Redefining insider threats : a distinction between insider hazards and insider threats

Redefining insider threats: a distinction between insider hazards and insider threats

Abstract

This article suggests a new definition of insiders and insider threats. It refrains from applying a harm-oriented perspective that concentrates on the insider's intention to cause harm because it defines the insider threat either too narrow or too broad. Instead, a privilege-oriented perspective is applied that focuses on the insider's intention to misuse his privileged access to or knowledge about the organizational assets. Because existing privilege-oriented definitions refrain from making an explicit and clear-cut division between intentional and unintentional misuse of privilege, a new conceptualization is suggested that distinguishes insider hazards from insider threats. If the insider unintentionally misuses his insider privilege, it concerns an insider hazard. If the insider intentionally misuses his insider privilege, it is regarded as an insider threat.

Key words: Insider threat – Insider hazard – Organizational culture – Organizational behavior – Security policy - Trust

1. Introduction

This article redefines insiders and insider threats. Existing insider threat definitions originate from two different perspectives, namely a harm-oriented perspective and a privilege-oriented perspective (Information Security Forum, 2015; Krull, 2016; Maasberg, Warren & Beebe, 2015; Willison & Warkentin, 2013). Although harm-oriented definitions also refer to the insider privilege, the difference between both perspectives lies in the insider's intentionality. On the one hand, the harm-oriented definitions emphasize the insider's intention to harm the organization. On the other hand, privilege-oriented definitions put emphasis on the insider's intention to misuse his[1] insider privilege.

In this article, preference is given to the privilege-oriented perspective. Although other scholars have already put emphasis on the misuse of privilege in their conceptualization (Gelles, 2016; Greitzer, Kangas, Noonan, Dalton & Hohimer, 2012; Padayachee, 2016), they refrain from making an explicit and clear-cut division between intentional and unintentional misuses of privilege. As a result, this paper proposes a new conceptualization of insider threats. A distinction between insider hazards and insider threats is suggested, based on the question whether the insider wittingly misuses the access/knowledge, or whether the insider can be held accountable for the misuse of privilege. If the insider unwittingly misuses the privilege (i.e. no accountability), the incident is considered to be an insider hazard. In contrast, if the insider wittingly misuses the access or knowledge (i.e. accountability), the incident is considered to be an insider threat. Hence, it is suggested in this article that only the intentional misuse of privileged access/knowledge by insiders, whether or not with the intention to inflict harm, should be interpreted as an insider threat.

From a policy perspective, the distinction between insider hazards and insider threats is suitable because both raise different policy questions and therefore require different policy orientations. While insider hazard policy concerns communication, education and training to prevent insufficient proficiency, insider threat policy relates to compliance, norm enforcement and norm internalization to prevent insufficient trustworthiness. In other words, insider hazard policy is concentrated on imparting the code of conduct of the organization, while insider threat policy is focused on ensuring that insiders adhere to the code of conduct.

In what follows, the article first starts with an outline of the existing definitions originating from both the harm-oriented and the privilege-oriented perspective. After explaining why the contemporary definitions are unsatisfactory, we suggest a new conceptualization by elaborating on the division between insider hazards and insider threats. To conclude, the advantages and shortcomings of our conceptualization will be outlined.

2. Existing insider threat definitions

This article first elaborates on the two existing perspectives to define the insider threat concept, one centered on the intention to harm the organization and one concentrated on the intention to misuse the privilege given by the organization.

2.1. Harm-oriented perspective

Starting from a harm-oriented perspective, the insider threat definition depends on whether or not the insider has the intention to harm the organization. Generally, a distinction is made between malicious and non-malicious insider threats (Bunn & Sagan, 2016; Noonan, 2018; Nurse et. al., 2014; Sarkar, 2010). Some tend to interpret insider threats narrow by restricting it to the so-called malicious insider who has the explicit intent to negatively affect the organization. Cole & Ring (2006: 8) for instance refer to the insider threat as "anyone who has special access or knowledge with the intent to cause harm or danger". Also the United States (US) Transport Security Administration (TSA) defines the insider threat as "one or more individuals with access or insider knowledge that allows them to exploit the vulnerabilities of the Nation's transportation systems with the intent to cause harm" (Deffer, 2012: 2). Also other entities, like for instance the International Atomic Energy Agency (IAEA) in their Nuclear Security Series (NSS), interpret insider threats narrow by concentrating on the malicious insider (IAEA, 2008). The common thread that runs through the narrow definitions is insider access/knowledge and intent to harm. An example of a malicious insider threat is the terrorist shooting at Fort Hood where US Army psychiatrist Nidal Malik Hasan killed 13 colleagues and injured several others out of ideological convictions (Zegart, 2016).

In contrast to the above interpretation a number of researchers tend to apply a broader scope by including non-malicious insiders, or insiders that inflict harm without the intention to inflict harm. For example the Computer Emergency Response Teams (CERT) at the Software Engineering Institute of Carnegie Mellon University, an expert organization in (cyber)security, define insider threat as "the potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the

organization" (Elifoglu, Abel & Tasseven, 2018: 62). Steele & Wargo (2007: 25) too include unintentional insider incidents in their conceptualization, stipulating that a "common mistake in defining insider threats is limiting focus on malicious insiders. Failing to recognize the threats from insiders' unintentional or accidental actions also has led to a number of high-profile security breaches". Also other researchers, like for instance Nurse et al (2014), interpret insider threats more broad by considering all insider actions that cause harm to the organization as insider threats. The US soldiers that recorded their work-out session on the social media application Strava and that thereby accidentally revealed the location of the US military base (Hern, 01/28/2018) can be used as an illustration of a non-malicious insider threat.

Applying a harm-oriented perspective is problematic because harm-oriented definitions define the concept either too narrow or too broad. Given that the principal objective of each organization is to prevent harm to the organization, confining the insider threat to malicious incidents provides an interpretation that is too strict. Focusing solely on the malicious insider would ignore an important sub-group of insider threats, namely the insiders that wittingly misconduct themselves without intent to cause harm (Bunn & Sagan, 2016; Neumann, 2010). If insiders decide to intentionally misconduct themselves, this should be considered an insider threat, even if the misconduct has no harmful purpose.

The fact that each organization wants to prevent harm to the organization might however give the impression that the broad interpretation, regarding all harmful incidents involving an insider as an insider threat, is desirable. However, the broad interpretation runs the risk of turning insider threat into a container concept, which complicates the formation of an adequate mitigation policy. In other words, one should be careful not to make the insider threat concept a catch-all term, because container concepts make room for ambiguity and therefore complicate the formation of adequate policy to counter the problem. Analogy can be made to the concept of 'radicalization' that too suffers

from ambiguity and lacks a clear-cut standard definition that everybody agrees upon, resulting in difficulties to develop adequate deradicalization policies (Coolsaet, 2015; Coolsaet, 2016).

2.2. Privilege-oriented perspective

In contrast to the harm-oriented perspective, the privilege-oriented perspective does not focus on the (intentionality of the) harm to the organization, but on the privilege that the insider gets, and more specifically on whether or not the insider has the intention to misuse this privilege (Information Security Forum, 2015; Krull, 2016; Maasberg, Warren & Beebe, 2015; Willison & Warkentin, 2013). It starts from the assumption that the organization gives insiders access to and/or knowledge about the organizational assets. It further assumes that in order to stimulate the proper handling of the organizational assets, the organization provides the insiders with guidance on how to behave themselves in an appropriate way. In other words, the organization can establish a code of conduct that reflects the organizational culture and that contains organizational norms that insiders have to adhere to. Analogous to Katzenstein's (1995) definition of norms, an organizational norm will be interpreted in what follows as a behavioral guideline on the usage of the access to and/or knowledge about the organizational assets that the organization perceives as legitimate and that insiders are expected to comply with. The organizational norms function as a red line that separates acceptable use of the privilege from unacceptable use of the access/knowledge (Dekker, 2009; Dekker, 2017; Von Solms & Von Solms, 2004). Nevertheless, the provision of behavioral guidelines does not guarantee compliance with the organizational norms. The norms are expectations from the organization, meaning that insiders have the possibility to, whether or not wittingly, deviate from these expectations (Neumann, 2010; Robinson & Bennett, 1995).

