Insider Threats Among Dutch SMEs: Nature and Extent of Incidents, and Cyber Security Measures

Asier Moneva (ORCID: 0000-0002-2156-0213) [1,2] * &

E. Rutger Leukfeldt (ORCID: 0000-0002-3051-0859) [1,2]

[1] *Netherlands Institute for the Study of Crime and Law Enforcement (NSCR)*

[2] *Centre of Expertise Cyber Security, The Hague University of Applied Sciences*

* *Corresponding author: De Boelelaan 1077, 1081 HV Amsterdam, Netherlands.*

Email: amoneva@nscr.nl

Moneva, A., & Leukfeldt, E. R. (2023). Insider Threats Among Dutch SMEs: Nature and Extent of Incidents, and Cyber Security Measures. *Journal of Criminology*.

https://doi.org/10.1177/26338076231161842

Abstract

Insider threats represent a latent risk to all organizations, whether they are large companies or SMEs. Insiders, the individuals with privileged access to the assets of organizations, can compromise their proper functioning and cause serious consequences that can be direct—such as financial—or indirect—such as reputational. Insider incidents can have a negative impact on SMEs, as their resources are often limited, making it paramount to implement adequate cyber security measures. Despite its indisputable relevance, the empirical study of insider incidents from a criminological point of view has received little attention. This paper presents the results of an exploratory study that aims to understand the nature and extent of three type of insider incidents—malicious, negligent, and well-meaning—and how they are related to the adoption of cyber security measures. To that end, we administered a questionnaire among a panel of 496 Dutch SME entrepreneur and managers and analysed the results quantitatively and qualitatively. The results show that although the prevalence of insider incidents is relatively low among Dutch SMEs, few organizations report a disproportionate number of incidents that often entail serious consequences. A regression model shows that there are cyber security measures related to both higher and lower incident likelihood. The implications of these findings for the cyber security policies of SMEs are discussed.

Keywords

insider threats, insider incidents, insiders, SMEs, organizations, cyber security

1. Introduction

The increasing digitization of business means that organizations and among them, especially small and medium-sized enterprises (SMEs), must face cyber security challenges that often overwhelm them. Threats can be external, when they originate outside the organization, or internal, when they originate inside. Due to privileged access to information, the latter are arguably the most dangerous (e.g., CERT National Insider Threat Center, 2019). To protect against insider threats, SME managers must consider a myriad of cybersecurity solutions to develop a strong cybersecurity culture that is tailored to the organization's needs and resources and encourages secure behaviour among its employees (Bada & Nurse, 2019). However, little is known about how the adoption of these cyber security measures in SMEs relates to insider victimization, as few criminological studies have addressed this issue (Williams et al., 2019), especially outside the Anglosphere. This paper presents an exploratory study using a survey design about the nature

and extent of insider threats affecting Dutch SMEs and how they relate to the adoption of cyber security measures.

Some international figures illustrate the complex cyber security landscape faced by organizations. In the 2021 edition of the United Kingdom (UK) Cyber Security Breaches Survey, 39% of businesses reported cyber security incidents in the past year (Johns, 2021), down 7% on the previous year (Johns, 2020)—probably due to the pandemic (Buil-Gil et al., 2020; Kemp et al., 2021). These incidents had a mean cost of £8,460 per business. Data from the Canadian Survey of Cyber Security and Cybercrime indicates that, in 2019, 21% of all businesses reported being impacted by cyber security incidents (Statistics Canada, 2020). This affected 18% of the small businesses and 29% of medium-sized businesses. In the Netherlands, a report by the CPB Netherlands Bureau for Economic Policy Analysis, indicates that 48% of Dutch companies experienced a cyber security incident in 2018 (Overvest et al., 2019). According to two reports based on two different online surveys, in the case of Dutch SMEs, this figure was 29% in 2013 (Veenstra et al., 2015) and 19% between 2016 and 2017 (Notté et al., 2019). Although it seems that, in general, larger companies report more incidents (Johns, 2021), they also have more resources and therefore probably better detection tools and reporting mechanisms (Buil-Gil et al., 2021). One of the reasons why estimates of cyber victimization in companies may differ is that the definitions of cybercrime, cyber-attack, or cyber security incident are neither clear nor consistent across studies and may include different crime measures. Such differences may also be masked by a large dark figure among SMEs (Statistics Canada, 2020; van de Weijer et al., 2021; Veenstra et al., 2015).

A Delphi study involving 129 cyber security experts in Spain suggests that government, large enterprises, and public cybersecurity institutions are aware that SMEs are not prepared to defend against cybersecurity threats (Del-Real & Díaz-Fernández, 2022). These findings align with survey data from other countries. Although most SMEs in the UK, Canada, and the Netherlands adopt basic cyber security measures such as having up-to-date antivirus software and firewalls, it appears that they are still unprepared to respond adequately to many cyber security incidents. In fact, only 13% of small and 36% of medium-sized companies in the UK train their employees in cyber security, and 19% and 42% respectively have evaluated their response to such situations (Johns, 2020, 2021). In Canada, less than half of the businesses that reported using Internet of Things devices assessed their security (Statistics Canada, 2020). Although Dutch companies are increasingly adopting cyber security measures, such as two-factor authentication and log file creation, SMEs have yet to adopt more sophisticated measures like SSL certificates, biometric unlocks, and data encryption (Notté et al., 2019; Overvest et al., 2019). This leaves SMEs vulnerable to many external attacks. Yet cyber security threats do not only come from outsiders, since malicious or negligent data handling by (ex)employees within an organization—even if well-meaning—can also put sensitive

information of individuals and companies at risk. From their vantage point, they do not need advanced technical knowledge to wreak havoc, they just need to be in the right place at the right time. These are the insider threats.

2. Insiders, insider incidents, and cyber security measures

Specialized literature identifies three elements that define an insider threat: privileged access to the assets of an organization by individuals or groups such as employees, contractors, and partners; an intent, malicious or otherwise, that defines the type of threat; and the potential to negatively affect the organization, either directly as in a theft or indirectly as through reputational damage (e.g., CERT National Insider Threat Center, 2019; Wall, 2013; Williams et al., 2019). There is consensus on the elements that define an insider threat, but terminology can still be confusing. An *insider* is a person who damages an organization from a privileged position within it. An *insider incident* is a single damaging case by an insider. An *insider threat* is then the situation that enables an incident. Generally, insider incidents are divided between intentional or *malicious* and unintentional or *non-malicious* (e.g., CERT National Insider Threat Center, 2019; Cummings et al., 2012). Non-malicious incidents can be further subdivided into *negligent* and *well-meaning* depending on whether they pursue their own or their organization's self-interest (Wall, 2013). Depending on their profile, insiders are given different self-explanatory names such as underminers, over-ambitious, socially engineered, and data leakers (Wall, 2013); and they can engage in different types of incidents such as sabotage, theft, fraud, espionage, data leaks, and even episodes of violence in the workplace (Costa, 2017; Mazzarolo et al., 2021). The cyber dimension therefore does not define an insider threat, but it certainly magnifies its potential impact.

Insiders pose a threat to all organizations, even the most prepared. Some of the most recent notorious incidents caused by insiders have in fact affected some of the organizations most renowned for their cyber security. In mid-2018, a former CISCO employee deployed malware on the company's cloud infrastructure wiping 456 virtual machines and affecting more than 16,000 WebEx accounts. The U.S. Department of Justice estimated that the malicious employee cost about $2.4 million to the company (U.S. Department of Justice, 2020). In late 2019, a cyber security company informed Microsoft that a search engine had indexed some 250 million of their customer records spanning 14 years. This exposure was caused by negligent misconfiguration of the security rules of an internal customer support database. The data was unprotected for 26 days (MSRC Team, 2020). In mid-2020, hackers posed as Twitter IT staff and, using a social engineering technique known as phone spear phishing or *vishing*, tricked some employees into providing their company credentials. Well-meaning to cooperate with company personnel, these employees enabled the hackers to gain access to 45 Twitter accounts, including those of Jeff Bezos, Joe Biden, and Elon Musk

(Twitter Inc., 2020). These insider incidents had an obvious direct financial cost, but also an indirect reputational cost, which can sometimes be more harmful. If some of the most resourceful organizations in the world are suffering the consequences of insiders, how exposed are the rest?

There is abundant case study research that provides rich insights into the human, technical, and organizational aspects of insider incidents, such as the nature of the incident, the damage caused to the organization, and the organizational response. The Insider Threat Studies are a good example of this. In a series of four reports, researchers examine a total of 160 malicious incidents from 1996 to 2002 in the United States that affected the sectors of banking and finance, critical infrastructure, IT and telecommunications, and government. With a certain degree of variation across sectors, their collective key findings indicate that most incidents consisted of fraud and sabotage, most were planned, many required little technical skills, most were detected too late, most caused financial damage and some also reputational damage (Keeney et al., 2005; Kowalski, Cappelli, et al., 2008; Kowalski, Conway, et al., 2008; Randazzo et al., 2005). In a subsequent study, researchers examined 80 cases of fraud in the financial sector, 67 of which were committed by insiders. In line with previous studies, the results show that despite not requiring much technical expertise, the financial consequences for organizations that are too slow to detect them can be devastating. This study also highlights that personal information is one of the main targets of insiders (Cummings et al., 2012). Over the years, the insider threat studies have compiled 1154 malicious incidents, mostly related to fraud, intellectual property theft and sabotage, which have served as the evidence base for a well-known guide to 21 measures to mitigate such incidents (CERT National Insider Threat Center, 2019). It recommends, for example, being especially vigilant on social media, implementing strict password and account management and practices, and monitoring and controlling remote access from all endpoints, including mobile devices.

