Battling the rising insider threat: aligning academic and practitioner approaches

Makienko, Diana

Universiteit Leiden

Battling the rising insider threat: aligning academic and practitioner approaches

Diana Makienko

S3114511

31-01-2023

Executive Security Master Thesis
Thesis Supervisor: Tommy van Steen
Second reader: Zekeriya Erkin

Table of Contents

I. PROBLEM DEFINITION

Insider threats is not a new problem, it has existed since the beginning of humankind. People were using their internal knowledge and access to recourses to commit fraud, to trade secrets and to spy, to sabotage and destroy. They were doing this for different reasons – for the reasons of personal enrichment, political power and ideological convictions, seeking justice or vengeance. With the evolution of information technology, intrusion means for an insider have significantly evolved and despite continuous efforts of cyber security professionals, the number of the crimes committed by the insiders is growing. According to the research done by Tessian[1], a number of incidents that was caused by insiders have increased by 47% between 2018 and 2020. Moreover, results of a survey run by the same company Tessian in 2021 revealed that 57% of organizations believe that insider incidents have become more frequent over the past 12 months. And what is interesting is that, according to the Cybersecurity Insiders 2021 reports, about one third of those incidents were caused by malicious insiders.

When referring to the malicious insiders first what comes to mind is a cyber espionage, where an employee steals and sells a company's intellectual property for own financial gain potentially causing this company a loss of business, or a whistleblowing where for, usually, political or moral reasons, organisations' secrete information is being shared with the world, or a deliberate sabotage, where an employee injects a malware into a company's network or disables access to the main server causing a disruption of operations and the likes. However, many deeds that have a more innocent feeling to it should also be seen as malicious insider incidents. Here we are referring to downloading or copying company owned information, customers' contact details, obtaining information on behalf of a company for own use and the likes.

Other than the growing number of malicious cyber incidents, the other reason why this is the most concerning issue is the extent in which a harm can be caused to an organisation, as has been rightly outlined by the security guru Bruce Schneier "Insiders are especially pernicious attackers because they're trusted. They have access because they're *supposed* to have access. They have opportunity, and an understanding of the system, because they use it—or they designed, built, or installed it. They're already inside the security system, making them much harder to defend against." [2] Insiders know what the company's crown jewels are, where they are located and what can harm the most. They have knowledge of the organisation, it's culture, habits and rituals, its processes and procedures, what works and what does not and what are the vulnerabilities. Hence, an adversary is often detected too late, when the harm is already done.

The damage to companies' that insiders can inflict is significant. It varies from a financial loss to the loss of business or reputation and potentially a long-term negative effect on the organisation's moral and culture. According to the Ponemon Institute[3], the costs of incidents committed by insiders have gone up from $4,7 billion in 202 t $6.8 billion in 2022.
At the same time the attention to cyber security within organisations has seen a rapid growth over the last two decades. The concept of building a strong Security Culture became a priority

[1] https://www.tessian.com/blog/insider-threat-statistics/ accessed on January 2023
[2] https://www.schneier.com/blog/archives/2009/02/insiders.html accessed on January 2023
[3] https://www.ponemon.org/news-updates/blog/security/data-breaches-caused-by-insiders-increase-in-frequency-and-cost.html accessed on January 2023

for companies' leadership[4]. Various organisations have been established with a goal to bring controlled and structured governance to cyber space, as well as to advise on control mechanisms and mandate norms that also include security controls that are meant to prevent an insider incident.[5] So why, despite of having a high priority on the agenda of leadership and continuous effort of cyber security professionals, the number of cyber incidents committed by insiders, and malicious insiders in particular is still growing? Do we underestimate the threat or overestimate our defence?

Considering the high costs – direct or indirect - associated with the insider attack and a potential catastrophic consequence in case an attack is raged on a high-risk critical infrastructure like electrical or a nuclear plant it is paramount for security professionals to act before the damage is done. Therefore, in this research we will focus on the measures that are planned and taken to prevent and timely detect (read- immediately, at the moment of occurrence) the attack.

Various studies have been conducted over the years to understand how to identify malicious insiders and what measures – or security controls – should be put in place to prevent them from acting. Different cyber security bodies and regulators of specific sectors have been recommending and even mandating implementation of security controls that prevent an attack from within. At the same time, cyber security professionals have been confronted with either effectiveness or the lack thereof of these controls.

Therefore, the **Research Question** that we are trying answer in this research is: Is there an alignment between academia and practitioners on effectiveness of the measures designed to prevent a malicious insider threat.

II. LITERATURE REVIEW

Problem of a malicious insider is not necessarily a problem of cyber space; it is a generic issue that has always existed. The means have changed or rather improved with the computer age. Articles and media news of various data leaks, that caused several companies and even the governmental agencies severe business and reputation damage have been making headlines over the years. Cases of espionage at various private, public, and scientific organisations have been making the news more and more often. Tense geopolitical situation making leaders of various high-risk organisations ever more conscious of the need to place security very high on the agenda. And taking into account that the damage inflicted by someone who knows the organisation and has access to its crown jewels can be even more devastating than the one coming from outside, the attention to the malicious insider threat has been rightfully sharpen.

1 INSIDER THREAT

Prior to discussing various security controls that are directed to counter the insider threat it is important to define what it exactly means. There are many definitions of an insider threat that have been formulated by the official cyber security bodies as well as academia. According to CISA, "Insider threat is the potential for an insider to use their authorised access or

[4] Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387.

[5] Cyber Security Culture in organisations. (n.d.). ENISA. Retrieved September 17, 2022, from https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

understanding of an organization to harm that organization"[6]. Academics are giving a similar description of an insider threat, also referring to an abuse of legitimate and entrusted permissions, as stated by Bishop et al, "a trusted entity that is given the power to violate one or more rules in a given security policy (...) the insider threat occurs when a trusted entity abuses that power" [7].

One of the most elaborated definition is given by CERT Insider Threat centre (2018, p 17). According to them, an insider threat is "a current or former employee, contractor, or another business partner who has or had authorised access to an organisation's network, system, or data; and has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, availability, or physical well-being of the organisation's information, information systems, or workforce; or who through their action or inaction without malicious intent causes harm or substantially increases the probability of severe future harm to the confidentiality, integrity, or availability of the organisation's information, or information systems."[8]

Companies are typically used to deal with external threats, putting in place various, mainly technical controls, to prevent an attack from outside. Dealing with insiders is particularly challenging as these are the employees that have been granted access to specific applications or have acquired a particular knowledge that is required to do their job and that access or knowledge is used intentionally or unintentionally to harm organisations, individuals, or a nation. To design and implement most effective measures to battel these adversities a distinction should be made between different types of insiders, between people that do not mean to cause any harm to their employer but do so by either careless behaviour or negligence and people whose intent is to either harm the organisation or abuse their knowledge or account credentials for personal gain as well as people who in one way or another have been convinced or manipulated into acting maliciously[9].

All definitions of insiders point to an intent, which is the main differentiating factor between a malicious and benign insider, where a malicious insiders are typically being described through harmful actions they take. However, intentional inactivity or a conscious failure to act can also be seen as malicious insider threat.[10] The intent, on its turn is a result of a motivation to either harm an organisation or to pursue personal reasons like an enrichment or a revenge.

---

[6] https://www.cisa.gov/defining-insider-threats viewed on January 2023

[7] Bishop, Matt & Gates, Carrie. (2008). Defining the Insider Threat. 10.1145/1413140.1413158.

[8] Carnegie Mellon University. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2019_005_001_540647.pdf.