The definitions provided by scholars that have already applied a privilege-oriented perspective are problematic because they either 1) refrain from eliminating the unintentional misuses of privilege from the insider threat concept, 2) do not adequately indicate whether the unintentional misuses fall within the scope of the insider threat concept or 3) do not distinguish misconduct from misbehavior.

The first group includes both intentional and unintentional misuses in their conceptualization of the insider threat. For instance the US National Insider Threat Task Force (2016: 3) refers to the insider threat as “the risk an insider will use their authorized access, wittingly or unwittingly, to do harm to their organization”. The same applies to the studies of Willison & Warkentin (2013) and the Information Security Forum (2015). Consequently, these conceptualizations mirror the broad interpretation of the harm-oriented perspective, with a similar risk of turning insider threat into a container concept.

The second group provides definitions that are unclear on whether or not insiders that unwittingly misuse their privilege fall under the scope of the insider threat concept, leaving too much room for interpretation for the reader. The Commonwealth of Australia (2014: 2) for example defines the insider threat as a “threat posed by unauthorized access, use or disclosure of privileged information, techniques, technology, assets or premises by an individual with legitimate or indirect access, which may cause harm”. Here, it is imprecise whether it relates to intentional or unintentional unauthorized access, use or disclosure. Also the definitions of Padayachee (2016), Gelles (2016), and Greitzer, Kangas, Noonan, Dalton & Hohimer (2012), the latest also used by Noonan (2018), Krull (2016) and BaMaung, McIlhatton, MacDonald & Beattie (2018), refrain from explicitly mentioning the intentionality of the misuse of the privilege. Therefore, they leave too much ambiguity on whether or not insiders that unwittingly misconduct fall under the scope of the insider threat concept. Although it can be argued that it can be implicitly deduced from these definitions that unintentional misuses of privilege are not included in the definition of insider threat, it is better to have an unambiguous definition that explicitly defines the scope of the insider threat concept to increase the comparability of insider threat research (Pfleeger, 2008). Without eliminating ambiguity, the other conceptualizations resemble the broad interpretation of the harm-oriented perspective, with a similar risk of turning insider threat into a container concept.

The last group of privilege-oriented insider threat definitions refrain from distinguishing misconduct from misbehavior. Ho, Kaarst-Brown & Benbasat (2018: 271-272) define the insider threat as "a reference to situations in which a "focal actor"—someone with authorized access—inflicts damage to their own organization by behaving against the interests of the organization (i.e., betraying), generally in an illegal and unethical manner. (…) [I]nsider threat always involves some aspect of betrayal, which is an intentional act of trust violation against the interest of another party (...). Although there are many types of nonmalicious (well-intentioned or negligent) insiders who might inadvertently betray the organization, there are also those who do so maliciously, with deliberate intent to harm the organization for some benefit".

We argue that the definition of Ho, Kaarst-Brown & Benbasat is problematic not only because it collides with the second group, but also by leaving ambiguity on whether or not the betrayal is linked to the privilege of the insider. Concerning the former, the definition is contradictory, as an insider cannot inadvertently betray an organization if betrayal is considered to be an intentional act. Concerning the latter, we advocate a distinction between misconduct and misbehavior, depending on whether the insider uses the privileged access or knowledge to deviate from the norm. To illustrate the difference, think of an employee who is convicted for stealing. If the employee stole from the company he or she works for because he or she had insider access/knowledge, it is considered to be misconduct. An example is a cocktail waitress in a casino who conspires with one of the casino dealers to steal tokens (Bunn & Glynn, 2016). However, if the employee did not steal from the company but instead randomly robbed a bank in his or her spare time, it is not considered to be misconduct but rather misbehavior, given that the bank robbery has nothing to do with the insider's privileged access or knowledge. An example is the involvement of former municipal officer of Lommel Anick Berghmans in the explosion of an Automated Teller Machine (ATM) of Bpost (Het Nieuwsblad, 10/18/2019). Both thefts can be considered a deviation from a norm the organization embraces (i.e. not stealing), but the difference between both incidents lies in whether or not the culprit misused his or her insider privilege to steal. While the employees of the casino misconducted themselves by misusing their access/knowledge to

steal from the company, the former municipal officer of Lommel misbehaved herself given that her stealing was not related to her job at the municipality. In brief, the deviation from the organizational norm has to be related to the insider intentionally misusing the access to or knowledge about the organizational assets. Misbehavior should not be considered an insider threat, as the norm deviation is not related to the 'insiderness', or to the trusted privilege of access and/or knowledge. This nuance is not explicitly present in the definition of Ho, Kaarst-Brown & Benbasat.

3. A new conceptualization: insider hazards vs. insider threats

The previous section illustrated that existing definitions of insider threats are unsatisfactory. As a result, this paper presents a new conceptualization. The conceptualization starts with the assumption that each organization possesses assets that it wishes to protect (Bishop, Gates, Fricke & Greitzer, 2009; Bunn & Sagan, 2016; Sarkar, 2010). Organizational assets are interpreted as being valuable resources controlled by the organization that are situated within the proverbial security perimeter and that need to be protected. Examples of organizational assets are among other things intellectual property, financial resources and reputation. Organizational assets can be clustered in four groups, namely people, tangibles, intangibles and data (Bunn & Sagan, 2016; Gelles, 2016; Thompson & Friedlander, 2016).

The ultimate goal of each organization is to protect its assets as much as possible. However, in order to be successful, the organization has no other choice than to provide access to and/or knowledge about the organizational assets to certain individuals, simply because they need it in order to do their job. The organization has to trust that these individuals, referred to as insiders, will handle the assets with care. In what follows, we will first elaborate on the insider concept and subsequently on the insider threat concept.

3.1. Insiders

Insiders are given a certain privilege that is characterized by three aspects: access to the organizational assets, knowledge about the organizational assets and trust by the organization (BaMaung, McIlhatton, MacDonald & Beattie, 2018; Bishop et al., 2010; Probst, Hunker, Gollmann & Bishop 2010).

Firstly, access refers to the free permission that the organization gives to the insider to penetrate the security perimeter that protects the organizational assets. The access can be physical, like for instance the authorization to enter a building, or virtual, like the password to enter the network system (Colwill, 2009; Munshi, Dell & Armstrong, 2012). The access is privileged because insiders get access to the assets while outsiders don't get access. The privileged access is also given for free, since the individual does not have to pay to enter the security perimeter but is simply trusted by the organization.

Secondly, organizational knowledge is interpreted as the free information on the organizational assets that the organization gives to the insider. Bunn & Glynn (2016) make a distinction between first-degree and second-degree critical knowledge. While the former is knowledge about the organizational assets, like for instance the location or code of the company vault, the latter is knowledge about vulnerabilities (or security holes) that are related to the organizational assets, like for instance blind spots on the closed-circuit television (CCTV) that is monitoring the vault (Cole & Ring, 2006; Nurse et al., 2014; Sarkar, 2010). Similar to access, knowledge is privileged because insiders possess the knowledge while outsiders do not possess it. Moreover, the knowledge is free since the individual is simply trusted by the organization.

