage is contextualized and transformed into knowledge and wisdom upon which the organization can take an informed decision for further action (De Graaff, 2019; George et al., 2019; Lanssens, 2020; US National Insider Threat Task Force, 2016; Waltz, 2003). The outcome of the investigation either shows that the red flag is a misinterpretation and that the insider is still trustworthy (Gelles, 2016), or reveals that the insider indeed shows traces of employee alienation from the organization that the organization needs to worry about.

If the investigation reveals that the red flag is indeed an early warning signal that needs to be anticipated, it is perceived the insider is about to intentionally misconduct in the near future (Belk & Hix, 2018; Lee & Kulkarni, 2011). In the *anticipation stage* (V), the main objective of the organization is therefore to preempt what is perceived to be a likely insider threat incident. In an ideal situation, the conceptual model would stop here and no insider threat incidents would happen. However in reality, organizations are not able to avert every insider threat incident.

If the organization is unable to anticipate the situation, an insider threat incident will happen. As a result, the theoretical insider threat mitigation framework also considers the aftermath of the insider threat incident. When an insider intentionally commits misconduct, the situation evolves into the *damage limitation stage* (VI). The primary concern of the organization is limiting the harm resulting from the insider threat to a minimum (Bunn & Sagan, 2016; Mehan, 2016). Once the damage resulting from the insider threat incident has been ceased, it is time for the organization to reconstruct the incident.

During the *reconstruction stage* (VII), the organization has to become fully aware of what happened in order to learn from it and prevent its recurrence. Apart from looking into the specific circumstances that allowed the insider to commit intentional misconduct, reconstruction also includes debriefing the insider to find out the reason behind the intentional misconduct, and eventually adjudicating the insider's justification (Steneck, 1994).

After reconstructing the incident in a detailed manner, the organization has to re-examine the currently unknown trustworthiness level of the insider. This happens in *the deliberation stage* (VIII), where the main objective of the organization is to determine whether the insider responsible for the

insider threat incident can remain employed at the organization, and if so, under what conditions (Steneck, 1994; Cools, 1994).

Finally, when the organization comes to the conclusion that the trust relationship with the insider is at the end of the rope, the organization should terminate the insider's contract, which happens at the *termination stage* (IX). Important here is that the insider's dismissal proceeds according to proper exit procedures (Beattie & BaMaung, 2015; Power & Forte, 2006; UK Centre for the Protection of National Infrastructure, 2019; US National Insider Threat Task Force, 2016).

If the organization properly follows the exit procedures, the insider threat mitigation process returns to the recruitment stage as (at least in a lot of cases) a new insider has to be recruited to fill the open spot in the organization. This means that the theoretical insider threat mitigation framework is actually a cyclical process, as demonstrated on figure 1.

Figure 1: *Theoretical insider threat mitigation framework*

In an ideal situation, the organization always takes the right decision, correctly judging threats as threats (i.e. true positives) and non-threats as non-threats (i.e. true negatives). Unfortunately, this is not how reality works. In reality, organizations run the *risk of mismanaging (X)* the situation (Martinez-Moyano et. al., 2008), leading to false positives, false negatives and nulls. False positives refer to non-threats that are incorrectly judged as threats. False negatives are the opposite situation and relate to threats that are considered to be non-threats. Finally, null either refers to oversight of the threat, like for instance red flags that slip through the net and are not observed, or to omission of threat mitigation, like for instance not performing pre-employment screenings or exit procedures.

3. Research design

Since the conceptual model alone is too abstract for organizations to make use of it in practice[2], we considered it necessary to supplement the theoretical framework with empirical research to concretize the different steps of the conceptual model. The main goal of this study is therefore to dig deeper into the theoretical insider threat mitigation model to refine the abstract terms and make it more user-friendly for organizations. To reach this goal, we used the Delphi technique, "a widely used method of gathering group consensus from a panel of knowledgeable persons" (Stone Fish & Busby, 2005: 238).

3.1. The Delphi technique

According to Hasson & Keeney, "Delphi is a method for the systematic collection and aggregation of informed judgement from a group of experts on specific questions and issues" (2011: 1696). The absence of standardized methodological guidelines however makes that a range of different interpretations and approaches of the Delphi technique exist (Hasson et. al., 2000; Hasson & Keeney, 2011; Keeney et. al., 2006; Skulmoski et. al., 2007). Nevertheless, generally four conditions have to be met when applying the Delphi technique (Foth et. al., 2016; Gossler et. al., 2019; Kozak & Iefremova, 2014; Landeta, 2006; Skulmoski et. al., 2007; Rowe & Wright, 2001; von der Gracht, 2012):

- A first characteristic is *anonymity*. Since true anonymity is impossible because the research team has to be aware of the identity of the panel members to allow targeted reminders (Keeney et. al., 2006), reference is often made to quasi-anonymity (Hasson et. al., 2000; Chuenjitwongsa; 2017). Delphi studies use quasi-anonymity to reduce the negative effects related to other methods of group communication (e.g. focus groups), like for instance groupthink or dominant panel members (Dalkey & Helmer, 1963; Hsu & Sandford, 2007; Turoff, 2002). Quasi anonymity can either refer to anonymity of the panel or only to anonymity of the responses of the panel. In case of the former, participating experts are unaware of the identity of the fellow members of the panel as well as of the individual answers of each expert. Concerning the latter, members of the panel are not informed on the identity behind each particular opinion addressed in the context of the study, but are however aware of the composition of the panel.

- A second characteristic is *iteration*, which means that the study has to consist of at least two rounds to give the members of the panel the opportunity to change their answer to the previous round(s).

- A third characteristic is *controlled feedback*, whereby the researchers inform the panel of experts on the results of the previous round. Since "there are still no agreed guidelines about how to provide feedback in a Delphi study" (Barrios et. al., 2021: 2), it is usually up to the researchers to decide the type of feedback (von der Gracht, 2012). The controlled feedback should however stick with essential information necessary to complete the next round of the study, eliminating irrelevant information or 'noise' (Hsu & Sandford, 2007).

[2] To give an example: at the recruitment stage, it is recommended to do pre-employment screenings, without specifying what these pre-employment screenings should look like.

- A fourth and last characteristic is *statistical aggregation*, which implies that a number of statistics are used to determine the degree of consensus among the expert panel. To determine the opinion of the group, often reference is made to statistical indicators of central tendency and dispersion (Hsu & Sandford, 2007; von der Gracht, 2012) which are presented in a numerical or graphical way (Hasson et. al., 2000; Schmidt, 1997).

To conclude, it is worth noting that "while all Delphi studies share these common characteristics, the flexibility of the Delphi method has led to a high diversity of methodological variants" (Gossler et. al., 2019). Later in this report we will thoroughly explain our 'methodological variant' of the Delphi technique, but we will start by explaining the reader why we wanted the use the Delphi technique in the first place.

3.2. Why the Delphi technique?

The Delphi technique fits the research purpose for several reasons. From a practical point of view, the technique allows to include insights from a geographically dispersed panel of expert (Okoli & Pawlowski, 2004; Rowe & Wright, 2001; Stone Fish & Busby, 2005) without the need to gather them in an (online) event. Bringing together 25 experts from around the globe in online meetings would be challenging given the busy schedules of the experts and the different time zones, while gathering them in multiple face-to-face events would require a lot of funding and would be complicated during the COVID-19 pandemic. Instead, the Delphi technique gives the panel members considerable freedom to complete each online questionnaire at their own pace, making it a more time- and cost-efficient method for all stakeholders of the research project.

Our choice for the Delphi technique was however not solely based on reasons of practicality, as the decision to use the Delphi technique has also substantive underpinnings. Remember that the main goal of the study is to increase the practicality of the conceptual model outlined in section two of this report (see supra). The tendency to avoid public announcements in order to safeguard the organization's reputation (Sarkar, 2010; Mehan, 2016) implies a rather high dark or hidden number of insider threats, which in its turn causes empirical data to be scarce. Insider threat incidents are therefore statistically rare phenomena (Catrantzos, 2009), making a purely quantitative approach difficult.

In contrast to hindsight investigations of insider threats[3] that "work their way back in history to find out what happened" (van de Linde & van der Duin, 2011: 1558), we therefore decided to take a different road by looking forward to potential indicators of insider threat, mitigation measures or obstacles of insider threat mitigation (van de Linde & van der Duin, 2011). Our quest for such an alternative approach led us to use the Delphi method because the use of expert judgement is an appropriate alternative when statistical models are problematic due to insufficient empirical data (Barrios et. al. 2021; Catrantzos, 2009; Rowe & Wright 2001). Moreover, the use of the Delphi technique is considered to be appropriate in a risk analysis context (von der Gracht, 2012) and has already been used by other researchers to explore insider threat mitigation, with Catrantzos (2009) employing it in the context of critical infrastructure protection, Dupuis & Khadeer (2016) using it to compare the psychological profile of malicious and non-malicious insiders and Padayachee (2016)

[3] See for instance Randazzo et. al. (2005)

using it to explore the state-of-the-art on opportunity-reducing measures to mitigate insider threats related to information security.

We want to use the technique to refine our theoretical framework with broad-based practical guidelines on insider threat mitigation. The Delphi technique allows to explore the insider threat topic (Padayachee, 2016; Gossler et. al., 2019) by compiling insights from experts that look at the insider threat problem from a range of perspectives (Van Dolderen et. al., 2017). Consulting a multidisciplinary team of experts in a range of insider threat fields allows us to first identify a variety of potential early warning signals (i.e. red flags) of insider threat (van de Linde & van der Duin, 2011) and to subsequently find agreement among this multidisciplinary panel on which of the potential red flags are insider threat indicators organizations should be vigilant of (Mukherjee et. al., 2015). The same principle applies to the identification of 'good practices' on insider threat mitigation, as the Delphi technique allows to identify a variety of potential insider threat mitigation measures (Cantrantzos, 2009; Mukherjee et. al., 2015), followed by a triage of these suggested mitigation measures according to desirability for insider threat policy (Baker et. al. 2006; Gossler et. al., 2019; Padayachee, 2016). In brief, the use of expert judgements allows to pool insights from a broad spectrum of insider threat researchers and practitioners (Hsu & Sandford, 2007; Mukherjee et. al., 2015; Skulmoski et. al., 2007), making the technique valuable to discover the state-of-the-art on insider threat mitigation.

3.3.Research sample

In view of the foregoing, the prominent role of the expert panel in the Delphi technique implies that the credibility of the research outcome largely depends on the research sample, i.e. the composition of the panel of experts (Baker et. al., 2006; Chuenjitwongsa, 2017; Kozak & Iefremova, 2014; Stone Fish & Busby, 2005). Still, Okoli & Pawlowski indicate that choosing appropriate experts is "perhaps the most important yet most neglected aspect of the Delphi method" (2004: 16). Indeed, "literature fails to debate the practicalities of defining 'experts' for use within Delphi panel research" (Baker et. al., 2006: 59), which means that firm rules on the composition of the expert panel are currently absent. Therefore, it is important to explain the reasoning behind our panel of experts in greater detail, not only to give readers the opportunity to judge the quality of the panel (Schmidt, 1997) but also in view of reproducibility of the study (Diamond et. al., 2014; Santaguida et. al., 2018).

3.3.1. Purposive sampling

The absence of standardized guidance on the composition of the expert panel implies that the research sample could be gathered in a number of ways. One possibility was to follow the example of Hackett et. al. (2006), who used contacts from their professional network. We refrained from this option because it is however recommended in literature to use official selection criteria to select the members of the expert panel (Keeney et. al., 2006; Mukherjee et. al., 2015). We used purposive sampling strategies (Hasson et. al., 2000; Padayachee, 2016; Santaguida et. al., 2018; Vogel et. al., 2019) to compose our research sample, whereby we supplemented the criterion-based sampling with opportunity sampling (Gossler et. al., 2019).

Although standardized guidelines regarding the selection criteria for the criterion-based sampling are currently absent (Gossler et. al., 2019; Keeney et. al., 2006, Steurer, 2011; Stevenson, 2010), Skulmoski et. al. (2007) and Giannarou & Zervas, (2014) recommend to select panelists on the basis of four attributes:

- The first attribute is *capability*, determined by an individual's knowledge (Mukherjee et. al., 2015; Rowe & Wright, 2001; Santaguida et. al., 2018; Stone Fish & Busby, 2005) and experience (Catrantzos, 2009; Gossler et. al., 2019; Hsu & Sandford, 2007; Kozak & Iefremova, 2014;

Mukherjee et. al., 2015). Our panel of experts consisted of individuals with at least 5 years of experience in a field related to insider threat or with at least 5 years of experience in research related to insider threats. It is however worth noting that 2 of the 25 experts that participated did not fulfill the selection criteria because these experts were recommended by experts we initially contacted (that met our selection criteria) but that were not able to participate themselves. Given that recommendation by other participants can also be used to select panel members (Baker et. al., 2006), we decided to combine our criterion-based sampling with opportunity sampling (Gossler et. al., 2019) and included the recommended experts in the panel.

- The second attribute is *willingness***,** implying that the incentive to participate in the study primarily originates from professional interest in the topic (van de Linde & van der Duin, 2011). The individual is intrinsically motivated to contribute to the study, without getting much in return besides the results of the study (Landeta, 2006; Kozak & Iefremova, 2014).

- The third attribute is *time-commitment*, as it is "important that those who have agreed to participate, maintain involvement until the process is completed" (Hasson et. al., 2000: 1011), limiting the number of drop-outs to a minimum.

- The final attribute is *communication skills*, which means that the participants should be skilled in writing (Keeney et. al., 2006) as well as in English (Vogel et. al. 2019) to be able to explain their opinions to their fellow panelists.

3.3.2. Sample size

Concerning the number of experts to include in the panel, a variety of recommendations are given in the literature. Skulmoski et. al. (2007) show the wide variety in panel sizes that was used in previously published Delphi research, with a lower limit of three participants and an upper limit of 171 participants. While Gossler et. al. argue that most Delphi studies are composed of eleven to 50 panelists, Kozak & Iefremova (2014) limit the range to 15 à 35 experts. Vogel et. al. (2019) rather set the lower limit of the sample size on twelve respondents, whereas Baker et. al. indicate that "most reliable samples for Delphi studies should be small - fewer than 20 participants" (2006: 66). This upper limit of 20 respondents is echoed by Rowe & Wright (2001) and Hsu & Sandford (2007), who respectively recommend a lower limit of five and 15 participants. Giannarou & Zervas (2014) and Van Dolderen et. al. (2017), on the other hand, argue that the sample size in Delphi studies usually consists of seven to 30 participants, an upper limit that is endorsed by Rayens & Hahn (2000), though they suggest a lower limit of ten participants. Chuenjitwongsa, to conclude, increases the lower limit to 30, arguing that "the minimum number of samples needs to be at least 30 to provide rigour for statistical analysis" (2017: 1). Trying to find a golden mean in the diverse set of recommendations, we aimed for a panel of at least 20 experts because "20 panelists may be adequate for the development of diagnostic indicators" (Steurer, 2011: 960), one of the main goals of this study, and because "it is believed that a sample size of 20 tending to retain the members" (Giannarou & Zervas, 2014: 67).

3.3.3. Procedure for selecting the panelists

To identify potential candidates for our panel of experts, we drew inspiration from the procedure for selecting experts outlined by Okoli & Pawlowksi (2004), although not following the procedure down to the last detail. Their procedure consists of five steps. The first step is to make an overview of relevant disciplines that relate to the main subject of the Delphi study. In the second step, each discipline mentioned in step one is populated with names of potential candidates. The third step consists of contacting the list of potential experts to obtain extra nominations. In the fourth step, all experts are

ranked according to their suitability, which is determined by their qualifications. Step five, to conclude, consists of inviting the experts to participate in the study.

As prescribed by Okoli & Pawlowksi (2004), we started with an examination of the disciplines related to the insider threat problem (i.e. step one), leading us to fields like corporate security, national security, nuclear security, counterterrorism, whistleblowing, private investigation, counterintelligence and so on. Subsequently, we started our quest for names (i.e. step two) to construct a shortlist of experts, whereby both national (i.e. Belgian) and international experts were taken into account to enable the composition of a heterogenous, multidisciplinary panel (Baker et. al., 2006; Catrantzos, 2009; Gossler et. al., 2019; Mukherjee et. al., 2015; Padayachee, 2016; Rowe & Wright, 2001). Our target audience consisted of both academics and field practitioners (Vogel et. al., 2019; Foth et. al., 2016). Therefore, our inspiration mainly originated from (1) relevant academic and practitioner literature on insider threats, (2) international insider threat events like the 2019 'Insider Threat Mitigation Symposium'[4] and the 2020 'Insider Risk Summit'[5], and (3) a LinkedIn search on the search terms 'insider threat' and 'insider risk'.

Instead of contacting the approximately 100 experts on our initial shortlist (i.e. step three), we decided to pilot (see infra 3.4.1) our shortlist to a group of practitioners[6] and academics[7] that would not be part of the expert panel to get feedback on the experts we shortlisted (Steurer, 2011). Participants to the pilot study were asked to go through our shortlist of candidates to indicate which experts they endorsed or opposed as well as to suggest any experts not appearing on our shortlist. On the basis of the pilot feedback, we selected 75 experts (i.e. step four) that were invited to be part of our panel (i.e. step five), hoping to get at least 20 positive responses. The invitation included a brief outline (one page) of the procedure and the estimated timing of the research study. Although the difference between the number of invitations (75) and the expected number of experts that would commit themselves to participate the full study (20) might seem extensive, we anticipated the potential for a low response rate (Keeney et. al., 2006; Hsu & Sandford, 2007), taking into consideration a high rejection rate as the experts invited are all professionals with busy schedules not necessarily able to make the commitment to a multiple-round Delphi study (Keeney et. al., 2006; Okoli & Pawlowski, 2004; Skulmoski et. al., 2007; van de Linde & van der Duin, 2011).

3.3.4. The composition of the expert panel

In the end, 29 experts of the 75 experts that were invited indicated their willingness to participate in our study, implying a 39% response rate to our initial call (Schmidt, 1997; Santaguida et. al., 2018). This was well above our initial goal of 20 participations, meaning we had a buffer for potential drop-outs (Okoli & Pawlowski, 2004). All 29 experts received the first round of our Delphi study (see infra 3.4.2). As illustrated in table 1, 25 experts eventually completed the online questionnaire of the first round.

[4] For more information, see http://insiderthreatmitigation.org/program

[5] For more information, see https://www.code42.com/news-releases/code42-to-host-inaugural-insider-risk-summit-in-september-2020/

[6] The sponsors of our research project (see supra).

[7] Colleagues of the research team as well as the members of the doctoral committee of the principal researcher. Concerning the former, dr. Marlies Sas and prof. dr. Kenneth Lasoen were consulted for feedback on the content of questionnaire 1, while prof. dr. Jarl Kampen was consulted for methodological questions. Concerning the latter, em. prof. dr. Rona Beattie and prof. dr. Genserik Reniers serve in the doctoral commission of the principal researcher and also provided their feedback on the shortlist.

Table 1: *Members of the panel of experts*

Name	**Affiliation**
Dr. BaMaung David	Honorary Professor at Glasgow Caledonian University
Dr. Bongiovanni Ivano	Lecturer at the University of Queensland Business School
Dr. Buckley Oli	Associate Professor in Cyber Security - School of Computing Sciences, University of East Anglia
Catrantzos Nick	StratCoLab.org
Charney L. David, M.D.	Psychiatrist and Medical Director, Roundhouse Square Counseling Center and President, NOIR for USA
De Bie Bart	Director of i-Force and Vice-president of the Institute of Fraud Auditors (IFA)
De Greef Stefanie	Competence center manager at Robrechts & Thienpont at the time of the study but not anymore at time of publication.
Engels J.	Owner of Engels & Partners Detectives
Prof. Furnell Steven	Professor at the University of Nottingham, UK
Dr. Haelterman Harald	Professor at the Ghent University Faculty of Law and Criminology Department of Criminology, Criminal Law and Social Law
Dr. Homan Zenobia S.	Project Coordinator & Research Fellow at the Centre for Science & Security Studies (CSSS), King's College London.
Moris Marc	Proximus Group Dept Lead Corporate Prevention & Protection.
Dr. Noonan Christine	Pacific Northwest National Laboratory
Rettig Stefan	European Commission, Security Directorate Seconded National Expert - Germany
Theis Michael C.	CISSP, CCII, SAC (Retired) Chief Engineer, Strategic Engagements National Insider Threat Center at the CERT Division, Software Engineering Institute (an FFRDC)
Tinsley Herbert	Staff researcher at the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the time of the study Currently PhD student at the University of Arizona's School of Government and Public Policy
Van Hauwe Stephan	Managing Consultant OpSeC BV
Van Limbergen Kris	Crime Control
Dr. Vande Walle Gudrun	Forensic auditor - Centre for Integrity - federal Ombudsman and Visiting professor Integrity Management at Ghent University, Faculty of Economics and Business Administration
Vanhoey Herwig	Security Manager bpost
Verhasselt Frederik	Partner Forensic & Integrity Services at EY Bedrijfsrevisoren BV
Anonymous	Anonymous UK Government expert
Anonymous	/
Anonymous*	/
Anonymous**	/

* Participated in the first round only

** Participated in the first and second round only

As required in a Delphi study, we applied quasi-anonymity (Hasson et. al., 2000; Chuenjitwongsa; 2017; Keeney et. al., 2006) which implies that throughout the study participating experts were unaware of the identity of the other members of the panel. However, at the end of the study, experts were ask to provide an informed consent in which we asked them whether they wanted to forego anonymity (Mukherjee et. al., 2015). Acceptance of this opportunity means that their participation as expert in our Delphi research is made public in the final report of the study, whereas refusal of this opportunity means that their participation in our study remains anonymous[8]. Table 1 shows that the majority of the experts agreed to reveal their participation in the panel, which provides the reader with additional information to interpret the quality of our research results (Foth et. al., 2016; Schmidt, 1997).

Moreover, table 1 shows that the attrition rate, a major challenge in Delphi studies (Giannarou & Zervas, 2014; Kozak & Iefremova, 2014; Stevenson, 2010), was minimal with only one expert dropping out after round 1 and another one after round 2 of the study. Follow-up on the respondents that dropped out (Keeney et. al., 2006) taught us that the reasons for not continuing their participation were not substantive but practical, with one referring to sick leave and one referring to busy work schedules. Since only experts that completed the previous round were allowed to complete the subsequent round (Vogel et. al., 2019), round 2 was completed by 24 experts and round 3 was completed by 23 experts. This attrition rate implies that for each Delphi round, the response rate is well above the recommended 70 to 75% response rate[9] (Hasson et. al., 2000; Chuenjitwongsa, 2017; Santaguida et. al., 2018).

Table 2 gives an overview of the demographics of the panel (Padayachee, 2016; Raskin, 1994; Schmidt, 1997; Stevenson, 2010; Vogel et. al., 2019). It shows that the panel was equally divided between national (Belgian) and international experts, whereby the latter predominantly originated from the United States and the United Kingdom. The breakdown of the respondents by sex reveals an imbalance with 76% of male experts. As stated before, the panel consisted of both academics and practitioners, as well as of a significant number of experts that is double-hatted. Looking at the different backgrounds of the members of the panel, table 2 shows that we composed a multidisciplinary panel from a range of insider threat fields, whereby a number of experts indicated affiliation with more than one insider threat domain. Finally, more than 70% of the panel indicated that they had more than 10 years of experience in their respective insider threat domain(s). As previously explained, two of the experts that participated in our study had less than 5 years of experience (see supra 3.3.1).

Table 2: *Profile of the panel of experts*

		N
Country of residence	Australia	1
	Belgium	12
	Germany	1
	the Netherlands	1
	United Kingdom (UK)	5
	United States of America (USA)	5
	Total	25
Sex	Male	19
	Female	6
	x	0
	Total	25

[8] Regardless of the response, no one except the research team is provided with the individual responses.
[9] Round 1: 86% (25/29); Round 2: 96% (24/25); Round 3: 92% (23/25).

Origin of Expertise	Academic	4
	Practitioner	11
	Both	10
	Total	25
Insider threat domain	Academia	4
	Corporate security	4
	National Security	3
	Private investigation	3
	Security consultancy	2
	Whistleblowing	2
	Insider threat training	2
	Legal	1
	Counterintelligence	1
	Counterextremism/terrorism	1
	Nuclear security training	1
	Total	25
Level of experience	Less than 1 year	1
	2-3 years	0
	3-4 years	1
	5-6 years	3
	7-8 years	2
	9-10 years	0
	More than 10 years	18
	Total	25

3.4. The Delphi process

The flexibility of the research design of the Delphi technique implies that there are "no formal, universally agreed guidelines on the use of the Delphi technique nor does any standardization of methodology exist" (Keeney et. al. 2006). Consequently, it is crucial to discuss in detail the interpretation of the technique that was used in this study to leave an audit trial (Gossler et. al., 2019; Skulmoski et. al., 2007).

Our interpretation of the Delphi technique is based upon a thorough examination of existing literature on the technique. One study particularly inspired the philosophy behind our application of the technique, namely the study of Padayachee that can be summarized as follows: "Round 1 (Brainstorming), Round 2 (Consolidation) and Round 3 (Refinement)" (Padayachee, 2016: 50). However, it is important to note that it does not concern an exact copy of Padayachee's research design. The flexibility of the technique allowed us to incorporate insights from other Delphi studies and adapt Padayachee's research design according to our own study objectives (Keeney et. al., 2006).

Table 3 gives an overview of our Delphi process, discussing the different steps of the process in relation to the time frame to complete the step, the goal of the step and the method used to reach that particular goal. It shows that our Delphi study consists of three rounds, whereby round 1 is preceded by a pilot. This format is in conformity with the number of rounds suggested in literature on the Delphi technique (Giannarou & Zervas, 2014; Gossler et. al., 2019; Hsu & Sandford, 2007; Skulmoski et. al., 2007; Turoff, 2002), as well as with the number of rounds used in previous Delphi studies (e.g. Catrantzos, 2009; Padayachee, 2016; Stone Fish & Busby 2005; Vogel et. al. 2019).

The number of rounds was defined prior to the start of the study (Kozak & Iefremova, 2014). For each round, we used the online survey tool Qualtrics to establish an online questionnaire, making it an e-Delphi study (Gossler et. al., 2019). After receiving the link to the questionnaire via e-mail, the panelists were expected to submit their responses within 12 days[10]**.** To guarantee quasi-anonymity, we used a coding system (Hasson et. al. 2000) whereby each expert was assigned an expert number (Catrantzos, 2009; Santaguida et. al., 2018) that had to be filled in to enable access to the questionnaire. Each questionnaire then started with a short introduction outlining the purpose and estimated time required to complete it. After that the panelist was redirected to the actual questionnaire of the particular round of the study. The remainder of this section will discuss each step of the Delphi process in greater detail, starting with the pilot study.

Table 3: *The Delphi process*

Delphi Round	**Time frame**	**Goal**	**Method**
Pilot study	February 2021	Feedback on both the selection of the expert panel as well as on the development of the first questionnaire.	Consult academics and practitioners that are not part of the expert panel
Round 1	March 2021	Each expert individually brainstorms for issues (i.e. red flags, good practices, actors and difficulties)	Open-ended questions
Round 2	June 2021	Divide the lists of issues collected in round 1 in: • high-rated issues; • medium-rated issues; • low-rated issues.	Rating questions • 5-point Likert-scale (agree-disagree) • Number of starts (0-5)
Round 3	August 2021	Check to what extent each expert agrees with the panel's list of high-rated issues	Provide experts with a list of the high-rated issues and ask • to select the issue if they disagree with the panel • to explain their reasoning behind that disagreement

3.4.1. The pilot study

According to Skulmoski et. al., "the Delphi pilot is especially important for inexperienced researchers who may be overly ambitious regarding the scope of their research or underestimate the time it will take a Delphi research participant to fully respond to the Delphi survey" (2007: 4). Consequently, during the pilot study we consulted practitioners and academics[11] that would not be part of the expert panel to get feedback on our panel selection and to pre-test the first online questionnaire. Participants to the pilot study were asked to go through our shortlist of the research sample to indicate which experts they endorsed or opposed and to suggest any experts not appearing on our shortlist. Moreover, they were requested to comment on the questions of the first questionnaire, both with respect to the content of the questions as to the way they were formulated since the wording of the

[10] Due to the summer holidays, the deadline for round 3 was extended to 18 days.
[11] See footnote 6 and 7

question matters as well (Hasson & Keeney, 2011; Christie & Barela, 2005). The pilot study allowed us to finetune both the expert panel and the first questionnaire.