[9] Saxena N, Hayes E, Bertino E, Ojo P, Choo K-KR, Burnap P. Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. *Electronics*. 2020; 9(9):1460. https://doi.org/10.3390/electronics9091460

[10] Prabhu, sunitha, & Thompson, N. (2020). A Unified Classification Model of Insider Threats to Information Security.

As financial gain is one of the biggest motivations for the insider threat, fraud has always been and still is one of the most common malicious insider activities. Fraud is a broad concept that covers various malicious activities from unauthorised use of companies accounting systems to manipulation of payments and loans, colleagues or clients' credentials theft and abuse, abuse of a company e-commerce and similar activities for personal gains, and the likes.

Disclosure or theft of confidential information is another example of a common malicious insider adversary. Majority of companies have a set of data that is privileged and confidential and the theft of which can bring a significant damage to organisations, diminish their competitive position, or even cause bankruptcy. Here we can consider documents associated with product design, software code, intellectual properly. Leak of personal data, but also whistleblowing, can not only cause organisation a potential existential threat but can also create legal consequences that can include high fines or even a termination.

IT sabotage and especially sabotage of a critical infrastructure is an area of an increased concern that is associated with an insider threat. Sabotage is an act of intentional use of technology to disrupt or terminate normal business operations. The biggest danger of sabotage is that it is usually committed by technical experts that operate or have been operating the system and typically know all its ins and outs.[11] Consequences of a sabotage can potentially be deadly when inflicted on a nuclear power plant, but effect of a sabotage on hospitals, electrical grids, water supply and other critical infrastructures can be quite severe as well.

Corporate and industrial espionage seems to be on the rise. Various cyber security investigators and bloggers have reported on a worrying number of espionage cases, mainly committed by so called super malicious insiders – insiders that have a full access to the infrastructure or systems and have solid knowledge thereof.[12] Often espionage is state-sponsored, mainly considering the time required and hence high cost associated with it. Although, not a new phenomenon, the level of sophistication due to the almost limitless recourses can pose a significantly higher risk of a serious damage than when committed by an individual or a group facilitated espionage.

Over the years, many companies have been taking measures against malicious insiders, from applying a number of security controls to implementing a full insider threat programme, consisting of an extensive set of security controls. To evaluate effectiveness of the security controls it is important to understand who the malicious insiders are and what motivates them to commit an adversary.

[11] William Claycomb, Carly L. Huth, Lori Flynn, David McIntire, & Todd Lewellen. (2012). Chronological Examination of Insider Threat Sabotage: Preliminary Observations. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 3, 4–20.

[12] https://www2.dtexsystems.com/2022-insider-risk-report accessed in January 2023

1.2 THE PORTRAIT OF A MALICIOUS INSIDER

When talking about different cyber criminals many of us have a specific picture in our minds; but not everyone is Plague from the Millennium trilogy of Stieg Larsson or a guy in a balaclava and gloves, most of them have likely less striking looks. There are numerous research papers that contain various characteristics of malicious insiders based on their personality, historical data, behaviour and other. Many attempts have been made to classify malicious insiders based on their personality traits.

Brian T Contos points out that a typical malicious insider shows signs of antisocial behaviour or narcissism. Additionally, Mr. Contos adds that an excessive stress and personal suffering can also push a person to commit a security crime.[13] Nan Liang et al have taken the idea of personal traits further and conducted very detailed research where various personality and character traits, medical conditions and social standing were analysed with the goal to create a deployable insider profile that would help to prevent a cyber adversary. However, the results were not always conclusive and at times even misleading, as e.g. there have appeared to be more people with narcissistic traits amongst organisations' leadership than amongst malicious insiders.[14]

Homoliak at al provide a comprehensive summary of different classifications of the insiders published by various researchers, covering it in very granular details, based on different criteria that in broad lines can be split between human and technical[15]. From the technical point of view Homoliak et al classify insiders by their ability to access network and bypass the security. From the human – possessed knowledge. In addition, a distinction is made amongst three level of the insider threats: self-motivated, recruited and planted insiders.

Many research projects are classifying malicious insiders based on their motivation. At the same time, most of the practice-based documents, when describing malicious insiders, focus on combination of motivation and personal traits.[16]

Majority of the research papers, in addition to the personality traits also analyse typical behaviour that is demonstrated by malicious insiders. Working extra or unusual hours, unusually elevated interest in projects or functions outside of their job responsibilities, poor performance, distorted behaviour, bad attitude, addictions and financial troubles were often named as possible behavioural indicators of a malicious insider.[17] Some authors are making reference to different

[13] Contos, B. T. (2006). Enemy at the water cooler real-life stories of insider threats and Enterprise Security Management countermeasures (1st edition). Rockland, MA: Syngress.

[14] Liang, N. (2017). Characteristics of malicious insiders and their relationships with different types of malicious attacks.

[15] Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight Into Insiders and IT. ACM Computing Surveys, 52(2), 1–40.

[16] CERT National Insider Threat Center Releases Sixth Edition of Common Sense Guide to Mitigating Insider Threats. (2019). Targeted News Service.

[17] Dupuis, Marc & Khadeer, Samreen. (2016). Curiosity Killed the Organization: A Psychological Comparison between Malicious and Non-Malicious Insiders and the Insider Threat. 35-40. 10.1145/2978178.2978185.

behavioural theories that help to predict and anticipate malicious insider crime, based on opportunities, social surrounding, believes and situations.

According to the Verizon Insider Threat report of 2021[18] malicious insiders can be differentiated by the motivation, which is split between financial, espionage, fun, convenience, grudge, and ideology. Not surprisingly, majority of the crimes have financial motivation, whether for the reason of enrichment or to resolve financial issues an insider or his close surrounding is facing.

Another large category is the cybercrime committed as an act of revenge by disgruntled employees, by people that feel they have not been treated appropriately by the employer. Political reasons or rather a discrepancy between a personal moral standard or believes and the company's culture is also seen as a motivator. It is, however, important to differentiate political reason from holding a grudge against employer, as in the first case no personal "wrongdoing" has been done to an employee.

However less common, some of the cybercrimes are committed for fun or because it was convenient. Although not much information seems to be available regrading this type of motivation, it has been observed that in many of such cases an insider wants to demonstrate his or her level of superiority, a proof to be able to break through security.

Last but not least, malicious insiders do not necessary act on their own behalf. Cybercrimes where an employee turns out to be on a payroll of a nation state have lately been reaching news headlines.

Solid understanding of the behavioural indicators and the motives of a malicious insider should cater for appropriate and adequate response, whether it is laid down in an organisation insider threat programme or an application of a number of security controls.

2. Security Controls

Now that we have sketched a good picture of what is it we are up against, we can try to answer the first part of the question: what academia believes to be the effective measures against malicious insiders.

Frist of all, prior to looking into various measures that are advised to be taken, it is good to understand what is exactly meant by the term "security control". Various definitions have been found in the literature, all having a similar description and referring to security controls as preventive, detective, counteractive means and measures directed to protect confidentiality, integrity and availability of the organisational data.

Security Controls are typically divided into different groups, based on the goal or a function and based on the content or approach. Here again different institutions (e.g. NIST, ISACA and etc.) use different methodology when classifying Security Controls, however, in broad lines most of

[18] https://www.verizon.com/business/resources/executivebriefs/insider-threat-report-executive-summary.pdf accessed in January 2023

the security bodies group controls into preventive, detective and corrective controls. Later in this chapter will have a closer look at these three groups.