Thirdly, trust refers to the organization's belief that the access and/or knowledge is safe with the insider, meaning that the organization is convinced that the individual will use it in an appropriate way (Ho, Kaarst-Brown & Benbasat, 2018). A division is made between the individuals that belong to the organization and are allowed to come into contact (access/knowledge) with the organizational assets, and the individuals that do not belong to the organization and should be kept out of the security perimeter. While the former belong to the trusted insider-group, the latter are part of the distrusted outsider-group. The trust criterion is not only applicable to current confidants of the organization, but

also to former ones. To put it in a different way, insiders are not only individuals currently belonging to the organization, but are also individuals that used to be part of it and were trusted by the organization in the past (Krull, 2016; Nurse et al. 2014; Randazzo, Keeney, Kowalski, Cappelli & Moore, 2005). An example is the case of David Burke, the man who was responsible for the crash of the Pacific Southwest Airlines Flight 1771. Although Burke was dismissed from the airline company, he was still able to retain both his identification badge and uniform. As a result, Burke could misuse this privileged access to bypass security screening, smuggle a gun on board, kill his former manager and crash the plane (Greco, 2017; Loffi & Wallace, 2014). Hence, if individuals were previously trusted by the organization and are still able to misuse their privileged access and/or knowledge to the organization's assets, they should still be considered insiders and should be taken into account when discussing the insider threat.

So far, we systematically referred to insiders as being individuals. However, we argue that insiders can appear in many guises, including as individuals, as enterprises or even as states. Notwithstanding this acknowledgment, we will interpret insiders as individuals in the remainder of the paper, unless otherwise stated.

In sum, access to the organizational assets, knowledge about the organizational assets and trust by the organization can be used as distinctive criteria to separate the insider from the outsider. As a result, the following definition of the insider is suggested:

> *An insider is an actor who is or used to be trusted by the organization with the free privilege of access to and/or knowledge about the organizational assets.*

On the basis of the definition, a clear distinction can be made between the insider, or the one who is or used to be trusted and granted the free privilege of access to and/or knowledge about the organizational assets, and the outsider, the one who is not trusted and not granted the free privilege.

Our definition illustrates that insiders are not only individuals that work on a permanent basis for their employer. Also other individuals, like for instance contract employees or apprentices, that are not part

of the permanent labor force of the organization might be trusted by the organization with privileged access or knowledge (Colwill, 2009). To illustrate, reference can be made to Aaron Alexis who was outsourced to the Washington Navy Yard by one of the Navy's prime contractors and who during his employment murdered 12 colleagues (Gelles, 2016; Shaw & Sellers, 2015), or to the 15-year-old student that stole a car during his internship (Het Nieuwsblad, 12/11/2019).

Moreover, our definition illustrates that the insider should have at least access to or knowledge about the organizational assets to be considered an insider, but that he does not necessarily has to possess both. Indeed, only one of the two has to be present - in combination with trust - to speak of an insider. The trust criterion is however pivotal, as only access or knowledge is insufficient to speak of an insider. As stated before, insiders do not have to pay to obtain access or knowledge, but are simply trusted by the organization that they will handle the privileged access/knowledge in an appropriate way. Hence, individuals that pay to acquire access or knowledge are excluded from the insider category. Think for instance of the difference between a pilot who gets access to the airplane for free, and passengers who buy a ticket to get access to the airplane. Only pilots are considered to be insiders because they are trusted by the organization with privileged access.

Also individuals that obtain access or knowledge not via trust by the organization but through manipulating a trusted individual fall out of the scope of the insider concept. In contrast to Cole & Ring (2006) and Sarkar (2010) who consider individuals who are not trusted by the company like spouses, friends and social engineers (i.e. individuals that have no access to or knowledge about the organizational assets, but that manipulate an insider that has access/knowledge in order to reach the organizational assets) as insider threats, our definition limits the insider concept, and consequently the insider threat, to individuals that are trusted by the organization. Although it is recognized that spouses, friends or social engineers might get access to or knowledge about the organization's assets, they will always have to get it from an individual that the organization trusts or trusted with the access/knowledge, the actual insider. Also from a policy perspective it is beneficial to limit the insider

category to trusted individuals, as the organization is less able to develop policies that influence the behavior of spouses, friends and social engineers. Instead, the organization's policy is only applicable to the individual that the organization trusts or trusted with the access/knowledge, or the individual from which the spouse, friend or social engineer gets the access or knowledge.

To conclude, we argue that not all insiders should be treated alike. Although we distinguish insiders from outsiders, the insiders should not be huddled into one category contrary to the outsider category. Instead, the insider category should be viewed as a continuum of insiders that can be sorted on the basis of the scope and application area of the granted privilege, or on their "degree of insiderness" (Bishop et al., 2010: 135). Insiders whose privilege consists of a large privilege (i.e. large amount of trust, access to and/or knowledge about the assets), or a privilege that applies to the most important assets of the organization, pose a different (i.e. greater) threat than insiders whose privilege corresponds with a small privilege (i.e. small amount of trust, access to and/or knowledge about the assets) or a privilege that applies to less important assets (Bishop, Gates, Frincke & Greitzer, 2009; Bishop et al., 2010; Probst, Hunker, Gollmann & Bishop, 2010).

3.2. Insider threats

After clarifying the insider concept, we move on to explain our conceptualization of the insider threat . In this paper, preference is given to the privilege-oriented perspective. As already stated before, privilege-orientation assumes that the organization provides the insiders with guidance on how to behave themselves in an appropriate way to stimulate the proper handling of the organizational assets (Dekker, 2009; Dekker, 2017; Von Solms & Von Solms, 2004). The provision of behavioral guidelines does not guarantee compliance with the organizational norms, as insiders will deviate from organizational norms and pose a danger to the organizational assets (Neumann, 2010; Robinson & Bennett, 1995). In this paper, we do not intend to have a moralistic perspective on the norm deviation itself. In other words, whether or not it is a good or a bad thing to deviate from the norm is not the main focus of the article. Instead, the main focus is the fact that the insider deviates from one of the

imposed standards of behavior that the organization demands adherence to from its insiders (Wikström, 2014).

The fact that norm deviation poses a danger to the organizational assets does not mean that each norm deviation should be considered an insider threat. To clarify what should and what should not be considered an insider threat, this article draws upon Albrechtsen's (2003) distinction between hazards that are related to safety and threats that are related to security. According to Van Nunen et al. (2018), safety should be distinguished from security based on the intention to inflict harm. In other words, Van Nunen et al. look at the safety/security division from a harm-oriented perspective. As stated before, this article does not apply a harm-oriented perspective, but a privilege-oriented perspective. Interpreting the distinction of Van Nunen et al. between safety and security from a privilege-oriented perspective, we distinguish safety from security according to the intention to deviate from an organizational norm, or the intention to misuse the organizational privilege. A distinction is made between intentional deviations from organizational norms, or intentional misconduct, and unintentional deviations from organizational norms, or unintentional misconduct. Parallel to Van Nunen et al., witting misconduct (with or without intent to harm) is security-related, while unwitting misconduct is safety-related. In analogy with Albrechtsen's distinction between hazards that are safety-related and threats that are security-related, insider hazards refer to insiders that unintentionally misconduct themselves, while insider threats refer to insiders that intentionally misconduct themselves. As a result, the following definition of the insider threat is suggested:

> *An insider threat is the possibility that an actor who is or used to be trusted by the organization with the free privilege of access to and/or knowledge about the organizational assets, causes harm to the organization because he intentionally misuses his access to or knowledge about the organizational assets.*

Insider threats are thus posed by insiders who are aware that their intentional misuse might cause harm to the organization. In contrast, unintentional or unwitting misconduct should be excluded from

the insider threat concept and should be referred to as insider hazards. An insider hazard is the possibility that an insider unintentionally causes harm to the organization by unintentionally misusing his access to or knowledge about the organizational assets. It concerns insiders that unwittingly or accidently take actions and make honest errors (Steneck, 1994), insiders that wittingly take actions without knowing that those actions lead to a deviation from an organizational norm (Gundu & Flowerday, 2012), or insiders that simply do not possess a sufficient level of competence to properly handle the given privilege (Ho, Kaarst-Brown & Benbasat, 2018).