Beyond case studies, survey research helps to quantify and estimate the actual volume of insider incidents. In Wales, the Cardiff University UK Business Cybercrime Victimization Survey was administered on a random sample of organizations which, excluding single-employee organizations, based its representativeness on their size and industry sector (Williams et al., 2019). Estimates indicate that 4.1% of organizations experienced at least one insider incident with a cyber component in the last three years. Regression models indicate that companies with more employees and those that store sensitive data are more likely to be victimized. Organizations that have a security manager also have a higher likelihood of victimization, although it is possible that hiring these professionals occurs in response to an incident or that they contribute to the detection of incidents. Another example is the UK Cyber Security Breaches Survey, a representative data source for businesses and charities (Johns, 2021). Its data can be used to obtain estimates of the prevalence of insider incidents, defined as cyber security breaches or attacks in

organizations involving unauthorized use of computers, networks or servers by staff. In the 2018 edition, 2.4% of organizations reported having suffered at least one insider incident in the last 12 months (Buil-Gil et al., 2021). This survey also collects information on the consequences of the incidents, including their outcome, their cost, and the cyber security measures adopted by organizations to mitigate them.

Situational crime prevention measures, sometimes formulated as cyber security policies, are frequently proposed to mitigate cyber security incidents (e.g., Hartel et al., 2011; Newman & Clarke, 2003). Based on the matrix of 25 techniques (Cornish & Clarke, 2003), some authors developed an adapted version for insider incidents. With the help of a crime script, a theoretical paper suggests a set of measures aimed mainly at increasing the effort insiders must make and the risk they must take to cause an incident, such as using passwords for specific programs and auditing computer logs (Willison & Siponen, 2009). Building on this work, another theoretical paper proposes a broad list of security measures for 22 of the 25 techniques. These measures include regulating the use of USB devices or other media to reduce rewards, promoting prompt software patching to reduce provocations, and setting information system security policies to remove excuses (Theoharidou & Gritzalis, 2009). As an empirical example, a survey-based study collected data from 477 employees of organizations in the United Kingdom to determine the extent to which the five categories of situational crime prevention could alter their behaviour. Confirmatory factor analyses showed that while statements regarding increased effort, increased risk and reduced rewards were significantly perceived as behaviour-altering, statements regarding reduced provocations and removed excuses were not (Safa et al., 2019). Other conceptual research suggest measures beyond situational crime prevention that include developing cyber security education and awareness programs (Bada & Nurse, 2019), fostering a culture of cybersecurity in organizations through effective risk communication, and enhancing informal social control by employees to detect early warning signs (Hills & Anjali, 2017).

These studies are but a taste of the multitude of measures available to reduce cyber security incidents or mitigate their impact. But to what extent are organizations adopting them? And is there any link between their adoption and insider incidents?

3. The present study

Despite all the research conducted on insider incidents, it appears that the overall picture is unbalanced for three reasons. Firstly, there is a lack of empirical research on the most essential aspects of the incidents, such as their prevalence, incidence, and frequency. The broad scope of insider threats makes them a complex unit of analysis to study but obtaining a clear picture of these aspects is crucial before considering studies on more advanced issues such as the implementation of adequate security measures in organizations. Secondly, there is a predominance of studies with samples from the anglosphere, which may contribute to

a biased view of the nature and extent of insider threats in other countries. To avoid this, it is necessary to carry out studies in other countries. And third, research has overlooked SMEs in this area; organizations that, by nature, operate distinctly and have different needs than larger organizations. To fill this gap in the literature, this exploratory study focuses on the insider incidents that affect SMEs in The Netherlands. The study empirically addresses four research questions (RQ):

- RQ_1: What is the prevalence, incidence, and frequency of the different types of insider incidents among Dutch SMEs?
- RQ_2: What happened in the incidents with the most impact and what were their consequences?
- RQ_{3a}: What measures do SMEs implement to prevent and mitigate cyber security incidents?
- RQ_{3b}: How does the implementation of cyber security measures by SMEs relate to insider incidents?

By answering these research questions, we aim to gain an overview of the prevalence, incidence, frequency, and consequences of insider incidents among Dutch SMEs, as well as the cyber security measures they implement. The knowledge generated will improve our understanding of insider incidents, provide cyber security recommendations for Dutch SMEs, and open new avenues of research.

4. Methods

This study uses a survey design to collect self-reported insider incident measures and a set of cyber security habits from a sample of Dutch SMEs. The European Commission defines SMEs as "enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million" (Commission Recommendation of 6 May 2003 Concerning the Definition of Micro, Small and Medium-Sized Enterprises, 2003). As we do not have access to the accounting records of the participating SMEs, we relied solely on their size as a criterion for inclusion. Descriptive quantitative and qualitative analyses are then carried out to answer the first three research questions. A binary logistic regression model was used to answer the last question.

4.1. Sample

To survey Dutch SMEs, a panel of respondents were contacted through I&O Research, a research firm for social issues. In December 2020, a total of 1420 panellists were invited to participate in an online survey, 953 of which opened the questionnaire (67.1%). When opening the questionnaire, respondents were asked two filter questions to ensure they belonged to the target group. If they identified themselves as entrepreneurs with staff or SME managers, a second filter question was asked, otherwise they were screened out. The second filter question asked whether respondents had a managerial position. A negative answer

screened them out. A total of 457 panellists were screened out or did not complete the questionnaire. The final sample consisted of 496 respondents, for a total response rate of 34.9%. Among them, 210 were entrepreneurs with staff (42.3%) and 286 were employees in a managerial position (57.7%). Of which, 69.2% were men with a mean age of 53.6 (*SD* = 12), and 30.8% were women with a mean age of 49.4 (*SD* = 12.2). Table 1 shows that the most represented sectors in the sample are business services (16.9%) and industry (14.9%) followed by retail (7.9%) and health and welfare (7.9%). One in five of the respondents' SMEs (20.2%) belong to another sector not listed.

4.2. Instrument

To collect the experiences of SMEs regarding insider victimization and examine how they relate to their cyber security practices, we developed an ad hoc questionnaire inspired by the Home Office's Cyber Security Breaches Survey (Johns, 2020). We draw on this survey for two reasons: the questions have been refined and validated over a decade; and a similar wording of the questions allows to compare results between the Netherlands and the UK. Through four blocks of questions, respondents were asked about the profile of their SME, the perceived importance of cyber security and preparedness of their organization, any insider incidents they might have experienced, and what cyber security measures and procedures they have in place. This study focuses in the last two blocks. After being reviewed by cyber security researchers and practitioners, and survey methodologists, the questionnaire was then made available in I&O Research's online platform for subsequent administration. The questionnaire can be found in Appendix A.

Table 1. Distribution of participating SMEs by sector

Sector	Frequency	
	n	%
Other	100	20.2
Business services	84	16.9
Industry	74	14.9
Retail	39	7.9
Health and welfare	39	7.9
Wholesale	31	6.2
Information and Communications Technology	29	5.8
Hospitality	27	5.4
Agriculture, forestry, fishery	14	2.8
Transport, haulage, and logistics	14	2.8
Culture, sport, and recreation	13	2.6
Education	10	2.0
Banking and insurance	6	1.2
Real state	6	1.2
Energy	3	0.6
Waste and water	3	0.6
Public Administration / Government	3	0.6
Extraction of minerals	1	0.2

Although the cybersecurity landscape surrounding SMEs is indeed complex, many business owners and managers are not cybersecurity experts, so questions had to be as comprehensive and simple as possible. We were able to gain some insight into this with a final open-ended question in which we collected the opinions of respondents about the questionnaire. Despite our efforts, four respondents found the questionnaire too technical: "Many questions are for the IT department or specialists, not for managers" (R5); "[This was] A very technical questionnaire for a small company with seven employees" (R126); "[This questionnaire] is something for IT managers" (R155); "I am certainly not an expert so it is difficult certainly to go into more depth" (R232). Another respondent, however, stated that the questionnaire contained: "Clear questions" (R316). We also asked the respondents to rate the questionnaire from 0 to 10. The mean rating of 99.3% of the respondents was 7.1 (SD = 1.4; NA = 3).

4.3. Measures

4.3.1. Insider incidents

Previous research on insider threats usually distinguishes between malicious and non-malicious insiders (e.g., CERT National Insider Threat Center, 2019; Cummings et al., 2012). Wall (2013) adds nuance to this distinction by dividing non-malicious insiders into two categories: negligent and well-meaning insiders. This research attempts to capture the resulting three types of incidents with a set of questions that cover several areas of interest. A first set serves to determine the prevalence of victimization by each type in the last 12 months, measured as the percentage of respondents who have experienced at least one insider incident in that period. This in turn allows to describe insider incident polyvictimization—the co-occurrence of different types of victimization (Ford, 2017). A second set measures the incidence or total volume of incidents experienced during that period (from "one" to "five or more"), which is sometimes accompanied by a description of the most impactful incident. A third set captures the consequences of those incidents as measured by their outcome and impact; and—separately—a fourth set collects an estimate of the direct and indirect economic cost of such incidents in euros.

According to the CERT National Insider Threat Center (2019; see also Costa, 2017), malicious insiders have privileged access to the assets of an organization and the intent to cause a negative impact on the organization. Therefore, to measure malicious insider incidents, we used the following formula: "[i]n the last 12 months, has someone who has or had authorized access to your organization's network used that privilege to intentionally act against the interests of the organization in a way that could negatively affect it?". This formula was then adapted to measure the two other types of insiders. Wall (2013) defines the negligent insider as "those employees, associates or affiliates who have legitimate access to an IT system and [...] whose eyes are not always on the ball and who might cut corners to make life easy for themselves" (p. 115). Therefore, we asked "[i]n the last 12 months, has someone who has or had authorized access to

your organization's network used that privilege to pursue their own interests—not against those of the organization—in a way that could unintentionally affect it negatively?". According to Wall (2013), well-meaning insiders are similar to negligent insiders in a broader sense but differ in one respect: they pursue the organization's interests rather than their own. And they do so by "pursuing performance goals set for them by their organization" (p. 116). Thus, we asked: "[i]n the last 12 months, has someone who has or had authorized access to your organizations network used that privilege to pursue the organization interests in a way that could unintentionally affect it negatively?". For all three questions, possible responses were "Yes", "No", or "I don't know". Given the similarity between these questions, a hint was provided to encourage respondents to read the questions carefully, as small nuances distinguish one type of insider threat from another (see Appendix A).