Additionally, security controls can be classified by the ones that are making use of the human characteristics and the ones that are making a use of technology. Under human-based controls we should consider controls directed to (human) physical, behavioural, and psychological factors. Under technological we can see those that apply to networks, hosts, systems, etc.[19]

Also, security controls can be classified by content. In this particular case, the classification is done by cyber security bodies or academia tend to differ. Some divide security controls into three groups as technical, socio-technical and organizational and for the effectiveness, a combination of these three is used[20]. In some literature security controls are grouped into operational, administrative, and physical. However, all of them seem to make a clear distinction between security controls that are focusing on technology and the ones focusing on humans, what can fail under categories of technical and human-based (some authors call it biometrical, some – soft) controls. Usually, organisations put in place a set of the security controls, combining different functions and types. In order to answer the research question, in this paper we will be looking at controls that are specifically aimed at malicious insiders.

Over the last decade, several high-profile insider cases were going viral on the internet and various news media. Whistle-blowers stories of Edward Snowden and Chelsea Elizabeth Manning (formerly known as Bradley Edward Manning) made to the front page of most national and international papers.

What was common between these cases and what made them especially harmful is that both Snowden and Manning were trusted employees who abused their legitimate access to collect classified information, which later was given to the press to make it public. What is particularly interesting to note is that both Snowden and Manning managed to steal data from the organisations that supposedly have the highest level of security – CIA, NSA and the US Army. This potentially points to the fact that the security measure that were put in place by those organisations were not sufficient to prevent or even detect malicious intent.[21]

Not all the crimes committed by the insiders become a public knowledge, some are likely not being disclosed due to a reputational risk. According to the Tessian survey data[22], 45% of employees before leaving a company take with them work related documents, some of which of a confidential nature. And often the theft is not recognised at al or recognised only when the harm becomes visible. Considering that the costs associated with an insider attack are significant,

---

[19] Alsowail RA, Al-Shehari T. Techniques and countermeasures for preventing insider threats. PeerJ Comput Sci. 2022 Apr 1;8:e938. doi: 10.7717/peerj-cs.938. PMID: 35494800; PMCID: PMC9044369.

[20] Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight Into Insiders and IT. ACM Computing Surveys, 52(2), 1–40. https://doi.org/10.1145/3303771

[21] Dennehy, M. (2021). Preventing Insider Cyberthreats in Organizations: A Qualitative Delphi Study. ProQuest Dissertations Publishing.

[22] https://www.tessian.com/blog/insider-threat-statistics/ accessed in January 2023

it is only logical that the main focus should be given to preventing such attacks and then timely detect, should preventive measures fail.

Preventive controls are measures that are put in place in order to avoid incidents from happening. When executed correctly, an attack or an intrusion is blocked or stopped before it takes place; similarly, a malicious insider it identified and consequently stopped before the harm is done. As there are no silver bullets and preventive actions might fail, which is especially true in case of malicious insiders who are potentially aware of all the control mechanisms and hence are able to avoid them, it is equally important to create a safety-net by putting in place detective measures. Well-designed detective controls should provide an early detection of all the adversaries that would allow security professionals take timely mitigating actions to limit the damage made by an attack.[23]

Corrective controls are the set of measures directed to bringing a compromised system or an infrastructure back to normal. However, considering that the corrective controls that potentially apply to the malicious insiders are primarily covered by the fields of criminal law and regulations, which is a different concept, in this research corrective controls will not be considered.

2.1 Security Controls with the insider focus

Different security bodies and authorities have published lists of security controls, some are recommended, some are mandatory in a specific industry and require compliance. Many controls are focusing specifically on protecting the IT perimeter of the organisation from an outside attack, however, many are as well applicable to the insider threat. The table below, however not exhaustive, summarises a number of most common security controls making a differentiation between technical vs human-based and preventive vs. detective. When we elaborate on each of them in details, we will see that some of these controls are not strictly preventive or detective and are applicable to both categories.

[23] https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2015/volume-5/cybersecurity-detective-controls_joa_eng_0915 accessed in January 2023

	Technical / Hard controls	Human- based / Soft controls
Preventive	Identity and access management System hardening	Contracts, NDAs and other agreements Pre-employment vetting Employment screening Security awareness and skill training
Detective	Logging and monitoring*	Confidential reporting procedures *

*Both security controls can be seen as preventive and detective; reasons why will be elaborated later in this paper.

In this research we are looking specifically at the malicious insiders and considering their nature, although perfectly valid to counteract a beaning insider, some of these controls might not be applicable to either prevent or detect someone who has a malicious intent.

For better understanding of what these controls entail, their benefits and potential limitations and flaws we will look at each and every one of them, some in more elaborate details.

2.1.1 Technical Security Controls

When looking at the evolution of cyber threats it is not surprising that the majority of the security controls are of technical nature: it seems to make sense to use technology to battel an IT related problem. Similarly, historically, most of the controls were initially designed to prevent and detect attacks from the outside and only a few – to deter or to detect an insider.

a) Identity and Access management

IAM is a framework of processes and technologies that is put together to manage identification of users and to ensure that right users have the right access to the systems and information. It determines who can access what (systems, applications, data), when (time-bound) and how (type of authentication if any). Over the last years, IAM has undergone needed evolution. Centralisation of the IAM systems introduced efficiency in managing it. With this came a single-sign-on, which at the same time introduced an additional concern: compromised credentials would give an intruder access to all the application the authentic owner had access to. Multi-factor authentication (MFA) addresses this concern to a large extent. It is typically a combination of something you know – password, something you have – a token and a something you are – biometrics, like a fingerprint. This way, if a user password was stolen, to access a

system an intruder will need to have in a possession the corresponding token or a smart phone and have the same biometrics as the original user, which is highly unlikely, if not impossible. Some access does not pose any potential risk if being abused. Similarly, some operations are too risky to be performed by one user. Segregation of duties ensures that a single user is not able to perform a high-risk operation or access sensitive data on his own (e.g. issuing of a high-value payment requires approval). Segregation of duties is usually complemented by setting up permissions using a principle of least privileged, where a user has access only to resources that are absolutely required to perform his or her job. Well designed and managed IAM includes regular reviews of users and their privileges, based on the job function and the required access, mainly using the principle of least privileged and to ensure that no accumulation of privileges occurs for users that have been at a company for a long time.

Although widely used and being seen as effective measure against cyber intrusions, IAM has some flaws when it comes to the malicious insiders. The principle of least privileged, double authorisation and segregation of duties might provide a strong defence against a fraud, but they are quite costly solutions in terms of money and time-efficiency to be introduced along the complete chain of operations. At the same time not all malicious insiders attempt to break in the systems they typically do not use. On the contrary! The whole concept of IAM is based on the trust to perform specific functions within given boundaries however, most of the malicious insiders use their own legitimate privileges to access data.[24] Edward Snowden has leaked the data he had a full legitimate access to. Had NSA introduced segregation of duties the breach might have not occurred; however, it would likely have introduced some inefficiency in day-to-day operations, due to recuring additional approvals.

b) System hardening

This is a combination of tools, processes and best practices directed to reducing possible attack surface, vulnerabilities and attack vectors; officially described as "a process intended to eliminate means of attack by patching vulnerabilities and turning off non-essential services."[25] System hardening is referred to not just protecting of physical user computers, but also networks, databases, Operating Systems, software and applications. Although typically implemented to protect the systems from attacks from outside, some of the techniques, mainly hardware and application hardening, can be implemented as preventive measures against insider attacks.

Hardware hardening is referred to the process where hardware devices that are not required to perform a job are removed from the system or blocked. By hardening we can see blocking of USB ports and computer camera, and the likes. Blocked USB port will make it difficult for a malicious insider to, for example, copy confidential documents on a portable disk for the purpose of leaking the data.