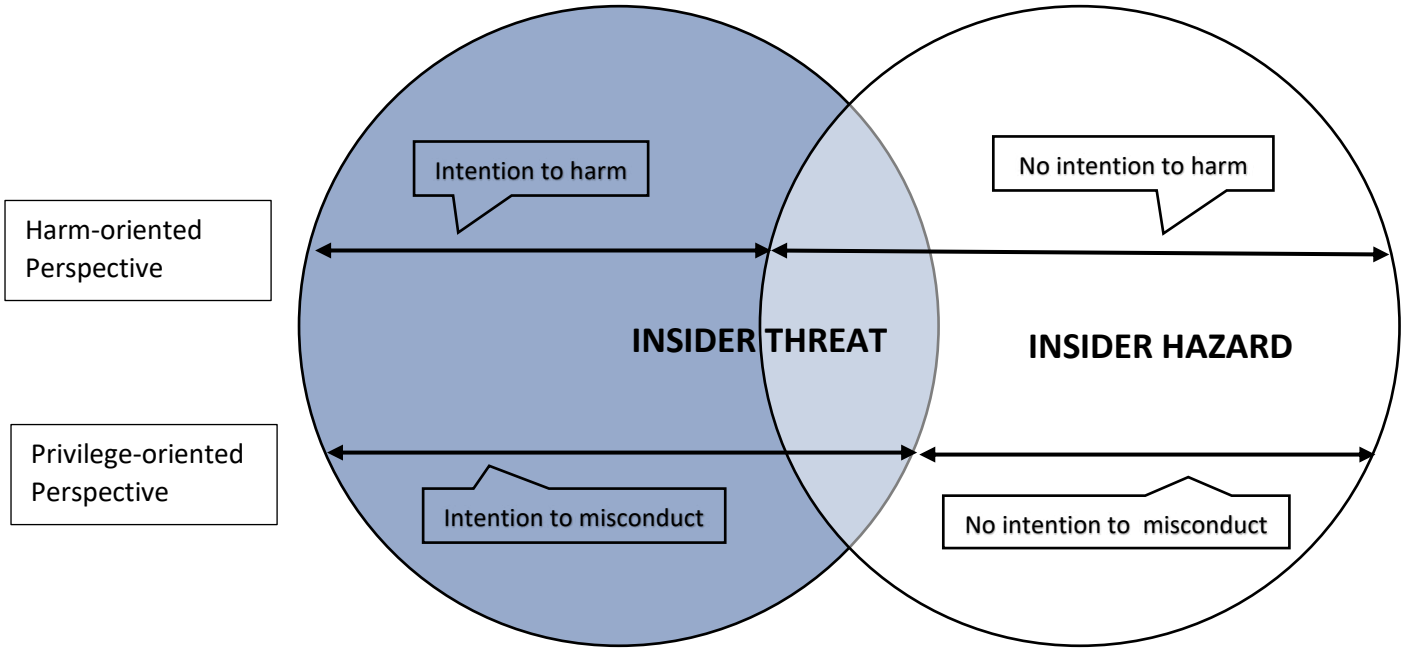
Our distinction between insider hazards and insider threats mirrors Dekker's (2017) distinction between technical and normative errors, whereby technical errors relate to the insider's proficiency and normative errors relate to the insider's trustworthiness. Similarly, insider hazards relate to insufficient proficiency, or not being able to comply with the organizational norms, while insider threats refer to insufficient trustworthiness, or not being willing to comply. The difference between insider threats and insider hazards thus lies in the breach of trust between the trustor (i.e. the organization) and the trustee (i.e. the insider) (Ho, Kaarst-Brown & Benbasat, 2018). Table 1 summarizes the distinction between insider hazards and insider threats.

Table 1 : Summary Insider hazards vs. insider threats

Insider hazard	Lack of profiency (ability)	Honest mistake (accident)
		Unawareness of the norm
		Incompetent to comply with the norm
Insider threat	Lack of trustworthiness (willingness)	Aware & competent, but unwilling to comply with norm

Figure 1, inspired by a diagram of Information Security Forum (2015: 2) but adapted to the current conceptualization, illustrates the distinction between insider hazards and insider threats in relation to the opposition between harm-orientation and privilege-orientation. The figure indicates that the paper is based on a privileged-oriented perspective as the difference between insider hazard and insider threat depends on the intention to misconduct and not on the intention to cause harm.

Figure 1: insider threat vs. insider hazard



To illustrate the difference between insider hazards and insider threats, we refer to misconduct in sports, or athletes that misuse the privileged access given by their team to compete in sports events. If the misconduct is the result of being human, or of an honest mistake, it concerns an insider hazard rather than an insider threat. Examples are the cases of Spanish cyclist Alberto Contador, who unsuccessfully claimed that his positive drug test on Clenbuterol was due to contaminated meat (Fotheringham, 02/06/2012), Belgian cyclist Iljo Keisse, who successfully claimed his positive drug test was due to a contaminated food supplement (De Morgen, 11/02/2009) or Belgian cyclist Tosh Van Der Sande who successfully claimed his positive drug test was due to accidentally reporting the wrong medicine to the doping controllers (De Standaard, 01/23/2019).

Furthermore, if the misconduct is the result of unawareness of the applicable norms, it concerns an insider hazard rather than an insider threat. Whether to speak of an insider hazard or insider threat is not inherent in the act of the insider or the organizational norm deviation itself, but in the intentionality of the act or the intentionality of the organizational norm deviation (Becker, 1963). When the insider wittingly takes actions without knowing those actions will lead to an organizational norm deviation, one can speak of an insider hazard rather than an insider threat. In other words, if the athlete deliberately takes a drug without knowing that the particular drug is prohibited, it also concerns an insider hazard rather than an insider threat. An example is the case of Belgian cyclist Björn Leukemans, who was accused of drug abuse because he took the prohibited substance Prasteron. As it turned out, Leukemans was unaware of the prohibition, as the drug was prescribed by the team doctor (De Morgen, 12/20/2007).

Moreover, if the misconduct is the result of incompetence to adhere to the norms, it concerns an insider hazard rather than an insider threat. Think for instance of the whereabouts system that obliges athletes to share residency data with controllers of drug abuse. Although athletes might be aware of the whereabouts system, they also need the competences to properly report their whereabouts, which is not always the case (De Morgen, 11/13/2009). For instance Belgian judoka Dirk Van Tichelt was on the verge of being suspended not because he intentionally falsified his whereabouts or because he was unaware of the obligation to report, but because he was incompetent to properly report his residency data (De Standaard, 07/12/2012).

If, on the other hand, the athlete is aware of the applicable norms and competent to adhere to the norms, but nevertheless wittingly decides to misconduct himself, it concerns an insider threat rather than an insider hazard, at least if the sports fraud is not orchestrated by the team and therefore deviates from the norms the team adheres to (i.e. fair sport/competition). Multiple athletes can be cited that deliberately deceived their sport, for any reason whatsoever. The most obvious reason is performance enhancement. One of the more recent cases of witting misconduct in sports is cross-

country skier Max Hauke, who as part of Operation Aderlass was caught red-handed in the middle of a blood transfusion (NOS, 11/26/2019). Besides performance-enhancing, athletes can also misconduct for personal reasons, like Danish cyclist Michael Rasmussen who falsified his whereabouts to conceal his extramarital affair (Gallagher, 11/15/2011).