3.4.2. Round 1

Round 1 corresponds with the brainstorming phase of the study (Padayachee, 2016). The design of the questionnaire can be either quantitative or qualitative (Chuenjitwongsa, 2017; Steurer, 2011). A quantitative design is based upon an examination of relevant literature on the subject of the Delphi study, whereby the panel is asked to rate existing ideas and opinions generated from this literature (Keeney et. al., 2006; Santaguida et. al., 2018; van de Linde & van der Duin, 2011; Vogel et. al., 2019). A qualitative design, on the other hand, allows the panel freedom to generate its own ideas and opinions (Catrantzos, 2009; Hasson et. al., 2000; Hsu & Sandford, 2007; Okoli & Pawlowski, 2004; Padayachee, 2016).

Our study opted for the qualitative approach. The first round contained level-setting questions whereby the different panelists individually brainstormed about the mitigation of insider threats. In concrete terms, the questionnaire consisted of 16 open-ended questions (see table 4) that addressed four kinds of research questions:

- What are important *'red flags'* (i.e. factors that may point to insider threat) of insider threat (question 1 and 6 in table 4)?
- What *good practices* can organizations implement to mitigate insider threats (question 2, 4, 5, 7, 9, 11, 13, 14, 15 and 16 in table 4)?
- *Who should be responsible* for insider threat mitigation (question 10 and 12 in table 4)?
- What (legal or non-legal) *difficulties* do organizations encounter in the mitigation of insider threats (question 3 and 8 in table 4)?

Table 4: *Questions round 1*

Insider threat mitigation phase	Step theoretical framework	Questions
a) Structural Prevention	I. Recruitment	1. What are important 'red flags' (= factors that may point to insider threat) that organizations should check during the recruitment of new insiders? 2. What good practices can organizations implement to detect the above-mentioned red flags during recruitment? 3. What (legal or non-legal) difficulties do organizations encounter in the detection of the above-mentioned red flags during recruitment?
	II. Organizational Socialization	4. What good practices can organizations implement to communicate their expectations regarding appropriate conduct to (new) insiders?

		5. What good practices can organizations implement to ensure that insiders not only know what conduct is expected but actually live up to these expectations?
b) Situational Prevention (≈ detection)	III. Observation	6. What are important 'red flags' (= factors that may point to insider threat) that organizations should be vigilant of during employment? 7. What good practices can organizations implement to detect the above-mentioned red flags during employment? 8. What (legal or non-legal) difficulties do organizations encounter in the detection of the above-mentioned red flags during employment?
	IV. Investigation	9. What good practices can organizations implement to investigate the validity of red flags (= factors that may point to insider threat) to avoid making false accusations? 10. Which organizational department (HR, Security, ...) should lead this investigation, and why?
c) Pre-emption	V. Anticipation	11. What good practices can organizations implement to counteract an imminent insider threat (= act to prevent it from happening)? 12. Which organizational department (HR, Security, ...) should lead this counteraction, and why?
d) Insider threat aftermath (≈ remedy)	VI. Damage limitation & VII. Reconstruction	13. If an insider threat incident happens, what good practices can organizations implement to limit the damage resulting from the incident?
	VIII. Deliberation	14. What good practices can organizations implement to respond to insiders that are responsible for an insider threat incident?
	IX. Termination	15. What good practices can organizations implement to dismiss insiders?
	X. Mismanagement	16. What good practices can organizations implement to respond to insiders that are wrongly accused of being responsible for an incident (= false positives)?

Table 4 shows that the questions of the first questionnaire relate to the different steps of the theoretical framework (I-X) outlined earlier in this study. For each step of the framework[12], at least one type of question (i.e. red flags, good practices, responsible actor and/or difficulties) was asked to the panel. However, we decided not to inform the panel on the theoretical framework as this would lead us too far. Instead, table 4 shows that we opted to group the different steps of the theoretical framework in four insider threat mitigation phases (a-d), namely structural prevention, situational prevention, pre-emption and insider threat aftermath.

3.4.3. Round 2

Round 2 corresponds with the consolidation phase of the study (Padayachee, 2016). The panel gets the opportunity to evaluate the answers of other experts to reconsider their own responses in light of the information the other panelists provided. The questionnaire of round 2 is therefore made up of the analysis of the responses to the questions asked in round 1, whereby the research team uses the information generated to construct a structured, quantitative questionnaire (Chuenjitwongsa, 2017). In round 2, we slightly modified the questionnaire design of round 1. First of all, the questions concerning organizational socialization (see supra table 4 questions 4 and 5) were combined into one single question[13]. Moreover, the questions regarding the actors responsible for insider threat mitigation (see supra table 4 questions 8 and 10) were equally grouped into one single question surveying the panel on the necessity of a formal insider threat mitigation team. Finally, the wording of some of the questions was slightly changed for reasons of clarity[14].

The responses to the questions asked in round 1 were per question consolidated in an overall list of issues (Padayachee, 2016; Stone Fish & Busby, 2005). Similar to Gossler et. al., who indicate that they used NVivo "to organize, store and retrieve the data [while] the actual analysis was carried out manually by the research team" (2019: 443), we used Qualtrics for data repository purposes but manually analyzed the data using paper and pencil, Word and Excel. While some authors, like for instance Hasson et. al. (2000), Okoli & Pawlowski (2004) and Gossler et. al. (2019), suggest to group the issues of round 1 into broader categories, Stone Fish & Busby argue that "if responses are grouped together into categories that are too broad, significance can be sacrificed for consensus" (2005: 250). Also Keeney et. al. take part in the debate, indicating that returning the large list of items in a raw, non-categorized form could frighten the panelists and encourage them to drop out while simultaneously arguing that grouping responses can produce a halo effect "where the responses are about the general category, rather than about the individual issues raised by participants" (Keeney et. al., 2006: 207). In this study, we decided not to group the issues in categories. Instead, we presented the information provided in round 1 as authentic as possible, retaining the language of the panelists as much as possible (Keeney et. al., 2006; Stone Fish & Busby; 2005) while still trying to keep the issues to the point and unambiguous (Stevenson, 2010).

After cataloguing a list of issues for each question presented to the panel in round 2, the different lists of issues were fed back to the panel to give each individual panelist the opportunity to validate and reject ideas generated in round 1. In more concrete terms, the panel was asked to judge the value of each issue on the list for that particular question, whereby the rating could take place in two different ways. As illustrated in figure 2, questions related to possible red flags or to difficulties concerning

[12] Damage Limitation (step 6) and Reconstruction (step 7) were grouped in 1 question, while also the possibility of mismanagement (see supra section 2) was addressed by asking a question about false positives.

[13] The question was: "Please rate the following practices to make employees aware of and willing to live up to the organization's expectations regarding appropriate conduct".

[14] For instance, we replaced 'dismiss' with 'terminate the contract of', or specified between brackets whether the incident had already happened or not.

insider threat mitigation were rated on a five-point Likert scale with one indicating strong disagreement with the issue and five indicating strong agreement with the issue (Giannarou & Zervas, 2014; Mukherjee et. al., 2015). Questions related to good practices, on the other hand, had to be rated by rewarding the proposed practice with a number of stars ranging from one to five with one indicating strong opposition to the proposed practice and five indicating strong endorsement of the proposed practice, as illustrated in figure 3. To verify whether the research team included all ideas generated in round 1 in the list of issues, panelists were explicitly asked at the end of each question to add any crucial information they provided in round 1 that was missed by the research team (Hasson & Keeney, 2011; Schmidt, 1997).

Figure 2: *Questionnaire design 2 - example Likert-scale questions*

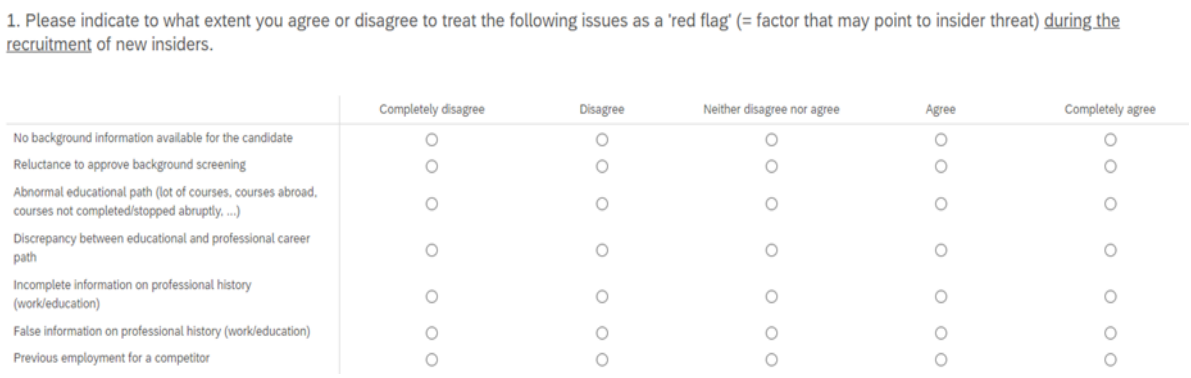
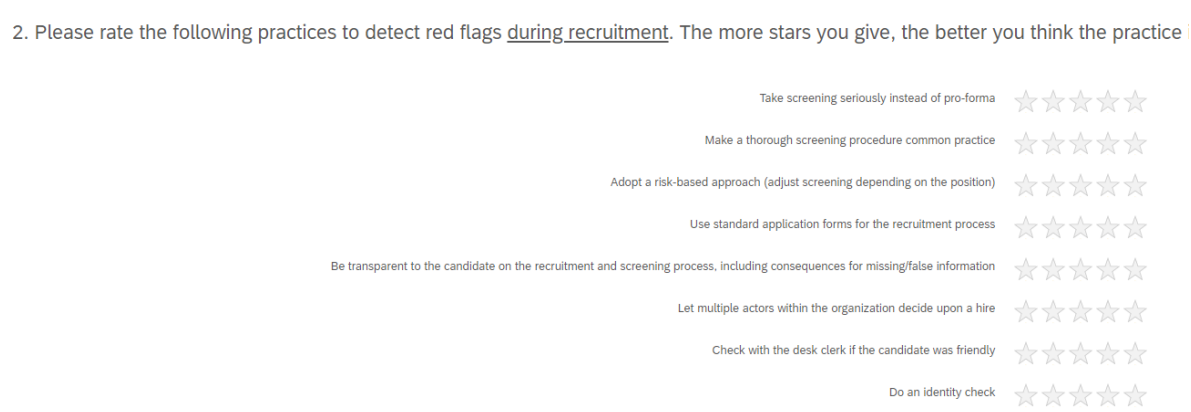


Figure 3: Questionnaire design round 2 - *example star-rating questions*



While the main goal of the first round of our study was to discover as much issues as possible (Schmidt, 1997), the goal of the second round was to measure the degree of consensus between the panelists, looking at consensus on an item level (Christie & Barela, 2005). von der Gracht indicates that "consensus is one of the most contentious components of the Delphi method, and its measurement greatly varies" (2012: 1528), which implies that "standards for consensus in Delphi research have never been rigorously established" (ibid: 1528) and that "this part of the methodology is also often poorly explained by researchers" (ibid: 1528). To avoid this mistake, we believe it is necessary to first explain in detail our understanding of consensus. Given that literature recommends to use simple statistical summaries (Hasson et. al., 2000; Keeney et. al., 2006; Polit et. al., 2007), we considered more advanced statistical measures[15] for consensus not suitable for our study. Instead, to meet Giannarou & Zervas'

[15] Think for instance of Chi square (Jakobsson & Westergren, 2005), Cronbach's alfa (Meijering et. al., 2013; Steurer, 2011), (multi-rater) Kappa coefficient (Barrios et. al., 2021; Meijering et. al., 2013; Polit et. al., 2007; Wynd et. al., 2003), Cohen's K-coefficient (Jakobsson & Westergren, 2005), Kendall W (Meijering et. al., 2013;

(2014) recommendation to use "more than one statistical measures in order to assess the consensus", we used Hackett et. al.'s (2006) consensus definition. As a result, consensus is based on three of the most basic statistical measures, namely percentage of agreement, median (MDN) and interquartile range (IQR).

3.4.3.3. Percentage of agreement

The most common definition for consensus (Diamond et. al., 2014; Mukherjee et al., 2015) in Delphi studies is percentage of agreement, a measure associated with "ease of computation, understandability and ease of communication"(Polit et. al., 2007: 462). Given that consensus implies a 100% agreement among the members of the panel, whereby all experts rate the same issue in exactly the same way, consensus in the theoretical sense of the word is rarely reached in practice (Keeney et. al., 2006; Meijering et. al., 2013). As a result, Delphi studies, including our study, tend to apply a more practical interpretation of the concept by relating it to the less strict concept of 'agreement' (Meijering et. al. 2013). Indeed, Polit et. al. indicate that "when there are more than five experts, there can be a modest amount of disagreement" (2007: 460). Moreover, von der Gracht stipulates that "the determination of consensus by a certain level of agreement is particularly meaningful if nominal scales or Likert scales are used for the degree of agreement" (2012: 1529-1530), as it is the case in this study.

In line with other Delphi studies (e.g. Hackett et. al., 2006; Lange et. al. 2020), we transformed the five-point Likert scale into a three-point scale for analysis purposes. Panelists that 'agreed' or 'totally agreed' with the issue were compiled in an overarching 'agreement' category, while panelists that 'disagreed' or 'totally disagreed' with the issue were compiled in an overarching 'disagreement' category (Vogel et. al., 2019). The same principle applied to the star-rating, where the panelists that rated the practice 'four stars' or 'five stars' were compiled in an overarching 'good practice' category, while panelists that rated the practice 'one star' or 'two stars' were compiled in the overarching 'bad practice' category. Panelists that 'neither disagreed nor agreed' with the issue or that rated the practice 'three stars' were considered in the 'neutral' category.

It was argued before that "when there are more than five experts, there can be a modest amount of disagreement" (Polit et. al., 2007: 460). Still, the question remains how large the 'modest amount of disagreement' may at most be to speak of consensus. Otherwise put, "what percentage agreement would a researcher accept as synonymous with consensus" (Keeney et. al., 2006: 210)? Like many other guidelines on the Delphi procedure, guidelines on the threshold percentage of agreement that proxies consensus differ from study to study. According to Hasson et. al. (2000), Chuenjitwongsa (2017) and Keeney et. al. (2006), the threshold value can range from 51% to 80%, whereby the latter indicate that the decision should depend on the importance of the research project[16]. Okoli & Pawlowski (2004) and Christie & Barela (2005) use the lowest percentage of agreement, applying 'more than 50%' as cut-off point. Likewise, Giannaro & Zervas (2014) and Padayachee (2016) lean towards the lower limit of the range with a threshold value of 51% and 55% respectively. Rayens & Hahn (2000) situate in between with a threshold value of 'more than 60%', while Raskin (1994) and Vogel et. al. (2019) move towards the upper limit of the range with 70% and 'more than 70%' respectively. Polit et. al.'s recommended percentage of agreement is even higher, indicating that "any I-CVI[17] greater than .78 would fall into the range considered excellent, regardless of the number of experts" (2007: 466).

Okoli & Pawlowski, 2004; Skulmoski et. al., 2007; Schmidt, 1997), Kendall T (Schmidt, 1997), McNamar test (Okoli & Pawlowski, 2004) or Spearman's rank order correlation (Jacobssen & Westergren, 2005; Lange et. al., 2020).

[16] Keeney et. al. for instance indicate that "if it were a life and death issue such as whether or not to switch off a respirator in an intensive care unit, a 100% consensus level may be desirable. Alternatively, if the topic was related to the selection of a new nurses' uniform, a consensus of 51% may be acceptable" (2006: 210).

[17] See footnote 15

In our study, a percentage of agreement of 75% agreement is used to determine consensus (see infra table 5). While Keeney et. al. (2006) intuitively suggested 75% to be the minimal cut-off point, Barrios et. al. (2021) gave a scientific rationale to use it as a threshold value. Aiming to "examine the influence of controlled feedback on opinion change between two Delphi rounds and how it may favor or hinder the reaching of consensus among participants" (Barrios et. al., 2021: 2), they found that the "recommended threshold based on [their] results would be 75% agreement" (ibid: 8). Polit et. al. (2007) too argue that a percentage of agreement of 75% is suitable for an expert panel of at least 16 people (as is the case here), as it reduces the risk of chance agreement. Additionally, according to Diamond et. al. (2014), Mukherjee et al. (2015), Foth et. al. (2016) and Lange et. al. (2020), the most common threshold percentage used in Delphi studies is 75%.

To conclude, when discussing percentage of agreement, a distinction should be made between agreement with the issue and agreement with each other (Keeney et. al., 2006). In other words, agreement with each other "can be either agreement or disagreement with a statement" (von der Gracht, 2012: 1530). The emphasis in this study is on agreement with each other in the form of agreement with the issues, spending relatively less attention on agreement with each other in the form of disagreement with the issues. As a result, the percentage of agreement for each issue[18] presented in round 2 "is computed as the number of experts giving a rating of either [four] or [five][19], divided by the number of experts—that is, the proportion in agreement about relevance" (Polit et. al., 2007: 460).

3.4.3.2 Median

Apart from the percentage of agreement, also measures of central tendency can be used to determine consensus (Hasson et. al., 2000; Hsu & Sandford, 2007; Rayens & Hahn, 2000; von der Gracht, 2012). Reference is often made to summary statistics like the mean and the median (Barrios et. al., 2021; Keeney et. al., 2006; Kozak & Iefremova, 2014; Rowe & Wright, 2001; Steurer, 2011), and sometimes also the mode (Giannarou & Zervas, 2014; Stevenson, 2010). Some studies (suggest to) solely use the mean (e.g. Gossler et. al., 2019; Okoli & Pawlowski, 2004; Rayens & Hahn, 2000), whereas other studies (suggest to) solely use the median (e.g. Landeta, 2006; Raskin, 1994; Stone Fish & Busby, 2005; van de Linde & van der Duin, 2011). In this study, preference is given to the median (MDN) over the mean because Hsu & Sandford (2007) indicate that the use of the median is recommended by literature when using Likert-type questions. Moreover, von der Gracht explains the choice for median rather than mean as follows:

> "The fact that the mean is solely valid with interval/ratio data needs to be accounted for. In many Delphi studies, the mean is calculated without considering that the scales used are actually ordinal scales. (…). The general understanding is that Likert data is similar to that of an interval scale and that the degree of resultant measurement error is not significant. However, Argyrous stresses that the calculation of the mean for ordinal data is, strictly speaking, not a correct procedure" (2012: 1530)

Consequently, it is argued that the median is a better fit than the mean to measure central tendency in our study. The median represents the value that separates the upper half of the data from the lower half of the data and can be found by listing the data in order from smallest to greatest and selecting the middle number (Stone Fish & Busby, 2005).

[18] Polit et. al. (2007) refer to percentage of agreement as the content validity index (CVI), and to the percentage of agreement for each individual issue as the item-level content validity index (I-CVI).

[19] Polit et. al. (2007) use a 4-point scale, meaning they accumulate the number of experts rating the issue 3 or 4. Since our study uses a 5-point Likert scale, we accumulate the number of experts rating the issue 4 or 5.

3.4.3.3 Interquartile range

Next to the percentage of agreement and the median, also a measure of dispersion can be used to determine consensus (Hasson et. al., 2000; Hsu & Sandford, 2007; Rayens & Hahn, 2000; von der Gracht, 2012). With respect to dispersion, reference is often made to summary statistics like the interquartile range and the standard deviation (Giannarou & Zervas, 2014; Hasson et. al., 2000; Hsu & Sandford, 2007; Steurer, 2011; Stevenson, 2010). While some studies (suggest to) solely use the interquartile range (e.g. Landeta, 2006[20]; Kozak & Iefremova, 2014; Stone Fish & Busby, 2005), other studies (suggest to) solely use the standard deviation (e.g. Christie & Barela, 2005; Chuenjitwongsa, 2017).

Here, preference is given to the interquartile range (IQR) because, similar to the mean, the standard deviation should not be applied to ordinal data (Meijering et. al. 2013). According to Schmidt "there are no fixed intervals between ranks and no absolute reference point to calibrate ranks between panelists. Providing such data to the experts, or using it in research reports, is misleading" (1997: 771). In contrast, the interquartile range is "generally accepted as an objective and rigorous way of determining consensus" (von der Gracht, 2012: 1530).

Consequently, it is argued that the interquartile range is a better fit than the standard deviation as dispersion measure. Stone Fish & Busby explain the computation of the interquartile range as follows:

> "Interquartile ranges are calculated by taking half the difference between the "upper quartile," or the point in the distribution below which 75% of the cases lie (the 75th percentile), and the "lower quartile," the point below which 25% of the cases lie (the 25th percentile). This type of statistic provides information about the range of scores that lie in the middle 50% of the cases, and in doing so provides information about the consensus of response on a particular item" (2005: 247).

3.4.3.4. Consensus: categorization of issues

In view of the foregoing, each individual issue could be assigned to a certain category on the basis of the three consensus measures. In contrast to Hackett et. al. (2006), who differentiate four categories[21], we opted to divide every list of issues in three categories, namely high-rated, medium-rated and low-rated issues. Regarding percentage of agreement, 75% agreement was used as cut-off point for the high-rated issues (Barrios et. al., 2021; Diamond et. al., 2014; Foth et. al., 2016; Lange et. al., 2020; Mukherjee et al., 2015), while 51% agreement was used as threshold value for the medium-rated issues (Christie & Barela, 2005; Giannaro & Zervas, 2014; Okoli & Pawlowski, 2004). With respect to central tendency, a median of at least four was needed to assign the issue to the high-rated or medium-rated category, with a median below four resulting in a low-rated categorization (Hackett et. al., 2006). Regarding dispersion, to conclude, an interquartile range of at most one was used as cut-off point for the high-rated category, given that "an IQR of 1 or less is usually found to be a suitable consensus indicator for 4- or 5-unit scales" (von der Gracht, 2012: 1531). An interquartile range of two was the threshold value for the medium-rated category, whereas issues with an interquartile range above two were assigned to the low-rated category (Hackett et. al., 2006).

[20] Landeta (2006) refers to the relative interquartile range (i.e. the interquartile range divided by the mean).
[21] These four categories are 'essential', 'desirable', 'additional' and 'not indicated' (Hackett et. al., 2006: 148).

Table 5 summarizes the reasoning behind assigning each issue to a specific category. Firstly, proposed red flags/difficulties/practices that were rated 'four' or higher by at least 75% of the panel, that had a median score of 'four' or higher **and** that had an interquartile range of at most one were assigned to the high-rated category. Secondly, proposed red flags/difficulties/practices that were rated 'four' or higher by between 74% and 51% of the panel, that had a median score of 'four' or higher **and** that had an interquartile range of at most two were assigned to the medium-rated category. Finally, proposed red flags/difficulties/practices that were rated 'four' or higher by at most 50% of the panel, that had a median score of less than 'four' **or** that had an interquartile range of more than two were assigned to the low-rated category.

Table 5: *Criteria to categorize the issues*

Criterium	High-rated	Medium-rated	Low-rated
Percentage of agreement	At least 75% of the panel • Agrees (4) or strongly agrees (5) with the issue • Rates the issue 4 or 5 stars **AND**	Between 74% and 51% of the panel: • Agrees (4) or strongly agrees (5) with the issue • Rates the issue 4 or 5 stars **AND**	50% or less of the panel: • Agrees (4) or strongly agrees (5) with the issue • Rates the issue 4 or 5 stars **OR**
Central tendency *(Median)*	The median is at least 4 **AND**	The median is at least 4 **AND**	The median is less than 4 **OR**
Dispersion *(Interquartile range)*	IQR is at most 1	IQR is at most 2	IQR is higher than 2

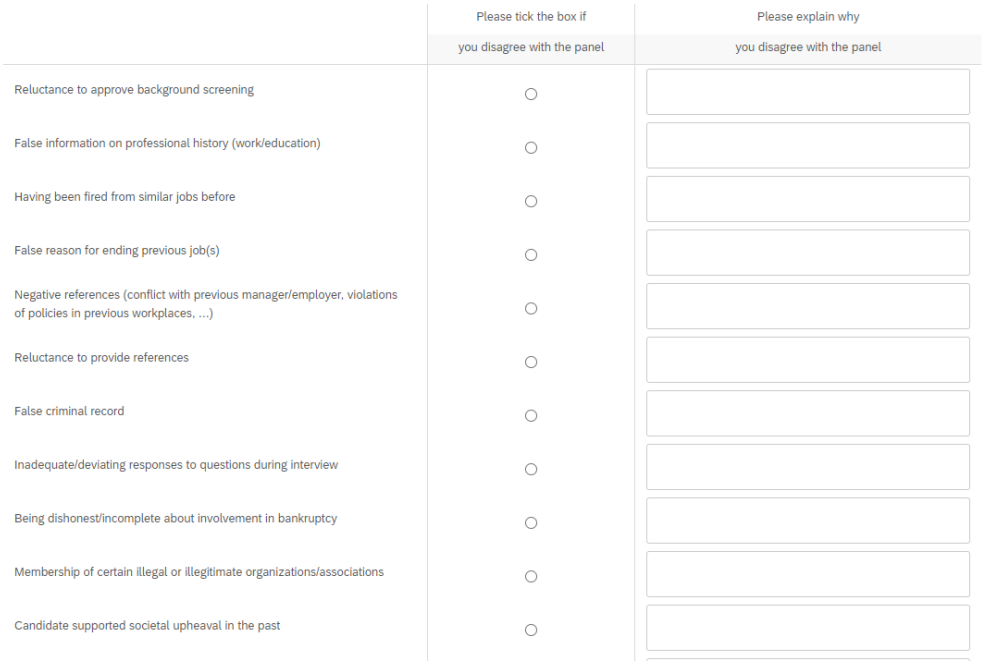
3.4.4. Round 3

Round three, to conclude, corresponds with the refinement phase of the study (Padayachee, 2016). One last time, panelists get the opportunity to reconsider their own opinion in view of the collective expert opinion. The questionnaire of round 3 is based upon the analysis of the results of round 2. In contrast to the analysis of round 1, we did not manually analyze the data of round 2 but used SPSS and Excel. As recommended by Diamond et. al. (2014), who indicate that "clear criteria for dropping or combining items should also be specified based on the level of agreement or disagreement with individual items", we used the categorization to reduce the extensive lists of issues handled in round 2 to a more manageable size for round 3.

On the basis of the categorization, round 3 could go two ways. On the one hand, we could dig deeper into the issues on which consensus was reached in round 2 (i.e. high-rated issues), like Okoli & Pawlowksi (2014) and Padayachee (2016). On the other hand, we could explore the issues on which no consensus was reached in round 2 (i.e. medium-rated and low-rated issues), like Rayens & Hahn (2000), Christie & Barela (2005) and van de Linde & van der Duin (2011). Given that the main emphasis in this study is on consensus in the form of agreement with the issues, we followed the example of Okoli & Pawlowski (2004) and Padayachee (2016) and solely concentrated on the issues in the high-rated category, leaving aside the medium-rated and low-rated categories.

While the main goal of the second round was to measure the degree of consensus between the panelists in the form of agreement with the issues, the goal here is to check to what extent each individual expert agreed with the panel's list of high-rated issues. Figure 4 shows that per question, the panel is provided with a list of the issues assigned to the high-rated category, whereby each member of the panel is asked to select the issue if he or she disagreed with the panel's decision to assign the issue to the high-rated category and asked to explain his or her reasoning behind that disagreement. The questionnaire of round 3 also consists of questions regarding the characteristics of the panel (see supra table 2), as well as questions gauging the panelists' evaluation of the Delphi technique (Raskin, 1994; Van Doldereren et. al., 2017), both in general as with respect to the present study (see infra 4.15).