[24] Almehmadi, A., & El-Khatib, K. (2017). On the Possibility of Insider Threat Prevention Using Intent-Based Access Control (IBAC). IEEE Systems Journal, 11(2), 373–384. https://doi.org/10.1109/JSYST.2015.2424677

[25] https://csrc.nist.gov/glossary/term/Hardening visited in January 2023

Application hardening is referred to removing application that are not needed for a particular function, which will limit possibilities to, for example, integrate or use a malicious application to spread a virus or capture data.
Taking the same example of Edward Snowden, hardened system in combination with well implemented AIM would have likely hindered him from leaking the data. It is however not sure if he would have not found an alternative ways of transferring it, if the USB port was blocked.

Further, we will not look into other techniques that fall under the category of system hardening, considering they are mainly directed to prevent intrusions or attacks from the outside.

c) Monitoring and logging

This control is used to identify patterns of normal behaviour, alert on deviations and log for further reference. When discussing logging and monitoring we should make a distinction between human and data monitoring. Also, when looking at various implementation of this control we mainly consider practices within Europe, considering significant differences in other regions of the world, mainly due to regulations or an absence thereof.

Some cyber security organisations suggesting employee monitoring as an effective measure to spot and understand behavioural signs of a potential adversary in order to prevent or timely detect an incident[26]. Some go further and suggest some biometric (e.g. eye movement) physiological biometric measure (e.g. brain activity) as effective measure to have a real-time detection of actions with a malicious intent[27]. Therefore, this security control can be seen as both preventive and detective.

Employee monitoring is the use of different tools, processes and procedures of workplace surveillance in order to obtain information about employee's activities and whereabouts. Most of the solutions provide key loggings, application and website usage, Internet access, file access, incoming and outgoing chats and e-mails, screen capture, software installations, and the likes. These tools are also typically configured to alert employers (e.g. company IT or security department or a SOC) when a suspicious behaviour has been noticed.

Workspace employee monitoring is not a new concept, it has been employed for many years, initially to monitor employees' productivity and performance and to protect corporate asset. Various methods are used to monitor employees.

Employee monitoring using surveillance cameras is one of the oldest methods of monitoring on the workplace. Through various surveillance tools, organisations can monitor their employees for irregular behaviour, which includes time of entering the workplace and/or logging in to systems, accessing different work zones and etc.

---

[26] Delosreyes, G. C. (2017). Mitigating insider threat risk (Order No. 10686094). Available from ProQuest Dissertations & Theses Global. (1991511291). Retrieved from https://login.ezproxy.leidenuniv.nl/login??url=https://www.proquest.com/dissertations-theses/mitigating-insider-threat-risk/docview/1991511291/se-2

[27] Alsowail, R. A., & Al-Shehari, T. (2022). Techniques and countermeasures for preventing insider threats. PeerJ. Computer Science, 8, e938–e938. https://doi.org/10.7717/peerj-cs.938

Companies are making use of the technologies allowing screen capture and video recording of the key loggings. This allows employer to ascertain that the time employees are spending on the work computer is not used for leisure activities. From the security point of view, through key logging in combination with the Internet monitoring, employers are monitoring Internet usage of the employees to ensure questionable sites are not visited; also, the usage of the social media is monitored[28].

Devices used by employees, especially those that belong to the employer - mostly PCs and mobile phones - are being monitored for the activates, normally during the working hours. Deviation of normal patters, like logins outsider of the office hours are being flagged as potential suspicious activity that requires further investigation.

E-mail is by far the most popular channel for cyber-attacks. It is an entry vector for viruses and trojans, for ransomware and impersonation attacks and the likes. At the same time, most of the security breaches were caused by sharing sensitive company's' information with the outside world through emails, whether maliciously or unintentionally[29]. To battel this, employers are using various e-mail monitoring tools to safeguard company's information and potentially identify negligent uses and bad actors.

Network monitoring is an important component in preventing and detecting malicious activities. Various types of network monitoring are deployed to prevent attacks mainly from outside but also from within the organisation. Here we can consider different network anomaly detection systems. These systems typically do not examine the content of the traffic but rather flag unusual activities that can be investigated further at a later stage.

During the last years, different DLP solutions are gaining momentum in organisations. Data Loss Prevention is a framework of tools and processes directed to prevent unauthorised access to a company's data. Advanced DLP solutions use algorithms that block sensitive data when it is being transferred outside of the company either through an email, network or even printed. It can also remove sensitive information or add a digital watermark when an unauthorised action is detected. In addition to blocking the data, DLP tools help to monitor what is being transmitted and even identify stolen data through digital fingerprinting, which is more of a detective measure. Although very helpful in preventing unauthorised actions, current DLP solutions cannot stop a user from taking pictures with a digital camera.

Sometimes, especially at data centres or other critical infrastructure environment, the work area has surveillance cameras that monitors and records employees' behaviour. This allows companies to spot undesired behaviour which can range from bullying and harassment to stealing or copying confidential information and sabotaging systems.

---

[28] Trivedi , S. ., & Patel, N. (2021). Virtual Employee Monitoring: A Review on Tools, Opportunities, Challenges, and Decision Factors. *Empirical Quests for Management Essences*, *1*(1), 86–99.

[29] https://www.verizon.com/business/resources/executivebriefs/insider-threat-report-executive-summary.pdf accessed in January 2023

Companies that have more mature cyber security in place often make use of different Security Information and Event Management systems (SIEM) that correlate different events occurred as a result of monitoring to flag suspicious activities.
Monitoring at work obviously brings many advantages, considering its prime concept of overall surveillance. At the same time, it brings some concerns that must not be underestimated.

First and foremost is the concern of legality. Employee privacy should be taken into account and under various privacy laws the balance between what can be monitored and what needs to be monitored is likely weight heavier in favour of an employee protection[30]. EU General Data Protection Regulation (GDPR) article 41 allows monitoring; however, it clearly stipulates the need for transparency, ensuring that the monitoring is in line with the GDPR requirements and employees are advised thereof[31]. Legal requirements might differ from country to country, and considering possible negative consequences for organisations, it is paramount that monitoring is implemented strictly in compliance with corresponding regulations.

Other than a legal concern, personal privacy and safeguarding thereof is considered to be one of the basic humans right. Different studies provide empirical evidence that conclude that the perception of personal privacy to be breached or compromised cause employees to experience stress and job anxiety, which in its turn create frustration and low the productivity and creativity in the workspace.[32]

Another big concern is a potential damage to employee social engagement. With overall monitoring, employees will likely not feel motivated to report any suspicious behaviour, as they will feel it is not needed, considering "The Big Brother is watching your" anyway.
However, it is questionable if monitoring helps to spot persistent and sophisticated malicious insiders. It is interesting to note, that there are additional "social costs" due to unconscious bias. As many monitoring results require human interpretation, sociable, friendly, and likable employees will likely be given a benefit of a doubt when demonstrating suspicious behaviour.[33]

We see that although monitoring potentially helps to increase productivity, decrease theft, and improves basic security, it comes with the costs of legal constrains, possible employee demotivation and potentially decrease of a social control. It is also questionable if monitoring helps to spot sophisticated malicious insiders, like a nation-state hired actor.

According to Lockheed Martin et al, typical attack begins with the Reconnaissance, phase, a phase where an intruder becomes familiar with the environment.[34] Consequently, a malicious insider takes time to get to know the organisation, its' culture and rituals, processes, people and

[30] Eklund, M. C. (2019). Monitoring employees' e-mail correspondence and Internet use – A Finnish perspective – PART II. European Labour Law Journal, 10(2), 134–153. https://doi.org/10.1177/2031952519861478
[31] https://gdpr-info.eu/art-41-gdpr/ accessed in January 2023
[32] Becker, W. J., Belkin, L. Y., Conroy, S. A., & Tuskey, S. (2021). Killing Me Softly: Organizational E-mail Monitoring Expectations' Impact on Employee and Significant Other Well-Being. Journal of Management, 47(4), 1024–1052. https://doi.org/10.1177/0149206319890655
[33] Bradbury, J. C. (2019). Monitoring and Employee Shirking: Evidence From MLB Umpires. Journal of Sports Economics, 20(6), 850–872. https://doi.org/10.1177/1527002518808350
[34] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html accessed in January 2023

all what is needed to commit a successful attack. Combining with the legal requirements to be transparent regarding employee monitoring, it is very unlikely that a sophisticated malicious insider will resort to the obvious modus operandi to either compromise or steal data. However, monitoring mechanisms in place will likely prevent or help to timely detect malicious insiders that acted on impulse or opportunity.