As previously mentioned, insiders can appear in many guises, including as enterprises or even as states. Consequently, also entire enterprises or even states can misconduct themselves. In the context of sports misconduct, reference can be made to the team-orchestrated doping scheme of Festina that overshadowed the 1998 Tour de France (Van Cauwelaert, 07/29/1998), or the state-orchestrated doping scheme in Russia (Duval, 2017).

4. Advantages

As Becker (1963: 14) indicates, "[s]ome people may object that this is merely a terminological quibble, that one can, after all, define terms any ways he wants to". We argue that, from a policy perspective, the distinction between insider hazard and insider threat is worthwhile because they both raise different policy questions. While insider hazard policy concerns awareness of the norm and competence to adhere to the norm, or communication, education and training, insider threat policy relates to enforcement and eventually internalization of the norm, or compliance and persuasion (Siponen, 2000).

Insider hazard policy is centered on finding ways to communicate the organization's expectations regarding the appropriate use of the access/knowledge so that insiders are aware of these behavioral expectations. Moreover, it is concentrated on ensuring that insiders have enough skills to be able to adhere to the norm. In other words, the organization has to educate insiders to make sure that they know how they are supposed to use the access or knowledge that is provided to them, and train them so that they are able to do it.

In contrast, insider threats refer to insiders that are already aware of the behavioral expectations of the organization and already have the competence to comply with them, but wittingly choose to

deviate from these expectations. Therefore, insider threat policy is not a question of awareness, communication, education or training, but of compliance and deviance. Insider threat policy is centered on making sure that insiders adhere to the organization's behavioral expectations and on limiting deviance. Initially, it concentrates on enforcing compliance through positive and negative sanctions, but in the end insiders should be persuaded by the organization of the appropriateness and the usefulness of the organizational norms so that they internalize the norms and adopt the organizational culture. In other words, the eventual objective is not compliance through enforcement, but through acceptance (Siponen & Kajava, 1998; Siponen, 2000).

In what follows, we explain why our conceptualization is more suitable than the existing definitions.

4.1. In comparison with the existing harm-oriented definitions

In contrast to the existing definitions originating from the harm-oriented perspective, where the intention to harm the organization is decisive, the pivotal issue in case of privilege orientation is accountability. Accountability means that the insider is expected to explain and defend his decision to misuse his privileged access or knowledge (McCall & Pruchnicki, 2017). Applying a privilege-oriented perspective to separate insider hazards from insider threats actually advocates that insiders should be held accountable "not necessarily for the outcomes they create, but for the choices they (supposedly) make while doing their work" (Dekker, 2017: 2). In other words, accountability is unnecessary in case of insider hazards, while accountability is required in case of insider threats.

In case of an insider hazard, the individual did not wittingly deviate from the organizational norm and therefore acted in good faith. As a result, the insider should not be held accountable. There is no purpose in holding the insider accountable because he cannot provide good reasons for misconduct, except for not being sufficiently skilled, not being aware of the norm or making an honest mistake. Although it is still beneficial to analyze the circumstances that made the insider hazard happen in order to learn from it (De Vleeschauwer, 2019), the insider should not face a grilling.

In the case of non-malicious but intentional misconduct, the individual cannot invoke good faith as an argument, as he is aware that his behavior deviates from an organizational norm. Therefore, insiders who deliberately go against organizational norms should be held accountable, even though the deviation is not intended to harm the organization. The fact that the insider is aware that he misuses his access/knowledge also implies that he is aware, or at least is expected to be aware, of the potential negative consequences that misuse entails. An insider that wittingly continues to misconduct while knowing the possible harm that is associated with it, should be held accountable and should be regarded as an insider threat rather than an insider hazard.

It is useful to hold insiders that wittingly deviate from the organization's prescribed standards of behavior accountable to know the reason behind the misconduct. As Wall indicates, "[the insider threat] encompasses a range of different motivations, including some that are certainly malicious, but also others that are the knock-on effects of organizational cultures and even the organizations' own policies" (Wall, 2013: 108). Hegghammer & Daehli (2016) for instance refer to two interns in a nuclear facility in the US who misconducted themselves out of security concerns. The interns deliberately damaged the control room panel of the nuclear power plant as a cautionary tale of what would happen to the nuclear facility when security remained lax. Hence, holding the intentional wrongdoers accountable and urging them to defend and/or explain their misconduct might help to detect deficiencies in the organization's culture and/or policies.

Even though insiders that wittingly deviate from an organizational norm without harmful intentions are included in our conceptualization, these insiders should not be demonized or named and shamed (Wall, 2013). In an analogy with Dekker (2017), who makes a separation between a guilt-phase and a penalty-phase, the misconduct should be divided in an abuse-phase and a response-phase. While the abuse-phase examines whether or not the insider should be held accountable for the misconduct, the response-phase examines the culpability of the insider. The question whether the insider should be held accountable thus differs from the question whether the insider is culpable. While accountability

means that the insider is expected to explain and defend his decision to misuse his privileged access or knowledge, culpability judges that the validity of the insider's arguments (McCall & Pruchnicki, 2017). To put it in a different way, being accountable means that the insider faces a grilling, while being culpable means that the insider is found guilty, allowing the organization to blame the insider for the misconduct.

It could thus be that an insider is held accountable for his misconduct, but is not found culpable because he had a valid reason to misconduct. To pick up on the example of witting misconduct in sport, reference can be made to the Salbutamol affair of British cyclist Christopher Froome. Froome was accused of drug abuse because his test revealed abnormal levels of Salbutamol, after which he admitted that he took extra Salbutamol on the day of the test (Ingle & Kelner, 12/13/2017; Ingle, 12/13/2017). Nevertheless, the governing body of cycling (UCI) deemed Froome not guilty, thereby judging he had a valid reason to take the extra Salbutamol (Ingle, 07/02/2018). The scope of our article is limited to the abuse-phase where the goal is to determine whether the insider deliberately crossed the red line of acceptable use of the organizational privilege, or whether the insider has to be interrogated to explain why it made sense to him to misuse his privilege.

4.2. In comparison with the existing privilege-oriented definitions

In contrast to the existing definitions originating from the privilege-oriented perspective, the definitions suggested in this article, and the accompanying distinction between insider hazards and insider threats, to a large extent reduce the interpretability of insiders and insider behavior. We previously argued that the definitions provided by scholars that have already applied a privilege-oriented perspective either 1) refrain from eliminating the unintentional misuses of privilege from the insider threat concept, 2) do not adequately indicate whether the unintentional misuses fall within the scope of the insider threat concept, or 3) do not distinguish misconduct from misbehavior.

Concerning the first group, Pfleeger (2008: 8) states that "because the word 'threat' has a negative connotation, some people would understandably not ordinarily use it to describe unintentional or non-

malicious behavior. We must be especially careful when using the term 'insider threat' to be sure our meaning is not misconstrued and insiders are not offended". The distinction between insider threat and insider hazard addresses this concern as it differentiates insiders that unintentionally misuse their access or knowledge, or insiders that make a genuine mistake that everybody can make, from insiders that deliberately choose to misuse their access or knowledge, or insiders that make a willful decision to deviate from an organizational norm. Hence, in contrast to the definitions that include unintentional misconduct, the conceptualization in this article refrains from putting all incidents involving an insider under the same insider threat umbrella.

Concerning the second group, we argue that although it can be implicitly deduced from the definitions of for instance the Commonwealth of Australia (2014), Greitzer, Kangas, Noonan, Dalton & Hohimer (2012), Padayachee (2016) and Gelles (2016) that unintentional misuses of privilege are not included in the definition of insider threat, it is better to have an unambiguous definition that explicitly defines the scope of the insider threat concept. Pfleeger (2008: 8) correctly indicates that "we need standard definitions of insiders and insider behavior so studies and discussions can compare". Although we acknowledge that every definition is susceptible to ambiguity and grey areas (Steneck, 1994), we argue that the definitions suggested in this article, and the accompanying distinction between insider hazards and insider threats, to a large extent eliminate the ambiguity around the intentionality of the insider's misuse of the privilege. As a consequence, our conceptualization reduces the interpretability of insiders and insider behavior, increasing the comparability of insider threat research.