Figure 4: *Questionnaire design round 3*



3.5. Methodological rigor

It is often said that "in its design and use Delphi is more of an art than a science" (Linestone & Turoff, 2002: 3) because "it is impossible to eliminate all problems associated with Delphi" (ibid, 2002: 7). It is true that due to the flexibility of the research design of the Delphi technique, "identifying and gauging methodological rigour for the Delphi technique remains elusive" (Hasson & Keeney, 2011: 1695), a criticism that applies to other consensus methods as well (Foth et. al., 2016).

As a result, a distinction can be made between Delphi purists and Delphi cynics (Keeney et. al., 2006; Hasson & Keeney, 2011), or believers and non-believers of the research method. Non-believers will argue that "expert opinion is considered as the lowest level in the hierarchy of available evidence" (Foth et. al., 2016: 119) and that "it is the least-confident individuals who change their estimates the most over rounds, rather than the least expert" (Rowe & Wright, 2001: 140). Believers, on the other hand, will argue that experts judgements are a "valuable and underrated source of knowledge" (Steurer, 2011: 959) and that "panel members change their minds and move towards consensus because they see that someone else has identified a more relevant issue that they had not thought of" (Keeney et. al., 2006: 210).

Even though we are closer to the believers of the Delphi technique than to the non-believers, throughout this report we repeatedly criticized the lack of methodological standardization of the technique that has led to a proliferation of applications of the method, and emphasized the need for universal guidance. Still, we do not want to go as far as throwing away the baby with the bathwater. The fact that the technique requires methodological standardization does not alter the fact that "the Delphi technique is widely accepted as a research technique today and [that] its value has been scientifically and practically proven" (von der Gracht, 2012: 1526). Landeta too emphasizes that "the scientific community has accepted this [Delphi] technique as another research technique" (Landeta, 2006: 471)

Still, it does not imply that every Delphi study meets the quality requirements. Researchers tend to underestimate the workload related to the Delphi technique (Keeney et. al., 2006), which leads to poor applications of the method (Rowe & Wright, 2001). This criticism is echoed by Turoff who indicates that "the Delphi concept seems so simple that many people have thought it an easy thing to do. Consequently there have probably been more poorly done Delphis than ones that have been well done." (2002: 89). To maximize the quality of our Delphi study, we tried to meet the four requirements of trustworthiness of qualitative research (i.e. credibility, dependability, confirmability and transferability) as much as possible (Gossler et. al., 2019). According to Hasson & Keeney,

> "there are four main strategies to establish trustworthiness credibility, dependability, confirmability and transferability. Engles and Kennedy suggested credibility of a Delphi can be enhanced by ongoing iteration and feedback given to panellists, which can be viewed as member checks and by undertaking additional research methods. Cornick proposed that dependability can be achieved, by including a range and representative sample of experts in a Delphi study. Confirmability can be assessed by maintaining a detailed description of the Delphi collection and analysis process, whilst transferability can be established through the use of verification of the applicability of Delphi findings" (Hasson & Keeney, 2011: 1700).

It is argued that this Delphi study to a large extent meets this trustworthiness criteria for the following reasons:

- Regarding *credibility*, the Delphi study consisted of three iterations whereby the panel was provided with feedback, thereby applying the suggested member check.

- Concerning *dependability*, we believe we composed a multidisciplinary panel of experts that covers the insider threat problem from a range of perspectives. Moreover, the fact that the majority of the experts agreed to reveal their participation in the panel (see supra table 1) provides the reader with additional information to interpret the dependability of our research results (Foth et. al., 2016; Schmidt, 1997).

- With respect to *confirmability*, "a clear decision trail of all key theoretical, methodological and analytical decisions made in the research from beginning to end" (Skulmoski et. al., 2007: 11) was provided in the research design section (section 3 of this study). Moreover, we not only took into account the methodological checklist outlined by Hasson et al. (2000), but also met the key methodological criteria outlined by Diamond et. al. (2014), thoroughly explaining the study objective, selection of participants, consensus definition and the Delphi process of the study.

- Regarding *transferability*, to conclude, it should be clear that the results in the present study "provide a snapshot of expert opinion at a specific moment in time" (Gossler et. al., 2019: 447), which implies limitations with respect to the generalizability of the results (Giannarou & Zervas, 2014; Skulmoski et. al., 2007). To validate the outcomes of the Delphi study, it is recommended to do a follow-up study (Keeney et. al., 2006), complementing the Delphi technique with other research methods like literature study (Mukherjee et. al., 2015; Raskin, 1994), focus groups (Gossler et. al., 2019; Hasson & Keeney, 2011; van de Linde & van der Duin, 2011) or vignette studies exploring insider threat scenarios (Grime & Wright, 2016; Stevenson, 2010; von der Gracht, 2012). Another possibility to verify the validity of the research output is to replicate the Delphi study, either by providing the exact same panel with the same questionnaire at a different moment in time (for instance a year later) or by composing a new panel with similar characteristics and comparing the results from those two groups (Hasson & Keeney, 2011). Also measurement of post-group consensus (von der Gracht, 2012), whereby the panel is presented with the results of the Delphi study and asked to what extent they agree with the results, can be used as a verification mechanism. In this report, validation is based upon a comparison of the results with the insights found in the insider threat literature, and it is our intention to further verify the Delphi results by supplementing this Delphi study with additional follow-up research.

4. Results

The results of the study are outlined below. In contrast to Hasson et. al.'s (2000) recommendation to report the results of each round of the study separately, we prefer to use the theoretical framework as a guide to report the results of the study, as illustrated in table 6.

Table 6: *Categorization of issues per question*

Theoretical framework	**Content of the question**	**High-rated Issues**		**Medium-rated issues**		**Low-rated issues**		**Total number of issues**
Stage	*Issue type*	*Count*	*%*	*Count*	*%*	*Count*	*%*	*Count*
I. Recruitment	Red flags	22	39,29%	12	21,43%	22	39,29%	56
	Good practices	15	36,59%	12	29,27%	14	34,15%	41
	Difficulties	10	29,41%	14	41,18%	10	29,41%	34
II. Organizational Socialization	Good practices	17	34,69%	19	38,78%	13	26,53%	49
III. Observation	Red flags	27	36,99%	25	34,25%	21	28,77%	73
	Good practices	20	33,90%	21	35,59%	18	30,51%	59
	Difficulties	10	32,26%	13	41,94%	8	25,81%	31
IV. Investigation	Good practices	11	32,35%	15	44,12%	8	23,53%	34
V. Anticipation	Good practices	4	10,81%	10	27,03%	23	62,16%	37
VI. Damage Limitation & VII. Reconstruction	Good practices	21	42,86%	18	36,73%	10	20,41%	49
VIII. Deliberation	Good practices	8	42,11%	7	36,84%	4	21,05%	19
IX. Termination	Good practices	16	50,00%	8	25,00%	8	25,00%	32
X. False positives	Good practices	9	56,25%	6	37,50%	1	6,25%	16
Formal insider threat mitigation team*								
Total		190	35,85%	180	33,96%	160	30,19%	530

*The panel was asked a dichotomous question (yes/no).

Table 6 shows that the manual coding of the information provided by the panel in round 1 resulted in a total of 530 issues that were presented to the panel in round 2. It simultaneously displays the quantitative analysis of round 2, illustrating that the 530 issues were more or less equally divided between the high-rated, medium-rated and low-rated categories, with 36% of the issues rated high, 34% rated medium and 30% rated low.

Noteworthy is that in comparison with the other stages of the framework, the total number of practices with respect to deliberation and false positives was relatively scarce, with only 19 and 16 suggested practices respectively. Notwithstanding the limited number of proposed practices, the panel assigned a high number of these suggested practices to the high-rated category. In general, the proportion of high-rated issues at the stages of the framework that relate to the aftermath of an insider threat incident was higher (between 40% and 50%) than those relating to the stages preceding an insider threat incident (between 30% and 40%). The issues related to good practices to anticipate an imminent insider threat incident were a negative outlier in this respect with only four out of 37 suggested practices (11%) that received a high rating.

To avoid the "danger of placing too much reliance upon the final results" (Keeney et. al., 2006: 210), we do not want to solely focus on round 3 of the study and insist on presenting the results of round 2 in its entirety. In this way, the reader is informed on the panel's rating of all 530 issues. Still, an in-depth discussion of every single issue would lead us too far. Therefore, in the remainder of the report each step of the framework is discussed by on the one hand providing the reader with summary tables of the categorization of all issues for that particular step, and on the other hand zooming in on the results of round 2 that we find noteworthy or the high-rated practices that were subject to discussion in round 3 of the study, with quotes of panelists appearing in italics. While some of the nuances put forward in round 3 are discussed in the text, others are discussed in a footnote.

4.1. Recruitment - Red flags

The first question related to the recruitment stage, asking the panelists to what extent they agree or disagree to treat the listed issues as a red flag during the recruitment of new insiders. Tables 7, 8 and 9 respectively show the red flags that receive a high-, medium- and low rating from the panel.

Table 7: *High-rated red flags during recruitment*

High-rated red flags	**% 4 or 5**	**Median**	**Interquartile Range**
False information on professional history (work/education)	100,00%	5	0,75
Membership of certain illegal or illegitimate organizations/associations	100,00%	5	1
False reason for ending previous job(s)	95,83%	5	1
Current or previous extremist ideology	95,83%	5	1
Negative advice following security clearance screening by government authorities	95,83%	5	1
Reluctance to approve background screening	95,83%	4	1
False criminal record	91,67%	5	0
Conflict of interest	91,67%	4	0
Low score on integrity	91,67%	4	1
Gambling addiction	87,50%	5	1
Indiscretion	87,50%	4	0,75
Current or previous interpersonal violence (harm to self or others)	87,50%	4	0,75
Being dishonest/incomplete about involvement in bankruptcy	87,50%	4	1
Drug addiction	87,50%	4	1
Alcohol addiction	87,50%	4	1
Manipulative nature	83,33%	4	0
Having been fired from similar jobs before	79,17%	4	0,75
Negative references (conflict with previous manager/employer, violations of policies in previous workplaces, …)	79,17%	4	1
Maladaptive behaviors in current or previous affiliations outside workplace (school, church,..)	79,17%	4	0
Reluctance to provide references	79,17%	4	1
Candidate supported societal upheaval in the past	79,17%	4	1
Inadequate/deviating responses to questions during interview	75,00%	4	0,75

Table 7 shows that issues appearing in the high-rated category for instance relate to different kinds of falsifications, like false information on professional history, false reasons for ending previous job(s) or false criminal records. Related to falsifications is low integrity, which is also perceived by the panel as a potential red flag. Likewise, the panel considers addictions to drugs, alcohol and gambling to be factors that may point to insider threat. The same applies to current or previous affinity with extremist ideology or membership of illegal or illegitimate organizations, as well as to negative advice concerning the candidate's application, either stemming from the candidate's references or following a security clearance screening by government authorities. The provision of inadequate or deviating responses to questions asked during the job interview falls just above the threshold of the high-rated category and is therefore too considered to be a potential red flag of insider threat during recruitment.

In round 3 of the study, several high-rated issues were put into perspective. Six panelists indicated that considering dismissal at a similar job a potential red flag of intentional misconduct largely depends on the reason behind that dismissal, as dismissal can also be due to other reasons like performance issues, incompetence or economic reasons. Additionally, six panelists argued that support for societal upheaval in the past is only considered problematic when it happened in the recent past and/or when the theme of the activism was related to the insider's function. A similar argument is used by three panelists who believe the context of the interpersonal violence determines whether it has to be regarded as a red flag, or by one member of the panel who urged to evaluate maladaptive behaviors in current or previous affiliations outside the workplace on a case by case approach taking into account the context of the maladaptive behavior.

Also the suspicion on applicants that show a unresponsive attitude during the recruitment process, either by showing reluctance to approve background screening or reluctance to provide references, was nuanced. Concerning the former, one panelist urged to make "*a distinction between reluctance, especially if the background screening in question is unusually invasive and inadequately justified, as opposed to outright refusal to participate in any background screening whatsoever"*. Concerning the latter, one panelist pointed out that the applicant might want to keep his application for a new job secret for his current employer. Related to the relativization of unresponsiveness is one panelist's stance on the relevance of dishonesty or incompleteness about involvement in bankruptcy, arguing that withholding this information can originate from shame rather than from bad faith[22].

Moreover, three panelists argued that 'conflict of interest' and 'indiscretion' were too ambiguously worded and needed further clarification, whereas one expert considered manipulative nature to be "*highly subjective, hence open to inconsistent and highly variable interpretation*". One panelist echoed this remark as a general concern of detection of red flags, indicating that apart from the red flags related to falsification, the high-rated potential red flags *"appear to allow for highly subjective interpretation, which could lead to unreliable determinations. People are fallible creatures, and not all fallible creatures turn into insider threats by virtue of having made reversible mistakes"*. In relation to this subjective interpretation, one panelist wrote the following comment in the context of round 2 of the study we find noteworthy to share: "*the content of the open position is important (a conviction for driving under influence may be relevant for a chauffeur but less for a office clerk). All the information has to be contextualized (some behavior can be accepted for a youngster, schoolboy/girl, but not for an adult)*". To conclude, two panelists emphasized the difference in strength of the red flags, whereas one panelist argued that "*the biggest 'red flag' is a combination of multiple of these 'red flags'*".

[22] Two panel members did not see bankruptcy as such as a potential red flag, with one expert arguing that "*Bankruptcy does not have a direct logical connection to individual insider behaviors, as such*" and the other one arguing that bankruptcy can be a sign of entrepreneurship.

Table 8: *Medium-rated red flags during recruitment*

Medium-rated red flags	% 4 or 5	Median	Interquartile Range
Unexplained periods of unemployment	70,83%	4	1
Unclear reason for ending previous job(s)	70,83%	4	1
Incomplete information on professional history (work/education)	66,67%	4	1
Inappropriate social media footprint	66,67%	4	1
Current or previous anger management issues	66,67%	4	1
No background information available for the candidate	66,67%	4	1,75
Non-blanco criminal record	62,50%	4	1
Illogical responses to questions during interview	62,50%	4	1
Lack of financial stability	62,50%	4	1
Irrelevant/sensitive questions asked by candidate during interview	58,33%	4	1
High score on narcissism	58,33%	4	1
High score on immaturity	54,17%	4	1

Table 9: *Low-rated red flags during recruitment*

Low-rated red flags	% 4 or 5	Median	Interquartile Range
Illogical motivation why candidate wants to work for the organization	50,00%	3,5	1
High score on arrogance	50,00%	3,5	1
Social network risks (like family, friends or foreign contacts)*	45,83%	3	1
Inability to receive constructive criticism	45,83%	3	1
Cold applications (without open/announced vacancy) for critical positions	37,50%	3	2
Low score on conscientiousness	33,33%	3	1,75
Abnormal educational path (lot of courses, courses abroad, courses not completed/stopped abruptly, ...)*	29,17%	3	1
High frequency of moves between employers (job-hopping)	29,17%	3	2
Mental health issues (like depression)	29,17%	3	2
No clear motivation why candidate wants to work for the organization	25,00%	3	0,75
Instable relationship status (frequent different partners, divorce, ...)*	25,00%	3	1,5
Previous employment for a competitor	25,00%	3	1,75
Low score on resilience	16,67%	3	0,75
Discrepancy between educational and professional career path	16,67%	3	1
Father-deficiency (abusive or absent father)	16,67%	3	1
Low score on friendliness	16,67%	3	1
Low score on humility	16,67%	3	1
Excessive social media footprint	12,50%	3	1
Multiple citizenship	12,50%	3	1
History of intensive travel	8,33%	3	1
Physical health issues	8,33%	2	1
No social media footprint	0,00%	2	1

Whereas falsifications are rated high by the panel, incompleteness of information, like incomplete information on professional history, unclear reasons for ending previous job(s) or unexplained periods of employment, is rated medium by the panel, being considered a potential red flag by more than two thirds of the panel. Providing illogical responses to questions asked during the job interview, as well as asking irrelevant or sensitive questions during the job interview, too receive a medium rating from the panel, with respectively 63% and 58% of the panel perceiving it as a potential red flag. Other issues that can be found in the group that receives a medium rating are for instance the possession of a non-blanco criminal record or current or previous anger management issues.

Issues appearing in the low-rated category, on the other hand, are for example previous employment for a competitor, job-hopping and applying for critical positions without an announced vacancy, with less than 40% of the panelists considering it a factor that may point to insider threat. Also abnormal education paths or discrepancies between educational and career path are much less perceived as potential red flags.

Furthermore, it is noteworthy that personality characteristics other than low score on integrity and manipulative nature are either rated medium by the panel, like narcissism and immaturity, or rated low, like arrogance and lack of humility, consciousness or friendliness. Also the applicant's social media footprint is discussed by the panel, whereby an inappropriate footprint is rated relatively higher (medium-rated) than an excessive or absent footprint (low-rated), with none of the experts considering absence of a social media footprint a potential indicator of insider threat.

A bit to our surprise, the panel gave relatively little attention to the applicant's motivation to work for the organization, with an illogical motivation and absence of a clear motivation respectively being perceived as a red flag by only half and a quarter of the panel. Likewise, apart from addictions, low priority is given to the applicant's personal problems, given that issues like lack of financial stability (medium-rated) and instable relationship status (low-rated) did not make the high-rated category. The same goes for mental health and physical health issues, which is perceived to be a potential red flag during recruitment by less than 30% and less than 10% of the panelists respectively, and other aspects related to the applicant's private life like social network risks and multiple citizenship, which also received a low rating from the panel. Nevertheless, in the literature (e.g. Shaw & Sellers, 2015; Noonan, 2018) it is argued that personal problems can be a possible breeding ground of insider threats, and also in our survey on insider threat awareness and behavior that was performed in 2021 among Belgian security officers (Reveraert & Sauer, 2021b), personal problems were among the top 5 underlying causes of insider threats (mentioned by 36% of the respondents).

4.2. Recruitment - Good practices

The second question too related to the recruitment stage, this time asking the panelists to rate practices to detect red flags during recruitment. Tables 10, 11 and 12 respectively show the practices that receive a high-, medium- and low rating from the panel.

Table 10: *High-rated practices to detect red flags during recruitment*

High-rated practices	% 4 or 5	Median	Interquartile Range
Take screening seriously instead of pro-forma	100,00%	5	0,75
Do an identity check	95,83%	5	0,75
Adopt a risk-based approach (adjust screening depending on the position)	95,83%	5	1
Be transparent to the candidate on the recruitment and screening process, including consequences for missing/false information	95,83%	5	1
Check criminal record	91,67%	5	0,75
Make a thorough screening procedure common practice	91,67%	5	1
Have a coherent list of non-acceptable convictions	91,67%	5	1
Verify CV	87,50%	5	1
Check open sources like the internet	87,50%	4	1
Check listed professional references (like previous employers/co-workers)	87,50%	4,5	1
Training and awareness of recruiters (investigative interviewing, insider threat indicators, ...)	83,33%	5	0,75
Follow-up on any issues raised by references	83,33%	5	1
Let trained interviewers conduct an in-depth interview with the candidate	83,33%	5	1
Let multiple actors within the organization decide upon a hire	79,17%	4	1
Verify every single credential (diplomas, licenses, professional certifications, ...)	79,17%	4	1

The good practice that the panel unanimously agrees upon is taking screening seriously instead of carrying it out pro-forma. Furthermore, the high-rated category contains practices that correspond with recommendations found in the insider threat literature (e.g. BaMaung et. al., 2018; Power & Forte, 2006), like verification of curriculum vitae (CV), credentials, identity and criminal record. One panelist however emphasized in round 3 that all checks should occur within the constraints of the applicable laws, whereas another one urged to not only check the criminal record, but also the civil record of the applicant.

Moreover, more than 90% of the panelists recommends to adopt a risk-based approach during recruitment, adjusting screening depending on the position of the applicant. Several panelists put extra emphasis on this practice, with one panelist already arguing in round 2 of the study that "*A risk based approach will dictate what's most important for a certain role*". In round 3 of the study, one panelist emphasized the importance of a risk-based approach with respect to several of the recommended practices, whereas two panelists highlighted it as a general comment. These panelists point to what the insider threat literature denotes the 'degree of insiderness' (Bishop et. al.,2009; Bishop et al., 2010; Probst et. al., 2010) whereby the group of insiders is viewed as a continuum of insiders that can be sorted on the basis of the scope and application area of the granted privilege to the organizational assets. Applicants whose privilege will consist of a large privilege (i.e. large amount of access to the organizational assets), or a privilege that will apply to the most important assets of the organization, pose a greater threat than applicants whose privilege will correspond with a small privilege (i.e. small amount of access to the organizational assets) or a privilege that will apply to less important assets, and should therefore be subject to a tougher screening procedure (George et. al., 2019). Our insider threat survey (Reveraert & Sauer, 2021b) however showed a lack of awareness of the 'degree of insiderness' among the respondents, given that more than half of the respondents declared to subject all employees to the same pre-employment and in-employment screening.

Furthermore, transparency about the recruitment and screening process, as well as letting multiple actors within the organization decide upon a hire, are put forward by the panel as valuable practices to detect red flags during recruitment. The same goes for control of open sources like internet in general and more specifically social media, though a check of social media falls just below the threshold of the high-rated category and was therefore rated medium. We know from the literature (Brown et. al., 2013; Elifoglu et. al., 2018) that social media can equally help to identify potential insider threat indicators, even though our insider threat awareness and behavior survey (Reveraert & Sauer, 2021b) showed that during recruitment only 60% of the organizations checks the non-work related social media profile of applicants that will have access to the organizational assets.

Our survey (Reveraert & Sauer, 2021b) also showed that 68% of the respondents indicated that their organization contacts the references that future employees provide on their CV. It can be deducted from the results of this Delphi study that checks with listed professional references (high-rated) (i.e. provided by the applicant) are more popular among the panelists than checks with non-listed references (i.e. not provided by the panelist) elicited from listed references (medium-rated), or checks with social network references like family and friends (low-rated). One panel member however questioned the reliability of professional references, indicating that "*it is often based on a deal: you leave and [I] promise to write a positive reference on you".* In relation to reference checks, the panel equally advises to follow-up on any issues raised by references.

To conclude, although a non-blanco criminal record was not necessarily perceived as factor that may point to insider threat, the panel nevertheless recommends organizations to have a coherent list of non-acceptable convictions. One panelist however questioned both the necessity and feasibility of this recommendation. Another high-rated practice that was criticized by one panelist in round 3 was training and awareness of recruiters, as the expert perceived this as "*tipping the balance between risk management and being overly invasive. This seems like it comes from the perspective of assuming everyone is a threat".* In line with this, one expert wondered who should be trained to conduct in-depth interviews with the candidates and what kind of training they should receive.

Table 11: *Medium-rated practices to detect red flags during recruitment*

Medium-rated practices	**% 4 or 5**	**Median**	**Interquartile Range**
Implement a government security clearance program if possible	70,83%	5	2
Check social media	70,83%	4	2
Use probationary periods	70,83%	4	2
Make clear that passing from probationary status is by no means automatic	66,67%	4	2
Check psychological or mental fitness for duty	62,50%	4	1
Check financial records	62,50%	4	1,75
Give the candidate a questionnaire with a lot of open questions	58,33%	4	1
Let candidates reflect on integrity dilemma cases	58,33%	4	1,75
Conduct an interview with the manager of the team the candidate will be assigned to	58,33%	4	2
Request only original documents of educational and professional paths (do not allow copies)	54,17%	4	1
Check non-listed references elicited from listed references	54,17%	4	2
Conduct an integrity interview	54,17%	4	2

Table 12: *Low-rated practices to detect red flags during recruitment*

Low-rated practices	**% 4 or 5**	**Median**	**Interquartile Range**
Request written documentation of educational and professional paths (allow copies)	62,50%	4	2,75
Check vulnerability for manipulation by a hostile party (social engineering)	54,17%	4	2,75
Use standard application forms for the recruitment process	50,00%	3,5	1,75
Conduct a drug screening	50,00%	3,5	3
Verify self-reported claims (like salary history)	45,83%	3	2
Outsource background screening	45,83%	3	2
Conduct an alcohol screening	45,83%	3	2,75
Check listed social network references (like friends and family)	45,83%	3	3
Ask personal letters of recommendation (no standard letters)	37,50%	3	3
Ask non work-related questions (job of partner, number of recent house moves, hobbies, ...)	37,50%	3	3
Use personality tests (like Hexaco)	33,33%	3	1
Conduct a group interview with the team the candidate will be assigned to	29,17%	2	3
Check with the desk clerk if the candidate was friendly	25,00%	3	1,75
Conduct a group interview with the managers of the teams that often interact with the team the candidate will be assigned to	20,83%	2,5	2

With respect to the remaining suggestions to detect red flags during recruitment, it is noteworthy that apart from checking social media also the implementation of a government security clearance program and the use of probation periods narrowly miss a high-rating. Furthermore, conducting an interview with the manager of the team the candidate will be assigned to (medium-rated) receives a relatively higher rating than performing group interviews with (managers of) the team(s) the applicant will be assigned to (low-rated), the latter being supported by less than one third of the panel. Other low-rated practices are outsourcing background screening and asking personal letters of recommendation.

In line with the results of the first question on red flags during recruitment, the panel gives relatively little importance to the applicant's private life, given that less than half of the panel recommends to ask non work-related questions during the recruitment process (low-rated). The same applies to the relatively moderate ratings of checking financial records and mental fitness for duty, which respectively correspond with the moderate priority the panel gave to lack of financial stability as a potential red flag and the low priority the panel gave to mental health issues as a potential indicator of insider threat.

In contrast to the results on red flags during recruitment, where addiction to drugs and alcohol were considered a high-rated potential red flag during recruitment, alcohol- and drug screenings are not considered to be high-rated practices to detect red flags. A possible explanation that was suggested by one of the panelists in round two of the study is that alcohol and drugs screenings are not commonly accepted recruitment tools in all countries, either for cultural or legal reasons. Likewise, a low score on integrity was perceived to be a potential red flag, whereas the ways to evaluate the candidate's integrity, like reflection on integrity dilemmas (medium-rated), conducting an integrity interview (medium-rated) or personality tests (low-rated), were not included in the high-rated category.

To conclude, the relatively low rating of the suggestion to check the applicant's vulnerability to social engineering goes against the findings of our insider threat awareness and behavior survey (Reveraert & Sauer, 2021b), given that social engineering was the number one type of insider threat that organizations worried about (mentioned by 45% of the respondents). A possible explanation for this is that the panel might perceive that it is relatively difficult to test vulnerability for social engineering during the recruitment process.

4.3. Recruitment - Difficulties

The final question with respect to the recruitment stage questions the panel on the difficulties to detect red flags during recruitment. Tables 13, 14 and 15 respectively show the difficulties that receive a high-, medium- and low rating from the panel.

Table 13: *High-rated difficulties to detect red flags during recruitment*

High-rated difficulties	% 4 or 5	Median	Interquartile Range
Lack of access to information (for instance foreign documentation)	95,83%	4	0
Veracity of information from listed and non-listed references is unclear	91,67%	4	0
Doubt about the accuracy of information of background screening	79,17%	4	0
Recruiters may have positive or negative biases/pre-conceived judgements	79,17%	4	0
It may not be possible to physically check with referees	79,17%	4	0
Resource limitations	79,17%	4	0,75
No willingness of previous employers to share needed information	79,17%	4	0,75
Background screening is not possible for all candidates	75,00%	4	0,75
Candidate may seek to conceal or misrepresent information	75,00%	4	0,75
Awareness and actions on insider threat are significantly dragging behind the actual threat	75,00%	4	0,75

According to the panel, the main difficulty to detect red flags during recruitment lies within gathering reliable information necessary to perform a background check. Although one panel member argued in round 3 of the study that every applicant can be subjected to a minimum of checks and another one indicated that "*access should be possible/provided if the candidate is applying for a sensitive position*", the majority of the panel believes that lack of access to information and unclarity about the accuracy of the information obtained hinders the detection of red flags during recruitment. Lack of access to information can for instance stem from the unwillingness of previous employers to share the needed information due to fear of lawsuits. Doubt about the accuracy of the information obtained can relate to information provided by the applicant, who may conceal or misrepresent information, as well as to information provided by (non-)listed references.