2.1.2 HUMAN-BASED SECURITY CONTROLS

Various cyber security bodies, like NIST, SANS, ISO and etc, have been publishing and updating their recommended security controls that have been made mandatory for some of the, mainly critical, organisations. And with some minor exceptions, most of the controls are focusing on the technical implementations to prevent an intrusion from outside. This might sound ironic, considering majority of the security incidents are committed either by or with a, conscious or unconscious help of insiders.

In the last version of security controls, published in May 2021, SANS proposes only one security control that is focusing on humans – Security Awareness and Skills training[35].

ISO277001 comprises three objectives and six security controls with the main goal to ensure that organisations employ and retain individuals that do not pose a threat to the organisation based on their background, personality, personal and the employment history and the likes. It also elaborates on management responsibilities and on the actions that must be taken in case of a termination or a change of a job responsibilities. Similarly to SANS, ISO27001 includes training and awareness as a key component to ensure employees contribute to the organisations' security culture. Additionally, there are controls related to reporting on the suspicious behaviour and disciplinary actions in case of security breaches.
Similar controls are described by NIST in more granularity and with the guidelines on reaching the objectives.[36]

d) NDA and contractual agreements

Many companies, especially those operating critical environments or dealing with sensitive information consider employing specific legally binding clause or a Non-Disclosure Agreement (NDA) in the employment contracts outlining potential legal actions that can be evoked in case of a breach. Typically, it is referred to the information that can either damage an organisation or even threaten the whole reason to exist, should it be leaked. By doing so, an employer ensures that every employee is aware of what information should be kept confidential and what are the consequences of not doing so.

Some authors believe that including an NDA or a confidentiality clause in the employment contract and ensuring that employees understand possible legal actions in case of a breach of this

[35] https://www.sans.org/blog/cis-controls-v8/ accessed in January 2023
[36] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final accessed January 2023

contract can be seen as a deterrence and hence prevent malicious insider threat.[37] NDA is also listed as a preventive measure by various cyber security providers in their documentation or websites.
Unfortunately, not much literature has been found elaborating benefits or limitations of using NDA or a similar legal clause in the employment contract as a measure preventing a malicious insider threat.

e) Personnel vetting and pre-employment profiling

Many cyber security bodies strongly recommend or even mandate using pre-employment personnel security vetting as one of the security controls to ensure the right people are hired. It is also believed that personnel vetting process provides additional assurance that employees are trustworthy, and hence it reduces the risk of insider threats.

What does it mean personnel security vetting? According to the Collins dictionary, personnel security vetting is "the process of investigating somebody to establish their trustworthiness"[38] The aim of this process is to establish if a job candidate does not pose a security risk to the organisation as he or she might be susceptible to a blackmail or a bribery. Additionally, it validates that the candidates' personal traits do not lead to an undesired behaviour that potentially poses a security risk.

Employee vetting can differ from job profiles, organisations and countries. It typically includes a background, credit and a criminal history checks. It can sometime go further and include, from the privacy point of view, intrusive checks like past risky, deceitful or secretive behaviour, breach of integrity, addictions, undesired influence and similar. The level of intrusiveness of such check differs based on the risk associated with the job function.

Obviously, there are many advantages of pre-employment vetting. By conducting background checks in combination with the reference check, companies, first of all, establish whether the candidates are who they say they are. It also indicates if a person has the right accreditation, skills, medical or other conditions, qualifications, and work experience to perform the job. In addition to reducing security risk, hiring the right person for the job lowers employee turnover, hence reduces the costs of hiring and training of new employees. Successful criminal history check should ultimately reduce instances of violent behaviour and thefts on the workflow. Checks of the social media account of a potential hire can give a good indication of the person's morals and values.[39]

[37] Brafford, H. R. (2021). Preventing malicious insider threat using non-disclosure agreements (Order No. 28490866). Available from ProQuest Dissertations & Theses Global. (2566019952)

[38] https://www.collinsdictionary.com/dictionary/english/security-vetting

[39] Brody, R. G. (2010). Beyond the basic background check: hiring the "right" employees. Management Research Review, 33(3), 210–223. https://doi.org/10.1108/01409171011030372

Despite these obvious advantages, pre-employment vetting is not a bulletproof solution. Let's look at some of the components of the vetting in more details.

Although mistakes can occur when conducing background checks, most of the time the data that comes out of it is reliable. Issues form the past or questionable situations can be discussed and clarified with the candidate during interviews. Alternatively, an organisation that is conducting such check can be contacted for clarification. And despite potential biases that could jeopardise the hiring process, all works well. Until it doesn't. In October 2022 most of the newspapers worldwide published a story of an alleged Brazilian researcher that has worked as a university lecturer in Norway who has been arrested on a suspicion of being a Russian spy and causing a significant risk to the national security[40]. Has the university conducted a background check? Was it a thorough one? Perhaps, but possibly not. But what about another famous story that made headlines in most of the newspapers just a few months before the Norway case where the secretary of Naples Lions Club International, a jeweller, a socialite "Maria Adela" was discovered to be a GRU officer? Although not entirely employment related, but considering the Naples brunch of the social club was established by a NATO officer, one would expect a thorough background check to be done on the employees and associates. Was it conducted? NATO office seemed to have refrained from commenting.[41]

These are just two examples where the background information has been carefully crafted to successfully pass all kinds of scrutiny or the background check was not conducted properly or was obscured by biases. Biases play an important role when it comes to vetting, background checks and profiling and we will look into it in more details later in this pater. In any case, considering these two are not isolated examples, it is safe to conclude that when referring to the sophisticated malicious insiders' background checks do not always prove to be reliable.

Over the last few decades pre-employment personally tests as a part of the vetting process became popular. The initial goal of these tests is to establish whether the candidate is the right fit for the job and the company, based on the character, personal traits, preferred behaviour, and the likes. More recently various studies have been conducted to outline behavioural indicators of malicious insiders. Dr. Eric D Shaw and Dr. Harley V. Stock in their paper "Behavioural Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall" propose a framework to identify a malicious insider threat through the Insider Risk Critical Pathway model that consists of five components. Shaw and Stock see personal predisposition as the first component of this model that consists of history of serious mental health problems, social skills problems or biases in interpersonal decision-making, previous violations of law, or organizational policies or practices, a social or professional network risk

[40] https://www.bbc.com/news/world-europe-63395323 accessed in January 2023
[41] https://www.bellingcat.com/news/2022/08/25/socialite-widow-jeweller-spy-how-a-gru-agent-charmed-her-way-into-nato-circles-in-italy/ accessed in January 2023

such as a friendship, family member, or social or work contact who is affiliated with an adversary or competitor or a source of risk for the employee (an addicted spouse)[42].

Although both personality tests and the attention to the behavioural indicators have been proven to be effective generally, based on the large number of successful hiring, there is a number of challenges and concerns that must be looked into.