4.3.2. Cyber security measures

Cyber security measures are often complex and cover several areas. Accordingly, the questionnaire also includes multiple answer questions to cover aspects such as SME risk management arrangements: "Which of the following governance or risk management arrangements has your organization put in place?"; the organizational rules and controls they have in place: "Which of the following rules or control measures has your organization put in place?"; and the cyber security policies they adopted: "Which of the following aspects are covered by your cyber security policy?"; as well as the frequency with which SMEs' management reviews or updates cyber security guidelines: "When was the last time your cyber security policies or guidelines were updated or revised to make sure everything was up-to-date?" (from "24 months ago or earlier" to "within the last six months") (see Appendix A). These measures combined provide a rich overview of the adoption of cyber security measures among Dutch SMEs.

4.4. Modelling strategy

To examine the relationship between the cyber security measures adopted by SMEs and having reported one or more insider incidents, we use a binary logistic regression model. Due to the low proportion of reported incidents in the sample, this time we do not distinguish between the three types of incidents but aggregate them into a single dichotomous category when respondents report at least one incident of any type. As predictors, we used the 28 cyber security measures listed in the questionnaire as part of the risk management arrangements, rules and controls, cyber security policies, and cyber security updates. All these measures are binary except for the measure of updates, which is ordinal. To homogenize the interpretation of the model, we also dichotomize this variable by differentiating between having received an update "within the last six months" or not. As the model has a disproportionately high number of predictors (e.g., Bijleveld et al., 2018), we remove variables that have little explanatory power by employing backward stepwise selection. This strategy not only suits the exploratory purpose of the study, but also facilitates the

interpretation of the model by eliminating unnecessary noise. Model diagnostics can be found in Appendix BAppendix A.

5. Results

5.1. Prevalence, incidence, and frequency

Prevalence figures show that 7.1% of the respondents reported having experienced at least one type of insider incident in the last 12 months (Table 2). Note that some respondents reported having experienced more than one type of incident, and several cases of some types.

Table 2. Prevalence of insider incidents in the last 12 months

Victimization	Respondents	
	n	%
No	461	92.9
Yes	35	7.1

Given that the unfolding of each type of incident described in the literature—malicious, negligent, and well-meaning—is different, we identified the specific type of incident to which organizations are exposed. As shown in Table 3, there was little variation in the type of incident reported. A 2.4% of the respondents reported one or more malicious cases, 2.8% reported at least one negligent case and 3.2% reported a minimum of one well-meaning case. These categories are not mutually exclusive. Between 12.7% and 22.2% of the participants did not know if their organization had suffered an insider incident.

Table 3. Reported insider incident victimization by type

Type of insider incident	Yes		No		Don't know	
	n	%	n	%	n	%
Malicious	12	2.4	421	84.9	63	12.7
Negligent	14	2.8	380	76.6	102	20.6
Well-meaning	16	3.2	370	74.6	110	22.2

Insider incident polyvictimization is further described in Table 4. Most respondents who reported at least one incident in their organization experienced only one of its types (82.9%), while only six respondents reported experiencing two or all three types of incidents in the last 12 months (17.1%). When examining frequency per type, most respondents who reported insider incidents were repeatedly victimized (59.5%) (i.e., reported more than one incident of the same type). In line with the usual right skewed distribution of repeat victimization, Table 5 shows that as the number of repeats increases, fewer respondents are affected by them. Based on these figures, the respondents' organizations suffered at least 87 incidents in the last 12 months regardless of their type.

Table 4. Reported insider polyvictimization

Types of insider incidents	Victimization	
	n	%
One	29	82.9
Two	5	14.3
Three	1	2.9

Table 5. Reported frequency of all three types of insider incidents

Frequency of victimization	Insider threat types		
	Malicious	Negligent	Well-meaning
One	6	6	5
Two	3	6	6
Three	0	1	3
Four	2	0	0
Five or more	1	1	2

5.2. Consequences

Entrepreneurs and SME managers were also asked about the outcomes, impact, and direct and indirect costs of the insider incidents they encountered. It appears that, regardless of their type, insiders mainly target personal data stored on SMEs' servers, either to alter, destroy, or steal it.

Insider incidents often required SME staff to spend additional time resolving the incident or informing their clients about it. Many SMEs also implemented new measures to prevent or mitigate future incidents. Respondents indicated that the estimated costs of the incidents were extremely diverse, ranging from less than €500 to more than €100,000. The consequences of each type of incident are outlined in more detail below. Some participants provided additional details in the open-ended questions about the insider incident with the greatest impact (see V10, V16, and V22 in the questionnaire).

5.2.1. Malicious insider incidents

Malicious incidents have often resulted in the compromise of personal data, damage to software or systems, and the loss or theft of industrial secrets or intellectual property. Physical assets of SMEs were of no interest to malicious insiders. The impact of such incidents translated into additional time spent on incident management, as these usually prevented staff from carrying out their everyday work. In addition, several SMEs implemented measures to prevent or mitigate future similar incidents. However, the impact was not so severe that SMEs had to stop the supply of goods or services, nor compensate their customers for this. Nor were SMEs sanctioned by the legal authorities. Direct costs derived from malicious insiders ranged from €1,000 to less than €50,000; indirect costs had greater variability, ranging from less than €500 to less than €100,000.

5.2.2. Some respondents provided additional details on the most impactful incident experienced (see Negligent insider incidents

The most common outcome of a negligent incident was the compromise of personal data, followed by some form of financial loss, and damage to software or systems. Like the malicious, negligent insiders did not cause any loss of physical assets. Neither did they cause a disconnection between SMEs and third-party service providers, nor the permanent loss of files. Direct and indirect costs derived from negligent insiders were highly variable, both ranging from less than €500 to €100,000 or more.

Table 6 for references). These included simple insider incidents involving the theft of files containing data or drawings (IM5, IM1), but also more technical cyber-attacks resulting in the hacking of computing devices (IM6), and the hijacking of servers for ransom (IM10). A case of misuse of the organization's social media accounts is also reported, involving the publication of sexually compromising images on Instagram (IM11). In another case, a respondent states that an employee carried out negotiations with third parties without consent and spread lies to sabotage the organization and gain, in turn, money and status (IM3). It was also reported that a finely crafted email was sent by an employee containing malware in an attachment file that looked like an applicant's curriculum vitae. Many employees downloaded the infected file. Fortunately, the existence of a backup copy of the organization's server, made the day before, largely mitigated the damage caused by the incident (IM2).

5.2.3. Negligent insider incidents

The most common outcome of a negligent incident was the compromise of personal data, followed by some form of financial loss, and damage to software or systems. Like the malicious, negligent insiders did not cause any loss of physical assets. Neither did they cause a disconnection between SMEs and third-party service providers, nor the permanent loss of files. Direct and indirect costs derived from negligent insiders were highly variable, both ranging from less than €500 to €100,000 or more.

Table 6. Consequences of the malicious insider incidents

Incident	Outcome	Impact	Costs (€)	
			Direct	Indirect
IM1	Lost or stolen secrets or IP	Other repair or recovery costs	Unknown	Unknown
IM2	Temp. loss of access to files or networks	Additional time to deal with the incident, Implemented measures for future incidents	Unknown	1,000 - 4,999
IM3	Personal data was compromised, Permanent loss of files, Lost or stolen secrets or IP, Financial loss or money stolen	Stopped staff from carrying out daily work, Loss of revenue or share value, or income, Additional time to deal with the incident, Other repair or recovery costs, Reputational damage, Discouraged from carrying out business	20,000 - 49,999	Unknown
IM4	Software or systems were damaged, Personal data was	Stopped staff from carrying out daily work, Additional time to deal with the	20,000 - 49,999	50,000 - 99,999

Incident	Outcome	Impact	Costs (€)	
			Direct	Indirect
	compromised, Lost or stolen secrets or IP, Online services we taken or slowed down, Lost access to third party services	incident, Implemented measures for future incidents, Reputational damage		
IM5	Software or systems were damaged, Permanent loss of files, Temp. loss of access to files or networks	Other—unspecified	Unknown	1,000 - 4,999
IM6	Software or systems were damaged	Stopped staff from carrying out daily work	Unknown	Unknown
IM7	Personal data was compromised	Additional time to deal with the incident	1,000 - 4,999	50,000 - 99,999
IM8	Personal data was compromised, Lost or stolen secrets or IP	Additional time to deal with the incident, Complaints from users	5,000 - 9,999	5,000 - 9,999
IM9	Software or systems were damaged	Stopped staff from carrying out daily work	5,000 - 9,999	10,000 - 19,999
IM10	Software or systems were damaged, Personal data was compromised, Permanent loss of files	Stopped staff from carrying out daily work, Additional time to deal with the incident, Other repair or recovery costs, Implemented measures for future incidents	Unknown	Unknown
IM11	Personal data was compromised, Temp. loss of access to files or networks, Lost access to third party services	Implemented measures for future incidents, Complaints from users	1,000 - 4,999	5,000 - 9,999
IM12	External personal data stored internally	Additional time to deal with the incident, Implemented measures for future incidents	10,000 - 19,999	< 500

Despite the broad similarities with malicious incidents, negligent incidents have a unique unintended nature, as evidenced by respondents' experiences (see Table 7 for references). For example, an employee caused important financial losses to their organization simply by signing the wrong document (IN9). Another respondent stated that an employee used confidential information of the organization to start up a business (IN5). Negligent incidents can also be a consequence of cyber fraud victimization, as in the case of the organization that was affected by an advanced-fee scam targeting one of its employees (IN11). In a similar vein, one organization was the target of a spear-phishing campaign, in which fraudsters fabricated a series of emails as if they originated from management, resulting in the issuance of several large payments (IN2). One more negligent incident occurred because an intern used a private laptop containing pirated software at work. Another employee reported this malpractice to the owners of the software and the organization had to pay dearly for it (IN8).