Concerning the last group, distinguishing misbehavior from misconduct, and excluding misbehavior from the insider threat concept, is desirable because the organization's ability to develop policy is limited to misconduct and because the impact of misconduct is higher than the impact of misbehavior. On the one hand, the organization's ability to develop policy against misbehavior is minimal, as an organization has few means to manage the personal life of its insiders. In contrast, the ability to work out policy against misconduct is more extensive, given that the organization has more tools to

administer insiders' use of the organizational privilege. To pick up on the examples given earlier on insiders that steal, an organization can develop policy to prevent that employees steal company property, but it cannot develop policy to prevent employees to rob a bank in their spare time. On the other hand, it is believed that misconduct will probably have a higher impact on the organizational assets than misbehavior. Misconduct can have a direct impact on company property by negatively affecting the confidentiality, availability or integrity of the organizational assets (Cole & Ring, 2006). This direct impact is absent in case of misbehavior. Moreover, misconduct can have an indirect impact by negatively influencing the organization's reputation, given that the possibility exists that the general public will equate the trusted insider with the organization he works for and will depreciate the organization for trusting those kind of individuals. Although reputational damage might also originate from misbehavior, it is assumed that the reputational damage resulting from misconduct is more extensive than that arising from misbehavior because the organization bears more responsibility in case of the former. In other words, it is presumed that in case of misbehavior, the focus will be on the vicious employee with the organization perceived as a victim, while in the case of misconduct, the proneness of the organization to fall victim to the misconduct will be discussed too, with people wondering what the organization did wrong to allow the employee to misconduct himself. Although we do not advocate that misbehavior has a negligible impact or that it should be tolerated, both the extensive ability to develop policy and the higher negative impact of misconduct make that insider threat policy has to be centered on misconduct rather than misbehavior.

5. Shortcomings

Notwithstanding the advantages, our conceptualization is limited by some weaknesses. Firstly, the article starts from the assumption that it is easy to draw a red line between acceptable and unacceptable behavior regarding the use of the privileged access/knowledge. However, it is not easy to draw an indisputable line between appropriate and inappropriate behavior (Dekker, 2009, Dekker, 2017). In reality, insiders are confronted with unforeseen circumstances for which they are not prepared, meaning that they have to make a judgement on imperfect information and use the

available information to interpret the red line. It is therefore impractical to think that each course of action of personnel can be perfectly directed by the organization (Pfleeger, 2008; Probst, Hunker, Gollmann & Bishop 2010). It is recognized that the red line between acceptable and unacceptable behavior is difficult to draw and that there are not only black and white areas but also grey ones. Moreover, it is true that not all behavior of insiders can be exactly prescribed as they are confronted with unforeseen events. This means that insiders need a certain degree of freedom while on the job, or "room for maneuvering" (Dekker, 2009: 183), that gives them the opportunity to make their own choices. Nevertheless, insider behavior can only be judged misconduct if acceptable use of privilege is differentiated from unacceptable use of privilege (Neumann, 2010). The fact that it is difficult to draw the line does not mean that no attempt should be made to do it. Trying to provide insiders with directions on how to handle organizational assets beats the alternative situation of anarchy in which insiders are allowed to do whatever they want.

Secondly, norms are (sometimes) ambiguous. This vagueness might lead to a discrepancy between the interpretation of the norm by the insider and the interpretation of the norm by the organization and could give the insider the propensity to refute his awareness of the norm. One could therefore wonder why the article is not based on rules instead. Our answer is that it is impractical and undesirable for an organization to translate all expected behavior in rules and regulations. In contrast, the organization counts on its organizational culture to guide the behavior of its employees, whereby norms function as a reflection of this organizational culture (Von Solms & Von Solms, 2004). The ultimate objective of an organization is not enforcement of organizational rules, but rather acceptance and internalization of organizational norms. The organization wants to persuade the insiders with argumentation and justification into accepting the organizational norms, rather than to hegemonically enforce a regulatory framework without their buy-in (Siponen & Kajava, 1998; Siponen, 2000). The ultimate recommendation for organizations is thus to develop "work arrangements that afford high degrees of autonomy to individuals who base their decision making on internalized norms of appropriate practice" (McCall & Pruchnicki, 2017: 14). Again, reference can be made to misconduct in sports, and

more precisely to cycling. It is an unwritten rule that cyclists from the same team cooperate and refrain from chasing teammates (Pauli, 07/06/2011). It can be assumed that cyclists that let self-interest prevail over the interest of the team do not violate an official rule, but rather sin against an informal norm. In other words, the organization's expectation to think in terms of group interest is probably not officially translated into formal rules and regulations but is still part of the organizational culture. Hence, deviations from this organizational norm should be considered an insider threat, not least because it might lead to considerable sporting losses (Pauli, 07/06/2011), as well as corresponding financial losses.

Lastly, the whole article depends on the ability to "recognize—objectively, unarguably—willful violations, negligence, or destructive acts" (Dekker, 2017: 3). In other words, insiders have the opportunity to claim that the organizational norm deviation was unwittingly, because it was an accident, because they were not aware of the norm or because they lack skills to comply with the norm, while they in fact were aware of the prescribed behavioral guidelines and were competent to comply with them but deliberately chose to misconduct themselves. Furthermore, the article draws upon the assumption that organizations provide insiders with clear guidance on how to behave themselves in an appropriate way, which will not always be the case (Chipperfield & Furnell, 2010). Although this shortcoming is acknowledged, we argue that in most instances the organization can accurately evaluate whether the insider's misuse of privilege is witting or not, as well as whether the claim of unawareness or incompetence is credible or not (Ho, Kaarst-Brown & Benbasat, 2018; Probst, Hunker, Gollmann & Bishop 2010). By any means, it should be the organization's first objective to properly inform its insiders on the behavioral guidelines that proscribe the way in which the insider has to use his privilege as well as to properly train them so that they are able to adhere to the norms. The organization should communicate to its insiders in a clear way which behavior is expected to make sure they are aware of the applicable organizational norms, and should train them to acquire the necessary skills that enable norm compliance (Gundu & Flowerday, 2012). If the organization can succeed in this ambition, insiders have no opportunity to assert that they are unaware of the norm or

incompetent to comply with it, eliminating the possible ambiguity. Moreover, it should be mentioned that the same setback applies to the harm-oriented definitions that focus on the maliciousness of the insider, as the determination of malicious intent is also subjective rather than objective.

In sum, it is advocated that the advantages of our conceptualization outweigh the shortcomings. Our conceptualization addresses the negative aspects of the existing definitions while simultaneously covering all harmful insider incidents that the organization can face.

6. Discussion and Conclusion

This article suggested a new definition of insiders and insider threats. It started with an outline of the deficiencies of the existing definitions, elaborating on both the harm-oriented and privilege-oriented definitions. Concerning the former, the definitions that are limited to the malicious insider do not encompass the whole spectrum of insider threats, while the definitions including unwitting insider actions increase the risk of turning insider threat into a container concept. Concerning the latter, the existing definitions leave too much room for interpretation for the reader, making it difficult to compare insider threat research. As a result, misconduct, or misuse of access to or knowledge about the organizational assets, was distinguished from misbehavior and sub-divided into insider hazards and insider threats, based on the intentionality of the misconduct or whether the insider should be held accountable. If the insider unintentionally misuses his privilege, it concerns an insider hazard. If the insider intentionally misuses his access to or knowledge about the organizational assets, it concerns an insider threat. Ultimately, a new definition of insiders and insider threats is proposed, defining the insider as an actor who is or used to be trusted by the organization with the free privilege of access to and/or knowledge about the organizational assets, and the insider threat as the possibility that an insider causes harm to the organization because he intentionally misuses his access to or knowledge about the organizational assets.