One of the concerns is "faking good" on the personality tests. The results of the personality tests only make sense if they are correct, meaning, when a future employee has replied to all the answers honestly, with integrity and with the right level of self-reflection. However, as the stakes of "correctness" are quite high (e.g. getting a job) some candidates tend to present themselves in a more favourable light, hence faking good. According to Ziegler et al: "Faking represents a response set aimed at providing a portrayal of the self that helps a person to achieve personal goals. Faking occurs when this response set is activated by situational demands and person characteristics to produce systematic differences in test scores that are not due to the attribute of interest" [43]. Other than faking good on the personality tests, the reliability of behavioural tests has also been contested by various researchers mainly due to the fact that human behaviour is normally context-based, while the tests assume that the behaviour of an individual is static and will remain the same in all circumstances and through the time. [44]

In addition to the questionable reliability of such research results, it is important to note that the level of details that can be disclosed to a potential employer is a subject to regulations and privacy laws and differs from country to country. For the consistency in this research, we will only consider GDPR rules.

In the Critical pathway Dr Shaw et al points to the mental health problem as one of the important indicators to the personal predisposition to become a malicious insider. However, an employer might face some legal implications to collect data, like medical history. According to GDPR article 9, paragraph 2, medical record, being a sensitive data, cannot be disclosed, unless explicitly consented by the data subject. This creates an implication in basing a potential employee profile on one of the major criteria the personal predispositions – medical condition and history.

---

[42] Eric D. Shaw, Ph.D., Harley V. Stock, Ph.D., ABPP, Diplomate, American Board of Forensic Psychology Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall

[43] Ziegler, M., MacCann, C., and Roberts, R. D. (2012). Faking: Knowns, unknowns, and points of contention. In Ziegler, M., MacCann, C., and Roberts, R.D. (Eds.). New Perspectives on Faking in Personality Assessment. New York: Oxford University Press, pp. 3-16; p 8

[44] Goffin, R. D., Jang, I., & Skinner, E. (2011). Forced-choice and conventional personality assessment: Each may have unique value in pre-employment testing. Personality and Individual Differences, 51(7), 840–844. https://doi.org/10.1016/j.paid.2011.07.012

Based on the above consideration we can conclude that although in general cases vetting proves to be effective, it should not be seen as a silver bullet to preventive malicious insider threat, especially when it comes to more sophisticated actors.

f) In-employment screening

Pre-employment checks can give a fair picture of an employee's past history, however, things might change as life goes on. People change, grow, develop. Individuals can get into difficult financial or medical situations, acquire undesirable habits or additions, experience personal issues and many other things that potentially can make them susceptible to bribes or a blackmail. Not only negative situations in people lives can ignite their potential malicious behaviour. Promotions and change in a job position or in responsibilities can also become a trigger. Therefore, to deal with these changes in addition to the pre-employment vetting, many security organisations encourage or even mandate in-employment screening. The extent and the frequency of these checks depend on the job function and responsibilities, company's' profile, industry, regulators and the likes. Some (regulated) industries, like financial or medical, mandate regular rescreening of employees and even a frequency and types of checks.

The rescreening exercises takes place periodically (e.g. every two years) or in case of a significant change of an employee's responsibility and are there to ascertain the level of employees trustworthiness and suitability for the job. Additionally, with the increasing trend in the organisations of (partially) working from home (or a remote working during Covid pandemic) and hence a limited view on the employees' displayed behaviour, rescreening can be very beneficial.

Typically, the rescreening is very similar to the pre-employment screening, or a lighter version thereof and usually conducted by the same vendor. Consequently, the benefits and the challenges of rescreening are very similar to those of screening with one additional caveat – unconscious bias.

Negative or alerting screening results typically require human interpretation and as a follow-up are being discussed with an employee and/or an employee manager in order to clarify findings. And here is where unconscious bias can jeopardise the process. According to various research there are around 150 unconscious biases that are rooted into human beings to, initially, protect us. But not all of them are being helpful when it comes to interpreting and understanding a behaviour of others.[45]

In addition to be qualified for the job, successful hiring process ensures that employees are a good match with the organisation. Organisations have their own culture, rituals, habits and over time, behaviour of all employees is, to some extent, shaped accordingly to blend into it, making them express similar views and have similar values. As results of rescreening are usually discussed by either a security or an HR professional with their colleague, who most likely in some ways is quite similar to them, affinity bias can colour their judgement. Affinity bias is the tendency to gravitate towards people that are similar to ourselves and when this bias is

[45] McCormick H. The real effects of unconscious bias in the workplace. UNC Executive Development, Kenan-Flagler Business School. DIRECCIÓN. 2015.

"activated" the "investigators" are likely to accept an explanation even it if is not fully watertight, based on the perception they have of an investigated employee[46]. Other biases, like halo effect – the tendency to see a person in a better light due to liking the person, or a confirmational bias – the tendency to look for information that confirms pre-existing believes can also jeopardise investigation, making an investigator ignore red flags only because he or she likes the person in question.

g) Security awareness and skill training

The goal of this controls is to ensure that all personnel is aware of and fulfil their security responsibilities. Through the awareness and training, employees are meant to be encouraged to consciously adopt secure behaviour and to follow security practices to contribute to the overall security of the organisation. Different organisations adopt different approaches to the security training, some through group training and gamification, some through interactive online exercises with a compulsory examination.

Hunker et al point that security training programmes should aim to achieve three levels of the security awareness: "1) perception (the user is able to detect threats in the environment), (2) understanding (the user is able to combine information from different sensors, interpret them and use the resulting knowledge to reduce risk in the environment), and (3) prediction (the user is able to predict future attacks and proactively change own behaviour to reduce or remove risk)"[47]

Through the training modules and awareness sessions employees are to learn to understand what poses a security risk whether it is generated from outside or from within the organisation, and how to adopt secure behaviour. Here we can see various programmes – interactive or computer-based trainings, awareness campaigns, simulation exercises directed on creating a habit of a secure behaviour. It promotes regular change of passwords, teaches to recognise phishing mails, social engineering and deep fake, alerts on tailgating and shoulder serving. For it to be effective, security training should not only be regularly repeated, but organisations should ensure that employees feel responsible for overall security, motivating people to become part of the solution.

Although the concept of secure behaviour seems to be a universal one, for the security programme to be most successful, organisations are recommended to tailor their approach to their organisations.[48] It should take into account size, business and demographics, but also specific contains of this organisation and it must fit, so it can become a part of the organisational culture. At the same time, considering that a malicious insider is not interested in adopting a

---

[46] Lattal, Ashley. "The Hidden World of Unconscious Bias and Its Impact on the Neutral Workplace Investigator." Journal of Law and Policy, vol. 24, no. 2, 2016, pp. 411-466. HeinOnline, https://heinonline.org/HOL/P?h=hein.journals/jlawp24&i=427.

[47] Hunker, J., & Probst, C. W. (2011). Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications, 2(1), 4–27.

[48] Vasileiou, I., & Furnell, S. (Eds.). (2019). Cybersecurity Education for Awareness and Compliance. Advances in Information Security, Privacy, and Ethics. https://doi.org/10.4018/978-1-5225-7847-5

secure behaviour, it is questionable how effective these types of security training is against malicious insiders.

Additional vector of the security awareness and training, which seems more applicable to battling malicious insiders, is creating understanding of indications of compromise, whether these are jammed printers or an erratic behaviour of a colleague and what actions to take in such cases. In addition to monitoring, which was covered earlier in this paper, employees are encouraged to be vigilant and to recognise signs that point into potential insider activities, like excessive increase of data transfer can be an indicator of a data leak[49].

During these trainings employees receive insights into what behavioural signs can point to a potential malicious intent, like open disgruntlement. Some organisations introduce a safe whistleblowing or a confidential reporting programme that enables employees to safely report suspicious behaviour of a colleague for the corresponding internal authorities to investigate and take actions. As we discussed in the Chapter 1.2, many scientists and researchers have made an attempt to sketch a portrait of a malicious insider, to outline typical character traits and behavioural signs, however these attempts did not seem to be fully conclusive.