Table 7. Consequences of the negligent insider incidents

Incident	Outcome	Impact	Costs (€)	
			Direct	Indirect
IN1	Personal data was compromised	Additional time to deal with the incident	1,000 - 4,999	20,000 - 49,999
IN2	Financial loss or money stolen	Other repair or recovery costs	> 99,999	Unknown
IN3	Software or systems were damaged	Stopped staff from carrying out daily work	1,000 - 4,999	5,000 - 9,999
IN4	Software or systems were damaged, Personal data was compromised, Online services we taken or slowed down	Loss of revenue or share value, or income, Additional time to deal with the incident	50,000 - 99,999	20,000 - 49,999
IN5	Personal data was compromised, Temp. loss of access to files or networks, Lost or stolen secrets or IP	Additional time to deal with the incident, Other repair or recovery costs, Implemented measures for future incidents, Reputational damage, Interrupted provision of goods or services, Discouraged from carrying out business	50,000 - 99,999	> 99,999
IN6	Other—unspecified	Stopped staff from carrying out daily work, Additional time to deal with the incident, Other repair or recovery costs, Implemented measures for future incidents	5,000 - 9,999	1,000 - 4,999
IN7	Software or systems were damaged, Temp. loss of access to files or networks	Stopped staff from carrying out daily work, Additional time to deal with the incident, Other repair or recovery costs, Implemented measures for future incidents	Unknown	1,000 - 4,999
IN8	Financial loss or money stolen	Implemented measures for future incidents	10,000 - 19,999	< 500
IN9	Financial loss or money stolen	Other—unspecified	1,000 - 4,999	Unknown
IN10	Unknown	Additional time to deal with the incident, Implemented measures for future incidents	< 500	Unknown
IN11	Financial loss or money stolen	Loss of revenue or share value, or income, Reputational damage	10,000 - 19,999	1,000 - 4,999
IN12	Other—unspecified	Reputational damage	Unknown	Unknown
IN13	Personal data was compromised, Lost or stolen secrets or IP	Additional time to deal with the incident, Other repair or recovery costs	1,000 - 4,999	50,000 - 99,999
IN14	Personal data was compromised	Other—unspecified	Unknown	Unknown

5.2.4. Well-meaning insider incidents

The outcomes for well-meaning incidents were different from the other types in the sense that the options we offered were not exhaustive enough, since six respondents indicated that none of the options were applicable. Nevertheless, in line with the other two types, the compromise of personal data was a common denominator, followed by temporal loss of access to files or networks. The well-meaning incidents were also different from the others in that none resulted in the loss or theft of secrets or intellectual property. In

many cases the cost of suffering a well-meaning insider was unknown, but when it was known, the direct costs ranged from less than €500 to €100,000 and indirect costs ranged from €500 to €50,000.

5.3. Comments from three respondents provide further insight into this type of insider (see Cyber security measures

In this section we first examine the extent to which SMEs adopt a range of cyber security measures and then explore how such adoption relates to insider incidents. The questionnaire divided cyber security measures in four categories: risk management arrangements, rules and controls, cyber security policies, and cyber security updates. Figure 1 displays the extent to which SMEs adopt each of the measures included in each category. As shown in Figure 1a, the most common risk management arrangement is to outsource cyber security to a specialist provider, followed by having board members, trustees, a governor or senior manager responsible for cyber security. Around one in four SMEs have staff whose role includes information security or governance and/or a formal policy or policies covering cyber security risks. A similar proportion of organizations do not have, or do not know if they have, any such arrangements.

Table 8 for references). The well-meaning incidents described here resemble the negligent ones but note that in this case insiders were pursuing the benefit of the organization and not their own. Such similarities can be observed in the case of the employee who downloaded and opened the attachment of an email which contained malware capable of spreading throughout the organization's system. A forced system shutdown stopped the spread of the virus, but inevitably caused financial loss to the organization. Again, having a back-up prevented further damage (IW3). Another employee entered into agreements regarding the terms and conditions of delivery of products—including some cancellations due to COVID-19—without proper authorization, which caused substantial financial losses (IW6). Finally, there is a reported incident related to the use of the same device for both personal and work purposes, but no further details are provided (IW15).

5.4. Cyber security measures

In this section we first examine the extent to which SMEs adopt a range of cyber security measures and then explore how such adoption relates to insider incidents. The questionnaire divided cyber security measures in four categories: risk management arrangements, rules and controls, cyber security policies, and cyber security updates. Figure 1 displays the extent to which SMEs adopt each of the measures included in each category. As shown in Figure 1a, the most common risk management arrangement is to outsource cyber security to a specialist provider, followed by having board members, trustees, a governor or senior manager responsible for cyber security. Around one in four SMEs have staff whose role includes information security or governance and/or a formal policy or policies covering cyber security risks. A similar proportion of organizations do not have, or do not know if they have, any such arrangements.

Table 8. Consequences of the well-meaning insider incidents

Incident	Outcome	Impact	Costs (€)	
			Direct	Indirect
IW1	Other—unspecified	Other repair or recovery costs, Reputational damage	5,000 - 9,999	500 - 999
IW2	Personal data was compromised, Lost access to third party services	Fines or legal costs imposed by authorities	5,000 - 9,999	20,000 - 49,999
IW3	Software or systems were damaged, Permanent loss of files, Temp. loss of access to files or networks	Stopped staff from carrying out daily work, Loss of revenue or share value, or income, Additional time to deal with the incident, Other repair or recovery costs, Implemented measures for future incidents, Reputational damage, Interrupted provision of goods or services	20,000 - 49,999	20,000 - 49,999
IW4	Personal data was compromised	Additional time to deal with the incident	1,000 - 4,999	10,000 - 19,999
IW5	Other—unspecified	Additional time to deal with the incident, Reputational damage, Complaints from users	Unknown	Unknown
IW6	Financial loss or money stolen	Loss of revenue or share value, or income, Additional time to deal with the incident, Implemented measures for future incidents, Interrupted provision of goods or services, Complaints from users	20,000 - 49,999	10,000 - 19,999
IW7	No direct consequences	Implemented measures for future incidents	Unknown	Unknown
IW8	Software or systems were damaged, Personal data was compromised, Temp. loss of access to files or networks	Stopped staff from carrying out daily work, Implemented measures for future incidents, Reputational damage, Goodwill compensations given to users	50,000 - 99,999	10,000 - 19,999
IW9	Personal data was compromised, Temp. loss of access to files or networks, Lost or stolen physical assets, Financial loss or money stolen	Loss of revenue or share value, or income, Additional time to deal with the incident, Other repair or recovery costs, Implemented measures for future incidents, Reputational damage, Interrupted provision of goods or services, Discouraged from carrying out business, Complaints from users, Goodwill compensations given to users	Unknown	Unknown
IW10	Temp. loss of access to files or networks	Implemented measures for future incidents	500 - 999	Unknown
IW11	Other—unspecified	Unknown	Unknown	Unknown
IW12	Other—unspecified	Implemented measures for future incidents, Fines or legal costs imposed by authorities, Reputational damage	Unknown	Unknown
IW13	Lost or stolen physical assets	Additional time to deal with the incident, Implemented measures for future incidents	< 500	1,000 - 4,999
IW14	Other—unspecified	Other—unspecified	Unknown	Unknown
IW15	Other—unspecified	Additional time to deal with the incident, Discouraged from carrying out business	Unknown	Unknown
IW16	Personal data was compromised, Permanent loss of files, Financial loss or money stolen, Online services we taken or slowed down	Stopped staff from carrying out daily work, Loss of revenue or share value, or income, Additional time to deal with the incident, Reputational damage	Unknown	Unknown

Figure 1b shows that most SMEs apply basic measures in terms of cyber security rules and controls, such as applying software updates when available, having firewalls covering their entire network—including individual devices, as well as up-to-date malware protection systems, and restricting IT management and access rights to specific users. About half of SMEs keep these IT rights up to date and use cloud services to back up their data, sometimes offline (R58). Regarding the strong password policy, one respondent indicated that passwords were only valid for limited periods (R16), and another stated that passwords also applied to portable devices (R282). Two other stated that they had some form of two-step verification control (R378) , such as an authenticator (R101). Another indicated that they used Ethernet instead of Wi-Fi connections (R459). It is also worth noting that most respondents are aware of the cyber security rules and controls in place in their organization, as evidenced by the anecdotal percentage of respondents who chose the options "Don't know", "None of these" or "Other".

As with risk management measures, Figure 1c shows that the cyber security policies of most SMEs do not cover many important aspects. Except for remote or mobile working, which is covered in about half of the cases, all other measures are mostly neglected. In about one in three cases, SMEs regulate what staff can do on the IT devices of the organization and/or have a document management system in place. Other measures are less widely adopted. Approximately one in five respondents indicate that their policies do not cover any of these aspects or do not know if they do.

Finally, Figure 1d shows the distribution of the time since SMEs created, updated, or last reviewed their cyber security policies or documentation to ensure they were up to date. Nearly half of respondents indicate that their organization performed such updates in the last six months, while approximately one in three do not know when or if they were carried out. A small percentage of respondents indicate that the latest cyber security updates in their organization happened two years ago or more.