In addition to this information deficit, resource limitations were put forward as constraining the detection of red flags during recruitment. Furthermore, two panelists opposed in round 3 of the study that the detection of red flags during recruitment is restricted when awareness and actions on insider threat are significantly dragging behind the actual threat, rather perceiving it as an incentive to establish an insider threat awareness program within the organization. Moreover, one expert disputes the presence of recruiter biases, as organizations should ensure that recruiters receive the necessary training to remain objective during the recruitment process and should give clear instructions on possible conflicts of interest. To conclude, a difficulty that did not appear in the high-rated list of difficulties but that was suggested by one panelist was unclarity about legal restrictions.

Table 14: *Medium-rated difficulties to detect red flags during recruitment*

Medium-rated difficulties	% 4 or 5	Median	Interquartile Range
Recruitment staff is not appropriately qualified/trained to conduct thorough background screening	75,00%	4	1,5
Actual court cases are not mentioned on the extract of criminal record (only convictions)	75,00%	4	1,5
Technical advancements make forged documents difficult to detect	70,83%	4	1
Social media check of publicly available social media does not truly reflect the candidate's internet activity	70,83%	4	1
Not all sectors can use a government security clearance system	66,67%	4	1,75
If recruitment has been outsourced, it is difficult to confirm how extensive the screening has been	66,67%	4	1,75
Candidate may refuse permission for background screening	66,67%	4	2
Laws and regulations are too much focused on privacy	62,50%	4	1
Candidate may feel pressure to sufficiently demonstrate passion for the organization (hiding motivation or risks they bring)	58,33%	4	1
It is not clear on what base the authorized government gives a positive or negative security screening advice	58,33%	4	1
Authorities are behind in updating the extract of the criminal record	58,33%	4	1
Authorized government intelligence and security services are not equipped to conduct a proper government security screening	54,17%	4	1,75
Prohibition to access and use government databases	54,17%	4	2
Manager of team the candidate will be assigned to plays no substantive role in screening the candidate	54,17%	4	2

Table 15: *Low-rated difficulties to detect red flags during recruitment*

Low-rated difficulties	% 4 or 5	Median	Interquartile Range
Primary goal is to find efficient workers	50,00%	3,5	1
The hiring process becomes too time-intensive	50,00%	3,5	1
Lower level positions do not have to disclose certain issues (like gambling addiction)	50,00%	3,5	1,75
It is not allowed to keep a copy of the extract of the criminal record	50,00%	3,5	2
Bank confidentiality	45,83%	3	1
Government security clearance system takes too much time	45,83%	3	1
Difficult to evaluate whether recruitment policies are effectively defending against insider threats	45,83%	3	1
Inability to verify forbidden domains (religion, politics, ...) without explicit permission	45,83%	3	2
Candidate will feel some discomfort about the questions	41,67%	3	2
No intrusion methods can be used	29,17%	3	2

Regarding the medium-rated difficulties, it is noteworthy that lack of qualifications or training among recruitment staff falls just short of the high-rated category, with three quarters of the panel believing that the competence level of recruitment staff is generally speaking insufficient to perform adequate background screenings. The detection of forged documents, which has become difficult due to technological advancement, and the screening of public social media profiles, which do not truly reflect the candidate's internet activity, too narrowly miss the high-rated category, with 71% of the panel that regards it as a constraining factor.

Furthermore, while the lack of access to information was rated high by the panel, explanations for this lack of access, like the prohibition to access and use government databases and the over-emphasis of laws and regulations on privacy, score relatively lower (medium-rated). The same applies to the inability to verify forbidden domains (religion, politics, …) without explicit permission or to bank confidentiality, issues that are rated even lower by the panel (low-rated). However, one panelists emphasized in round 2 of the study that "*privacy rules are never too stringent. The employee needs protection as well*".

Also notable is that a number of medium-rated difficulties relate to the government security clearance system, like the inability for certain sectors to use the system, the fact that authorized government intelligence and security services are not equipped to conduct a proper security screening, or the fact that it is not clear on what base the authorized government gives a positive or negative advice. On the other hand, less than half of the panel believes that the government security clearance system takes too much time (low-rated).

Other practices assigned to the medium-rated category relate to the criminal record, with the panel referring to the fact that only convictions are mentioned on it instead of actual court cases (close to a high rating), as well as the fact that authorities are behind in updating the extract of the criminal record. Only half of the panel argued that the inability to keep a copy of the extract of the criminal record complicates the detection of red flags during recruitment (low-rated).

Other issues that put relatively less strain on the detection of red flags during recruitment are among other things the fact that the primary goal of organizations is to find efficient workers, the fact that the hiring process becomes too time-intensive or the fact that the applicant might feel some discomfort about the questions.

4.4. Organizational Socialization – Good practices

The next list of issues the panel was asked to rate concerned practices to make insiders aware of and willing to live up to the organization's expectations regarding appropriate conduct. Tables 16, 17 and 18 respectively show the practices that receive a high-, medium- and low rating from the panel.

Before elaborating on the results, it is noteworthy that one panelist argued in round 2 of the study that the list of practices suggested in the context of organizational socialization "*clearly shows that there is a gray zone between pure HR tools and programs and detection of insider threat"* and that *"Finding a good balance between both is essential*".

Table 16: *High-rated practices to socialize insiders to the organizational culture*

High-rated practices	**% 4 or 5**	**Median**	**Interquartile Range**
Have a clear code of conduct that undiscussable[23] states expectations regarding appropriate conduct	95,83%	5	0,75
Take appropriate measures if there are violations of the code of conduct	95,83%	5	1
Lead by example by senior leadership	91,67%	5	0
Lead by example by middle management	91,67%	5	0
Organize mandatory onboarding training that provides detailed information on expectations regarding appropriate conduct	91,67%	5	1
Clarify not only appropriate conduct, but also what conduct is considered as inappropriate (including reasons for termination)	91,67%	5	1
Create an open culture where employees can ask questions about integrity issues	91,67%	5	1
Employ a strong security culture within the organization so that expectations are reinforced through colleagues	91,67%	5	1
Orientate new employees to their unit and their role in the larger organization (ensure inclusion)	91,67%	4	1
Be transparent on control measures	87,50%	4	1
Make expectations concrete and achievable	83,33%	5	1
Installation of a point of contact for questions	83,33%	5	1
Build trust between supervisors and employees	83,33%	5	1
Foster a spirit of belonging (being part of the team)	83,33%	4,5	1
Have a welcome policy outlining the organization's history, mission, values, ...	79,17%	5	1
Show that you care about the employee	79,17%	5	1
Use the code of conduct and policies and procedures in case of detected issues	79,17%	5	1

[23] For reasons of clarity, one expert suggested to change 'undiscussable' with 'clearly'.

Regarding the high-rated practices of organizational socialization, in round 3 of the study one panelist drew attention to the overlap between the suggested practices which according to him or her leads to "*the impression that the newly hired employee is going to be bombarded by rules, codes, policies, and manuals*". As a result, the panelist recommends organizations to apply the Aristotelian method, characterized by precept, by habit and by demonstration. Or to put it in the words of the panelist:

> "(…) *avoid being heavy-handed with lectures and policy documents (precept) as the exclusive means of acculturation. Instead, provide foundational references for the employee (precept) and then proceed to immerse that employee in a work unit where the desired behaviors are on daily display (habit) and where managers and supervisors lead by example (demonstration)".*

The panel seems to agree with the suggestion to use the Aristotelian method, as the list of high-rated practices includes practices related to precept, habit and demonstration.

- With regard to *precept*, the list of high-rated practices includes the possession of a code of conduct in which concrete and achievable expectations regarding both appropriate and inappropriate conduct are explained. Moreover, the panel suggests to combine a welcome policy that outlines the organization's history, mission and values with mandatory onboarding training to provide the new insider more detailed information on the code of conduct at the start of the new insider's employment.

- Concerning *habit*, a number of cultural recommendations were given by the panel, like the creation of a strong security culture so that expectations are reinforced through colleagues, or the presence of an open culture where insiders can ask questions about integrity issues. In line with this is the recommendation to install a point of contact for questions on appropriate conduct, although one expert argued that "*formal channels are useful but informal channels may be more useful and should be protected by the company*".

- Regarding *demonstration*, the panel mentions the necessity to lead by example, both by senior leadership and middle management, while two thirds of the panel recommend the use of a mentor/buddy system (medium-rated).

Other high-rated practices apart from the Aristotelian method revolve around a supportive attitude towards the insider, whereby the organization orientates new insiders to their unit and their role in the larger organization, fosters a spirit of belonging, builds trust between supervisors and employees and shows care when needed. Furthermore, in similarity with transparency about the recruitment process, also transparency about control measures during employment is encouraged by the panel. To conclude, the panel advises organizations to use the code of conduct in case of detected issues, and to take appropriate measures if there are violations of the code of conduct.

Table 17: *Medium-rated practices to socialize insiders to the organizational culture*

Medium-rated practices	**% 4 or 5**	**Median**	**Interquartile Range**
Use positive reinforcement (reward appropriate conduct)	75,00%	5	1,75
Translate policy requirements in internal regulations or employee handbooks	75,00%	4	1,75
Recurrent company-wide awareness campaigns on expectations regarding appropriate conduct	75,00%	4	1,75
Make integrity part of the regular evaluation procedure by management	75,00%	4	1,75
Explain the code of conduct in more detail in policies and procedures	70,83%	4,5	2
Develop a small but clear document with 'golden rules'	70,83%	4	2
Casual/informal reminders on expectations during ongoing communications from line managers (like staff briefings)	70,83%	4	2
Underline open feedback culture and transparency	70,83%	4	2
Regular employee performance evaluation conducted by management	66,67%	5	2
Recurrent security awareness programs	66,67%	4,5	2
Use a mentor/buddy system	66,67%	4	1,75
Let employees accept policies and procedures in written	62,50%	4,5	2
Use a meaningful professional development process	62,50%	4	1,75
Visibility of integrity as a core value on corporate website/social media/recruitment campaigns	62,50%	4	2
Install a culture of social control and confidentiality	58,33%	4	1,75
Have an appeal process to resolve management-employee disputes before they fester	54,17%	4	1
Have compliance registers	54,17%	4	1
Communication of sanctions taken against misconduct by an employee	54,17%	4	1
Regular formal meeting with line manager to ensure employees are aware of expectations regarding appropriate conduct	54,17%	4	2

Table 18: *Low-rated practices to socialize insiders to the organizational culture*

Low-rated practices	**% 4 or 5**	**Median**	**Interquartile Range**
Create a culture of constructive dissent	62,50%	4	2,5
Enquire employees on a regular basis to get a feeling of general mood	50,00%	3,5	1
Team building events/days	50,00%	3,5	2
Embrace continuous improvement principles to rapidly respond to changing needs of the workforce	45,83%	3	1
Use peer or '360' evaluation	45,83%	3	1,75
Use intranet to communicate expectations regarding appropriate conduct	45,83%	3	2,5

Ask explicit consent for control	41,67%	3	1
Use negative reinforcement (punish inappropriate conduct)	41,67%	3	2,5
Phase in granting of access to more privileges and responsibilities based on performance	37,50%	3	1,75
Develop newsletters, email campaigns, posters, screen savers, with key rules regarding appropriate conduct	37,50%	3	2,75
Use game-design elements and game principles (Gamification)	29,17%	3	2
Use self-evaluation	25,00%	3	1,5
Foster friendly competition between work units	25,00%	3	1,75

Regarding medium-rated practices of organizational socialization, it is noteworthy that positive reinforcement falls just below the threshold of the high-rated category, thereby scoring significantly better than negative reinforcement, a practice that is rated relatively low by the panel. Additionally, notwithstanding the previously discussed concern of one of the panelists to place too much emphasis on acculturation via policy documents (i.e. precept), a number of initiatives to refine the code of conduct in additional documents, like policies and procedures, internal regulations, employee handbooks or 'golden rules', are close to a high rating. Letting employees accept policies and procedures in written is relatively less of a priority, being recommended by less than two thirds of the panel. Similarly, whereas transparency on control measures is encouraged, the panel does considers it less necessary to ask explicit consent to implement these control measures (low-rated).

Furthermore, except for recurrent company-wide awareness campaigns on the code of conduct, a practice that falls just short of the high-rated category, instruments to communicate the expectations outlined in the code of conduct, like the use of intranet, newsletters, email campaigns, posters and screen savers, receive a relatively low rating from the panel. The same applies to the usefulness of team building events, gamification or fostering friendly competition between work units, which the panel perceives as less appropriate practices for organizational socialization. Regarding bilateral communication on the code of conduct between employees and line managers, it is notable that informal reminders on expectations during ongoing communications from line managers are relatively more important than regular formal meetings.

When it comes to evaluating of the insider's affiliation with the organizational culture, the panel has relatively more confidence in evaluations conducted by management than in peer- or self-evaluations. Related to this is the panel's advice to make integrity part of the regular evaluation procedure by management, which is also close to a high rating from the panel. Ensuring visibility of integrity as a core value in public communication, to conclude, received a relatively moderate rating from the panel, with less than two thirds of the panel recommending it.

4.5. Observation - Red flags

Apart from the question related to red flags during recruitment, the panel was also asked to indicate to what extent they agree or disagree to treat issues as a red flag during employment. Tables 19, 20 and 21 respectively show the red flags that receive a high-, medium- and low rating from the panel.

Table 19: *High-rated red flags during employment*

High-rated red flags	% 4 or 5	Median	Interquartile Range
Attempts to remove sensitive data (physical and cyber methods)	100,00%	5	0
Participating in illegal activities	100,00%	5	0
Making threats against employer or other employees	100,00%	5	1
Warnings received from other employees, clients or third parties on the behavior of the employee	100,00%	4,5	1
Making or defending statements of extremist/radical point of view	100,00%	4,5	1
Unauthorized access attempts to systems or physical locations not necessary for the job	95,83%	5	1
Unnecessary copying of material (physical or digital)	95,83%	5	1
Abnormal cyber activities on- and off-site (for example large up/downloads)	95,83%	5	1
Vulnerability to blackmail	95,83%	5	1
Participating in manifestations of extreme organizations	95,83%	5	1
Signals of radicalization (like change in physical appearance)	95,83%	4	1
Unexplained wealth	95,83%	4	1
Negative security screening advice from government authorities	91,67%	5	1
Employee is not open to audits	91,67%	4	1
Unexplained irregularities in the accountancy of the organization	91,67%	4	1
Organizational culture of fear and silence	91,67%	4	1
Being flexible with ethics or morals[24]	87,50%	4	0
Employee pushes rules to see whether he/she can get away with it (boundary probing)	87,50%	4	0,75
Gambling	87,50%	4	0,75
Increase in organizational losses	83,33%	4	0
Drug abuse	83,33%	4	1
Alcohol abuse	83,33%	4	1
Remotely accessing systems at uncharacteristic hours	79,17%	4	1
Not complying to safety and (cyber)security policies and procedures	79,17%	4	1
Disgruntlement as a result of career disappointment	75,00%	4	0,75
Inappropriate communications (in person or online)	75,00%	4	0,75
Changes in lifestyle (new car, expensive clothes, ...)	75,00%	4	0,75

[24] One panelist argues that this "*Depends on agreed ethics and morals in the organisational culture*"

In line with the insider threat literature, the high-rated red flags during employment concern both individual and organizational factors (Greitzer et. al., 2012; Greitzer et. al., 2016), with the majority relating to the former. The most obvious warning signals that were unanimously accepted by the panel in round 2 of the study are situations when insiders make threats against their employer or co-workers, when organizations receive warnings from other stakeholders (e.g. employees, clients or third parties) about the behavior of the insider or when the insider participates in illegal activities. Other examples of potential early warnings during employment in round 2 that received a high-rating from more than 90% of the panel are attempts to remove sensitive data, unnecessary copying of material and unauthorized access attempts to systems or physical locations not necessary for the job.

In similarity with the list of red flags during recruitment (see supra 4.1), alcohol- and drug abuse, as well as gambling[25], are rated high. The same applies to affiliation with extremist organizations, expressed by insiders who make or defend statements of extremist/radical point of view, show signals of radicalization[26] or participate in manifestations of extreme organizations. The latter was however refined in round 3, as two panelists argued that it should only be considered problematic when the manifestations are in any way related to the insider's function within the organization.

Furthermore, the panel regards grievance as something the organization should be vigilant of, more specifically disgruntlement as a result of a career disappointment[27]. Vigilance for grievance is line with the insider threat literature that considers it one of the main motivators of insider threat (Greitzer et al., 2012; Randazzo et. al., 2005; Willison & Warkentin, 2013), as well as with the findings of our survey on insider threat awareness and behavior (Reveraert & Sauer, 2021b) whereby revenge out of disgruntlement with the organization was considered to be the second motivator of insider threats (44% of the respondents).

Another branch of high-rated red flags during employment relates to insiders that deviate from their normal or baseline behavior, which is equally in line with the insider threat literature (BaMaung et. al., 2018; Gelles, 2016; Shaw & Sellers, 2015). Unexplained wealth and changes in lifestyle[28] therefore receive a high rating from the panel, as well as abnormal cyber activities on- and off-side[29], boundary probing and lack of compliance with safety and security policies and procedures. One panelist however emphasized in round 3 that the "*interpretation of what is uncharacteristic or unnecessary should be set against the individual's role and norms, rather than the norms for the staff base as a whole*".

Also in round 3, one panelist shared the following general comment that relates to the interpretation of red flags:

> *"While all of these seem useful on the surface, some could be counterproductive depending on who makes the interpretation at issue. For example, who determines what is an "extreme point of view" as opposed to one that just happens to reflect a political disagreement? Also, who determines when a communication is inappropriate rather than just unpopular? For such red flags to provide useful value, there must be in place a means of assuring that the people making threat determinations are not abusing their discretion or asserting their personal or political preferences at the expense of the employee being assessed."*

[25] One panelist argued that only gambling abuse is problematic, as small scale gambling can be tolerated.
[26] One panelist argued that care needs to be taken not to discriminate when interpreting changes in physical appearance.
[27] One panelist believed that this is difficult to detect this kind of disgruntlement
[28] One panelist nuanced by stating that it depends on the change, indicating that the example of the new car was not convincing.
[29] One panelist wondered how the organization will observe this off-site considering privacy regulations.

One panelist echoed the concern regarding inappropriate communications. Other issues that were put into perspective during round 3 of the study are vulnerability to blackmail and negative security screening advice from government authorities. Concerning the former, one panelist thought it to be difficult to discover whether an insider is vulnerable to blackmail whereas another one viewed it rather as a trigger "*to 'harden' the employee*". Concerning the latter, one panelist argued that the reliability of the screening procedure has to be taken into account when evaluating the negative advice. To conclude, remotely accessing systems at uncharacteristic hours was put into perspective by one panelist who stated that the difficult circumstances of the COVID-19 pandemic have made unusual working hours normal rather than deviant behavior.

Even though the majority of the issues that receive a high rating from the panel relate to the insider, some of the issues are related to the organization, more particularly the presence of an organizational culture of fear and silence, of unexplained irregularities in the accountancy of the organization and increases in organizational losses. The latter two were however nuanced in round 3, with one panelist indicating that irregularities in the accountancy can have a variety of reasons and are not necessarily the result of intentional misconduct and two panelists applying the exact same reasoning with respect to increases in organizational losses.

Table 20: *Medium-rated red flags during employment*

Medium-rated red flags	**% 4 or 5**	**Median**	**Interquartile Range**
Sudden and unexplained change in performance	75,00%	4	1,75
Abnormal high absenteeism	70,83%	4	1
Directly expressing negative feelings towards employer/co-workers online	70,83%	4	1
Time pressure leading to unwanted shortcuts	70,83%	4	1
Red tape leading to unwanted shortcuts	70,83%	4	1
Unauthorized absence	70,83%	4	1,75
Impending termination of contract	70,83%	4	1,75
Working a lot of overtime (come early/stay late)	66,67%	4	1
Maladaptive behaviors outside workplace	66,67%	4	1
Repeatedly declining to allow others to serve as back-up for handling responsibilities (control freak)	66,67%	4	1
Financial difficulties	66,67%	4	2
Indirectly expressing negative feelings towards employer/co-workers instead of openly addressing them (passive aggression)	62,50%	4	1
Indications of unmet personal expectations (personal stressors)	62,50%	4	1
Sudden changes in working hours	62,50%	4	1
Directly expressing negative feelings towards employer/co-workers in person	58,33%	4	1
Absence of interest by employer/co-workers in the employee's frustrations about the job	58,33%	4	1
Changes in mental health	58,33%	4	1
Compulsive behavior	58,33%	4	1
Being easily frustrated or disappointed (anger management issues)	58,33%	4	1
Working less than expected (come late/leave early)	54,17%	4	1
Employee receives strange phone calls	54,17%	4	1

Changes in online or social media behavior	54,17%	4	1
Narcissism	54,17%	4	1
Lack of responsibility	54,17%	4	1
Team members leaving the organization	54,17%	4	1

Table 21: *Low-rated red flags during employment*

Low-rated red flags	**% 4 or 5**	**Median**	**Interquartile Range**
Sudden intensive travel	50,00%	3,5	1
Repeatedly declining to take annual leave	50,00%	3,5	1
Employee wants to define his/her job him-/herself	50,00%	3,5	1
Not being able to deal with criticism	50,00%	3,5	1
Changes in the way an employee expresses him-/herself	45,83%	3	1
Lone wolves who have contact with colleagues	37,50%	3	1
Too heavy workload	37,50%	3	1
High level of competitiveness	37,50%	3	1
Changes in physical health	37,50%	3	2
Uneasiness with fellow employees	33,33%	3	1
Lack of adaptability in adverse circumstances	33,33%	3	1
Interest in matters outside of the scope of his/her job	33,33%	3	2
Changes in personal status (divorce, new partner, ...)	33,33%	3	2
Employee volunteers for new sensitive projects	29,17%	3	1
Burn-out	29,17%	3	2
Not responding well under stress or during crises	29,17%	3	2
Love relationship with a colleague	25,00%	3	1,75
Poor personal hygiene	20,83%	3	1
Not being very empathetic	20,83%	3	1
Employee takes long lunch breaks without colleagues	12,50%	3	1
Introversion	8,33%	2	1

It is again noteworthy that a number of issues fall just short of the threshold of the high-rated category. Similar to the high-rated issues, some of them relate to the insider, like sudden and unexplained changes in performance, abnormal high absenteeism and unauthorized absence, while others relate to the organization, like time pressure and red tape that leads to unwanted shortcuts. Also impending termination of contract is close to the high-rated category, which is in line with the findings of the Carnegie Mellon University Software Engineering Institute's Community Emergency Response Team (CERT) that "found that an individual is most likely to steal intellectual property within 30 days of termination" (Luckey et. al., 2019: 33).

Concerning underlying reasons of insider threats, the panel rates disgruntlement with the organization (high-rated) relatively higher than personal strains other than addictions, like financial difficulties or unmet personal expectations, as well as personality disorders like narcissism, something that is in line with the results of our insider threat awareness and behavior survey (Reveraert & Sauer, 2021b). In relation to disgruntlement, it is notable that the panel considers directly expressing negative feelings towards employer/co-workers online relatively more worrying than directly expressing negative feelings towards employer/co-workers in person, with indirectly expressing negative feelings towards employer/co-workers instead of openly addressing them (i.e. passive aggression) scoring in between the two.

Furthermore, even though it was argued that deviation from normal or baseline behavior can be considered a potential early warning of insider threat, the results show that not all deviant behavior is worrisome. Behavioral changes that were rated medium are sudden changes in working hours, with working a lot of overtime scoring relatively higher than working less than expected but relatively lower than absenteeism. Also changes in online or social media behavior and changes in mental health are considered worrisome by only part of the panel (respectively 54% and 58%). Concerning the latter, mental health issues are rated relatively higher as red flag during employment (medium-rated) than as a red flag during recruitment (low-rated). Behavioral changes receiving a relatively low rating from the panel are for instance sudden intensive travel, changes in personal status (divorce, new partner, …) or changes in physical health.

Additionally, a number of personality characteristics were not regarded by the panel as a potential red flag of intentional misconduct. In concrete terms, this concerns not being able to deal with criticism, not being very empathetic and introversion, which all were rated low by the panel. Similarly, behavior related to control freaks did not receive a high rating from the panel, with repeatedly declining to allow others to serve as back-up for handling responsibilities receiving a relatively moderate rating and repeatedly declining to take annual leave being rated relatively low. To conclude, it is noteworthy that a number of organizational factors were not considered to be indicative of future insider threat incidents, like too heavy workloads and high levels of competitiveness.

4.6. Observation - Good practices

After identifying red flags that organizations should be vigilant of during employment, the panel was asked to rate practices to observe those red flags. Tables 22, 23 and 24 respectively show the practices that receive a high-, medium- and low rating from the panel.

Table 22: *High-rated practices to observe red flags during employment*

High-rated practices	% 4 or 5	Median	Interquartile Range
Use a system to monitor the use of badges/access rights (electronic access control)	95,83%	5	1
Restrict access for critical systems/applications/sites	91,67%	5	0
Avoid that an employee can consult data/facilities he/she doesn't need for his/her job (role-based access)	91,67%	5	0,75
Audit access registration systems	91,67%	5	1
Four-eyes principle/two-person rule	91,67%	4,5	1
Put in place alarms on access systems	87,50%	5	1
Secure endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices (endpoint security tools)	87,50%	5	1
Invest in a culture of open feedback and trust	87,50%	5	1
Create a culture of reporting where employees know they are actually helping co-workers by disclosing concerns	87,50%	5	1
Repeat screening when employee moves to a more vulnerable position	83,33%	5	1
Ensure insider threat awareness on Board, CEO and management levels	83,33%	5	1
Have various means to report red flags	83,33%	5	1
Do not punish employees that make a wrong call when reporting red flags in good faith	83,33%	4,5	1
Tailor-made training for managers and staff to detect and report red flags in their context	83,33%	4	1
Ensure an active role of line manager/supervisor following-up if someone appears unhappy or different from usual	83,33%	4	1
Risk analysis based on access and impact	79,17%	5	1
Physical protection and technical measures (decent camera systems, ...)	79,17%	5	1
Installation of a point of contact to report red flags	79,17%	4,5	1
Require management sign-off for potentially disruptive actions	79,17%	4	1
Structure coordination and communication along the organization (avoid information silos)	79,17%	4	1

The panel puts emphasis on internal whistleblowing to observe red flags during employment, a recommendation that is also present in the insider threat literature (Bell et. al., 2019; Colwill, 2009; Mehan, 2016; UK Centre for the Protection of National Infrastructure, 2011; US National Insider Threat Task Force, 2016). In concrete terms, the panel recommends organizations to organize tailor-made training for managers and staff to detect and report red flags in their context, to have various means to report red flags[30] including a point of contact, to create a culture of reporting where employees know they are actually helping co-workers by disclosing concerns and to not punish employees that make a wrong call when reporting red flags in good faith[31]. Contrary to the panel's advice, the results of our insider threat awareness and behavior survey (Reveraert & Sauer, 2021b) show that less than two thirds of the respondents indicated that their organization has a point of contact where employees can report suspicious behavior of colleagues or that their organization trains its employees so that they have the necessary skills to report insider threats (respectively 64% and 57% of the respondents).