The provision of new definitions paves the way for new insider threat research. Future research on insider threat should be centered on finding policy recommendations to mitigate both insider hazards

and insider threats. Concerning insider hazard policy, research should look at the effectiveness of different methods like classroom lectures, e-learnings, table top exercises, and simulations in communicating, educating and training insiders on the organizational norms. Regarding insider threat policy, research should focus on both enforcement techniques and internalization techniques to increase compliance to the organization's code of conduct.

Notes

1. Although insiders can be both male or female, we systematically use the male pronoun to refer to the insider instead of always referring to he or she for reasons of text readability.

Funding

Funding was provided by Bel-V, Brussels Airport Company, Elia, Engie-Electrabel, the Federal Agency of Nuclear Control (FANC) and G4S.

Conflict of interest

On behalf of all authors, the corresponding author states that there is no conflict of interest.

Word count

- Abstract = 122 words
- Text (including title, excluding references) = 8503 words

References

Albrechtsen, Eirik. "Security vs safety." *Semantic Scholar.* August 2003. https://pdfs.semanticscholar.org/451c/18d9b07ecda89b367095c48582358a1f3c51.pdf (accessed November 13, 2019).

BaMaung, David, David McIlhatton, Murdo MacDonald, and Rona Beattie. "The Enemy Within? The Connection between Insider Threat and Terrorism." *Studies in Conflict & Terrorism*, no. 41:2 (2018): 133-150.

Becker, Howard. "Outsiders." In *Outsiders: Studies in the Socioloy of Deviance*, by Howard Becker, 1-15. New York: The Free Press, 1963.

Bishop, Matt, Carrie Gates, Deb Frincke, and Frank L. Greitzer. "AZALIA: an A to Z Assessment of the Likelihood of Insider Attack." *IEEE Conference on Technologies for Homeland Security.* Boston: IEEE, 2009. 385 - 392.

Bishop, Matt, et al. "A Risk Management Approach to the 'Insider Threat'." In *Insider Threats in Cyber Security*, by Christian W. Probst, Jeffrey Hunker, Dieter Gollmann and Matt Bishop, 115-137. Boston: Springer, 2010.

Bunn, Matthew, and Kathryn M. Glynn. "Preventing Insider Theft: Lessons from the Casino and Pharmaceutical Industries." In *Insider Threats*, by Matthew Bunn and Scott Sagan, 121-144. Ithaca: Cornell University Press, 2016.

Bunn, Matthew, and Scott Sagan. *Insider Threats.* Ithaca: Cornell University Press, 2016.

Chipperfield, Caroline, and Steven Furnell. "From security policy to practice: Sending the right messages." *Computer Fraud & Security*, 2010: 13-19.

Cole, Eric, and Sandra Ring. "What Is There to Worry About?" In *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft*, by Eric Cole and Sandra Ring, 3-48. Rockland, MA: Syngress Publishing, Inc., 2006.

Colwill, Carl. "Human factors in information security: The insider threat - Who can you trust these days?" *Information Security Technical Report*, 2009: 186-196.

Commonwealth of Australia. *Managing the Insider Threat to your business: A personnel security handbook.* Australia: Commonwealth of Australia, 2014.

Coolsaet, Rik. *Facing the Fourth Foreign Fighters Wave: What Drives Europeans to Syria, and to Islamic State? Insights from the Belgian Case.* Brussels: Egmont Royal Institute for International Relations, 2016.

Coolsaet, Rik. "Wat drijft de Syriëstrijder?" [What motivates the Syrian foreign figher?]. *Samenleving & Politiek*, 2015: 4-13.

De Morgen . "Iljo Keisse vrijgesproken voor positieve dopingplas." [Iljo Keisse cleared from drug abuse]. *De Morgen*, November 2, 2009.

De Morgen. "Leukemans positief door blunder arts." [Leukemans tests positive due to mistake from doctor"]. *De Morgen*, December 20, 2007.

—. "Vlaamse topsporters krijgen extra infosessies over whereabouts." [Flemish top athletes get information sessions on whereabouts].*De Morgen*, November 13, 2009.

De Standaard. "Van Tichelt dicht bij schorsing." [Van Tichelt close to suspention]. *De Standaard*, July 12, 2012.

—. "Wielrenner Tosh Van der Sande vrijgesproken na positieve dopingtest: “Ik werd bestempeld als dopingzondaar terwijl ik enkel verklaring moest geven”." [Cyclist Tosh Van der Sande cleared from drug abuse: "I was labelled as a traitor while I only had to provide an explanation"]. *De Standaard*, January 23, 2019.

De Vleeschauwer, Thomas. *BEVEILIGING VAN DE KRITISCHE INFRASTRUCTUUR: Het succes of falen van de veiligheidscultuur binnen Brussels Airport.* [Securing the critical infrastructure: the success or failure of the security culture of Brussels Airport]. Antwerpen: Masterproef voorgelegd met het oog op het behalen van de graad van Master in de Internationale Betrekkingen en Diplomatie aan de Universiteit Antwerpen, 2019.

Deffer, Frank. *Transportation Security Administration Has Taken Steps To Address the Insider Threat But Challenges Remain.* Department of Homeland Security Office of Inspector General, 2012.

Dekker, Sidney. *Just Culture: Restoring Trust and Accountability in your Organization.* London: CRC Press, 2017.

Dekker, Sidney W.A. "Just culture: who gets to draw the line?" *Cognition, Technology & Work* 11, no. 3 (2009): 177–185.

Duval, Antoine. "The Russian doping scandal at the court of arbitration for sport: lessons for the world anti-doping system." *International Sports Law Journal* 16 (2017): 177-197.

Elifoglu, I. Hilmi, Ivan Abel, and Özlem Tasseven. "Minimizing Insider Threat Risk with Behavioral Monitoring." *Review of Business: Interdisciplinary Journal of Risk and Society*, no. 38:2 (2018): 61-73.

Fotheringham, William. "Alberto Contador gets two-year ban and stripped of 2010 Tour de France." *The Guardian*, February 6, 2012.

Gallagher, Brendan. "Michael Rasmussen admits he lied over missed doping tests ahead of 2007 Tour de France." *The Telegraph*, November 15, 2011.

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

Greco, Peter J. "Insider Threat: The Unseen Dangers Posed by Badged Airport Employees and How to Mitigate Them." *Journal of Air Law and Commerce*, 2017: 717-742.

Greitzer, Frank L., Lars J. Kangas, Christine F. Noonan, Angela C. Dalton, and Ryan E. Hohimer. "Identifying At-risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats." *Hawaii International Conference on System Sciences.* Hawaii: IEEE Computer Society, 2012. 2392-2401.

Gundu, Tapiwa, and Stephen V. Flowerday. "The Enemy Within: A Behavioural Intention Model and an Information Security Awareness Process." *Information Security for South Africa (ISSA).* South Africa: IEEE, 2012. 1-8.

Hegghammer, Thomas, and Andreas Hoelstad Daehli. "Insiders and Outsiders: A Survey of Terrorist Threats to Nuclear Facilities." In *Insider Threats*, by Matthew Bunn and Scott Sagan, 10-41. Ithaca: Cornell University Press, 2016.

Hern, Alex. "Fitness tracking app Strava gives away location of secret US army bases." *The Guardian*, January 28, 2018.