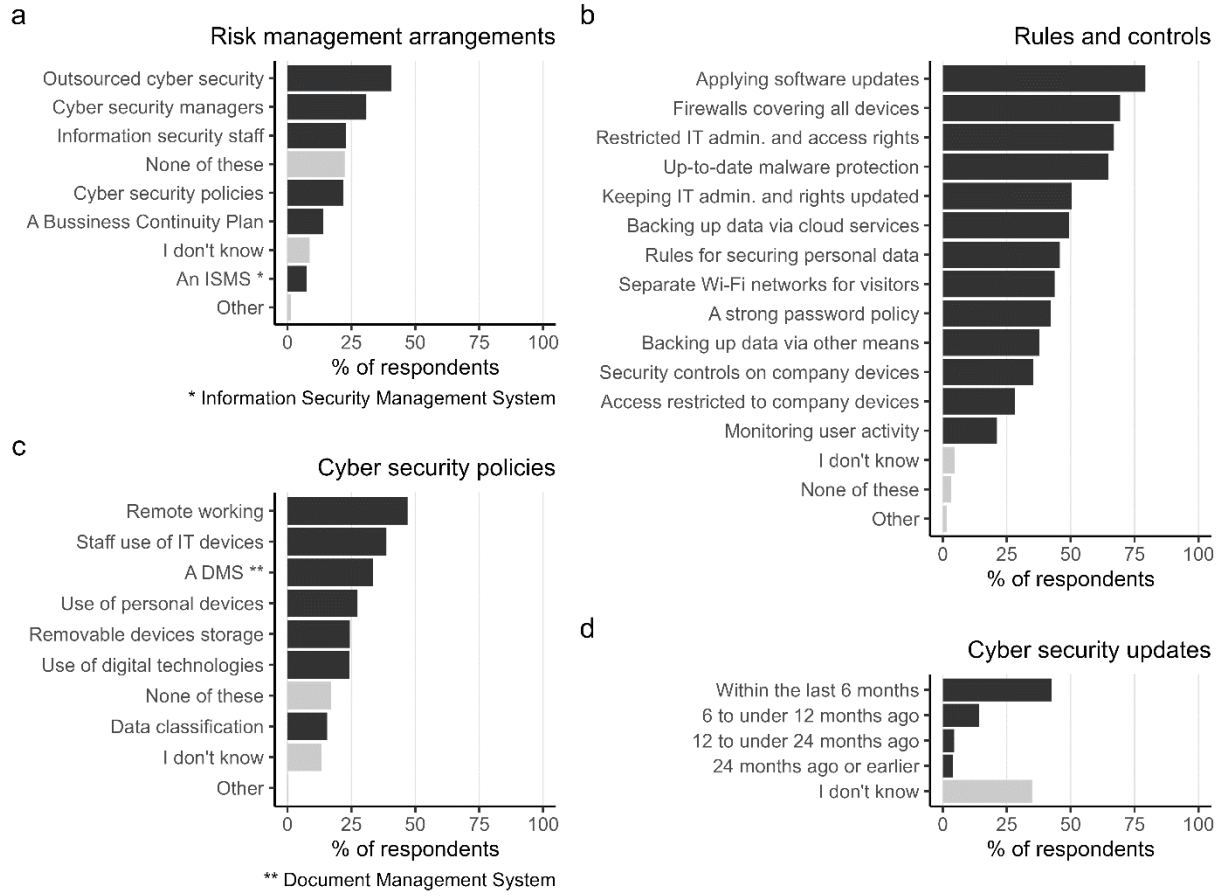

Figure 1. Adoption of cyber security measures by category: (a) risk management arrangements; (b) rules and controls; (c) cyber security policies; and (d) cyber security updates

To explore the relationship between the implementation of the 28 cyber security measures by SMEs and insider incidents of any type, we fitted a binary logistic regression model. We then performed a backward stepwise selection of variables to build a more parsimonious model. This resulted in the seven variables in Table 9. A Likelihood Ratio Test reveals no statistically significant differences between the deviance of the original 28-variable model and the fitted model [χ^2 (-20) = 12.848, p = 0.884], suggesting that the variables dropped during the stepwise selection process did not provide substantial explanatory power. The model coefficients show that the effect of having an information security management system (ISMS) (*OR* = 3.696; p = 0.016), and monitoring user activity (*OR* = 3.335; p = 0.009) is statistically significant, moderate, and positive; that is, it is associated with an increased probability of experiencing insider incidents. The effect of another two variables, applying software updates when they are available (*OR* = 0.244; p = 0.003), and backing up data securely via cloud services (*OR* = 0.304; p = 0.008), is also significant and moderate, but negative; in other words, it is associated with a lower probability of experiencing insider incidents.

Table 9. Backward stepwise binary logistic regression model to estimate odds of experiencing an insider incident with cyber security measures

Cyber security measures				95% CI	
	OR	p-value	sig.	low	high
(Intercept)	0.120	0.000	***	0.060	0.222
Risk management arrangements					
Cyber security managers	2.184	0.055		0.977	4.863
An ISMS	3.696	0.016	*	1.226	10.507
Rules and controls					
Applying software updates	0.244	0.003	**	0.095	0.612
Monitoring user activity	3.335	0.009	**	1.358	8.391
Rules for securing personal data	2.242	0.093		0.880	5.864
Access restricted to company devices	0.399	0.061		0.141	0.988
Backing up data via cloud services	0.304	0.008	**	0.122	0.712
-2 Log-likelihood	215.387				
Mc Fadden's Pseudo-R2	0.149				

6. Discussion and conclusions

This exploratory study provides a detailed overview of how three types of insider incidents—malicious, negligent, and well-meaning—affect SMEs in the Netherlands. The results add to the literature by focusing on the understudied population of SMEs in a context outside the anglosphere, and by providing new insights that contribute to contextualize the three types of insider incidents described by Wall (2013), such as their prevalence, incidence, and frequency. Additional qualitative analyses yield a comprehensive account of the most serious incidents reported, breaking each one down into its consequences, which include their outcome, impact, and estimated direct and indirect costs. Lastly, quantitative analyses describe the extent to which SMEs adopt different cyber security measures and how they relate to insider incidents.

6.1. Insider incidents

The results show that the prevalence of insider incidents of any type is 7.1%, which is comparable to that reported in other studies in the UK based on survey methodology. Compared to the study by Williams and colleagues (2019) this figure is similar to the 7.2% reported by small businesses, but higher than the 2.8% reported by micro businesses and lower than the 22.5% reported by medium-sized businesses. The prevalence we report is also higher than the 2.4% reported by Buil-Gil and colleagues (2021) but it is likely that this latter figure underestimates the true extent of insider incidents as it refers only to "unauthorized use of computers, networks or servers by staff (even if accidental)" (p. 294), which is just one expression of incident out of many. When disaggregated by type of incident, the prevalence figures reported in our study logically decrease, with malicious incidents being the least common with 2.4%, not far behind the other two types, with 2.8%, and 3.2% respectively. Taking into account the "I don't know" response rate, it is possible that these figures underestimate the incident rate of initiates due to underreporting (van de Weijer et al., 2021). Compared to the 8% reported by Kowalski and colleagues (2008) for government

organizations, our study shows that repeat victimization is much more frequent among SMEs, at 59.5%. Despite recording an incidence of more than 87 in the last 12 months, most SMEs experience only one type of incident. This suggests that each SME is vulnerable to specific insiders and would benefit from customized cyber security measures.

As for the consequences of the incidents, the results are—in general—diverse, but they show some common patterns that were also observed in other studies (Keeney et al., 2005; Kowalski, Cappelli, et al., 2008; Kowalski, Conway, et al., 2008; Randazzo et al., 2005). Firstly, the incidents result in both direct costs in terms of economic losses and disruption to business operations, and indirect costs in terms of reputational damage. According to estimates by respondents, the incidents produce a wide range of costs, which would make it difficult to accurately predict the costs of future incidents. Secondly, incidents mainly affect the data stored by organizations, and occasionally their software and systems; a clear reflection of how digitized the operations of SMEs are. And thirdly, although these outcomes impact organizations in different ways, one of the most common is work interruption, either by interrupting the supply of goods or services, by preventing staff from performing their daily work, or by taking extra time to deal with the incident. These patterns observed in SMEs have also been observed, to varying degrees, in critical infrastructures, technology and communications companies, government institutions, and the banking and financial sector.

The distinction between the three types of insider incidents allowed us to observe that the consequences of malicious insiders are similar to those of negligent insiders, but both differ from those of well-meaning insiders. This suggests that malicious and negligent incidents may be tackled with similar cyber security measures, which in turn may not be effective against well-meaning incidents. Therefore, to mitigate the consequences of incidents, it may be more useful to distinguish between selfish (i.e., malicious, and negligent) and altruistic (i.e., well-meaning) incidents as opposed to the distinction currently made in the literature between intentional and unintentional incidents (e.g., CERT National Insider Threat Center, 2019; Cummings et al., 2012). Selfish insiders would fit into what Reveraert and Sauer (2021) call insider threats, the actors lacking trustworthiness who are aware and competent but unwilling to comply with the norm. Altruistic insiders would constitute insider dangers, the actors lacking proficiency who make honest mistakes, are unaware of the norm, or simply incompetent. Although our analysis provides empirical support for this theoretical distinction, more research is needed in this area.

6.2. Cyber security measures

To mitigate the consequences of incidents, or prevent them altogether, some of the SMEs represented in this study implement cyber security measures. Comparable international figures indicate that Dutch SMEs implement risk management arrangements to a lesser extent than other countries such as the UK and Canada. For example, 22% of respondents indicate their organization has a formal policy that covers cyber

security risks. This figure is similar to that reported in 2019 in Canada, where 14% of small businesses and the 29% of medium-sized businesses reported having formal cyber security (Statistics Canada, 2020), and somewhat lower than the 31% reported by micro and small businesses in 2021 in the UK (Johns, 2021). About 13.9% of the Dutch SMEs have a business continuity plan that covers cyber security versus 30% of the micro and small businesses in 2021 in the UK (Johns, 2021). Another example is that 30.8% of respondents also indicate that their organization has board members, trustees, a governor o senior manager with responsibility for cyber security, which is a lower percentage than the 48% of medium-sized businesses in the UK that have board members with a cyber security brief (Johns, 2021). Similarly, 22.8% of respondents also employ staff whose job role includes information security or governance; while in Canada this figure is considerably larger, since 58% of small businesses and 67% of medium-sized businesses have at least one employee that regularly completed cyber security tasks (Statistics Canada, 2020).

Survey data from 2021 reveals that Dutch SMEs also seem to lag behind UK companies in terms of cyber security rules and controls (Johns, 2021). Compared to micro and small businesses, 25.7% fewer Dutch SMEs have security controls on company-owned devices such as laptops; 18.3% fewer have up-to-date malware protection; and 3.2% fewer have specific rules for storing and moving personal data files securely. Compared to medium-sized businesses, 46.8% fewer Dutch SMEs monitor user activity in any way, which makes a drastic difference. Regarding cyber security policies, and compared to medium-sized businesses in the UK (Johns, 2021), 19.6% fewer Dutch SMEs use personally-owned devices for business activities; and 15% fewer cover remote or mobile working—like working from home. Cross-country comparative studies using homogeneous cybercrime and cyber security measures would help to understand the reasons for such large discrepancies.