Among the high-rated practices to observe red flags during employment are also other practices that the insider threat literature recommends, like the risk-based approach already discussed in relation to the detection of red flags during recruitment (see supra 4.2) and the principle of least privilege (Cole & Ring, 2006; International Atomic Energy Agency, 2008; Mehan, 2016). Concerning the latter, the panel urges organizations to restrict access for critical organizational assets, as well as to avoid that an employee can consult data/facilities that are not needed for the job. In contrast to internal whistleblowing practices, our insider threat awareness and behavior survey (Reveraert & Sauer, 2021b) shows that the principle of least privilege seems to be more embedded given that 85% of the respondents indicated that their organization ensures that employees solely have access to the information needed to perform their job. More or less related to the principle of least privilege is the recommendation to require management sign-off for potentially disruptive actions.

To observe unauthorized access attempts, the panel recommends organizations to not only implement electronic access control systems but to also place alarms on these systems and to audit them. One expert however discouraged alarms on access systems, arguing that an employment relationship has to be based on trust between employee and employer. Also the implementation of endpoint security tools are highly recommended by the panel, with the use of data loss prevention tools being recommended by two thirds of the panel (medium-rated). Furthermore, with disgruntlement perceived as a potential red flag, the panel advises line managers and supervisors to take an active role in following-up employees that are unhappy or different from usual. The final recommendation included in the high-rated category is structuring coordination and communication along the organization (i.e. avoid information silos) to make sure it has all the pieces to solve the insider threat puzzle in time.

Apart from the role of line managers and supervisors, the role of Human Resources (HR) was pointed out by one panelist in round 3 of the study, a practice not appearing in the high-rated list. In concrete terms, the panelist indicated that insider threat indicators should be taken into account during performance evaluations. Additionally, several high-rated practices were subject to discussion in round 3. One panel member for instance suggested that ensuring insider threat awareness on Board, CEO and management levels often turns into a token activity rather than a meaningful contribution to insider threat mitigation. The same applies to the four-eyes principle, which one panelist believed to give a false sense of security "*as the second reviewer often relies on the first and approves without reviewing*".

[30] According to one panelist not too many because this might lead to confusion.
[31] According to one panelist only if it happens occasionally.

With respect to the suggestion to repeat screening when the employee moves to a more vulnerable position, opinions were divided with two experts advocating an even stricter practice of repetitive screening irrespective of an internal promotion or transfer, and one expert opposing repetition of screening because an employment relationship has to be based on trust between employee and employer. To conclude, one panelist believed physical protection measures are more effective against external perpetrators, while another expert would only use it in case of huge money transactions.

Table 23: *Medium-rated practices to detect red flags during employment*

Medium-rated practices	**% 4 or 5**	**Median**	**Interquartile Range**
Implement an anonymous whistleblower system (compliant with relevant legislation and not only ticking the box)	75,00%	5	1,75
Create a supportive culture	75,00%	5	1,75
External audit	75,00%	4	1,5
Put in place a hotline to report red flags	75,00%	4	1,75
Separation of key roles/duties	70,83%	5	2
Put responsibility for monitoring behavior with all members of staff, not just the security team (vigilant managers & staff)	70,83%	5	2
Development of a formal threat assessment	70,83%	4,5	2
Insist on a regular use of vacation and holiday time off from work	70,83%	4	2
Internal audit	66,67%	4	1,75
Periodic and variable workplace climate surveys	66,67%	4	1,75
Scrutinize workforce segments that have wider access/greater impact	66,67%	4	2
Data loss prevention (DPL) tools	66,67%	4	2
Oversight of line management	66,67%	4	2
Let employees work in teams	66,67%	4	2
Conduct red team tests	62,50%	4	1
Job rotation	62,50%	4	1
Promote self-reporting	62,50%	4	2
Trustworthiness evaluation/investigation by police, military, or intelligence services	58,33%	4	1
Stage manipulation by a hostile third party (social engineering)	54,17%	4	1
Conduct random tests	54,17%	4	1
Drug screening	54,17%	4	2

Table 24: *Low-rated practices to detect red flags during employment*

Low-rated practices	**% 4 or 5**	**Median**	**Interquartile Range**
Conduct desktop simulations	50,00%	3,5	1
Annual professional development interviews	50,00%	3,5	2
Utilize a formal appraisal process supported by regular catch-up sessions	50,00%	3,5	2
Declaration by the organization of assets and interests	45,83%	3	1
Use artificial intelligence/machine learning to find red flags	45,83%	3	1,75
Scrutiny of internet use and social media activity	45,83%	3	1

Computationally identify unexpected items or events in data sets which differ from the norm (anomaly detection)	45,83%	3	2
Periodic and variable psychological assessment (fitness for duty screening)	45,83%	3	2
Let security report directly to the CEO	45,83%	3	2
Formally inform employees that use of time during work hours can be checked by private investigators	41,67%	3	2
Alcohol screening	41,67%	3	2
Encourage isolated or withdrawn employees to participate in informal gatherings	37,50%	3	1
Track company vehicles during work hours (in a legal manner)	37,50%	3	2
User and entity behavior analytics (UEBA) tools	33,33%	3	2
Reward employees that report red flags	29,17%	2,5	2
Behavior observation program	25,00%	3	0,75
Keyword matching (emails, chats, web usage)	20,83%	3	1,75
Computationally analyze employee's opinions, sentiments and emotions expressed in text (sentiment analysis)	8,33%	2	2

The fact that the suggestions to implement an anonymous whistleblower system and a hotline to report red flags fall just below the threshold of the high-rated category again reflects the value the panel attributes to internal whistleblowing in the observation of red flags during employment. The same applies to putting responsibility for monitoring behavior not just with the security team but with all members of staff, although we would have expected the latter to receive a high(er) rating given that we know from the literature that the entire workforce bears responsibility in insider threat mitigation (Gelles, 2016; Thompson, 2018). While reporting of red flags is considered to be important, the panel simultaneously recommends organizations not to go as far as to reward employees that report red flags (low-rated). Furthermore, it is worth noting that separation of key roles also narrowly misses the high-rated category, another practice we expected the panel to assign to the high-rated category based on the insider threat literature (Cole & Ring, 2005; Mehan, 2016; Sarkar, 2010). External audits too were close to the high-rated category, receiving a relatively higher score than internal audits which is supported by two thirds of the panel.

Moreover, the relatively low importance given by the panel to drug- and alcohol screening during employment is similar to the moderate evaluation of these practices to detect red flags during recruitment (see supra 4.2). Also the relatively little importance given to fitness for duty screenings corresponds with the relatively low rating of it as a practice to detect red flags during recruitment. The relatively moderate rating of the suggestion to stage social engineering attacks is equally in line with the relatively low rating the panel gave to testing vulnerability for social engineering during the recruitment process. Nevertheless, the findings of our insider threat awareness and behavior survey (Reveraert & Sauer, 2021b) illustrate that social engineering was the number one type of insider threat that organizations worried about (45% of the respondents). While we acknowledged the difficulty of testing vulnerability for manipulation by a hostile third party during recruitment, we expected this suggestion to be more popular among the panel as a practice during employment (like staging phishing attacks).

Less in line with earlier results is the relatively high score of insisting on a regular use of vacation and holiday time off from work, since repeatedly declining to take annual leave was not really perceived as a red flag during employment. Additionally, the use of work climate surveys, which might give an indication of possible employee disgruntlement, is only endorsed by two thirds of the panel and is therefore moderately recommended to detect red flags during employment. Also scrutiny of social media activity is considered to be less suitable to observe red flags during employment, especially in comparison with detection of red flags during recruitment. This is in line with the results of our survey on insider threat awareness and behavior (Reveraert & Sauer, 2021b), where 60% of the respondents indicated that their organization checks the non-work-related social media profiles of future employees who will have access to organizational assets during recruitment, while that number decreases to 44% for non-work-related social media checks during employment.

The results of our survey (Reveraert & Sauer, 2021b) also show that only 25% of the respondents indicates that their organization tests its insider threat policy via simulations. Regarding simulations, it can be deducted from the results of this Delphi study that the panel has relatively more confidence in red team tests and staging of social engineering attacks than in desktop simulations to observe red flags during employment, although all of them score relatively moderate with less than two thirds of the panel recommending them.

To conclude, one of the most striking results, if not the biggest one, is that the panel is reluctant to the use of artificial intelligence and machine learning tools, in particular anomaly detection, user and entity behavior analytics, keyword matching and sentiment analysis, to observe red flags during employment, given that less than half of the panel recommends them. This is in contrast to the literature on insider threat, where the use of artificial intelligence to automatically detect red flags of insider threats receives considerable attention (e.g. Brown et. al., 2013; Koutsouvelis et. al., 2020; Le & Zincir-Heywood, 2019). A possible explanation for this low rating might be that the panel perceives that the quality of the existing artificial intelligence tools is not sufficient, with the risk of false positives being still too high. Furthermore, it can be assumed that a panel composed of experts on cybersecurity, with more specific expertise on these tools, might have rated artificial intelligence tools higher. In any case, the discrepancy between the priority given to artificial intelligence in the insider threat literature and the minor role our panel assigns to these tools should be explored in further research.

4.7.Observation - Difficulties

In similarity with the difficulties to detect red flags during recruitment, the panel was questioned on difficulties to observe red flags during employment. Tables 25, 26 and 27 respectively show the difficulties that receive a high-, medium- and low rating from the panel.

Table 25: *High-rated difficulties to detect red flags during employment*

High-rated difficulties	% 4 or 5	Median	Interquartile Range
Lack of managerial support	91,67%	4	1
What may appear suspicious to one observer is a sign of initiative to another observer (subjective interpretation of red flags)	87,50%	4	0
Push back from unions/labor groups[32]	83,33%	4	0
Cultural change needed for accepting in-employment screening	83,33%	4	0
Manager and staff are not appropriately qualified/trained to detect red flags	83,33%	4	0
Resource limitations	83,33%	4	0
A tool is only as good as its follow-up	79,17%	4	0
Cultural change needed for accepting whistleblowing as a professional responsibility (unwillingness to report)	79,17%	4	1
Unequal treatment of employees in controls	75,00%	4	0,75
Employer is most of time not or very late informed on changes in private life/situation of employees (hard to detect)	75,00%	4	0,75

One of the main difficulties in the observation of red flags during employment, that to some extent was discussed in relation to detection of red flags during recruitment, is the fact that observation of a red flag depends on the subjective interpretation of the observer. This implies that what may appear suspicious to one observer might be a sign of initiative (i.e. a positive sign) to another observer.

Moreover, a number of high-rated difficulties identified by the panel actually relate to previously mentioned good practices, whereby the panel either identifies reasons that complicate the implementation of these recommended practices or identifies a discrepancy between the recommended situation and the actual situation.

Regarding the former, the panel for instance recommends to adopt a risk-based approach, but also recognizes that this implies unequal treatment of employees. The unequal treatment of employees might also explain the pushback from unions/labor groups, which is equally identified by the panel as a major difficulty in the observation of red flags during employment.

[32] Two experts believed this issue was formulated too ambiguously.

Regarding the latter, whereas the panel emphasized the importance of creating a culture of reporting to observe red flags during employment, it simultaneously claims that whistleblowing is currently not culturally accepted as a professional responsibility, leading to an unwillingness to report. Likewise, the panel recommends a number of in-employment screening practices (e.g. electronic access control, alarms on access systems, …), but simultaneously believes a cultural change is needed for accepting these practices. Additionally, the panel identified awareness of the insider threat problem on senior and middle management levels as a good practice, but at the same time puts lack of managerial support forward as a factor significantly constraining insider threat detection. A similar discrepancy between the recommended situation and the actual situation is present with respect to tailor-made training for managers and staff, with the panel identifying tailor-made training to observe and report red flags in their context as a good practice but simultaneously concluding that at the moment, manager and staff are not appropriately qualified/trained. The latter is in line with earlier findings regarding lack of qualifications of recruitment staff to conduct background screenings. Another similarity with the difficulties related to the detection of red flags during recruitment is resource limitations that equally constrain the detection of red flags during employment.

Table 26: *Medium-rated difficulties to detect red flags during employment*

Medium-rated difficulties	**% 4 or 5**	**Median**	**Interquartile Range**
Time-consuming	70,83%	4	1
Organizations downplay the role of work climate in security	70,83%	4	1
Dysfunctional work environment might lead to multiplication or oversight of insider threat	70,83%	4	1
Information is not always legally available	66,67%	4	1
Organizations do not always see concrete return on investment	66,67%	4	1
Relying too much on one employee to perform a task (monopoly position)	66,67%	4	1
Risk of creating a negative workplace culture if staff in general feel that they are being unduly controlled/surveilled	66,67%	4	2
Possibility of abuse of the reporting system by anyone bearing a grudge against the employee	62,50%	4	1
Leadership-level personnel tends to protect itself from monitoring and controls	62,50%	4	1
Lack of law, policy or regulation that enables post-employment screening	58,33%	4	1
No access to government databases	58,33%	4	1,75
Incorporation of (legal) precautions is often implemented when organizations are already confronted with red flags (too reactive)	54,17%	4	1
Laws and regulations are too much focused on privacy	54,17%	4	2

Table 27: *Low-rated difficulties to detect red flags during employment*

Low-rated difficulties	**% 4 or 5**	**Median**	**Interquartile Range**
Assumption of trustworthiness	50,00%	3,5	1
Follow-up procedure for internal job rotation/newcomers/consultants/contractors is complex	45,83%	3	1
Private investigator may be necessary	41,67%	3	1
Forcing isolated employees to socialize is an unacceptable intrusion.	37,50%	3	1
If suspect is reported by a colleague it is difficult to protect that colleague from criticism or threats by suspect or other employees	37,50%	3	1,75
Difficult to investigate suspicions without leaving the organization open to (legal) challenges	29,17%	3	2
Not ethical to monitor an employee	29,17%	2,5	2
Anonymous hotline has not a lot of success	20,83%	3	0,75

Table 26 shows that the medium-rated category contains rather straight-forward difficulties like the fact that detection of red flags is time-consuming, that organizations do not always see concrete return on investment or that there is a possibility of abuse of the reporting system by anyone bearing a grudge against the employee.

Furthermore, some of the suggestions resemble the difficulties mentioned when discussing the detection of red flags during recruitment, like the over-emphasis of laws and regulations on privacy and the prohibition to access government databases. Additionally, the relatively high score of the statement that organizations downplay the role of workplace climate in security, which narrowly missed the high-rated category, relates to disgruntlement as red flag of insider threats.

More striking results are the relatively high score of the statement that leadership-level personnel tends to protect itself from monitoring and controls, as well as the relatively low score of fear of reprisal. In relation to the former, two thirds of the panel highlights the risk of creating a negative workplace culture if staff feels that they are being unduly controlled (medium-rated). Concerning the latter, Cools (1994), Nitsch et. al. (2005) and Bell et. al. (2019) for instance found that fear of reprisal is one of the main barriers to report red flags, a finding echoed by one of the panelists who indicated that "*A recent case has shown our company that other employees knew the incident was happening but kept silent to avoid conflict with the offenders".*

4.8. Investigation - Good practices

Subsequent to the observation of red flags during employment, the panel was asked to rate practices to investigate the validity of potential red flags that were observed during employment. Tables 28, 29 and 30 respectively show the practices that receive a high-, medium- and low rating from the panel.

Table 28: *High-rated practices to investigate the validity of red flags observed during employment*

High-rated practices	% 4 or 5	Median	Interquartile Range
Respect the (legal) rights of the suspect	100,00%	5	0,75
Have an internal investigation protocol regarding concerns reported through the whistleblowing system	95,83%	4	1
Have trained and experienced staff to conduct the investigation	91,67%	5	0
Detect and use only what is legally authorized	91,67%	5	1
Avoid a witch hunt	91,67%	5	1
Have a formal investigation policy, procedures and process (who conducts investigation and how)	83,33%	5	1
Not act in a haste unless the situation appears urgent	79,17%	5	1
Make sure unauthorized staff members do not conduct their own investigation and make accusations	79,17%	5	1
Provide sufficient resources to conduct investigations	79,17%	4,5	1
Ensure you know what the normal situation is meant to be like to allow audit trails (like material inventories if suspicion of stolen material)	79,17%	4	1
Review emails and ICT history of the suspect	79,17%	4	1

Most of the high-rated practices suggested by the panel seem rather straight-forward, like for instance respecting the (legal) rights of the suspect, knowing what the normal situation is meant to be like, the provision of sufficient resources to conduct investigations and the avoidance of a witch hunt.

Furthermore, the panel advises organizations to have a formal investigation policy that outlines who conducts the investigation and how the investigation proceeds. The panel continues to give priority to internal whistleblowing, this time by recommending organizations to have an internal investigation protocol regarding concerns reported through the whistleblowing system. More or less in relation to the latter two recommendations is the recommendation of one panelist to find a balance between having trained and experienced staff to conduct the investigation and making sure unauthorized staff members do not conduct their own investigation and make accusations. Or to say it in his or her words:

> "*They [expert investigators] must prioritize, which makes it extremely unlikely that they will become involved at the earliest stage of a potential problem when it is still capable of being mitigated. While untrained employees should not be encouraged to make accusations, nor should they be encouraged to abdicate all responsibility for defeating insider threats by leaving it to the experts. The co-worker in a team who asks a team mate what is wrong and shows enough concern to address problems at the lowest level does more good to mitigate a budding insider threat than that same member does by channeling the same concerns to an elaborate whistleblower reporting system or by becoming an informant to a sanctioned investigator. Not that there is not room enough for overlapping and mutually supporting systems to work in concert to address insider threats*."

Apart from the above-mentioned commentary, three other high-rated practices where subject to discussion in round 3 of the study. Firstly, one expert agreed that detecting and using only what is legally authorized should be the general rule, but simultaneously argued that complying with this rule will not always be possible in reality, leaving the door open for "*grey and darker means*". Secondly, not acting in a haste unless the situation appears urgent was put into perspective by one expert, arguing that "*There is a difference between not acting in a haste and immediately taking the possible situation seriously and following up on it*". Finally, the panel's suggestion to review emails and ICT history of the suspect was refined by 4 panelists, with one member of the panel arguing that the intrusiveness of the practice implies the need for proportionality with the risk of intentional misconduct, two other panelist adding that it should always be applied within the constraints of the applicable laws, and yet another one urging to use it as "*a second line of investigation, if other indicators have already given a basis to proceed*". To conclude, one expert stressed in round 3 that "*investigations should always be à charge and à décharge*", a practice endorsed by less than two thirds of the panel and that therefore received a medium rating from the panel in round 2 of the study.

Table 29: *Medium-rated practices to investigate the validity of red flags observed during employment*

Medium-rated practices	**% 4 or 5**	**Median**	**Interquartile Range**
Mask the identity of the suspect until anomalies and allegations are confirmed	75,00%	4,5	1,75
Be transparent on the investigative process	75,00%	4	1,75
Senior ownership of the investigation process	70,83%	4	2
Culture of presumption of innocence	70,83%	4	2
Compare observed behavior with duties and tasks of the suspect	66,67%	4	1
Regularly interact with applicable police, prosecutor, security and intelligence services (proactive rapport)	66,67%	4	2
Have a formal conversation with the suspect	66,67%	4	2
Interview other stakeholders (like co-workers/managers)	66,67%	4	2
Triangulate information sources	66,67%	4	2
Have policies and procedures in place to determine if the behavior is concerning enough to warrant a response	66,67%	4	2
Assess whether there is a link with external criminality (suspect providing help to criminals outside the organization)	62,50%	4	2
Use a team approach	58,33%	4	2
Investigate à charge and à décharge	58,33%	4	2
Automate data aggregation rather than asking for data from different data owners for each new investigation	54,17%	4	1
Involve as few people as possible until anomalies and allegations are confirmed	54,17%	4	2

Table 30: *Low-rated practices to investigate the validity of red flags observed during employment*

Low-rated practices	% 4 or 5	Median	Interquartile Range
Explicitly define threshold of concerning behaviors that must be met before an investigation is launched	50,00%	3,5	1
Temporary reassignment of the suspect to a less sensitive area during the investigation (time-out)	50,00%	3,5	1
Review financial circumstances of the suspect	45,83%	3	1
Inform prosecutor & police	41,67%	3	2
Approval of formal investigation policies and procedures by social partners	37,50%	3	1
Have an informal conversation with the suspect	33,33%	3	3
Involve external expertise from the beginning (like a private investigator)	25,00%	2,5	2,75
Make sure different entities must give their consent to start an investigation	16,67%	3	1

Medium-rated practices that were close to a high rating are transparency about the investigative process, masking the identity of the suspect until anomalies and allegations are confirmed and senior ownership of the investigation process. Moreover, in line with the medium rating of the suggestion to investigate à charge and à décharge is the medium rating of culture of presumption of innocence. Although this practice falls just below the threshold of the high-rated category, we expected it to be assigned to the high-rated category rather than the medium-rated one, taking into account the generally accepted principle that someone is 'innocent until proven otherwise'.

While the panel highly recommends organizations to have a formal investigation policy that outlines how the investigation process proceeds, it is to a lesser extent recommended to formally outline what behavior would trigger the investigation process. This may be concluded from the relatively moderate rating of the suggestion to have policies and procedures to determine if the behavior is concerning enough to warrant a response, as well as the relatively low rating of the suggestion to explicitly define the threshold of concerning behaviors that must be met before an investigation is launched, respectively supported by two thirds and half of the panel. Other practices receiving a relatively moderate score are triangulation of information sources and assessing whether the suspect is providing help to criminals outside the organization.

A striking observation is that formal and informal conversations with the suspect did not make the high-rated category, respectively receiving support from two thirds and one third of the panel. Also interviewing other stakeholders than the suspect receives only a medium rating to investigate the validity of red flags, being encouraged by two thirds of the panel. Approval of formal investigation policies and procedures by social partners too scores relatively low, with only 38% of the panelists recommending it. Referring back to the identification of pushback from unions/labor groups as a significant difficulty to observe red flags, this relatively low rating is striking, as one could assume that letting social partners approve formal investigation policies and procedures could help to reduce the pushback from unions/labor groups.

To conclude, the panel considers it less necessary that different entities have to give their consent to start an investigation, to involve external expertise from the beginning or to temporary reassign the suspect to a less sensitive area during the investigation.

4.9. Anticipation - Good practices

The insider threat mitigation framework outlined earlier in this report illustrated that the insider threat process can evolve to the point where an insider threat incident is imminent. Therefore, the panel was asked to rate practices to anticipate red flags that were observed and investigated during employment, or to pre-empt what is perceived to be an imminent insider threat incident. Tables 31, 32 and 33 respectively show the practices that receive a high-, medium- and low rating from the panel.

Table 31: *High-rated practices to anticipate red flags observed and investigated during employment*

High-rated practices	**% 4 or 5**	**Median**	**Interquartile Range**
Ensure a respectful work culture (no bullying or harassment)	87,50%	5	1
See if further confirmatory evidence can be gathered before counteraction	87,50%	4	1
Have a response plan to concerns reported through the whistleblowing system	83,33%	4	1
Use a graded approach (consider threat level and potential consequences)	79,17%	4	1

As discussed earlier in this results section (see table 6), the anticipation stage contains considerably fewer high-rated practices in comparison with the other stages of the framework, with only four out of the in total 37 practices listed in round 2 assigned to the high-rated category. A possible explanation for the relatively few recommended practices is the lack of contextualization of the insider threat situation. Contextualizing the question might therefore generate different results, with practices receiving a low score from the panel possibly receiving a higher score when discussed in relation to a specific scenario. Still, the low number of recommended practices implies that the panel finds it easier to shows which practices are not recommended to pre-empt imminent insider threats than which practices are useful

Of the four high-rated practices, it is noteworthy that in similarity with the observation and investigation stage, the panel again refers to internal whistleblowing, recommending organizations to have a response plan to concerns reported through the whistleblowing system. However, in round 3 of the study, one panelist argued that the high-rated practices outlined in table 31 "*suggest over-reliance on a whistle-blowing system, which may not necessarily be optimized for preemption*". The same expert also pointed out that looking for confirmatory evidence before proceeding with counteraction will probably have as a result that the organization will lag behind the insider threat attack, failing to preempt it. This critique was more or less echoed by another expert, who argued that the practices "*may contradict each other in some cases (e.g. if the graded approach indicates no time to collect further evidence)*".

To conclude, one panelist urged to include positive incentives in the high-rated category, particularly referring to employee assistance programs that might halt the insider's path to intentional misconduct and get him or her back on the right track before an incident occurs. These positive incentives received a medium rating from the panel in round 2 of the study.

Table 32: *Medium-rated practices to anticipate red flags observed and investigated during employment*

Medium-rated practices	% 4 or 5	Median	Interquartile Range
Develop policies and procedures for counteraction (who, when, how, ...)	75,00%	5	1,75
Withdraw access of the suspect (virtual and physical)	70,83%	4	2
Implement the four-eyes principle/two-person rule	70,83%	4	2
Engage emergency procedures	66,67%	4	2
Involve social/psychological support to seek resolution before incident develops (employee assistance program)	62,50%	4	2
Include technology for remote disconnect and alarm response	58,33%	4	1
Confiscate the suspect's organizational equipment (mobile, computer, ...)	58,33%	4	2
Exchange information within the organization	58,33%	4	2
Institute positive incentives to seek resolution before incident develops	58,33%	4	2
Apply track and trace systems	54,17%	4	1

Table 33: *Low-rated practices to anticipate red flags observed and investigated during employment*

Low-rated practices	% 4 or 5	Median	Interquartile Range
Regularly update policies and procedures for counteraction	75,00%	5	2,5
Raise general awareness on expectations of appropriate conduct	54,17%	4	2
Develop policies that encourage employees to intervene expeditiously when they suspect a threat	50,00%	4	2
Monitor movements in real time using CCTV (remote surveillance)	45,83%	3	1
Review current deterrence practices	45,83%	3	1
Intervention by the line manager/supervisor	45,83%	3	1
Use additional physical protection measures	45,83%	3	1
Shut/lock down specific section/area of the organization	45,83%	3	2
Extra deterrence through reminder of applied monitoring practices	45,83%	3	2
Develop policies that encourage employees to operate as a team	45,83%	3	2
Recognize that mistakes will happen	45,83%	3	2
Monitor social dynamics (inter-group relations)	41,67%	3	1
Address the suspect directly (interview with hierarchy)	41,67%	3	2
Confront the suspect at the first opportunity before allowing a situation to fester	37,50%	3	1
Offer the suspect time off the job	37,50%	3	1
Request support and intervention by police/prosecutor, security or intelligence services	33,33%	3	2,75
Raise awareness in the direct environment of the suspect	29,17%	3	1,75
Physically intercept (without the use of violence) the suspect	29,17%	3	2
Suspend the suspect	29,17%	3	2
Terminate the contract of the suspect	20,83%	2	2
Send the suspect a document ordering him/her not to commit misconduct (cease-and-desist order)	16,67%	3	1
Set up a controlled decoy to monitor and expose a potentially larger group or network	16,67%	3	1
Transfer the suspect internally	16,67%	3	1,75

Issues that narrowly missed the high-rated category are the development of policies and procedures for counteraction, withdrawal of the suspect's access and implementation of the four-eyes principle. Regularly updating policies and procedures for counteraction was recommended by three quarters of the panel, but was vetoed by the remaining quarter of the panel that rated the practice 1 or 2 stars, which explains the assignment to the low-rated category.

As mentioned before, the positive incentives one panelist referred to in round 3 of the study received a medium rating in round 2, with both institution of positive incentives to seek resolution before an incident develops and involvement of social/psychological support being supported by less than two thirds of the panel. In contrast to these positive incentives, other practices that received a medium rating from the panel rather relate to negative incentives like confiscating the suspect's organizational equipment, applying track and trace systems and other technology for remote disconnect and alarm response, and engaging emergency procedures.

In similarity with the recommendations to investigate the validity of red flags, relatively little importance is given to interaction with the suspect, as intervention by the line manager/supervisor, addressing the suspect directly via an interview with hierarchy and confronting the suspect all received support from less than half of the panel. On the other hand, contrary to the recommendation to structure coordination and communication along the organization to observe red flags during employment, exchanging information within the organization in the anticipation stage is only recommended by 58% of the panelists.