Het Nieuwsblad. "Ex-schepen Anick Berghmans krijgt 30 maanden cel, waarvan 24 met uitstel, voor rol bij plofkraak in Lommel." [Former municipal officer Anick Berghmans sentenced to 30 monhts in jail, of which 24 suspended, for complicity with explosive attack in Lommel]. *Het Nieuwsblad*, October 18, 2019.

—. "Vijftienjarige stagiair-garagist knalt met gestolen BMW in op auto's op pechstrook na wilde politieachtervolging." [15-year-old apprentice mechanic crashes stolen BMW into cars on road service area after wild police chase]. *Het Nieuwsblad*, December 11, 2019.

Ho, Shuyuan Mary, Michelle Kaarst-Brown, and Izak Benbasat. "Trustworthiness Attribution: Inquiry Into Insider Threat Detection." *Journal of the Association for Information Science and Technology* 69, no. 2 (2018): 271–280.

Information Security Forum. *Managing the Insider Threat: Improving Trustworthiness.* London: Information Security Forum Limited, 2015.

Ingle, Sean. "Chris Froome cleared by UCI in anti-doping investigation." *The Guardian*, July 2, 2018.

—. "Chris Froome Q&A: how long could he be banned for and what happens next?" *The Guardian*, December 13, 2017.

Ingle, Sean, and Martha Kelner. "Chris Froome fights to save career after failed drugs test result." *The Guardian*, December 13, 2017.

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

Katzenstein, Peter J. "Introduction: Alternative Perspectives on National Security." In *The Culture of National Security: Norms and Identity in World Politics*, by Peter J. Katzenstein, 1-33. New York: Colombia University Press, 1996.

Krull, KE. *The Threat Among Us: Insiders Intensify Aviation Terrorism.* Richland, Washington: Pacific Northwest National Laboratory - Prepared for the US Department of Energy, 2016.

Loffi, Jon M., and Ryan J. Wallace. "The unmitigated insider threat to aviation (Part 1): a qualitative analysis of risks." *Journal of Transportation Security*, no. 7 (2014): 289-305.

Maasberg, Michele, John Warren, and Nicole L. Beebe. "The Dark Side of the Insider: Detecting the Insider Threat Through Examination of Dark Triad Personality Traits." *48th Hawaii International Conference on System Sciences.* Hawaii: IEEE Computer Society, 2015. 3518-3526.

McCall, Janice R., and Shawn Pruchnicki. "Just culture: A case study of accountability relationship boundaries influence on safety in HIGH-consequence industries." *Safety Science* 94 (2017): 143-151.

Munshi, Asmaa, Peter Dell, and Helen Armstrong. "Insider Threat Behavior Factors: A comparison of theory with reported." *45th Hawaii International Conference on System Sciences.* Hawaii: IEEE Computer Society, 2012. 2402-2411.

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

Neumann, Peter G. "Combatting Insider Threats." In *Insider Threats in Cyber Security*, by Christian W. Probst, Jeffrey Hunker, Dieter Gollmann and Bishop Matt, 17-44. Boston: Springer, 2010.

Noonan, CF. *Spy the Lie: Detecting Malicious Insiders.* Richland, Washington: Pacific Northwest National Laboratory Prepared for the US Department of Energy, 2018.

NOS. "Die langlaufer met het infuus in zijn arm is nu informant van politie en WADA." [The cross-country skier with drip in his arm is now informant of the police and WADA]. *NOS*, November 26, 2019.

Nurse, Jason R.C., et al. "Understanding Insider Threat: A Framework for Characterising Attacks." *IEEE Security and Privacy Workshops.* 2014. 214-228.

Padayachee, Keshnee. "An assessment of opportunity-reducing techniques in information security: An insider threat perspective." *Decision Support Systems* 92 (2016): 47-56.

Pauli, Walter. "In de koers is je ploegmaat vaak je eerste vijand." [In cycling your teammate is often your first enemy]. *De Morgen*, July 6, 2011.

Pfleeger, C.P. "Reflections on the Insider Threat." In *Insider Attack and Cyber Security. Advances in Information Security*, by S.J. Stolfo, S.M. Bellovin, S. Keromytis, A.D. Hershkop, S.W. Smith and S. Sinclair (eds), 5-15. Boston, M.A.: Springer, 2008.

Probst, Christian W., Jeffrey Hunker, Dieter Gollmann, and Matt Bishop. "Aspects of Insider Threats." In *Insider Threats in Cyber Security*, by Christian W. Probst, Jeffrey Hunker, Dieter Gollmann and Matt Bishop, 1-15. Boston: Springer, 2010.

Randazzo, Marisa Reddy, Michelle Keeney, Eileen Kowalski, Drawn Cappelli, and Andrew Moore. *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector.* Pittsburgh: Carnegie Mellon Software Engineering Insitute, 2005.

Robinson, Sandra L., and Rebecca J. Bennett. "A Typology of Deviant Workplace Behaviors: A Multidimensional Scaling Study." *The Academy of Management Journal* 38, no. 2 (1995): 555-572.

Sarkar, Kuheli Roy. "Assessing insider threats to information security using technical, behavioural and organisational measures." *Information Security Technical Report*, no. 15 (2010): 112-133.

Shaw, Eric, and Laura Sellers. "Application of the Critical-Path Method to Evaluate Insider Risks." *Studies in Intelligence* 59, no. 2 (2015): 1-8.

Siponen, Mikko, and Jorma Kajava. "Ontology of organizational IT security awareness-from theoretical foundations to practical framework." *Proceedings Seventh IEEE International Workshop on Enabling Technologies: Infrastucture for Collaborative Enterprises.* Stanford, CA, USA, USA: IEEE, 1998. 327 - 331.

Siponen, Miko. "A conceptual foundation for organizational information security." *Information Management & Computer Security* 8, no. 1 (2000): 31-41.

Steele, Sean, and Chris Wargo. "An Introduction to Insider Threat Management." *Information Systems Security*, no. 16 (2007): 23-33.

Steneck, Nicolas H. "Research Universities and Scientific Misconduct: History, Policies, and the Future." *The Journal of Higher Education* 65, no. 3 (1994): 310-330.

Thompson, Shawn M., and Gabriel Friedlander. "Scope." In *Insider Threat Program: Your 90-Day Plan, A Guide for Initiating, Developing and Implementing your Insider Threat Program*, by Shawn M. Thompson and Gabriel Friedlander, 9-13. United States: ObserveIT, 2016.

Van Cauwelaert, Rik. "Een beetje doping doet wonderen." [A little doping works miracles]. *Knack*, July 29, 1998.

Van Nunen, Karolien, Marlies Sas, Genserik Reniers, Geert Vierendeels, Koen Ponnet, and Wim Hardyns. "An integrative conceptual framework for physical security culture in organisations." *Journal of Integrated Security Science*, 2018: 1-7.

Von Solms, Rossouw, and Basie Von Solms. "From policies to culture." *Computers & Security* 23 (2004): 275-279.

Wall, David S. "Enemies within: Redefining the insider threat in organizational security policy." *Security Journal*, no. 26 (2013): 107-124.

Wikström, Per-Olof H. "Why crime happens: A situational actions theory." In *Analytical Sociology: Actions and Networks* , by Gianluca Manzo, 74-94. Chinchester: John Wiley & Sons, Ltd., 2014.

Willison, Robert, and Merrill Warkentin. "Beyond Deterrence: An Expanded View of Employee Computer Abuse." *MIS Quarterly* 37, no. 1 (2013): 1-20.

Zegart, Amy B. "The Fort Hood Terrorist Attack: An Organizational Postmortem of Army and FBI Deficiencies." In *Insider Threats*, by Matthew: Sagan, Scott Bunn, 42-73. Ithaca: Cornell University Press, 2016.