As of 2020, the SME cyber security landscape is complex. The analysis of the closed-ended questionnaire responses may give the wrong impression of simplicity. Some respondents provided insights that help to understand how they perceive cyber security. Statements from two respondents suggest that outsourcing cybersecurity prevents them from knowing how their organization deals with problems: "In our company we have outsourced IT through an external company. They do a lot of things for us but I don't know exactly what" (R114). "Even though I own my company, I hire a very good IT company that does this kind of thing for us. So I don't know everything that goes on (R331)". Another respondent, not so fortunate, complains that their organization cannot afford outsourcing:

> "I am aware that I should be doing a lot more in cybersecurity, but for a small business, external parties are often (much) too expensive and the ability to do it all myself is often too complicated for a layman. So a life between hope and fear" (R222).

One participant indicated that he had to adapt the cyber security strategy of his organization in response to a cyber-attack: "In December 2014 we were victims of the so-called ransomware. After that we reworked the entire IT system, and switched to cloud services, among other things" (R293). For others, cyber security does not seem to be a concern: "The topic of cybersecurity is not very high on our company's list of priorities. Personally, the subject doesn't really appeal to me either" (R191). Both the size of the company, its business, and its dependence on IT systems may be factors influencing this perception. Overall, it appears that the preparedness and priority given to cyber security by SMEs is highly heterogeneous and that there are no one-size-fits-all solutions.

Regarding the adoption of cyber security measures, our sample did not include enough incidents from each of the three categories of incidents to build a separate model for each one and obtain reliable estimates of their predictors (see Bijleveld et al., 2018), so we examined the relationship between cyber security measures and all types of incidents together. We therefore recommend interpreting the results with caution. Our model shows that some cyber security measures, such as monitoring user activity and the existence of an ISMS, are associated with a higher likelihood of incidents. This counter intuitive finding may be explained by the fact that such measures favour the detection of incidents and, therefore, their reporting. A precedent for this in the United States would be that most government agencies that experienced malicious incidents between 1996 and 2002 already had security measures in place to respond to illicit activity such as policies on acceptable use, intrusion detection systems, and internal audits (Kowalski, Cappelli, et al., 2008). Yet they still registered at least one incident. A similar circumstance is observed in the study by Williams and colleagues (2019), who find that having a cyber security manager is associated with incidents. They explain that hiring cyber security managers may be a reaction to previous victimization, but an alternative explanation could be that cyber security managers increase the detection capacity of organizations. Our model also shows a positive relationship between having a cyber security manager and experiencing at least one incident, but this is non-significant. However, the non-significance is likely due to the low sample size. We also observed that applying software updates and backing up data through cloud services are associated with a lower likelihood of incidents. It is unlikely that there is a causal relationship between these factors, as they alone cannot prevent an incident from happening. At best, these measures will simply mitigate the consequences to a large extent. A possible explanation for this finding is that companies that adopt these two measures also follow other good cyber security practices in the workplace, ultimately leading to fewer incidents.

6.3. Recommendations, limitations, and future research

Given that the resources of SMEs are often limited and the attack vectors for insider incidents are diverse, it is recommended that security measures be focused on critical assets (Keeney et al., 2005). Although the

initial recommendation was aimed at critical infrastructures, it makes sense for any organization—and perhaps especially for SMEs, whose assets are as varied as their business. It is possible that investing in preventive measures, such as hiring cyber security managers or having an ISMS, may be costly for SMEs, but the consequences of not detecting an incident may be even greater. In this regard, it may also be useful to explore any quick wins and high-impact solutions derived from some cyber security measures designed specifically for insider incidents (e.g., conducting a physical asset inventory, establishing a contract with an outside consulting firm, documenting all issues of suspicious or disruptive behaviour) (for a comprehensive checklist, see CERT National Insider Threat Center, 2019). In case preventive measures cannot be afforded, we recommend that SMEs adopt at least basic cyber security measures, such as applying software updates, reviewing account permissions, and having backups, to prevent and mitigate the consequences of some incidents. To implement essential cyber hygiene measures, SMEs do not require extensive cyber security knowledge. Such measures are described in the implementation group (IG) 1 of the Center for Internet Security (CIS) Critical Security Controls. Note that it is recommended to periodically undergo an audit to monitor the implementation of cyber security measures and evaluate their performance to understand which cyber security strategy is the most appropriate for each organization (Keeney et al., 2005) [1].

Although the lack of representativeness of the survey limits the scope of the results, they are validated by the position of the respondents within their organization—whether they are entrepreneurs with staff or employees in a managerial position. This study does not distinguish between SMEs of different sizes, as other studies do (e.g., Johns, 2021; Williams et al., 2019), which may cause the observed results to be different for other subgroups of SMEs, such as micro-organizations. In any case, the results were compared with similar samples whenever possible. It could also be argued that the questions we ask about the different types of insider threats are too complex. However, the feedback received through the survey does not suggest that this was the case. In fact, the overall rating of the questionnaire was positive: 7.1 out of 10 (*SD* = 1.4). There is also a low number of "other" and "none of these" responses, meaning that the response options are exhaustive in reflecting the SME cyber security landscape.

Current research has been unable to identify clear patterns in insider incidents due, in part, to their heterogeneity. Because insider incidents may have different aetiologies, involve different crimes, and produce different consequences, future research should strive to be specific in defining and analysing incidents whenever data permit. To involve more SMEs in this type of studies, it is important that

[1] In the United States, federal departments and agencies with access to classified information are advised to establish insider threat detection and prevention programs with the assistance of the National Insider Threat Task Force (Executive Order 13587, 2011).

researchers address real cyber security problems they face so that the results of the research have a practical application. More data could reveal new insights and patterns—for example, by comparing different cyber security models for different types of incidents—that lead to a better understanding of the phenomenon and therefore better cyber security recommendations. There is also a need to harmonize the metrics used in the various insider threat studies, as well as to synthesize their results to obtain a consensus overview of the problem. An important ally in this regard can be systematic reviews. To standardize how cybersecurity is measured across countries and disciplines, it would be useful to adopt a standard from Security, such as the CIS Critical Security Controls, and examine how it can complement a preventive framework from Criminology, such as situational crime prevention (Cornish & Clarke, 2003). Future research should collect objective measures of behaviour, such as those generated by monitoring systems, rather than self-reported ones, to overcome the limitations of survey-based studies. Partnerships with the private sector to conduct on-site experiments in organizations can contribute to gain valuable insights on how they implement cyber security measures.

Appendix A. Questionnaire

Introduction

The sustained digitization of society in recent decades has led organizations to incorporate Information Technologies (IT) into their daily operations. While IT has offered enormous advantages, it has also created risks. The correct use of IT can enhance efficiency in the management of company resources, for example, by facilitating the execution of daily processes and maintaining an electronic record of the information handled. But when it serves perverse purposes, IT can also pose a threat to the integrity of an organization's assets, even when used by employees themselves (i.e., insiders). Intentionally or unintentionally, insiders can cause significant damage to their organization, whether by leaking confidential information, destroying files and undermining the company's reputation, among other outcomes. Cyber security strategies, on the other hand, are designed to protect organizations from insiders and other threats. This questionnaire aims to explore the relationship between insider threats and cyber security in Dutch SMEs.

Business profile

First, we would just like to ask some general questions about your organization, so we can make sure we only ask you relevant questions later on.

Sector (*Sector*)

To which sector does your organization belong?

- ☐ Agriculture, forestry, fishery
- ☐ Banking and insurance
- ☐ Business services
- ☐ Culture, sport, and recreation
- ☐ Education
- ☐ Energy
- ☐ Extraction of minerals
- ☐ Health and welfare
- ☐ Hospitality
- ☐ Industry
- ☐ Information and Communications Technology
- ☐ Publica Administration / Government
- ☐ Real state

☐ Retail

☐ Transport, haulage, and logistics

☐ Waste and water

☐ Wholesale

☐ Other

Insider threats

Now we would like to ask some questions about three types of insider threats. Such threats can lead to many outcomes (e.g., damaged, lost, stolen) for various assets (e.g., technology, information). And small nuances distinguish one type of insider threat from another, so please read the questions carefully. We would like to insist in that your response is strictly confidential and during its treatment will undergo anonymization.

Malicious insider incidents (*V8*)

In the last 12 months, has someone who has or had authorized access to your organization's network used that privilege to intentionally act against the interests of the organization in a way that could negatively affect it?

☐ Yes

☐ No [go to V14]

☐ Don't know

Frequency of malicious insider incidents (*V9*)

How many incidents like this happened in the last 12 months?

☐ 1

☐ 2

☐ 3

☐ 4

☐ 5 or more

Description of the most notable insider incident (*V10*)

Can you (anonymously) describe the incident with the highest impact?

[open]

Outcome of malicious insider incidents (*V11*)

Did these incidents result in any of the following?

☐ Software or systems were corrupted or damaged

☐ Personal data (e.g., staff, customers, beneficiaries, donors, volunteers, or students) was altered, destroyed or taken

☐ Permanent loss of files (other than personal data)

☐ Temporary loss of access to files or networks

☐ Lost or stolen physical assets

☐ Lost or stolen trade secrets or intellectual property

☐ Financial loss or money was stolen

☐ Your organization's website or online services were taken down or made slower

☐ Lost access to any third-party services you rely on

☐ None of these

☐ Other. Please briefly describe what happened [open]

☐ Don't know

Impact of malicious insider incidents (*V12*)

Did these incidents impacted your organization in any of the following ways?

☐ Stopped staff from carrying out their day-to-day work

☐ Loss of revenue or share value, or income

☐ Additional staff time to deal with the incident, or to inform customers, beneficiaries, stakeholders, students or parents

☐ Any other repair or recovery costs

☐ New measures needed to prevent or protect against future insider threats

☐ Fines from regulators or authorities, or associated legal costs

☐ Reputational damage

☐ Prevented provision of goods or services to customers, beneficiaries, or service users

☐ Discouraged your organization from carrying out future business activity that was intended to be done

☐ Complaints from customers, beneficiaries, stakeholders, students or parents

☐ Goodwill compensation or discounts given to customers

☐ None of these

☐ Other. Please briefly describe what happened [open]

☐ Don't know

Cost of malicious insider incidents (*V13*)

If applicable, what was the approximate financial impact of these incidents on your organization over the last 12 months?