Furthermore, it can be observed that the panel gives preference to raising general awareness on expectations of appropriate conduct over awareness-raising in the direct environment of the suspect, though both receive a relatively low score with respectively 54% and 29% of the panel recommending it. The same applies to practices related to deterrence, given that less than half of the panel is convinced that reviewing current deterrence practices and implementing extra deterrence through a reminder of the applied monitoring practices could contribute to the preemption of imminent insider threat incidents.

To conclude, apart from withdrawing the suspect's access, other measures taken to keep the suspect (temporarily) away from his or her position, like suspension, offering the suspect time off the job, transferring the suspect internally or terminating the contract of the suspect, receive a relatively low rating with less than half of the panelists recommending it.

4.10. Damage Limitation & Reconstruction - Good practices

Since organizations are not always able to preempt insider threat incidents, the insider threat mitigation framework also takes into account the aftermath of the insider threat incident. The primary concern of the organization is limiting the harm resulting from the insider threat incident to a minimum, while the subsequent goal is to reconstruct the incident to learn from it. We therefore asked the panel to rate practices to react to an insider threat incident. Tables 35, 36 and 37 respectively show the practices that receive a high-, medium- and low rating from the panel.

Table 35: *High-rated practices to limit the damage from an insider threat incident*

High-rated practices	% 4 or 5	Median	Interquartile Range
Have a business continuity plan	91,67%	5	1
Collect and secure direct and indirect evidence	91,67%	5	1
Have trained staff in crisis communication	91,67%	4	1
Minimize damage to organization's reputation and public trust	91,67%	4	1
Identify systems, work areas or information affected by the insider incident	87,50%	5	1
Remove the offender's access (virtual and physical)	87,50%	5	1
Have an event notification tree (know who to call and notify after an incident)	87,50%	5	1
Implement lessons learned	87,50%	5	1
Have an internal crisis communications plan	87,50%	4	1
Have an external crisis communications plan	87,50%	4	1
Change compromised processes (like passwords/accesses)	83,33%	5	0
Conduct a post-incident analysis	83,33%	5	1
Define root causes of the incident[33]	83,33%	5	1
Implement quick and decisive action (tackle the incident immediately)	83,33%	4	1
Conduct a risk analysis upfront	79,17%	5	1
Brief the public information officer on what can/should be declared	79,17%	5	1
Designate a crisis management team upfront	79,17%	4,5	1
Regularly update the incident playbook	79,17%	4	1
Implement a multidisciplinary taskforce to improve policies and procedures[34]	79,17%	4	1
Designate someone as public information officer to deal with media	75,00%	5	1
Train employees to react appropriately to a malicious offender	75,00%	4	0,75

Table 35 shows that the high-rated category includes both preparatory and reactive practices. Concerning the former, reference can be made to preparatory plans like a business continuity plan, an event notification tree and the designation of a crisis team upfront. Concerning the latter, reference can be made to collecting and securing evidence, conducting a post-incident analysis, identifying and changing compromised processes and implementing lessons learned.

[33] One expert argued that defining the root causes of the incident is part of the post-incident analysis.
[34] One expert argued that implementing a multidisciplinary taskforce to improve policies and procedures is part of the post-incident analysis.

Furthermore, the panel spends considerable attention to practices related to incident communication, urging organizations to develop internal- and external crisis communication plans and to have trained staff in crisis communication, with for instance a public information officer who after the incident is briefed on what can or should be declared. The importance given to communication seems to relate to the panel's recommendation to minimize the damage to the organization's reputation. The recommendation to control public announcements in order to safeguard the organization's reputation also seems to explain why the dark or hidden number of insider threats remains high (see supra 3.2).

A number of high-rated practices were discussed during round 3 of the study. One panelist for instance stressed that implementing quick and decisive action is not always the appropriate solution, as sometimes other stakeholders, like for instance police forces, have to be involved. Another panelist specified that training employees to react appropriately to a malicious offender should be limited to reporting red flags to a designated team responsible for counteraction. Additionally, one panelist emphasized that removing the offender's access can only happen if the offender is proven guilty of the incident. Finally, two experts provided a general criticism regarding the high-rated practices, pointing out that the suggested practices relate to general crisis management, rather than management of insider threat incidents specifically.

On top of the high-rated practices that were put into perspective in round 3 of the study, three practices currently absent in the high-rated category were suggested. One expert pointed out the necessity of a plan to deal with victimization, whereas another expert suggested to add both confrontation of the person and termination of the employee's contract.

Table 36: *Medium-rated practices to limit the damage from an insider threat incident*

Medium-rated practices	**% 4 or 5**	**Median**	**Interquartile Range**
Review identity access management practices (IAM)	75,00%	5	1,75
Review privileged access management practices (PAM)	75,00%	5	1,75
Use a standardized approach to command and coordinate the emergency response (Incident Command System)	75,00%	4	1,75
Invest in resilience upfront	70,83%	5	2
Assess the crisis situation	70,83%	4,5	2
Use case study archives for training	70,83%	4,5	2
Advise all affected customers and partner organizations	70,83%	4	2
Suspend the offender	70,83%	4	2
Develop a case study archive (and add incident to it)	70,83%	4	2
Routinely conduct incident simulations (drills, table top, ...)	66,67%	4	1,75
Check the financial records of the organization (forensic audit)	66,67%	4	1,75
Develop a playbook for each type of insider incident that can occur upfront	62,50%	4	2
Assign a senior incident manager as single point of contact for incident management	62,50%	4	2
Organize aftercare for direct and indirect stakeholders (for instance co-workers)	62,50%	4	2
Inform police/prosecutor, security or intelligence services	58,33%	4	2
Refrain from private justice	58,33%	4	2
Take out insurance upfront	54,17%	4	2
Share lessons learned with entire organization as a form of reinforced learning	54,17%	4	2

Table 37: *Low-rated practices to limit the damage from an insider threat incident*

Low-rated practices	% 4 or 5	Median	Interquartile Range
Present the incident as a lesson to everyone	50,00%	3,5	1
Deal with incidents in an anonymous way	45,83%	3	1
Apply a reimbursement plan for the financial damage	45,83%	3	1
Be transparent throughout the whole organization as to what happened	45,83%	3	1,75
Confront the offender with the evidence	41,67%	3	1
Communicate with media and the public in a preemptive fashion (stealing thunder)	41,67%	3	1
File a complaint	37,50%	3	1,75
Consult external expertise (like a private investigator)	33,33%	3	2
Full and frank disclosure of the incident so that other organizations can learn from it	25,00%	3	0,75
Send the offender a document ordering him/her to stop the misconduct (cease-and-desist order)	16,67%	3	1

Similar to the high-rated category, practices in the medium-rated category relate to preparatory and reactive practices. Examples of preparatory practices that narrowly missed the high-rated category are the use of a standardized approach to command and coordinate emergency response and investment in resilience upfront. Other examples of medium-rated preparatory practices are developing a playbook for each type of insider threat incident that can occur, routinely conducting incident simulations and taking out insurance upfront, all practices recommended by at most two thirds of the panel.

Examples of reactive practices that are close to the high-rated category are short-run countermeasures like reviewing identity- and privileged access management, suspending the offender and advising all affected customers and partner organizations, as well as long-run countermeasures like adding the incident to a case study archive that should be used for training purposes. Other examples of medium-rated reactive practices supported by at most two thirds of the panel are forensic audits and organizing aftercare for direct and indirect stakeholders.

With respect to communication on the insider threat incident, it is noteworthy that whereas transparency was considered important by the panel in the stages that precede an insider threat incident (i.e. about the recruitment and screening process, about the in-employment control measures and about the investigation process), transparency is less recommended in the aftermath of an insider threat incident, both internally and externally. Regarding internal communication, only 54% of the panelists encourages organizations to share lessons learned with the entire organization. Regarding external communication, informing government authorities receives a medium rating, while communicating with media and the public in a preemptive fashion (i.e. stealing thunder) and full and frank disclosure of the incident so that other organizations can learn from it both receive a low score from the panel, being recommended by less than half of the panelists.

To conclude, the relatively low score of involvement of external expertise is in line with earlier results related to the investigation stage. Another similarity with the practices suggested with respect to the investigation and anticipation stage is that, with the exception of the one panelist advocating it in round 3 of the study, the panel considers interaction with the offender less necessary, as confronting the offender with the evidence is only recommended by 42% of the panelists.

4.11. Deliberation - Good practices

In the aftermath of an insider threat incident, the organization also has to decide how it will deal with the offender. Consequently, we asked the panel of experts to rate practices to deal with an insider that is responsible for an insider threat incident. Tables 38, 39 and 40 respectively show the practices that receive a high-, medium- and low rating from the panel.

Table 38: *High-rated practices to deal with an offender of an insider threat incident*

High-rated practices	% 4 or 5	Median	Interquartile Range
Have a fair & consistent disciplinary system	91,67%	5	1
Respect the rights of the offender (among others through the unions)	87,50%	5	1
Discuss different options with relevant stakeholders (Security, HR, IT, Legal, ...) and develop plan A/B/C	87,50%	5	1
Incorporate separation of duties	87,50%	5	1
Review access permissions	87,50%	4,5	1
Keep well-maintained personnel/contractor files	83,33%	5	1
Focus on acts, not on people	83,33%	4	1
Make sure other employees know appropriate measures are taken	79,17%	4,5	1

As discussed earlier in this results section (see table 6), the total number of practices related to the deliberation stage was scarce in comparison with the other stages of the framework (except for the practices related to mismanagement, see infra 4.13), with only 19 suggested practices. Still, of those 19 proposed practices, almost half received a high rating from the panel. More in particular, the panel recommends to have a fair & consistent disciplinary system whereby the rights of the offender are respected. Other practices worth noting include focusing on acts and not on people, discussing different options with relevant stakeholders to develop plan A/B/C and reviewing access permissions.

In round 3 of the study, one panelist emphasized the importance of making sure other employees know that appropriate measures are taken, indicating that "*A recent case has shown our company that other employees knew the incident was happening but kept silent to avoid conflict with the offenders. After termination of the offenders, the other employees were "relieved" the "bad apples" were weeded out. Therefore it is important, in my opinion, that other employees know appropriate measures are taken".* Moreover, in similarity with the previous question on damage limitation and reconstruction, one expert suggested to add confrontation of the person concerned and termination of the contract to the high-rated category, the latter receiving a medium rating in round 2 of the study.

Also in round 3, one expert touched upon one of the main shortcomings of the theoretical framework, namely that the focus of the framework is (too much) on 'bad apples', largely disregarding the question whether or not the barrel is corrupted (Searle et. al., 2017). By referring to deliberation (and termination) as a stage in the conceptual model, the framework mainly concentrates on the prevention of the recurrence of insider incidents caused by *one and the same* employee (i.e. the bad apple), not on preventing the recurrence of similar situations caused *by other* employees (i.e. corrupting barrels). Although we acknowledge this shortcoming, it is argued that the guidance to prevent repetition of similar insider threat incidents by different insiders was more or less discussed in the context of the previous stage on damage limitation and reconstruction. In any case, introspection whereby an organization looks at its own role in the insider incident is important as well.

Table 39: *Medium-rated practices to deal with an offender of an insider threat incident*

Medium-rated practices	% 4 or 5	Median	Interquartile Range
Handle the offender with care	70,83%	4	2
Consider motives and means by which insider incident is committed in harmony with considering the impact	66,67%	4	1,75
Try to stay on speaking terms with the offender	66,67%	4	2
Severity of the impact should inform the punishment	62,50%	4	2
Train extra on security rules/appropriate conduct on a regular basis	62,50%	4	2
Suspend the offender	54,17%	4	1
Terminate the contract of the offender	54,17%	4	1,75

Table 40: *Low-rated practices to deal with an offender of an insider threat incident*

Low-rated practices	% 4 or 5	Median	Interquartile Range
Question the offender applying a hear and confront approach	45,83%	3	1
File a complaint	41,67%	3	3
Issue a reprimand	37,50%	3	1,75
Transfer the offender internally	16,67%	2	2

The remaining practices that did not make the high-rated category concern both constructive and destructive practices. Examples of the former are handling the offender with care, trying to stay on speaking terms with the offender, and training extra on security rules/appropriate conduct on a regular basis. Examples of the latter are suspending the offender (medium-rated), filing a complaint and issuing a reprimand (low-rated). Moreover, it is striking that less than half of the panel recommends to question the offender by applying a hear and confront approach, given that the low rating does not appear to be compatible with the generally accepted principle that an offender has the right to defend him-or herself. Still, it is to some extent in line with the earlier recommendations to limit interaction with suspects and offenders of insider threat incidents and the limited support for an à charge and à décharge strategy during the investigation stage (see supra 4.8).

Also the fact that 63% of the panel believes that the severity of the impact should have an influence on the level of punishment is notable. Although intuitively it is indeed reasonable to relate punishment to the harm resulting from the incident, the literature shows that the focus should not be on the impact of the insider's witting decision to commit intentional misconduct, but rather on the decision itself (Goold, 2002; Hawley, 2014; Ho & Katukoori, 2013; Elangovan & Shapiro, 1998; Morris & Moberg, 1994). Think for instance of an insider that attempts to sell classified information to an undercover agent posing as a competitor of the organization (Anderson, 1994; Eoyang, 1994), like the recent espionage case of Jonathan Toebbe[35]. Since the classified information remains within the organization, the practical damage is averted but the sense of betrayal remains. Considering motives and means by which the insider incident is committed in harmony with considering the impact, a practice supported by two thirds of the panel, might therefore be more in line with the insider threat literature.

[35] Jonathan Toebbe was arrested by the FBI when he tried to sell sensitive information on US nuclear submarines to Brazil (Barnes et. al., 03/15/2022).

4.12. Termination - Good practices

When the organization comes to the conclusion that the trust relationship cannot be restored because the insider is no longer trustworthy, it has to terminate the insider's contract. Remember that impending termination of contract fell just short of the category of high-rated red flags of insider threat during employment (see supra 4.5) and that the CERT "found that an individual is most likely to steal intellectual property within 30 days of termination" (Luckey et. al., 2019: 33). As a result, it is important that the insider's dismissal proceeds in accordance with proper exit procedures. The panelists were therefore provided with a list of potential exit procedures asking them to what extent these practices are recommended when terminating the contract of insiders. Tables 44, 45 and 46 respectively show the practices that receive a high-, medium- and low rating from the panel.

Table 44: *High-rated practices to terminate the contract of insiders*

High-rated practices	% 4 or 5	Median	Interquartile Range
Comply with applicable laws	100,00%	5	0
Document the incident preceding the termination as fully as possible to motivate termination (strong factual basis)	95,83%	5	0
Reclaim equipment from the terminated employee (keys, badges, uniform, computer, books, ...)	95,83%	5	0
Develop termination procedures	95,83%	5	1
Have clear policies on appropriate and inappropriate conduct to ensure employees are aware of implications	91,67%	5	0
Document terminations	91,67%	5	0
Revoke access of the terminated employee (virtual and physical)	91,67%	5	0
Apply termination procedures consistently	91,67%	5	0,75
Escort the terminated employee to the exit if he/she is not permitted to return to his/her desk	87,50%	5	0,75
Keep well-maintained employee/contractor files	87,50%	5	1
Train termination procedures	83,33%	5	1
Regularly update termination procedures	83,33%	5	1
Give the terminated employee the possibility to defend him-/herself	83,33%	5	1
Consult legal support (internal or external)	83,33%	4	1
Document the history of what the organization has done to inform the terminated employee	79,17%	5	1
Conduct an exit interview	79,17%	4,5	1

Some of the high-rated exit procedures outlined by the panel seem straightforward, like the unanimously agreed upon recommendation to comply with the applicable laws and the development, consistent application and regular update of termination procedures.

Furthermore, documentation is important for the panel, referring both to general guidelines like keeping well-maintained employee/contractor files and documenting terminations in general, as well as to guidelines related to an insider threat incident like documenting the incident preceding the termination of the insider's contract.

Other high-rated exit procedures resemble practices suggested in the insider threat literature, like for instance reclaiming equipment from the terminated insider, revoking the insider's virtual and physical access or conducting an exit interview (Beattie & BaMaung, 2015; Power & Forte, 2006; UK Centre for the Protection of National Infrastructure, 2019). One panelist specifically emphasized the suitability of the latter practice in round 3, regarding it as a chance to "*terminate the employee without them thinking or acting hostile toward the organization after termination*". The results of our insider threat awareness and behavior survey (Reveraert & Sauer, 2021b) show that 95% of the respondents indicates that their organization immediately shuts down all accesses from employees that leave the organization, while 75% of the respondents states that their organization performs exit interviews.

In line with a comment shared with respect to the damage limitation and reconstruction stage, one expert argued in round 3 of the study that the high-rated practices are not specifically related to insider threat incidents but are rather procedures suitable for exits in general. Furthermore, one panelist questioned the relevance of giving the terminated employee the possibility to defend him- or herself, arguing that "*If you are at the point of terminating an individual there is no need for the individual to defend him/herself*". Moreover, two panelists elaborated on the recommendation to escort the terminated employee to the exit if the employee is not permitted to return to his or her desk. While both experts agreed that the suitability of the practice depends on the circumstances, one panelist put more emphasis on the negative aspect of the practice, perceiving it as public shaming, whereas the other expert rather highlighted that *"it may be prudent to arrange for a special escort for the terminated employee. (…) In a number of cases I have personally handled, such escorts were also armed, but not conspicuously so. Involuntary terminations can become last-straw events that turn violent".* Cultural differences may underlie this difference of opinion.

Finally, one expert pleaded to add conducting a social network analysis of the terminated employee within the organization to the high-rated category, a practice supported by only 54% of the panel in round 2 of the study.

Table 45: *Medium-rated practices to terminate the contract of insiders*

Medium-rated practices	**% 4 or 5**	**Median**	**Interquartile Range**
Report protocols for eventual future attempts by the terminated employee	75,00%	4	1,75
Do not treat the terminated employee as a special type of criminal	70,83%	4	2
Discuss termination options	66,67%	4	2
Have a caring attitude to prevent repercussions	66,67%	4	2
Protect the terminated employee's future as well as the interest of the organization (mutually agreed termination)	62,50%	4	1,75
Inform police/prosecutor in case of litigation	62,50%	4	2
Have the terminated employee re-sign a non-disclosure agreement (NDA)	54,17%	4	2
Identify and analyze the terminated employee's social network within the organization	54,17%	4	2

Table 46: *Low-rated practices to terminate the contract of insiders*

Low-rated practices	% 4 or 5	Median	Interquartile Range
Use termination as an opportunity to reinforce expectations regarding appropriate conduct with other employees	62,50%	4	2,75
Post-monitor social media	50,00%	3,5	1
Provide the terminated employee with appropriate guidance and counseling	50,00%	3,5	1,75
Post-monitor open sources like internet	45,83%	3	1
Share lessons learned with broader community (industry partners, law enforcement, ...)	45,83%	3	1
Inform the terminated employee's social network within the organization of the departure	45,83%	3	2,75
Have a transparent but confidential debriefing with the terminated employee's social network within the organization	45,83%	3	2,75
Offer the terminated employee career management support	16,67%	3	2

Practices that are close to the high-rated category are the development of reporting protocols in case the terminated employee attempts to regain access to the organizational assets and the recommendation to not treat the terminated employee as a special type of criminal.

Other practices supported by at most two thirds of the panel include 'hard' approaches like re-assignment of non-disclosure agreements or litigation by informing police forces and rather 'soft' approaches like having a caring attitude to prevent repercussions and protecting the terminated employee's future. However, practices supporting the terminated insider in finding a new job, like providing the terminated insider with appropriate guidance and counseling and offering the terminated insider career management support, are rated low by the panel.

In line with earlier recommendations from the panel, internal and external transparency is again not recommended in the aftermath of an insider threat incident, given that a debriefing with the terminated insider's social network within the organization and sharing lessons learned with the broader community is supported by less than half of the panel. In line with this, 63% of the panel recommends organizations to use termination as an opportunity to reinforce expectations regarding appropriate conduct with other employees, while a quarter of the panel discourages this practice (i.e. rating of only 1 or 2 stars), which explains the assignment to the low-rated category.

To conclude, just like with respect to the recommendations to observe red flags during employment, monitoring social media and other open sources post-employment receives a relatively low rating with less than half of the panel recommending it.

4.13. Mismanagement - Good practices

It was mentioned before that organizations run the risk of mismanaging an insider threat incident (Martinez-Moyano et. al., 2008), for instance by incorrectly judging non-threats as threats. As a result, we were also interested in the panel's opinion on practices to deal with insiders that are wrongly accused of being responsible for an insider threat incident (i.e. false positives). Tables 41, 42 and 43 respectively show the practices that receive a high-, medium- and low rating from the panel.

Table 41*: High-rated practices to deal with false positives*

High-rated practices	**% 4 or 5**	**Median**	**Interquartile Range**
Ensure that the incident is not recorded on the employee's record	91,67%	5	0,75
Explain why the organization suspected the employee	91,67%	5	1
Have a positive security culture so that wrong accusations are not interpreted as a negative judgement towards the employee	87,50%	5	0
Offer the employee welfare/psychological support	87,50%	5	1
Rehabilitate the employee (full restoration)	87,50%	5	1
Review the indicators and/or the reporting route that led to the false assessment	87,50%	5	1
Be aware of possible repercussions	87,50%	4,5	1
Offer the employee a personal apology	83,33%	4,5	1
Find out whether the accusations were made maliciously (debriefing with the reporter)	79,17%	5	1

The number of suggested practices to deal with false positives was with only 16 practices the lowest number of all questions asked to the panel. Notwithstanding the limited number of proposed practices, more than half of the suggested practices were assigned to the high-rated category.

While some practices are aimed at restoring the relation with the wrongly accused insider, others are targeted at preventing the reoccurrence of similar false positives. Restorative practices are for instance the full rehabilitation of the insider, whereby the wrongly accused insider is offered a personal apology[36] and/or welfare/psychological support and is ensured that the incident is not recorded on the insider's record. Preventive practices, on the other hand, are for instance reviewing the indicators and/or the reporting route that led to the false assessment or the implementation of a positive security culture so that wrong accusations are not interpreted as a negative judgement towards the insider.

During round 3 of the study, one panelist mentioned that for safety reasons, organizations cannot always explain to the wrongly accused insider why the organization suspected him or her. Moreover, one panelist urged organizations to seek legal advice, a practice supported by two thirds of the panel in round 2. The same panelist put an additional spotlight on the need to be aware of possible repercussions, and recommended organizations to retrain staff in case of false positives. Another panelist rather highlighted the necessity to inform colleagues that the accusations were false, a practice that narrowly missed the high-rated category in round 2.

[36] One panelist argued that "*if your investigation is done correctly you don't need to apology*"

Table 42: *Medium-rated practices to deal with false positives*

Medium-rated practices	**% 4 or 5**	**Median**	**Interquartile Range**
Debriefing with the team	75,00%	4	1,75
Seek legal advice	66,67%	4	1
Offer the employee time and space to have some distance from the workplace	66,67%	4	2
Register the incident in the organization incident database	66,67%	4	2
Debriefing with social partners	62,50%	4	1
Offer the employee public apologies	54,17%	4	1

Table 43: Low-rated practices to deal with false positives

Low-rated practices	**% 4 or 5**	**Median**	**Interquartile Range**
Offer the employee (financial) compensation	37,50%	3	2

While a debriefing with the team is close to a high rating, a debriefing with social partners is rated relatively moderate by the panel with 63% supporting it. Moreover, the panel considers offering the insider a public apology less appropriate than offering the insider a personal apology, but more appropriate than offering the insider a (financial) compensation.

4.14. Formal insider threat mitigation team

As a more general question transcending the different steps of the theoretical framework, we wanted to know whether the panel recommended organizations to implement a formal insider threat mitigation team. In contrast to the other questions, this question concerned a yes or no question in round 2 of the study whereby the panelist was also offered the opportunity to abstain ('no comment'). In round 3 of the study, the panelists were offered the possibility to explain the reasoning behind their answer.

Table 34: *Recommendation on the formation of a formal insider threat mitigation team*

Insider threat mitigation team	**Yes**	**No**	**No comment**
Do you recommend organizations to implement a formal insider threat mitigation team?	79,20%	16,70%	4,20%

Table 34 shows that in round 2 of the study, a large majority of the panel recommended the creation of a formal insider threat mitigation team. However, this recommendation was put into perspective. First of all, in round 3 of the study it was argued by six panelists that the formation of a formal insider threat mitigation team depends on the size and type of the organization, indicating that only for large organizations the benefits of such a team outweigh the costs.

Furthermore, one panelist commented in round 2 of the study that "*any management or analytical team assembled to evaluate or deal with an insider threat should draw its members and resources from existing staff and functions, rather than develop a standing army of specialists who will be destined to be seen as impediments to productive work in the eyes of the core business of the organization*". This was echoed by one panelist in round 3 of the study, who stated that the formal insider threat mitigation team should not necessarily be a distinct team, but can equally reside in an already existing team.

Which team this should be was however subject to debate. While one member of the panel stressed that line management should be the owner of insider threat mitigation oversight, another one urged to embed it in the security/investigation team. The results of our survey on insider threat awareness and behavior (Reveraert & Sauer, 2021b) illustrate that management is considered to be the key actor of insider threat mitigation by 61% of the respondents, followed by Security and ICT that are both mentioned by 42% of the respondents. One third of the respondents refers to Human Resources as having responsibility in insider threat policies, while the Legal Department is only mentioned by 14% of the respondents.

To conclude, one panelist indicated in round 3 of the study that "*If the threat mitigation team becomes the sole arbiter and expert body solely responsible for dealing with insider threats, the threats will invariably over match the defenses*". As a result, the panelist recommended to incorporate involvement from co-workers and line-management. Another member of the panel echoed cooperation of the formal insider threat mitigation team with other relevant stakeholders, specifically referring to social partners.

4.15: Evaluation of the Delphi study

Apart from our primary aim to discover potential red flags of insider threat incidents and good practices, relevant actors and difficulties related to insider threat mitigation, the secondary objective of the study was to "explore applicability of the [Delphi] research method" (Gossler et. al., 2019). In other words, both the panel's stance on the suitability of the Delphi technique for insider threat research in general as well as the panel's expectations regarding the results of the present study (Van Dolderen et al., 2017) was questioned. Concerning the former, table 47 shows that the large majority of the panelists perceives the Delphi technique as an appropriate method to research the insider threat problem. Concerning the latter, table 48 shows that the majority of the panel was confident that the current study would provide significant results.

Table 47: *Evaluation of the Delphi technique as a means to research the insider threat problem*

Question	Rating	N	%
Please indicate to what extent you consider the Delphi method in general an appropriate means to research the insider threat problem	Very poor	0	0,0%
	Poor	1	4,3%
	Average	0	0,0%
	Good	19	82,6%
	Excellent	3	13,0%
	Total	23	100%

Table 48: *Prediction of the significance of the results of the current Delphi study*

Question	Rating	N	%
Please indicate whether you think our Delphi study will provide significant results.	Very poor	0	0,0%
	Poor	1	4,3%
	Average	2	8,7%
	Good	16	69,6%
	Excellent	4	17,4%
	Total	23	100%

5. Limitations of the research

In spite of our efforts to take the elements of trustworthiness of qualitative research into consideration (see supra 3.5), it should be acknowledged that the study is limited by some weaknesses, both with respect to the research design and to the results.

5.1. Research design

First of all, we did not completely fulfill the recommendation to use a research team of at least two researchers who equally contribute to the data analysis (Turoff, 2002; Landeta, 2006). The reason for this is that this study was performed in the context of a doctoral project (see supra introduction), which implies that the study consisted of one principal researcher (i.e. the PhD-candidate) that was responsible for the qualitative analysis of round 1 and round 3 and the quantitative analysis of round 2, and one secondary researcher (i.e. the supervisor) who provided feedback and assisted with the interpretation of the results. The lack of inter-coder reliability increases the risk of investigator bias (Grime & Wright, 2016). In this regard, Turoff indicates that "there are many ways to abuse the use of the Policy Delphi: the manner in which comments are edited, the neglect of items, the organization of the results" (2002: 96). Although it is acknowledged that a research team can in principle try to bend the results in a certain direction of their preference (Dalkey & Helmer, 1963), Turoff simultaneously argues that such research fraud is unlikely in practice because "such a process is a rather dangerous game and not likely to go unnoticed by some segment of the respondents" (Turoff, 2002: 96). In this regard, we can only say that the research team performed every step of the Delphi study in good faith, without any attempts to steer the panel in a certain direction, and that we did not receive any negative reactions from the panel.