Another potential limitation of this security control is that some security professionals have a "tick-box" approach to the Security Awareness and training, which can create a false sense of security[50]. Often companies are camping with budget constrains forced to prioritise between different components of cyber security. As a result, when having to choose between modernising a firewall and investing in effective cyber security training, considering company's cyber security officials are mainly people with technical background, the choice is easily made in favour of the firewall. Similarly, many companies have one training budget, which is being taking care of by an HR representative and the security awareness and training fails under it. Similarly to the previous example, when having to choose between a job-related training and the security one, the former is chosen. For the reason of limited recourses or understanding, often security trainings lack creativity and do not call for engagement. Repeating the same exercise of spotting a phishing mail over and over again or giving a mandatory security refresher to all the employees will not likely bring a desired effect.

h) Confidential Reporting

Organisations with evolved security culture typically have a confidential reporting procedure - a process for the positive whistleblowing, where employees can report a suspicious and a disruptive behaviour without feeling threatened. This measure is based on the assumption that an employee, who is in the process of committing a malicious act, demonstrates some irregularities in his or her behaviour. Who better than a co-worker can spot the difference in a behaviour and gets the cues that something is going on? Working outside of regular office hours, erratic and violent behaviour, unwillingness to follow company's procedures and rules, sudden change of

[49] Delosreyes, G. C. (2017). Mitigating Insider Threat Risk. ProQuest Dissertations Publishing.

[50] Caldwell, T. (2016). Making security awareness training work. Computer Fraud & Security, 2016(6), 8–14. https://doi.org/10.1016/S1361-3723(15)30046-4

finical situation, physical signs of destress; although not exhaustive, these are the potential indicators of an insider who is in the process of committing a crime that should be observable and hence noticeable to the employee and peers.[51] Although this seems to be a fair conclusion, employee reporting presents a number of challenges.
As the majority of the cyber security incidents committed by malicious insiders are financially driven, in theory, employees that are suddenly experiencing financial difficulties should be put under the radar. Same applies to the disgruntled employees, as this is the second biggest group that potentially poses a risk to become malicious insiders. Co-workers are motivated to be attuned to strong voicing and expressions dissatisfaction with the employer.[52] However, people in general seem to consider financial troubles or gains as well as some level of frustration with an employer to be normal facts of life, a "human factor", making it difficult to estimate the gravity of it, according to McKinney.[53]

Additionally, this measure assumes that co-workers are equipped with sufficient understanding and knowledge of what behaviour should be considered suspicious and certainty to report it. Working-from-home practice that has gained popularity during and post-Covid pandemic significantly complicates identification of irregularities. Diminished social contact between employees limit options of noticing a financial gain or spotting financial troubles, as well as witnessing a non-compliance with processes and expression of disgruntlement. Similarly, working-from-home practice made working more flexible hours to become a norm in many organisations.

To complicate matters, according to McKinney, most employees are typically hesitant to report an irregular behaviour, especially if it potentially has some negative consequents for the employee in question. This is mainly caused by human biases, that we have touched upon earlier in this chapter.

Last but not least, a number of malicious intrusions has been committed by the insiders that have been intentionally planted into the organisation for the purpose of espionage or a sabotage. Therefore, we can assume that these are specially prepared individuals, trained on not leaving any clues on either who they are or their intent and hence, will not be identified as a potential threat by their peers.

Confidential reporting can be seen as both preventive and detective security control, considering a suspicious behaviour can be noticed and reported not only in a phase preceding a cyber-attack, but also during or even after the event has taken place.

---

[51] https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf accessed in January 2023

[52] Preventing and Profiling Malicious Insider Attacks
Journal article·2012·Agata McCormac, Kathryn Parsons, Marcus Butavicius

[53] McKinney, G. (2019). Understanding conditions which could improve department of defense contractor reporting of cyber insider threat pre-attack warning indicators in coworkers (Order No. 13899292). Available from ProQuest Dissertations & Theses Global. (2625996237).

III. METHODOLOGY

To answer the research question in this thesis a qualitative analysis was used, as our goal was not to quantify different methods of dealing with the insider threat, but rather to understand how the academia and practitioners see the insider threat and what they believe to be the effective ways of dealing with it. In this analysis we used language-based data that has been collected through the literature review and interviews.

3.1 LITERATURE REVIEW

To be able to understand how academia views the issue of a malicious insider and what means should be used to prevent a malicious insider crime, content analysis was done by studying academic research papers, document publications of official security bodies and journal articles. For the definitions we first looked into documents of the official cyber security bodies, followed by the publications on various cyber security sites and blogs. Academic articles were found through the search on Google Scholar and Leiden University Library using keywords based on the topic: malicious insider, malicious insider threat and etc.

The first question that had to be answered through the content analysis was who the malicious insiders are, what are their personality traits, characteristics, and typical behaviour and what are their motivations.

In the second part of the literature review we analysed different measures – security controls - directed mainly to prevent but also to timely detect malicious insider threat. We have looked into different security controls, limiting ourselves only to those that are specifically directed to malicious insiders, grouping them into detective and preventive and into technology and human based ones. We first investigated definitions and recommendations established by the official cyber security bodies, followed by the research papers. Overview of each security control is structured in a similar way: we describe what each control constitutes, what effects it brings in addressing malicious insider threat and what concerns and possible flaws this control presents.

3.2 INTERVIEWS

In the second phase of the research, cyber security practitioners were interviewed. For this research we decided on conducing a semi-structured interview, as we believe this approach to be the most suitable one to create a forum that allows flexibility and the ability to ask open-ended questions and to explore thoughts with follow-up questions. Interviews, as opposed to questionnaires, cater for establishing a good rapport with an interviewee that consequently creates an open dialog, which allows to collect more reach data.

Following selection criteria has been used in selecting the interviewees:

- Interviewee has been in a cyber security job for at least 5 years;
- In his or her current or a previous role, the interviewee has been involved in either security policy design, maintenance or execution;

Use of these criteria ensures that interviewees have a practical knowledge and relevant experience in cyber security and have spent sufficient time on the job to build own ideas and impressions. Practitioners from different cyber security domains were selected to have a more complete picture.

Two sampling methodologies were used to find the interview candidates: convenience sampling and a snowball sampling. Initially we have approached cyber security experts within and through our business and social circles. Subsequently, these experts have suggested their acquaintances or peers for other interviews.

Although some of the interview candidates were suggested by already interviewed experts, not all of them agreed to participate in this research, mainly due to the concern of their information being disclosed. The field of cyber security cares about confidentially, integrity and availability of data, knowledge, systems, and etc. Therefore, people that are involved in this field possess information, disclosure of which can potentially breach company's secrets, which makes them, in general, very reluctant to elaborate on any topic of cyber security. Good level of trust needs to be established between an interviewer and interviewees in order to have a meaningful and fruitful conversation. This presented a challenge of finding cyber security experts that were willing to fully engage in the discussion, without having already established trust relationship.

Some experts agreed to answer only a few questions without being mentioned, recorded, or quoted, which was useful to explore the subject but not suitable for this research paper. Two candidates have cancelled the interview last minute due to an illness. Consequently, a total of eight experts were interviewed. We realise that statistically, this sample of experts might not be seen as representative, however, we believe that, considering a good spread throughout different industries and cyber security domains, data that has been collected is sufficiently illustrative.