Direct costs (e.g., financial loss)

☐ Less than 500€

☐ 500€ to less than 1.000€

☐ 1.000€ to less than 5.000€

☐ 5.000€ to less than 10.000€

☐ 10.000€ to less than 20.000€

☐ 20.000€ to less than 50.000€

☐ 50.000€ to less than 100.000€

☐ 100.000€ or more

☐ Don't know

☐ Not applicable

Indirect costs (e.g., reputational damage)

☐ Less than 500€

☐ 500€ to less than 1.000€

☐ 1.000€ to less than 5.000€

☐ 5.000€ to less than 10.000€

☐ 10.000€ to less than 20.000€

☐ 20.000€ to less than 50.000€

☐ 50.000€ to less than 100.000€

☐ 100.000€ or more

☐ Don't know

☐ Not applicable

Negligent insider incidents (*V14*)

In the last 12 months, has someone who has or had authorized access to your organization's network used that privilege to pursue their own interests—not against those of the organization—in a way that could unintentionally affect it negatively?

☐ Yes

☐ No [go to V20]

☐ Don't know

Frequency of negligent insider incidents (*V15*)

How many incidents like this happened in the last 12 months?

☐ 1

☐ 2

☐ 3

☐ 4

☐ 5 or more

Description of the most notable insider incident (*V16*)

Can you (anonymously) describe the incident with the highest impact?

[open]

Outcome of negligent insider incidents (*V17*)

Did these incidents result in any of the following?

☐ Software or systems were corrupted or damaged

☐ Personal data (e.g., staff, customers, beneficiaries, donors, volunteers, or students) was altered, destroyed or taken

☐ Permanent loss of files (other than personal data)

☐ Temporary loss of access to files or networks

☐ Lost or stolen physical assets

☐ Lost or stolen trade secrets or intellectual property

☐ Financial loss or money was stolen

☐ Your organization's website or online services were taken down or made slower

☐ Lost access to any third-party services you rely on

☐ None of these

☐ Other. Please briefly describe what happened [open]

☐ Don't know

Impact of negligent insider incidents (*V18*)

Did these incidents impacted your organization in any of the following ways?

☐ Stopped staff from carrying out their day-to-day work

☐ Loss of revenue or share value, or income

☐ Additional staff time to deal with the incident, or to inform customers, beneficiaries, stakeholders, students or parents

☐ Any other repair or recovery costs

☐ New measures needed to prevent or protect against future insider threats

☐ Fines from regulators or authorities, or associated legal costs

☐ Reputational damage

☐ Prevented provision of goods or services to customers, beneficiaries, or service users

☐ Discouraged you from carrying out a future business activity you were intending to do

☐ Complaints from customers, beneficiaries, stakeholders, students or parents

☐ Goodwill compensation or discounts given to customers

☐ None of these

☐ Other. Please briefly describe what happened [open]

☐ Don't know

Cost of negligent insider incidents (*V19*)

If applicable, what was the approximate financial impact of these incidents on your organization over the last 12 months?

Direct costs (e.g., financial loss)

☐ Less than 500€

☐ 500€ to less than 1.000€

☐ 1.000€ to less than 5.000€

☐ 5.000€ to less than 10.000€

☐ 10.000€ to less than 20.000€

☐ 20.000€ to less than 50.000€

☐ 50.000€ to less than 100.000€

☐ 100.000€ or more

☐ Don't know

☐ Not applicable

Indirect costs (e.g., reputational damage)

☐ Less than 500€

☐ 500€ to less than 1.000€

☐ 1.000€ to less than 5.000€

☐ 5.000€ to less than 10.000€

☐ 10.000€ to less than 20.000€

☐ 20.000€ to less than 50.000€

☐ 50.000€ to less than 100.000€

☐ 100.000€ or more

☐ Don't know

☐ Not applicable

Well-meaning insider incidents (*V20*)

In the last 12 months, has someone who has or had authorized access to your organization's network used that privilege to pursue their own interests—not against those of the organization—in a way that could unintentionally affect it negatively?

☐ Yes

☐ No [go to V27]

☐ Don't know

Frequency of well-meaning insider incidents (*V21*)

How many incidents like this happened in the last 12 months?

☐ 1

☐ 2

☐ 3

☐ 4

☐ 5 or more

Description of the most notable insider incident (*V22*)

Can you (anonymously) describe the incident with the highest impact?

[open]

Outcome of well-meaning insider incidents (*V23*)

Did these incidents result in any of the following?

☐ Software or systems were corrupted or damaged

☐ Personal data (e.g., staff, customers, beneficiaries, donors, volunteers, or students) was altered, destroyed or taken

☐ Permanent loss of files (other than personal data)

☐ Temporary loss of access to files or networks

☐ Lost or stolen assets, trade secrets or intellectual property

☐ Lost or stolen physical assets

☐ Lost or stolen trade secrets or intellectual property

☐ Your organization's website or online services were taken down or made slower

☐ Lost access to any third-party services you rely on

☐ None of these

☐ Other. Please briefly describe what happened [open]

☐ Don't know

Impact of well-meaning insider incidents (*V24*)

Did these incidents impacted your organization in any of the following ways?

☐ Stopped staff from carrying out their day-to-day work

☐ Loss of revenue or share value, or income

☐ Additional staff time to deal with the incident, or to inform customers, beneficiaries, stakeholders, students or parents

☐ Any other repair or recovery costs

☐ New measures needed to prevent or protect against future insider threats

☐ Fines from regulators or authorities, or associated legal costs

☐ Reputational damage

☐ Prevented provision of goods or services to customers, beneficiaries, or service users

☐ Discouraged you from carrying out a future business activity you were intending to do

☐ Complaints from customers, beneficiaries, stakeholders, students or parents

☐ Goodwill compensation or discounts given to customers

☐ None of these

☐ Other. Please briefly describe what happened [open]

☐ Don't know

Cost of well-meaning insider incidents (*V25*)

If applicable, what was the approximate financial impact of these incidents on your organization over the last 12 months?

Direct costs (e.g., financial loss)

☐ Less than 500€

☐ 500€ to less than 1.000€

☐ 1.000€ to less than 5.000€

☐ 5.000€ to less than 10.000€

☐ 10.000€ to less than 20.000€

☐ 20.000€ to less than 50.000€

☐ 50.000€ to less than 100.000€

☐ 100.000€ or more

☐ Don't know

☐ Not applicable

Indirect costs (e.g., reputational damage)

☐ Less than 500€

☐ 500€ to less than 1.000€

☐ 1.000€ to less than 5.000€

☐ 5.000€ to less than 10.000€

☐ 10.000€ to less than 20.000€

☐ 20.000€ to less than 50.000€

☐ 50.000€ to less than 100.000€

☐ 100.000€ or more

☐ Don't know

☐ Not applicable

Policies and procedures

Now we would like to ask some questions about processes and procedures to do with cyber security. Again, just to reassure you, we are not looking for a "right" or "wrong" answer at any question.

Risk management arrangements (*V27*)

Which of the following governance or risk management arrangements has your organization put in place?

- ☐ Board members, trustees, a governor or senior manager with responsibility for cyber security
- ☐ An outsourced provider that manages your cyber security
- ☐ A formal policy or policies in place covering cyber security risks
- ☐ A Business Continuity Plan
- ☐ Staff members whose job role includes information security or governance
- ☐ An Information Security Management System (ISMS)
- ☐ None of these
- ☐ Other, namely: [open]
- ☐ Don't know

Rules and controls (*V28*)

Which of the following rules or control measures has your organization put in place?

- ☐ Applying software updates when they are available
- ☐ Up-to-date malware protection
- ☐ Firewalls that cover your entire IT network, as well as individual devices
- ☐ Restricting IT administration and access rights to specific users
- ☐ Maintaining or keeping IT administration and access rights up to date
- ☐ Any monitoring of user activity
- ☐ Specific rules for storing and moving personal data files securely
- ☐ Security controls on company-owned devices (e.g., laptops)
- ☐ Only allowing access via company-owned devices
- ☐ Separate Wi-Fi networks for staff and for visitors
- ☐ Backing up data securely via a cloud service
- ☐ Backing up data securely via other means
- ☐ A password policy that ensures users set strong passwords

☐ None of these

☐ Other, namely: [open]

☐ Don't know

Cyber security policies (*V29*)

Which of the following aspects are covered by your cyber security policy?

☐ What can be stored on removable devices (e.g., USB sticks)

☐ Remote or mobile working (e.g., from home)

☐ What staff are permitted to do on your organization's IT devices

☐ Use of personally-owned devices for business activities

☐ Use of new digital technologies such as cloud computing

☐ Data classification

☐ A Document Management System

☐ None of these

☐ Other, namely: [open]

☐ Don't know

Cyber security update (*V30*)

When was the last time your cyber security policies or guidelines were updated or revised to make sure everything was up-to-date?

☐ Within the last 6 months

☐ 6 to under 12 months ago

☐ 12 to under 24 months ago

☐ 24 months ago or earlier

☐ Don't know

Closing remark

Thank you for taking the time to participate in this study.

Appendix B. Binary logistic regression model diagnostics

Figure 2 displays the diagnostics of the binary logistic regression model for linearity and influential values. The "Residual vs Fitted" plot serves to visually check the assumption that the relationship between cyber security measures and the logit of insider incidents is linear. The horizontal red line suggests that this is the case, and that a generalized linear model may be a good approach to model such a relationship. The "Cook's distance" plot shows whether there are any abnormal observations or *outliers* in the model. In this case, there seems to be three outliers: observations 43, 57, and 269. However, not all outliers can alter the interpretation of the model or be *influential*. Only influential observations are critical. Using a red dashed threshold, the "Residuals vs Leverage" plot indicates whether that is the case. The outliers in our model do not trespass that threshold, which indicates that they are not influential observations.