Furthermore, one of the main characteristics of the Delphi technique can be subject to discussion, namely anonymity. Landeta for instance identifies "impunity conferred by the anonymity with respect to irresponsible actions on the part of the experts" (2006: 469) as a weakness of the Delphi technique. This worry is echoed by Foth et. al. (2016), who state that "due to the anonymity of the process, it has been argued that experts are not accountable for the views they express and the judgements they make" (2016: 115). Still, it can be argued that participants are to some extent accountable to the research team due to the fact that the study was not completely anonymous (i.e. quasi-anonymity). Related to anonymity is the limited interaction between the panelists, which is also a point of potential criticism. While the limited interaction is seen as a strength of the Delphi technique because it reduces the risk of groupthink or dominant individuals (Dalkey & Helmer, 1963; Hsu & Sandford, 2007; Turoff, 2002), the other side of the coin is that the risk of ambiguity is higher as there is less opportunity to discuss differences of opinion or to clarify vague statements (Landeta, 2006; Steurer, 2011; Lange et. al., 2020). Both the positive and negative aspects where echoed by the expert panel in their evaluation of the Delphi technique. One expert for instance indicated that the technique allowed "*for diverse points of view and experience to be considered in a non-challenging/threatening way (everyone's voice is heard and no egos are bruised)*", while another expert pointed out that "*There may still be some issues in terms of how different respondents are interpreting the statements and so agreement at the level of the survey may still mask divergences that would emerge if the issues were to be discussed more fully*".

The selection of the panel can be criticized as well. Delphi studies inherently suffer selection bias (Steurer, 2011) as "those who respond to the initial invitation are those who are more likely to be interested in the subject matter" (Keeney et. al., 2006: 208). Otherwise put, the composition of the panel, like the number of experts and their level of expertise, influences the results of the study, even though this problem is not unique to the Delphi technique (Hasson et. al., 2000). Also the heterogeneity of the panel has both positive and negative implications. One expert for instance believes the Delphi technique "*is an interesting method to gather information from a panel of experts when a variety of experts from different fields is consulted*", whereas another expert expressed his or her concern about a "*potential lack of consistency in terminology used in the study as respondents are from around the globe"*. With respect to our study, one can also argue that it suffers from Eurocentrism, as the African and Asian continent were not represented in our panel of experts (Gossler et. al., 2019). To include these experts could have resulted in another outcome (Lange et. al., 2020).

Moreover, while we looked to the level of experience to evaluate the capability of potential experts, Baker et. al. (2006) question whether this characteristic adequately measures capability. They argue that "it is tenuous to suggest that a certain number of years' experience means that an individual can be considered an expert" (ibid: 64). Although we not necessarily disagree with their statement, we believe a certain amount of experience is one of the few leads suggested in the literature on the Delphi technique to select an expert panel. It is true that we could have preceded round 1 with a round that formally validated the expertise of each individual panel member (Gossler et. al., 2019), but to lessen the already quite high burden on the expert panel we preferred to do a pilot study in which the qualification of the shortlisted candidates was evaluated by others. On top of that, possible miscasts of the expert panel could have been detected during the analysis of round 1, with panelists providing inadequate answers being eliminated for future rounds (which was not the case in our study). In any case, we believe that we fulfilled Baker et. al.'s recommendation that "until clear consensus appears within the literature, researchers need to be able to justify their decisions in order for readers to ascertain the expertness of the panel" (Baker et. al., 2006: 68).

Furthermore, it can be argued that the online questionnaire of round 1 contained (too) vague questions that provided little information on contextual factors, making it difficult to answer these questions (Dalkey & Helmer, 1963; Christie & Barela, 2005). One expert believed this study would provide poor results arguing "*the quality of findings [were] to be largely biased by the way in which the different questions were formulated. In most cases, my answer to the different questions would have been "It depends", and would have needed more information about the context of the question*". This remark was (frequently) echoed by other experts, with for instance one expert arguing that he or she "*did find it difficult to answer questions without context*" and another one indicating that it is "*important to address/define stakeholders first (private organization/public bodies*)". Indeed, we never specified the kind of misconduct (theft, espionage, sabotage, …), the severity of the intentional misconduct (minor or major violation of the organizational norm) or the type of organization that experiences the intentional misconduct (Small and Medium Enterprise, multinational, public organization, …). When discussing the limitations concerning the results (see infra 5.2), we will explain why we made this decision.

The questionnaire of round 2 also suffered from a certain degree of ambiguity, mostly because the statements were framed in the language of the respondents (Stone Fish & Busby; 2005; Keeney et. al., 2006). Even though all panelists were sufficiently skilled in English and writing, biased translations and linguistic misperceptions between natives and non-natives cannot be completely eliminated (Gossler et. al., 2019). This was also mentioned by several experts. One expert for instance indicated that *"there were a number of statements which were difficult to understand because they were not presented in*

the clearest terms. In some cases this is because of phraseology and in other cases because of mistranslations or portions of a statement that had not been translated". Another one stated that as a non-native speaker of English, "*it is also difficult to understand the nuances of the English language*". In combination with the heterogeneity of the panel, these language problems resulted in a lack of consistent terminology. Related, one panelist suggested in round 2 that "*It would be helpful if you defined 'screening.' This process is not standardized across industries and certainly not at the international level and is therefore open to interpretation by the survey respondent"*. This concern with respect to a lack of consistent terminology was echoed by two experts in their evaluation of the study. Moreover, the decision not to group the information gathered in round 1 resulted in an overlap between some of the issues, making it sometimes difficult for panelists to distinguish them.

Another criticism with respect to round 2 can be targeted at the decision to use a 5-point Likert scale for rating the questions. First of all, we did not carefully define the different items on the scale, as suggested by Turoff (2002). However, given that the goal was to aggregate those categories in overall 'agreement' and 'disagreement' categories, we believe that a clarification of the difference between on the one hand 'agree' and 'totally agree' and on the other 'disagree' and 'totally disagree' would have had limited added value. Furthermore, we ignored Rayens & Hahn's (2000) and Turoff's (2002) recommendation to force panelists to form an opinion by using a 4-point Likert scale that does not permit neutral answers. Since there is "no clear evidence of the superiority of one scale based on reliability" (Lange et. al., 2020: 9), our preference was the 5-point Likert scale because a 5-point Likert scale turns out to be the preferred scale among respondents (Lange et. al., 2020). In any case, presenting the issues on another scale (3-point[37], 4-point[38] , 7-point[39], 9-point[40] or 10-point[41]) could have resulted in different results (Lange et. al., 2020). Lange et. al. even question the use of ordinal scales *tout court*, arguing that "it remains unresolved whether it is better to define a scale-cutoff and then generate a dichotomous result or whether that result should be queried in a context-based dichotomous manner, e.g. whether one should formulate all questions in a yes/ no manner" (2020: 7). Future research will clarify which option provides the best results.

The use of rating scales in round 2 implies that we did not ask panelists to explain their reasoning behind their rating. This means that "in an effort to complete a long survey, responses might be selected without full consideration" (Christie & Barela, 2005: 111). Although knowing the arguments behind the ratings in round 2 would definitely have added value to the study, we estimated that the burden on the panel was already extensive (Landeta, 2006), having to process all steps of the theoretical framework[42]. Although we could have freed up time for argumentation by presenting the panel with only a fraction of the theoretical framework, our preference was questioning the entire framework without argumentative feedback from the panelists in round 2. We decided to focus on the rating of the entire framework and ask for argumentation in round 3 instead. This decision implies that unlike (recommendations from) other Delphi studies (e.g. Barrios et. al., 2021; Chuenjitwongsa, 2017; Gossler et. al., 2019; Rowe & Wright, 2001), we did not provide panelists with a summary of the arguments of other panelists (Lange et. al., 2020) or with individual feedback on the answers the expert provided in previous rounds (Barrios et. al., 2021; Stone Fish & Busby, 2005; Vogel et. al., 2019). The feedback provided to the panel was limited to stating that the questionnaire of round 2 contained all

[37] See for instance Lange et. al. (2020) and Barrios et. al. (2021)
[38] See for instance Rayens & Hahn (2000), Vogel et. al. (2019) and Gossler et. al. (2019)
[39] See for instance Turoff (2002)
[40] See for instance Lange et. al. (2020) and Barrios et. al. (2021)
[41] See for instance Hackett et. al. (2006) and Giannarou & Zervas (2014)
[42] It took approximately 1 hour to rate all 530 issues, meaning that asking for arguments behind these ratings would have been overkill and would have resulted in a large drop-out.

relevant issues mentioned by the panel in round 1, and that the questionnaire of round 3 contained the list of high-rated issues that met the selection criteria regarding percentage of agreement, central tendency and dispersion (see supra table 5).

Another potential criticism is the way we measured consensus. A weak point in this regard is that while we do take into account the stability of the group response (at least with respect to the high-rated issues), we did not take into account individual consistency (Vogel et. al., 2019), being the extent that the responses of the experts were consistent between the different rounds of the study (Barrios et. al, 2021). According to von der Gracht, this means that "group stability can happen although significant individual changes might have taken place, which compensate for each other" (2012: 1527). Moreover, the consensus definition in the present study implies that "certain items may fall just below the threshold for what is fundamentally an arbitrary cut off" (Diamond et. al., 2014: 405), as was demonstrated multiple times in the results section. In other words, it could be that we dropped issues in round 3 that fell just short of the high-rated category but that would have been valuable to discuss in round 3. To compensate for this shortcoming, we did not solely focus on round 3 of the study and presented the results of round 2 in its entirety so that the reader is informed on all (530) issues suggested by the panel in round 1.

To conclude, we acknowledge that round 3 of the study should in principle consist of the same content as round 2[43] and that omitting issues goes against the spirit of the Delphi technique (Hasson et. al., 2000). Moreover, we acknowledge that exploring consensus in the form of disagreement with the issues (Hackett et. al., 2006) would have added value to the study. Nevertheless, we argue that a reduction of the number of issues in combination with a focus on consensus in the form of agreement with the issue was necessary due to time pressure (Dalkey & Helmer, 1963; van de Linde & van der Duin, 2011) and therefore to reduce the risk of drop-outs due to participant fatigue (Chuenjitwongsa, 2017; Gossler et. al., 2019; Keeney et. al., 2006; Kozak & Iefremova, 2014; Mukherjee et. al., 2015). In other words, we did not want to repeat the mistake made by Stevenson (2010) who in retrospect believed to have included too many topics in the study, with direct consequences concerning response rate. The trade-off between feasibility and potential gains (Mukherjee et. al., 2015; Schmidt, 1997; Skulmoski et. al., 2007) therefore made that we had to "sacrifice questions and rounds in order to guarantee panel participation and continuity" (Landeta, 2006: 479).

5.2. Results

Apart from the research design, also the results of our study can be subject to debate. It was discussed before that the lack of contextualization of the questions made it difficult for experts to provide specific answers to those questions. One panelist summarized this concern as follows in relation to his or her answers provided in round 2:

> "*While I attempted to give an honest evaluation of each statement or suggested policy option, there were a large number which I may have evaluated differently given a specific scenario or context. Policies and responses to insider risks and incidences must differ considerably in respect to the types of risks, the consequences involved, and the organizations concerned*."

It should be mentioned that, although not with the exact same words, the above-mentioned commentary seems to represent the view of the majority of the panel, given that the lack of contextualization was emphasized by basically every panelist at some point during the study. This means that a number of answers contained the disclaimer 'it depends' and that specification of the

[43] Like in the studies of for instance Stone Fish & Busby (2005), Hackett et. al. (2006) and Vogel et. al. (2019).

contextual characteristics could have led to different ratings. One panelist even explicitly questioned the reliability of his or her own answers to the questionnaire of round 2 of the study for this reason[44].

Building on this, one of the panelists systematically argued in round 3 of the study that whether or not an issue should be considered a red flag depends on the type of the insider. In other words, red flags related to infiltrators are for instance different from disgruntled insiders. In concrete terms, this panelist for instance indicated with respect to the detection of red flags during recruitment that "*The goal of f.e. an infiltrator would be to get into the organization and to be trusted"* and that *"Reluctance to approve with background screening would not be in line with this goal*." With respect to observation of red flags during employment, the identification of reluctance to audits was also considered to be dependent on the type of the insider, as "*some insiders would not have anything against audits*".

Although we understand the panelist's reflections, it was not our goal to develop a single offender profile, given that previous research (e.g. Randazzo et. al., 2005) already showed that "there is no one accepted profile of an insider" (Noonan, 2018: 2.4). Similar to Eoyang's interpretation of espionage, who indicates that "espionage is not unitary and simple behavior" (1994: 88) and that "we must treat it as a class of criminal behaviors and not as a single distinct crime" (ibid: 88), we believe insider threat should be interpreted as a class of threats and not as a single distinct threat (Reveraert et. al., 2022b). The diversity of insider threats thus implies that there is not one holy grail that can mitigate the insider threat problem, but that every organization needs a tailor-made approach (BaMaung, 2018).

We certainly acknowledge that contextualizing the questions might have generated different results, with practices receiving a low score from the panel possibly receiving a higher score when discussed in relation to a specific scenario. However, in similarity with Gossler et al. who indicate that "reflecting all contextual factors of humanitarian logistics in the results would be nearly impossible" (2019: 447), we perceived that taking into account all contextual factors of insider threats would have been nearly impossible and even impractical, since providing the expert panel with too much context would not have suited the purpose of our study. Remember that the main goal of this study was to dig deeper into the theoretical insider threat mitigation model to make it more user-friendly for organizations. As a result, we did not want to include too many specifications because this would make the theoretical framework too much focused on one particular aspect of insider threat, missing the broader picture. In other words, rather than creating a theoretical framework solely dedicated to a particular kind of insider threat (theft, fraud, sabotage, ..) or a particular kind of organization (Small and Medium Enterprise, multinational, …), we preferred to create a more general insider threat mitigation framework that each individual organization can interpret within its own organizational context. Therefore, the main merit of this study, which was adequately summarized by one panelist in his or her evaluation of the study, is that it "*brings a huge number of possible reactions to the insider threat together, who have all their interest, and who can be chosen depending the context*".

In other words, instead of cataloguing a list of potential red flags that apply to all types of insiders or insider threat cases, or cataloguing a list of measures that mitigate all kinds of insider threats, the goal was to compose a list of factors that *may* point to insider threats and a list of measures that *may* help organization in mitigating insider threats. As a result, we agree with the panelist that stated in round 3 of the study that not all insiders that are responsible for insider threats have a history of illegal activities or that not all insiders that engage in intentional misconduct display signals of radicalization, but we do believe that participating in illegal activities or displaying signals of radicalization are factors that *may* point to an insider threat and that require vigilance from the organization. The same principle

[44] For reasons of transparency, it should be mentioned that this panelist did not participate in round 3 of the study, although the reason the panelist gave for dropping out was lack of time rather than substantive reasons.

applies to the insider threat mitigation measures proposed in this study, as we believe the study provides organizations with an inventory of possible insider threat mitigation measures that they can chose from to develop their tailor-made insider threat mitigation policy.

At the same time, we believe that we paved the way for parallel Delphi studies (Gossler et. al., 2019) that can add the contextualization that the panel requested and that can interpret the insider threat concept more narrowly, for instance solely asking questions to mitigate one particular insider threat type (e.g. insider theft), solely finding insider threat mitigation measures that suit one particular kind of organization (e.g. insider threat mitigation policy for Small and Medium Enterprises), or exploring one step of the theoretical framework in greater depth.

In any case, it is important to remember that the results in the present study are indicative rather than conclusive (Hacket et. al., 2006). One panelist made an interesting comment in his or her evaluation of the study in this regard:

> "*This is a sound study which should offer much food for thought. While it has surfaced a number of useful indicators, it must nevertheless contend with the dilemma of avoiding false positives. All of the indicators identified to date offer some value. However, some offer more than others. The ones which are open to subjective interpretation of what constitutes inappropriate behavior or affiliation in circumstances where the individuals making that determination have the discretion to label as inappropriate either beliefs or affiliations that run counter to their own personal preferences represent a potential Achilles' heel. This flaw, however, can be corrected by assuring some measure of oversight and alternative analysis, so that personal animosity is not allowed to infuse bias into the determination of a potential threat*".

To put it in a different way, the results of our study should be interpreted with some cautiousness and should not be viewed as definitive guidance (Vogel et. al., 2019). The fact that our expert panel composed a top-rated list of issues to be vigilant of does not mean that the presence of these issues indisputably implies that an insider threat is imminent (Keeney et. al., 2006; Landeta, 2006; Mukherjee et. al., 2015). The same principle applies to the top-rated list of good practices. Moreover, it is important to remember that the results "provide a snapshot of expert opinion at a specific moment in time" (Gossler et. al., 2019: 447) and "that the existence of a consensus does not mean that the correct answer, opinion or judgement has been found (…) [but] merely helps to identify areas that one group of participants or `experts' considers important in relation to that topic" (Hasson et. al., 2000: 1013).

Furthermore, it remains to some extent unclear whether "the findings represent the aspirations of experienced practitioners about how practice should be [or] a description of the ways in which current practice is limited or constrained" (Hackett et. al., 2006: 155). To put it in a different way, it remains somewhat unclear whether all experts took into consideration the feasibility of the suggested or endorsed practices. In this regard, one panelist indicated in relation to round 2 that "*we can check all boxes in an ideal situation but it depends on what's allowed in the country and what resources you can allocate*", while another one argued in his or her evaluation of the study that "*sometimes the proposed solutions are not always realistic for certain organizations*".

It is therefore possible that certain issues received a medium or low score because a number of panelist questioned the legal feasibility or cultural desirability in their specific region, which does however not alter the fact that the issue might be relevant for insider threat mitigation in another region where it is culturally or legally accepted. Think for instance of drug or alcohol screenings, which are subject to local laws and are therefore not legally (but also culturally) acceptable in all countries. The same principle applies to the difficulties related to insider threat mitigation, as a suggested difficulty can be present in one country but absent in another. Consequently, it is important to keep in mind the earlier

mentioned recommendation from Keeney et. al. (2006) to not solely look at the final results of this study (i.e. the high-rated practices), but to spend attention to the knowledge gathered throughout the different rounds of the study. Furthermore, a possible solution for future research is to keep track of subgroups within a larger panel (Turoff, 2002), or to use parallel panels based on cultural background (Gossler et. al., 2019).

To conclude, one expert questioned the novelty of our results, indicating that he or she is "*not sure the study is bringing any new insights to the surface [but is] only confirming existing methods"*. While we do not necessarily agree with the latter statement, we argue that even if the results are limited to a summary of existing methods, it provides useful insights on the state-of-the-art of insider threat prevention, detection and mitigation from the perspective of a multidisciplinary expert panel. As mentioned before, our study does not only provide organizations with a catalogue of possible insider threat mitigation measures that they can chose from to develop their tailor-made insider threat mitigation policy, but also paves the way for further research on insider threat mitigation, as "the method and results should be used as a means for structuring group discussion and as a means of raising issues for debate" (Hasson et. al., 2000: 1013).

6. Conclusion

6.1. Summary

This report elaborated on a three-round Delphi study on insider threat mitigation. The aim of the study was to transform our theoretical insider threat mitigation framework (Reveraert & Sauer, 2022a) into a tool with practical usability. In concrete terms, its main goal was to discover potential 'red flags' of insider threat incidents and good practices, actors and difficulties related to insider threat mitigation. The study employed the Delphi technique to iteratively compare and contrast the opinions of insider threat experts. A multidisciplinary panel of 25 international experts (e.g. corporate security, counterintelligence, insider threat training, …) completed three rounds of online questionnaires. Round 1 concerned open-ended, level-setting questions with panelists asked to share their expertise. In round 2, experts were presented with a list of all important information shared by the panel in round 1 in the form of a structured questionnaire whereby they were asked to rate each individual issue listed. The questionnaire of round 3, to conclude, provided the experts with the list of high-rated issues, after which they were asked whether they agreed or disagreed with the panel's decision and to explain their reasoning in case of disagreement.

Regarding the **evaluation of potential insider threat indicators**, the panel considers addictions to drugs, alcohol and gambling, as well as affinity with extremist ideology potential red flags of insider threats, both during recruitment and employment. Other factors that require vigilance from the organization *during recruitment* are falsifications of background information that indicates low integrity, an unresponsive attitude during the recruitment process and negative advice from either government authorities or references, while previous employment for a competitor, job-hopping, discrepancies between educational and career path and mental and physical health issues were less important factors. Furthermore, personality characteristics other than low score on integrity and manipulative nature (e.g. arrogance and lack of humility, consciousness or friendliness) are less perceived as factors that may point to insider threat. A bit to our surprise, the panel spent little attention to the applicant's motivation to work for the organization and (apart from addictions) to the applicant's personal problems. The latter finding is contrary to both the insights from the insider threat literature (Shaw & Sellers, 2015; Noonan, 2018) and our survey on insider threat awareness and behavior (Reveraert & Sauer, 2021b) where personal problems are seen as a possible breeding ground of insider threats.

Factors that may point to insider threat *during employment* concern both individual and organizational factors (Greitzer et. al., 2012; Greitzer et. al., 2016), with the majority relating to the former. The most obvious warning signals that were unanimously accepted by the panel in round 2 of the study are threatening employers or co-workers and receiving warnings from sttakeholders about the behavior of insiders. In line with the insider threat literature (BaMaung et. al., 2018; Gelles, 2016; Shaw & Sellers, 2015), the panel considers deviation from normal or baseline behavior an early warning of insider threat, although the results show that not all deviant behavior is worrisome. Behavioral anomalies like attempts to remove sensitive data, unauthorized access attempts to systems or physical locations not necessary for the job, unexplained wealth and changes in lifestyle all received a high rating from the panel. In contrast, sudden changes in working hours, changes in online or social media behavior and changes in mental health are considered worrisome by only part of the panel, while changes in personal status (e.g. divorce, new partner, …) or changes in physical health are considered alarming by less than half of the panel. Moreover, personality characteristics (e.g. not being able to deal with criticism, not being very empathetic and introversion) were less regarded by the panel as a potential red flag during employment. Concerning underlying reasons of insider threats, the panel rates disgruntlement with the organization relatively higher than personal strains (apart from addictions) like financial difficulties or unmet personal expectations, as well as personality disorders like

narcissism, which is in line with the results of our insider threat awareness and behavior survey (Reveraert & Sauer, 2021b). Regarding organizational factors, the presence of an organizational culture of fear and silence and unexplained irregularities in the accountancy of the organization are considered to be factors that may point to insider threat, while a number of organizational factors, like too heavy workloads and high levels of competitiveness, were considered by the panel as not necessarily indicative of future insider threat incidents.

Important with respect to red flags are subjective interpretation and contextualization. Concerning the former, it should be acknowledged that observation of a red flag depends on the subjective interpretation of the observer, which implies that what may appear suspicious to one observer might be a positive sign to another observer. Concerning the latter, whether a potential red flag is considered to be an indicator of insider threat depends on contextual factors. The panel for instance identified dismissal at a similar job and support for societal upheaval in the past as factors that may point to insider threat, but simultaneously argued that the context will determine whether it is actually considered a red flag of insider threat. In concrete terms, this means that the reason behind the dismissal (i.e. previous intentional misconduct or other reason not related to insider threat like performance issues, incompetence or economic reasons), the time frame (i.e. distant past or recent past) and/or theme of the activism (i.e. related or unrelated to the insider's position) are important to interpret whether it concerns an early warning signal of insider threat.

Regarding the **evaluation of insider threat mitigation measures**, the study resulted in a catalogue of possible insider threat mitigation measures that organizations can chose from to develop their tailor-made insider threat mitigation policy, organized according to the different steps of the theoretical framework. In the *recruitment stage* (I), recommended practices relate to screening background information of applicants (e.g. verifying CV, credentials, identity and criminal record) whereby organizations need to take screening seriously instead of carrying it out pro-forma, but also need to apply a risk-based approach. In the *organizational socialization stage* (II), the panel recommends organizations to apply the Aristotelian method, characterized by precept (e.g. a code of conduct), habit (e.g. a strong security culture) and demonstration (e.g. lead by example), as well as to have a supportive attitude (e.g. show care when needed) towards employees while simultaneously being strict but fair when it comes to violations of the code of conduct.

In the *observation stage* (III), the panel considers internal whistleblowing to be more effective than artificial intelligence tools to observe red flags of insider threat, although it does not completely disregard technology given that (alarms on) electronic access systems and endpoint security tools are recommended to guard the principle of least privilege. In the *investigation stage* (IV), the panel advises organizations to have a formal investigation policy that outlines who conducts the investigation and how the investigation proceeds, but does not necessarily recommend to formally outline in policies and procedures what behavior would trigger the investigation process. In the *anticipation stage* (V), it is noteworthy that only four out of the in total 37 proposed practices are recommended by the panel, meaning that the panel rather showed which practices are less useful to pre-empt imminent insider threats (e.g. positive incentives to seek resolution before an incident develops, deterrence practices, and awareness-raising initiatives) than which practices are useful.

In the *damage limitation* (VI) and *reconstruction stage* (VII), both preparatory practices (e.g. a business continuity plan and an event notification tree) and reactive practices (e.g. collecting evidence, identifying and changing compromised processes and conducting a post-incident analysis) are suggested by the panel to react to an insider threat incident, as well as practices related to internal and external incident communication (e.g. crisis communication plans and staff). In the *deliberation stage* (VIII), the panel mainly recommends to have a fair and consistent disciplinary system that

respects the rights of the offender, to focus on acts and not on people, to discuss different options with relevant stakeholders to develop plan A/B/C, to review access permissions and to make sure other employees know appropriate measures are taken. In the *termination stage* (IX), some high-rated exit procedures outlined by the panel are straightforward (e.g. compliance with applicable laws and the development, consistent application and regular update of termination procedures), whereas others resemble practices suggested in the insider threat literature (e.g. reclaiming equipment from the terminated employee, revoking virtual and physical access and conducting exit interviews).

Regarding *mismanagement* (X), practices that the panel recommends to deal with false positives concern both practices aimed at restoring the relation with the wrongly accused insider (e.g. full rehabilitation and welfare/psychological support) and practices targeted at preventing the reoccurrence of similar false positives (e.g. reviewing the indicators and/or the reporting route that led to the false assessment and awareness of possible repercussions). To conclude, the panel puts its own recommendation to implement a formal insider threat mitigation team in perspective, with panelists indicating that the desirability of a formal insider threat mitigation team depends on the size and type of the organization, that the formal insider threat mitigation team should not necessarily be a distinct team but can equally reside in an already existing team and that the formal insider threat mitigation team should cooperate with other relevant stakeholders like co-workers, line management and social partners.

6.2. Key take-aways

It is notable that two common threads seem to run through the recommendations from the panel. The first one is the suggestion to adopt a risk-based approach. During recruitment, this means that background screenings are adjusted depending on the 'degree of insiderness' related to the role of the new insider (Bishop et. al.,2009; Bishop et al., 2010; George et. al., 2019; Probst et. al., 2010). Applicants that will have a large amount of access to the organizational assets or access that will apply to the most important assets of the organization should be subjected to a tougher screening procedure (George et. al., 2019). During employment, this means that organizations apply and monitor the principle of least privilege, whereby access is role-based so that insiders can only consult organizational assets that they need for their job, whereby risk analyses check the possible impact of misuse of this access and (alarms on) electronic access systems detect unauthorized access attempts. The second common thread is internal whistleblowing. The panel puts considerable emphasis on internal whistleblowing to observe red flags during employment, as recommended in the insider threat literature (Bell et. al., 2019; Colwill, 2009; Mehan, 2016; UK Centre for the Protection of National Infrastructure, 2011; US National Insider Threat Task Force, 2016). The panel also advises organizations to have both an internal investigation protocol and a response plan to concerns reported through the whistleblowing system.

Another aspects that transcends the steps of the theoretical framework is transparency, which is considered important by the panel in the stages preceding an insider threat incident. It is however less recommended in the aftermath of an insider threat incident, both internally and externally. This does not mean that internal and external communication is trivial, given that the panel spends considerable attention to practices related to incident communication. The recommendation to control public announcements in order to safeguard the organization's reputation seems to explain the relatively high number of dark or hidden insider threats. Additionally, scrutiny of social media activity is considered to be suitable with respect to pre-employment screening, but less suitable for in- and post-employment screening, which is in line with the results of our survey on insider threat awareness and behavior (Reveraert & Sauer, 2021b). Apart from external audits, outsourcing insider threat mitigation activities is less recommended by the panel, both with respect to background screening during

recruitment as to the involvement of external expertise during the investigation stage or the damage limitation and reconstruction stage.

One of the most surprising results, if not the biggest one, is that the panel is reluctant to the use of artificial intelligence and machine learning tools to automatically observe red flags during employment. This is in contrast to insider threat literature, where the use of artificial intelligence receives considerable attention (e.g. Brown et. al., 2013; Koutsouvelis et. al., 2020; Le & Zincir-Heywood, 2019). A possible explanation for this low rating might be that the panel perceives that the quality of the existing artificial intelligence tools is not sufficient, with the risk of false positives being still too high. Moreover, it can be assumed that a panel composed of experts on cybersecurity, with more specific expertise on these tools, might have rated artificial intelligence tools higher. In any case, the discrepancy between the priority given to artificial intelligence in the insider threat literature and the minor role our panel assigns to these tools should be explored in further research.

Other striking results include the relatively limited interest the panel has in motivation of the employee to work for the organization, in the potential personal problems related to the private life of the insider (except for addictions), in the fear of retaliation against internal whistleblowers (i.e. reporters of red flags) and in the insider's vulnerability to social engineering, as well as the relatively high priority the panel gives to the impact of an incident in the determination of an offender's punishment. While the limited attention spent to vulnerability to social engineering seems to contradict the results of our survey on insider threat awareness and behavior (Reveraert & Sauer, 2021b), the other oddities are in conflict with the recommendations found in the insider threat literature. Also noteworthy is the panel's recommendation to limit interaction with suspects and offenders of insider threat incidents, and that although addiction to drugs and alcohol and low integrity were considered potential red flags, practices to discover these red flags were not endorsed by the panel. A possible explanation for the latter is that these mitigation measures are not commonly accepted in all countries, either culturally or legally. It is therefore possible that certain issues received a medium or low score from the panel because a number of panelist questioned the legal feasibility or cultural desirability in their specific region, which does however not alter the fact that the issue might be relevant for insider threat mitigation in regions where it is culturally or legally accepted. As a result, it is important to not solely look at the final results of this study (i.e. the high-rated practices), but to spend attention to the knowledge gathered throughout the different rounds of the study (Keeney et. al., 2006).

Additionally, it is striking to see that in a number of cases, the panel either identifies reasons that complicate the implementation of its own recommended practices or identifies a discrepancy between the recommended situation and the actual situation. Concerning the former, the panel for instance recommends to adopt a risk-based approach, but simultaneously recognizes that this implies unequal treatment of employees that might in its turn lead to push back from unions/labor groups. Concerning the latter, the panel emphasizes the importance of creating a culture of reporting to observe red flags during employment, but simultaneously claims that whistleblowing is currently not culturally accepted leading to an unwillingness to report. A similar discrepancy between the recommended situation and the actual situation is present with respect to tailor-made training for managers and staff to observe and report red flags, cultural acceptance of in-employment screening practices (e.g. electronic access control, alarms on access systems, …) and awareness of the insider threat problem on senior and middle management levels, which are all recommended by the panel but are also believed to be currently absent. Future research should therefore look at ways to bring the actual situation more in line with the recommendations from our panel.

In conclusion, although it is "unlikely that a clear-cut (to all concerned) resolution of a policy issue will result from such an analysis", we believe that the results of our study are valuable both for theoretical and practical purposes (Okoli & Pawlowski, 2004; Hasson & Keeney, 2011), as well as to bridge the gap between the two (Stone Fish & Busby, 2005). The results of the study provide participants with useful insights on what experts consider to be potential red flags, as well as with an inventory of insider threat mitigation measures to better secure organizations against insider threats. In any case, the insights derived from this Delphi study should be interpreted as complementary to other insider threat insights, as they further broaden the knowledge on the insider threat problem and stimulate debate on ways to mitigate it (Mukherjee et. al., 2015).

Implementation of results of Delphi studies in real life however remains a challenge (Kozak & Iefremova, 2014), which makes it important that "findings of consensus methods (…) are further explored, discussed, deliberated and put into theoretical context before being implemented into practice" (Foth et. al., 2016: 119). This was exactly the aim of our study, as the Delphi study was a first step in the refinement of the theoretical insider threat mitigation framework, allowing us to give the abstract terms used within the conceptual model a more concrete meaning. Still, it can be argued that the practical usability of the theoretical framework can still be further improved by verifying the results from this Delphi study.

Contact information:

If you have any questions or remarks concerning this study, please contact
mathias.reveraert@uantwerpen.be

7. References

Afolabi, M. B. (2017). An Insight to Security Vetting. In L. N. Asiegbu, *Unending Frontiers in Intelligence and Security Studies* (pp. 61-69). Ekiti, Nigeria: Intelligence and Security Studies Programme, Afe Babalola University, Ado.

Anderson, M. (1994). Introduction. In T. R. Sarbin, R. M. Carney, & C. Eoyang (eds.), *Citizen Espionage Studies in Trust and Betrayal* (pp. 1-17). United States of America: Greenwood Publishing Group.

Baker, J., Lovell, K., & Harris, N. (2006). How expert are the experts? An exploration of the concept of 'expert' within Delphi panel techniques. *Nurseresearcher, 14*(1), 59-70.

BaMaung, D. (2018). The Hidden Threat. *International Airport Review, 22*(4), 22-25.

BaMaung, D., McIlhatton, D., MacDonald, M., & Beattie, R. (2018). The Enemy Within? The Connection between Insider Threat and Terrorism. *Studies in Conflict & Terrorism*(41:2), 133-150. doi:10.1080/1057610X.2016.1249776

Barnes, J. E., Spigariol, A., Nicas, J., & Goldman, A. (2022, March 15). Submarine Spy Couple Tried to Sell Nuclear Secrets to Brazil. *New York Times*. Retrieved from https://www-nytimes-com.cdn.ampproject.org/c/s/www.nytimes.com/2022/03/15/us/politics/submarine-spy-brazil.amp.html

Barrios, M., Guilera, G., Nuno, L., & Gomez-Benito, J. (2021). Consensus in the delphi method: What makes a decision change? *Technological Forecasting & Social Change, 163*, 1-10. doi:https://doi.org/10.1016/j.techfore.2020.120484

Beattie, R., & BaMaung, D. (2015). Mind the Gap: HRD's Role in Keeping Organization's Safe. *16th International Conference on Human Resource Development Research and Practice across Europe.* Cork, Ireland: Academy of Human Resource Development.

Belk, W. R., & Hix, T. D. (2018). *Insider Threat Program: Maturity Framework.* US: National Insider Threat Task Force (NITTF).

Bell, A. J., Rogers, M. B., & Pearce, J. M. (2019). The insider threat: Behavioral indicators and factors influencing likelihood of intervention. *International Journal of Critical Infrastructure Protection*(24), 166-176.

Bishop, M., Engle, S., Frincke, D. A., Gates, C., Greitzer, F. L., Peisert, S., & Whalen, S. (2010). A Risk Management Approach to the 'Insider Threat'. In C. W. Probst, J. Hunker, D. Gollmann, & M. Bishop, *Insider Threats in Cyber Security* (pp. 115-137). Boston: Springer.

Bishop, M., Gates, C., Frincke, D., & Greitzer, F. L. (2009). AZALIA: an A to Z Assessment of the Likelihood of Insider Attack. *IEEE Conference on Technologies for Homeland Security* (pp. 385 - 392). Boston: IEEE.

Bunn, M., & Sagan, S. (2016). *Insider Threats.* Ithaca: Cornell University Press. doi:https://doi.org/10.7591/9781501705946

Catrantzos, N. (2009). *No dark corners : defending against insider threats to critical infrastructure.* Monterey, California: Naval Postgraduate School.

Christie, C. A., & Barela, E. (2005). The Delphi technique as a method for increasing inclusion in the evaluation process. *The Canadian Journal of Program Evaluation, 20*(1), 105-122.

Chuenjitwongsa, S. (2017). *How to conduct a Delphi Study.* UK: Wales Deanery. Retrieved from https://foundation.walesdeanery.org/sites/default/files/how_to_conduct_a_delphistudy.pdf

Cole, E., & Ring, S. (2006). What Is There to Worry About? In E. Cole, & S. Ring, *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft* (pp. 3-48). Rockland, MA: Syngress Publishing, Inc. Retrieved from https://www.elsevier.com/books/insider-threat-protecting-the-enterprise-from-sabotage-spying-and-theft/cole/978-1-59749-048-1

Colquitt, J. A., & Scott, B. A. (2007). Trust, Trustworthiness, and Trust Propensity: A Meta-Analytic Test of Their Unique Relationships With Risk Taking and Job Performance. *Journal of Applied Psychology, 92*(4), 909-927.

Colwill, C. (2009). Human factors in information security: The insider threat - Who can you trust these days? *Information Security Technical Report*, 186-196. doi:10.1016/j.istr.2010.04.004

Cools, M. (1994). *Werknemerscriminaliteit.* Brussel: VUB Press.

Costa, D. L., Collins, M. L., Perl, S. J., Silowash, G. J., & Spooner, D. L. (2014). An Ontology for Insider Threat Indicators: Development and Applications. *9th International Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS).* Fairfax, VA: CEUR Workshop Proceedings.

Dalkey, N., & Helmer, O. (1963). An Experimental Application of the Delphi Method to the Use of Experts. *Management Science, 9*(3), 458-467.

De Graaff, B. (2019). *Data en Dreiging: Stap in de Wereld van Intelligence.* Amsterdam: Boom Uitgevers.

Diamond, I. R., Grant, R. C., Feldman, B. M., Pencharz, P. B., Ling, S. C., Moore, A. M., & Wales, P. W. (2014). Defining consensus: A systematic review recommends methodologic criteria for reporting of Delphi studies. *Journal of Clinical Epidemiology, 67*, 401-409. doi:https://doi.org/10.1016/j.jclinepi.2013.12.002

Dupuis, M., & Khadeer, S. (2016). Curiosity Killed the Organization: A Psychological Comparison between Malicious and Non-Malicious Insiders and the Insider Threat. *Proceedings of the 5th Annual Conference on Research in Information Technology* (pp. 35-40). New York: Association for Computing Machinery. doi:10.1145/2978178.2978185

Elangovan, A., & Shapiro, D. L. (1998). Betrayal of Trust in Organizations. *The Academy of Management Review, 23*(3), 547-566.

Elifoglu, I. H., Abel, I., & Tasseven, Ö. (2018). Minimizing Insider Threat Risk with Behavioral Monitoring. *Review of Business: Interdisciplinary Journal of Risk and Society*(38:2), 61-73.

Eoyang, C. (1994). Models of Espionage. In T. R. Sarbin, R. M. Carney, & C. Eoyang (eds.), *Citizen Espionage: Studies in Trust and Betrayal* (pp. 69-91). United States of America: Greenwood Publishing Group.

Foth, T., Efstathiou, N., Vanderspank-Wright, B., Ufholz, L.-A., Dütthorn, N., Zimansky, M., & Humphrey-Murto, S. (2016). The use of Delphi and Nominal Group Technique in nursing education: a review. *International Journal of Nursing Studies, 60*, 112-120. doi:https://doi.org/10.1016/j.ijnurstu.2016.04.015

Gelles, M. (2016). *Insider Threat: Detection, Mitigation, Deterrence and Prevention.* Oxford: Elsevier - Health Science Division.

Giannarou, L., & Zervas, E. (2014). Using Delphi technique to build consensus in practice. *Int. Journal of Business Science and Applied Management, 9*(2), 66-82. Retrieved from https://business-and-management.org/library/2014/9_2--65-82-Giannarou,Zervas.pdf

Goold, S. D. (2002). Trust, Distrust and Trustworthiness Lessons from the field. *Journal of General Internal Medicine, 17*, 79-81.

Gossler, T., Sigala, I. F., Wakolbinger, T., & Buber, R. (2019). Applying the Delphi method to determine best practices for outsourcing logistics in disaster relief. *Journal of Humanitarian Logistics and Supply Chain Management, 9*(3), 438-474. doi:10.1108/JHLSCM-06-2018-0044

Greitzer, F. L., Imran, M., Purl, J., Axelrad, E. T., Leong, Y. M., Becker, D. (., & Laskey, K. B. (2016). Developing an Ontology for Individual and Organizational Sociotechnical Indicators of Insider Threat Risk. *The Eleventh International Conference on Semantic Technology for Intelligence, Defense, and Security (STIDS 2016)*, (pp. 1-9). Fairfax.

Greitzer, F. L., Kangas, L. J., Noonan, C. F., Dalton, A. C., & Hohimer, R. E. (2012). Identifying At-risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats. *Hawaii International Conference on System Sciences* (pp. 2392-2401). Hawaii: IEEE Computer Society. doi:10.1109/HICSS.2012.309

Grime, M. M., & Wright, G. (2016). Delphi Method. *Wiley StatsRef: Statistics Reference Online*, 1-6. doi:10.1002/9781118445112.stat07879

Hackett, S., Masson, H., & Phillips, S. (2006). Exploring Consensus in Practice with Youth Who Are Sexually Abusive: Findings from a Delphi Study of Practitioner Views in the United Kingdom and the Republic of Ireland. *Child Maltreatment, 11*(2), 146-156. doi:10.1177/1077559505285744

Hasson, F., & Keeney, S. (2011). Enhancing rigour in the Delphi technique research. *Technological Forecasting & Social Change, 78*, 1695-1704. doi:10.1016/j.techfore.2011.04.005

Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing, 32*(4), 1008-1015.

Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing, 32*(4), 1008 - 1015. doi:https://doi.org/10.1046/j.1365-2648.2000.t01-1-01567.x

Hawley, K. (2014). Trust, Distrust and Commitment. *Noûs, 48*(1), 1-20.

Ho, S. M., & Katukoori, R. R. (2013). Agent-based modelling to visualise trustworthiness: a socio-technical framework. *International Journal of Mobile Network Design and Innovation, 5*(1), 17-27.

Ho, S. M., Kaarst-Brown, M., & Benbasat, I. (2018). Trustworthiness Attribution: Inquiry Into Insider Threat Detection. *Journal of the Association for Information Science and Technology, 69*(2), 271–280.

Hsu, C.-C., & Sandford, B. A. (2007). The Delphi Technique: Making Sense of Consensus. *Practical Assessment, Research, and Evaluation*(12), 1-8.

International Atomic Energy Agency. (2008). *Preventive and Protective Measures against Insider Threats.* Vienna: IAEA Nuclear Security Series No. 8.

Jakobsson, U., & Westergren, A. (2005). Statistical methods for assessing agreement for ordinal data. *Scandinavian Journal of Caring Sciences*, 427-431. Retrieved from https://www.semanticscholar.org/paper/Statistical-methods-for-assessing-agreement-for-Jakobsson-Westergren/8c000e813c6eecfe26d124c1cf43decf4933188f

Keeney, S., Hasson, F., & McKenna, H. (2006). Consulting the oracle: ten lessons from using the Delphi technique in nursing research. *The Journal of Advanced Nursing (JAN)*, 205-212. doi: 10.1111/j.1365-2648.2006.03716.x

Klotz, A. C., Da Motta Veiga, S. P., Buckley, M. R., & Gavin, M. B. (2013). The role of trustworthiness in recruitment and selection: A review and guide for future research. *Journal of Organizational Behavior*, 104-119.

Koutsouvelis, V., Shiaeles, S., Ghita, B., & Bendiab, G. (2020). Detection of Insider Threats using Artificial Intelligence and Visualisation. *2020 2nd International Workshop on Cyber-Security Threats, Trust and Privacy management in Software-defined* (pp. 437-443). Netsoft.

Kozak, M., & Iefremova, O. (2014). Implementation of the Delphi technique in finance. *e-Finanse: Financial Internet Quarterly, 10*(4), 36-45.

Landeta, J. (2006). Current validity of the Delphi method in social sciences. *Technological Forecasting & Social Change, 73*, 467-482.

Lange, T., Kopkow, C., Lützner, J., Günther, K.-P., Gravius, S., Scharf, H.-P., . . . Schmitt, J. (2020). Comparison of different rating scales for the use in Delphi studies: different scales lead to different consensus and show different test-retest reliability. *BMC Medical Research Methodology, 20*(28), 1-11. doi:10.1186/s12874-020-0912-8

Lanssens, P. (2020). The Belgian civil intelligence service VSSE - general overview and current trends and threats. *Lecture at VUB for Master students European and Economic Governance* (pp. 1-18). Brussel: Veiligheid Van De Staat.

Le, D., & Zincir-Heywood, A. (2019). Machine learning based Insider Threat Modelling and Detection. *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)* (pp. 1-6). Washington D.C., USA: IFIP/IEEE.

Lee, G., & Kulkarni, U. (2011). Business Intelligence in Corporate Risk Management. *Proceedings of the Seventeenth Americas Conference on Information Systems* (pp. 1-11). Detroit, Michigan: AMCIS.

Linstone, H. A., & Turoff, M. (2002). *The Delphi Method Techniques and Applications.* Addison-Wesley Publishing Company. Retrieved from https://web.njit.edu/~turoff/pubs/delphibook/index.html

Luckey, D., Stebbins, D., Orrie, R., Rebhan, E., Bhatt, S. D., & Beaghley, S. (2019). *Assessing Continuous Evaluation Approaches for Insider Threats.* Santa Monica, Calif: RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR2684.html

Martinez-Moyano, I. J., Rich, E., Conrad, S., Andersen, D. F., & Stewart, T. R. (2008). A Behavioral Theory of Insider-Threat Risks: A System Dynamics Approach. *ACM Transactions on Modeling and Computer Simulation, 18*(2), 7:1-7:27.

McKnight, D. H., & Chervany, N. L. (2001). Trust and Distrust Definitions: One Bite at a Time. In R. Falcone, M. Singh, & Y. Tan (eds.) (Ed.), *Trust in Cyber-societies Integrating the Human and Artificial Perspectives - Lecture Notes in Computer Science* (pp. 27-54). Berlin: Springer. doi:https://doi.org/10.1007/3-540-45547-7_3

Mehan, J. E. (2016). *Insider Threat: A Guide to Understanding, Detecting, and Defending Against the Enemy from Within.* Cambridgeshire: IT Governance Publishing.

Meijering, J., Kampen, J., & Tobi, H. (2013). Quantifying the development of agreement among experts in Delphi studies. *Technological Forecasting & Social Change, 80*(8), 1607-1614. doi:https://doi.org/10.1016/j.techfore.2013.01.003

Morris, J. H., & Moberg, D. J. (1994). Work Organizations as Contexts for Trust and Betrayal. In T. R. Sarbin, R. M. Carney, & C. Eoyang (eds.), *Citizen Espionage: Studies in Trust and Betrayal* (pp. 163-187). United States of America: Greenwood Publishing Group.

Mukherjee, N., Hugé, J., Sutherland, W. J., McNeill, J., Van Opstal, M., Dahdouh-Guebas, F., & Koedam, N. (2015). The Delphi technique in ecology and biological conservation: applications and guidelines. *Methods in Ecology and Evolution, 6*, 1097–1109. doi:10.1111/2041-210X.12387

Neumann, P. G. (2010). Combatting Insider Threats. In C. W. Probst, J. Hunker, D. Gollmann, & M. Bishop, *Insider Threats in Cyber Security* (pp. 17-44). Boston: Springer.

Nitsch, D., Baetz, M., & Hughes, J. C. (2005). Why Code of Conduct Violations go Unreported: A Conceptual Framework to Guide Intervention and Future Research. *Journal of Business Ethics, 57*, 327-341.

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. *Information & Management, 42*, 15–29.

Padayachee, K. (2016). An assessment of opportunity-reducing techniques in information security: An insider threat perspective. *Decision Support Systems, 92*, 47-56. doi:http://dx.doi.org/10.1016/j.dss.2016.09.012

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Homeland Security & Emergency Management, 11*(4), 489-510. doi:https://doi.org/10.1515/jhsem-2014-0035

Polit, D. F., Beck, C. T., & Owen, S. V. (2007). Is the CVI an Acceptable Indicator of Content Validity? Appraisal and Recommendations. *Research in Nursing & Health, 30*, 459–467. doi:10.1002/nur.20199

Power, R., & Forte, D. (2006). Thwart the insider threat: a proactive approach to personnel security. *Computer Fraud & Security*, 10-15.

Probst, C. W., Hunker, J., Gollmann, D., & Bishop, M. (2010). Aspects of Insider Threats. In C. W. Probst, J. Hunker, D. Gollmann, & M. Bishop, *Insider Threats in Cyber Security* (pp. 1-15). Boston: Springer.

Raskin, M. S. (1994). The Delphi Study in Field Instruction Revised: Expert Consensus on Issues and Research Priorities. *Journal of Social Work Education, 30*(1), 75-89. Retrieved from https://www.jstor.org/stable/23043175?origin=JSTOR-pdf&seq=1#metadata_info_tab_contents

Rayens, M. K., & Hahn, E. J. (2000). Building Consensus Using the Policy Delphi Method. *Policy, Politics, & Nursing Practice, 1*(4), 308-315. doi:https://doi.org/10.1177%2F152715440000100409

Reason, J. (1998). Achieving a safe culture: Theory and practice. *Theory and practice, Work & Stress, 12*(3), 293-306.

Reveraert, M., & Sauer, T. (2021a). Redefining insider threats: a distinction between insider hazards and insider threats. *Security Journal, 34*, 755-775. doi:https://doi.org/10.1057/s41284-020-00259-x

Reveraert, M., & Sauer, T. (2021b). *Insider threat awareness and behavior: A survey among Belgian security officers.* Antwerpen: Universiteit Antwerpen.

Reveraert, M., & Sauer, T. (2022a). *Trust and betrayal in organizations: a conceptual model to mitigate insider threats*. Manuscript submitted for publication.

Reveraert, M., Sas, M., Reniers, G., Hardyns, W. & Sauer, T. (2022b). *Insider Threats to Critical Infrastructure: A Typology*. Manuscript submitted for publication.

Rowe, G., & Wright, G. (2001). Expert Opinions in Forecasting: The Role of the Delphi Technique. In J. (. Armstrong, *Principles of Forecasting. International Series in Operations Research & Management Science* (pp. 125-144). Boston, MA.: Springer. doi:https://doi.org/10.1007/978-0-306-47630-3_7

Santaguida, P., Dolovich, L., Oliver, D., Lamarche, L., Gilsing, A., Griffith, L. E., . . . Raina, P. (2018). Protocol for a Delphi consensus exercise to identify a core set of criteria for selecting health related outcome measures (HROM) to be used in primary health care. *BMC Family Practice, 19*, 1-14. doi:https://doi.org/10.1186/s12875-018-0831-5

Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report*(15), 112-133. doi:10.1016/j.istr.2010.11.002

Schmidt, R. C. (1997). Managing Delphi Surveys Using Nonparametric Statistical Techniques. *Decision Sciences, 28*(3), 763-774.

Searle, R., Rice, C., McConnell, A., & Dawson, J. (2017). *Bad apples? Bad barrels? Or bad cellars? Antecedents and processes of professional misconduct in UK Health and Social Care: Insights into sexual misconduct and dishonesty.* Coventry: Professional Standards Authority.

Siponen, M. (2000). A conceptual foundation for organizational information security. *Information Management & Computer Security, 8*(1), 31-41. doi:https://doi.org/10.1108/09685220010371394

Siponen, M., & Kajava, J. (1998). Ontology of organizational IT security awareness-from theoretical foundations to practical framework. *Proceedings Seventh IEEE International Workshop on Enabling Technologies: Infrastucture for Collaborative Enterprises* (pp. 327 - 331). Stanford, CA, USA, USA: IEEE. doi:https://doi.org/10.1109/ENABL.1998.725713

Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi Method for Graduate Research. *Journal of Information Technology Education, 6*, 1-21. doi:https://doi.org/10.28945/199

Steneck, N. H. (1994). Research Universities and Scientific Misconduct: History, Policies, and the Future. *The Journal of Higher Education, 65*(3), 310-330.

Steurer, J. (2011). The Delphi method: an efficient procedure to generate knowledge. *Skeletal Radiol, 40*, 959-961.

Stevenson, V. (2010). *Some initial methodological considerations in the development and design of Delphi Surveys,.* St. Andrews: Supergen XIV. Retrieved from http://orca.cardiff.ac.uk/id/eprint/9949

Stone Fish, L., & Busby, D. M. (2005). The Delphi Method. In D. Sprenkle, & F. (. Piercy, *Research methods in family therapy* (2nd ed., pp. 238-253). New York: Guilford. Retrieved from https://scholarsarchive.byu.edu/facpub/4584/

Thompson, E. E. (2018). Introduction. In E. E. Thompson, *The Insider Threat: Assessment and Mitigation of Risks* (pp. 1-34). New York: CRC Press Taylor and Francis Group.

Turoff, M. (2002). The Policy Delphi. In H. A. Linstone, & M. (. Turoff, *The Delphi Method: Techniques and Applications* (pp. 80-96). Retrieved from https://web.njit.edu/~turoff/pubs/delphibook/index.html

UK Centre for the Protection of National Infrastructure. (2011). *Investigating Employees of Concern: A Good Practice Guide.* London: UK Centre for the Protection of National Infrastructure. Retrieved from https://www.cpni.gov.uk/investigation-and-disciplinary

UK Centre for the Protection of National Infrastructure. (2019). *Exit procedures guidance.* London: Centre for the Protection of National Infrastructure (CPNI).

US National Insider Threat Task Force. (2016). *Protect your organization from the inside out: Government best practices.* Washington D.C.: The National Counterintelligence and Security Center.

van de Linde, E., & van der Duin, P. (2011). The Delphi method as early warning: Linking global societal trends to future radicalization and terrorism in The Netherlands. *Technological Forecasting & Social Change, 78*, 1557-1564. doi:http://dx.doi.org/10.1016/j.techfore.2011.07.014

Van Dolderen, B., Stoffers, J., & Kleefstra, A. (2017). Delphi als onderzoeksmethode voor consensus en draagvlak: een casus in de gezondheidszorg. *Tijdschrift voor Begeleidingskunde, 6*(1), 24-30.

Van Laethem, W. (2005). Veiligheidsmachtigingen, veiligheidsadviezen, veiligheidsattesten en andere veiligheidsdocumenten. Een snelle kennismaking. *Private Veiligheid – Sécurité privée*, 16-21.

Vogel, C., Zwolinsky, S., Griffiths, C., Hobbs, M., Henderson, E., & Wilkins, E. (2019). A Delphi study to build consensus on the definition and use of big data in obesity research. *International Journal of Obesity, 43*, 2573-2586. doi:https://doi.org/10.1038/s41366-018-0313-9

von der Gracht, H. A. (2012). Consensus measurement in Delphi studies Review and implications for future quality assurance. *Technological Forecasting & Social Change, 79*, 1525-1536. doi:10.1016/j.techfore.2012.04.013

Von Solms, R., & Von Solms, B. (2004). From policies to culture. *Computers & Security, 23*, 275-279. doi:10.1016/j.cose.2004.01.013

Waltz, E. (2003). *Knowledge Management in the Intelligence Enterprise.* Bosten: Artech House.

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly, 37*(1), 1-20.

Wynd, C. A., Schmidt, B., & Schaefer, M. A. (2003). Two Quantitative Approaches for Estimating Content Validity. *Western Journal of Nursing Research, 25*(5), 508-518.