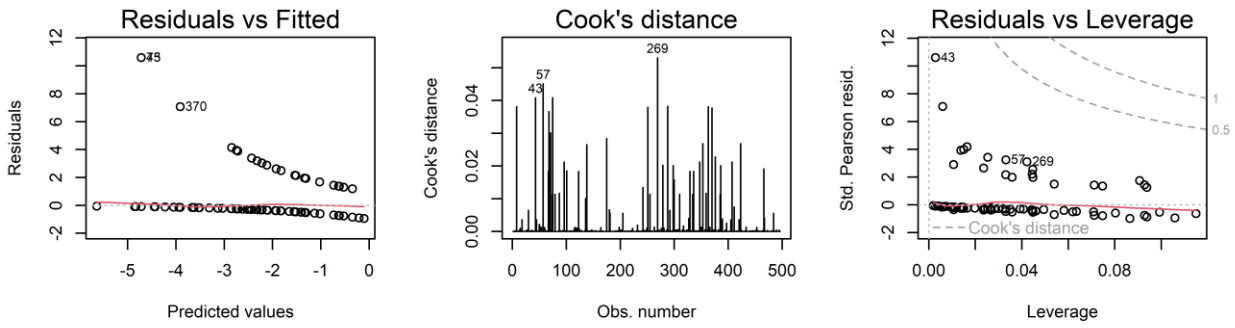

Figure 2. Diagnostics of linearity and influential values for the binary logistic regression model

CRediT Author Statement

Asier Moneva: Conceptualization, Software, Validation, Formal analysis, Investigation, Data Curation, Writing - Original Draft, Writing - Review & Editing, Visualization, Supervision. **E. Rutger Leukfeldt**: Conceptualization, Investigation, Resources, Writing - Review & Editing, Supervision, Project administration, Funding acquisition.

Acknowledgements

We thank Susanne van 't Hoff-de Goede and Raoul J. Notté, Center of Expertise Cyber Security of the Hague University of Applied Sciences, and Elsine van Os, Signpost Six, for their comments, which helped to improve the questionnaire. We also thank the two anonymous reviewers for their comments.

Data availability

Upon acceptance, data and code used will be uploaded to the Open Science Framework (OSF) repository <https://osf.io/dw9xb/> with DOI 10.17605/OSF.IO/DW9XB.

References

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Bijleveld, C. C. J. H., van de Weijer, S. G. A., Ruiter, S., & Van der Geest, V. (2018). *Analysis techniques for non-experimental data: An introduction*. Eleven International Publishing.

Buil-Gil, D., Lord, N., & Barrett, E. (2021). The Dynamics of Business, Cybersecurity and Cyber-Victimization: Foregrounding the Internal Guardian in Prevention. *Victims & Offenders*, *16*(3), 286–315. https://doi.org/10.1080/15564886.2020.1814468

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies*, *0*(0), 1–13. https://doi.org/10.1080/14616696.2020.1804973

CERT National Insider Threat Center. (2019). *Common Sense Guide to Mitigating Insider Threats, Sixth Edition* (CMU/SEI-2018-TR-010; pp. 1–168). Software Engineering Institute, Carnegie Mellon University. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=540644

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley´s critique of situational crime prevention. In M. J. Smith & D. B. Cornish (Eds.), *Theory for practice in situational crime prevention* (pp. 41–96). Criminal Justice.

Costa, D. L. (2017). CERT Definition of 'Insider Threat'—Updated. *Insider Threat Blog*. https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat—updated.html

Cummings, A., Lewellen, T., McIntire, D., Moore, A. P., & Trzeciak, R. (2012). *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector* (CMU/SEI-2012-SR-004; pp. 1–76). Carnegie Mellon University. https://resources.sei.cmu.edu/asset_files/SpecialReport/2012_003_001_28137.pdf

Del-Real, C., & Díaz-Fernández, A. M. (2022). Understanding the plural landscape of cybersecurity governance in Spain: A matter of capital exchange. *International Cybersecurity Law Review*, *3*(2), 313–343. https://doi.org/10.1365/s43439-022-00069-4

Executive Order 13587, Presidential Documents, 198 76 1 (2011). https://www.dni.gov/files/NCSC/documents/nittf/EO_13587.pdf

Ford, J. D. (2017). *Polyvictimization* (pp. 9780195396607–0223) [Data set]. Oxford University Press. https://doi.org/10.1093/obo/9780195396607-0223

Hartel, P., Junger, M., & Wieringa, R. (2011). *Cyber-crime Science = Crime Science + Information Security*.

Hills, M., & Anjali, A. (2017). A human factors contribution to countering insider threats: Practical prospects from a novel approach to warning and avoiding. *Security Journal*, *30*(1), 142–152. https://doi.org/10.1057/sj.2015.36

Johns, E. (2020). *Cyber Security Breaches Survey 2020: Statistical Release* (pp. 1–58). Department for Digital, Culture, Media and Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf

Johns, E. (2021). *Cyber Security Breaches Survey 2021: Statistical Release* (pp. 1–66). Department for Digital, Culture, Media and Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/972399/Cyber_Security_Breaches_Survey_2021_Statistical_Release.pdf

Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., & Rogers, S. (2005). *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors* (pp. 1–45). U.S. Secret Service & Carnegie Mellon University. https://resources.sei.cmu.edu/asset_files/SpecialReport/2005_003_001_51946.pdf

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19. *Journal of Contemporary Criminal Justice*, 104398622110279. https://doi.org/10.1177/10439862211027986

Kowalski, E., Cappelli, D., & Moore, A. (2008). *Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector* (pp. 1–59). U.S. Secret Service & Carnegie Mellon University. https://resources.sei.cmu.edu/asset_files/WhitePaper/2008_019_001_52266.pdf

Kowalski, E., Conway, T., Keverline, S., Williams, M., Cappelli, D., Willke, B., & Moore, A. (2008). *Insider Threat Study: Illicit Cyber Activity in the Government Sector* (pp. 1–36). U.S. Secret Service & Carnegie Mellon University. https://resources.sei.cmu.edu/asset_files/WhitePaper/2008_019_001_52247.pdf

Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, Pub. L. No. 2003/361/EC, 124/36 Legislation 1 (2003). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2003.124.01.0036.01.ENG&toc=OJ:L:2003:124:TOC

Mazzarolo, G., Fernández Casas, J. C., Jurcut, A. D., & Le-Khac, N.-A. (2021). Protect Against Unintentional Insider Threats: The Risk of an Employee's Cyber Misconduct on a Social Media Site. In M. Weulen Kranenbarg & E. R. Leukfeldt (Eds.), *Cybercrime in Context: Vol. I* (pp. 79–101). Springer International Publishing. https://doi.org/10.1007/978-3-030-60527-8_6

MSRC Team. (2020, January 22). Access Misconfiguration for Customer Support Database. *Microsoft Security Response Center*. https://msrc-blog.microsoft.com/2020/01/22/access-misconfiguration-for-customer-support-database/

Newman, G. R., & Clarke, R. V. (2003). *Superhighway robbery: Preventing e-commerce crime*. Willan.

Notté, R. J., Slot, L. K., van 't Hoff-de Goede, S., & E. Rutger, L. (2019). *Nulmeting: Cybersecurity in het mkb* (pp. 1–30). The Hague University of Applied Sciences. https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/cybersecurity-in-het-mkb_nulmeting_notte_et_al_2019.pdf

Overvest, B., Non, M., Dinkova, M., El-Dardiry, R., & Windig, R. (2019). *Cyber Security Risk Assessment for the Economy 2019* (pp. 1–38). CPB Netherlands Bureau for Economic Policy Analysis. https://www.cpb.nl/sites/default/files/omnidownload/CPB-Cyber-Security-Risk-Assessment-for-the-Economy-2019.pdf

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector* (CMU/SEI-2004-TR-021; pp. 1–36). U.S. Secret Service & Carnegie Mellon University. https://resources.sei.cmu.edu/asset_files/SpecialReport/2004_003_001_50299.pdf

Reveraert, M., & Sauer, T. (2021). Redefining insider threats: A distinction between insider hazards and insider threats. *Security Journal*, *34*(4), 755–775. https://doi.org/10.1057/s41284-020-00259-x

Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., & Sookhak, M. (2019). Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Generation Computer Systems*, *97*, 587–597. https://doi.org/10.1016/j.future.2019.03.024

Statistics Canada. (2020). *About one-fifth of Canadian businesses were impacted by cyber security incidents in 2019* (pp. 1–4). Statistics Canada. https://www150.statcan.gc.ca/n1/en/daily-quotidien/201020/dq201020a-eng.pdf

Theoharidou, M., & Gritzalis, D. (2009). *Situational Crime Prevention and Insider Threat: Countermeasures and Ethical Considerations*. 808–820.

Twitter Inc. (2020, July 30). An update on our security incident. *Twitter Blog*. https://blog.twitter.com/en_us/topics/company/2018/enabling-further-research-of-information-operations-on-twitter.html

U.S. Department of Justice. (2020, August 26). San Jose Man Pleads Guilty To Damaging Cisco's Network. *U.S. Attorney's Office Northern District of California*. https://www.justice.gov/usao-ndca/pr/san-jose-man-pleads-guilty-damaging-cisco-s-network

van de Weijer, S. G. A., Leukfeldt, E. R., & van der Zee, S. (2021). Cybercrime Reporting Behaviors Among Small- and Medium-Sized Enterprises in the Netherlands. In M. Weulen Kranenbarg & E. R. Leukfeldt (Eds.), *Cybercrime in Context: Vol. I* (pp. 303–325). Springer International Publishing. https://doi.org/10.1007/978-3-030-60527-8_17

Veenstra, S., Zuurveen, R., & Stol, W. (2015). *Cybercrime onder bedrijven: Een onderzoek naar slachtofferschap van cybercrime onder het Midden- en Kleinbedrijf en Zelfstandigen Zonder Personeel in Nederland* (pp. 1–242). NHL Stenden University of Applied Sciences. https://cybersciencecenter.nl/media/1054/2015-05-13-cybercrime-onder-bedrijven-def.pdf

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal*, *26*(2), 107–124. https://doi.org/10.1057/sj.2012.1

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory. *Deviant Behavior*, *40*(9), 1119–1131. https://doi.org/10.1080/01639625.2018.1461786

Willison, R., & Siponen, M. (2009). Overcoming the insider: Reducing employee computer crime through Situational Crime Prevention. *Communications of the ACM*, *52*(9), 133–137. https://doi.org/10.1145/1562164.1562198