All interviewees were asked to answer questions based on their thoughts, believes and perceptions and as private persons. This is an important consideration to understand that responses given do not represent interviewee's companies' cyber security position towards malicious insider threat. Interviewees have been consented to have their answered recorded and quoted in the thesis document. All the answers have been anonymised, hence the name of an interviewee and the name of the company he or she works for are not disclosed; we mention interviewees' job functions and the industry in the Appendix A. Further in this document interviewees are referred to as In1 (Interviewee 1), In2 (Interviewee 2) and etc.

Interviews were conducted in English through Microsoft Teams using a video recording and a transcript reporting. The transcript was adjusted based on the recording, considering not all the words were correctly captured. Each interview lasted about an hour and was done in a form of a dialog where interviewees were encouraged to elaborate on the topic without the necessary need to follow the order of the designed questions. This was done in order to explore the topic in more details without leading the discussion in one or another direction.

Questions were designed to collect information on what practitioners think about insider threat and what measures, they believe, should be taken to prevent an insider attack. Before exploring this matter in detail, we asked each interviewee to elaborate on whether they find a malicious

insider threat to be a real danger and if so – why, considering in case an interviewee believes this threat to be negligible all the following questions will become redundant.

Various researchers have made attempts to describe a malicious insider, find common personality traits and characteristics of a person that can potentially be a risk to an organisation. During interviews we asked the exerts to describe a malicious insider and the way he or she can be identified.

Further interviewees were asked if they believe the insider threat can be prevented and what are the best measures to do so. This part was followed by a detailed exploration on the level of effectiveness, constrains and barriers of security controls that have been described in the literature review part of this document.

Once interviews were conducted, we processed the generated transcripts using a thematic analysis. We looked for the patterns in the replies and group them per question.

In the final stage, we compared data that was analysed through the literature review with the interview analysis to see similarities and differences per question in order to draw the conclusion.

IV. INTERVIEWS

This chapter will present the outcome of the interviews with Cyber Security experts that have been conducted to answer the second part of the question: what measures Cyber security professionals see as the effective ones to counter insider threat and how do they view the "established" security controls. One important consideration is that all experts were presenting their personal point of view which is not necessarily aligned with the security policy of companies they are working for.

4.1 INSIDER THREAT AND MALICIOUS INSIDERS

Not surprisingly, all interviewees consider malicious insider threat to be a real danger to their organisations. Almost all interviewees have immediately replied "yes" and "definitely" when asked to the question. Moreover, security professionals operating critical infrastructures or the ones from the financial industry consider insider threat to be the biggest danger to their organisations and they extend the concept of the malicious insider even further. According to the In4 it is especially dangerous because "… if we have someone which is not part of the organisation that would want to commit an attack, they could simply try to be onboarded and then perform the attack instead of trying to attack us from the outside". The reason why we are facing this situation now has been well articulated by the In5 as "… organisation is very focused on keeping people out of the network. (…) Historically, they haven't really paid a lot of attention to what accesses people have internally within the organisation and how those would be potentially misused in various personal or professional situations" and because, according to In1 "… historically all organization working to detect".

In addition to the general believe that the insider threat is a real danger, In2 has shared a concern that it might not be correctly estimated, considering "…stilling knowledge (…) it is overlooked how much that happens; people are just stilling knowledge instead of financial…". In2 stressed this to be a serious problem, mainly due to the fact that the theft of knowledge is not visible, not tracible and the theft is likely cannot be proven even if detected; "when knowledge is stolen in most cases it is very hard to find out" if it was really stolen and by whom.

When asked to describe a malicious insider, responses of the interviewees were slightly less unified, mainly on the reasons and motivations. Some, like In5 and In7, believe that there must be some psychological reasons or predisposition in some people to commit an insider crime, while majority were convinced that anyone can become a malicious insider. In1 describes groups of insiders based on their motivation: "from disgruntled staff member who's unhappy with their last performance appraisal to someone who's involved in criminal activity, who's doing it for a personal gain or ideological reasons, or even a state sponsored where they're really interested in understanding, not necessarily to bring the system down, but maliciously looking at systems and influencing people within the organization". Similarly to In1, In5 names two reasons that "influence a person to make bad decisions" where one is a more generic one, where a person has an opportunity to do "bad things" and the other of a nation state activity. Additionally, according to In4 "…there's a difference between I want to do it, but it was an impulse thing and I plan something like the mastermind in the in the movie type of thing".

Some of the interviewees zoomed in into various reasons why someone can become a malicious insider, like getting into a difficult situation and hence committing an insider crime out of desperation. According to In4 "someone who's indeed gotten to the situation where either got (…) totally derailed and someone is blackmailing that person or (…) in a serious financial issues, et cetera".

Disgruntlement has been named by almost all interviewees as a reason to commit a malicious insider crime. Employees can become disgruntled for various reasons. According to In4 "When a company is being sold, many employees are being sold together with it, and some will be laid off. Feeling of wrongdoing and especially if this wrongdoing results in financial issues can motivate an individual to commit a crime. (…) it's no longer my company…it was maybe someone (…) very committed but then face with desperation you say (…) this employer won't save my life. I'm just an employee." The perception of employee that an employer does not care about him or her has been brought forward by almost all interviewees as a reason for disgruntlement and hence, potentially for becoming a malicious insider.

In6 raised a point of a culture where family, education and society but also a company culture are playing a big role. An organisation that does not have a supportive culture will likely face a bigger risk of an insider threat than otherwise. "And a city that is perfectly fine without any issue. Then the city with broken glass will become even worse because the people (...) don't care about what is happening. If you have a city that has dirt everywhere, you will also contribute to the littering and so on. If everything is clean and you will be punished for that (…) you will see that you create a different type of society, a different type of set of people". Regardless the fact that motivation and reasons to commit an insider crime seem to be seen differently by the interviewees, majority do believe that, as In4 stated: "everyone under the right or the wrong

circumstances could become a malicious insider", "…at some point (…) everyone has a price" as "everyone could become or could end up in a really bad situation".

The response to the question on whether it is possible to prevent an insider crime has been answered unanimously with either a strong or a subtle "no". The responses were ranging from "100% security does not exist" to "highly unlikely" and will be elaborated later in this document, when security controls and additional comments will be described.

It is important to mention that some interviewees have emphasised that preventing an insider attack orchestrated by a nation state is close to impossible, mainly due to, according to the In1, "capability and intent on many nation states".

4.2 Security Controls

Security advisory bodies and security experts recommend having a set of security controls that when put together are meant to prevent and timely detect a malicious insider crime. However, according to some of the interviewees, in particular In3 and In5, not many organisations have a comprehensive cyber security programme and not enough measures in place to prevent attacks from within.

4.2.1 Identity and Access Management (IAM)

Experts in IAM and security providers believe that, as stated by In3: "IAM is effective, providing people are following the procedures" who also stressed the importance of implementing least privileged (…) and (…) four eyes principles, that would make this security control more effective...".

According to In5 "having various levels of access for different levels of people is importance #1 …there's no argument about that, and if you have a critical organization with important information, you need to have these things in place." In8 suggested that the IAM should be a part of the zero trust concept, as "…It's the only way for us to (…) keep control, to stay in control".

Some of the interviewees were less optimistic about the effectiveness of the IAM in real life. According to the In1, "It is definitely a control that you can that you can" although "… the actual control itself is not necessarily the strongest as it can be bypassed". Similar thoughts were shared by In4: "If you can impersonate someone then it's game over". Additional caveat of practical effectiveness of this control was raised by the In2 as "culture of approval is a given", where often in organisations approvals are given without either appropriate knowledge or based on trust.

However, all stressed the importance of this control in combination with many other ones, providing it is properly applied and have a right balance between the effectiveness and the costs, either job efficiency or financial.

4.2.2 System Hardening

Not many comments were given about system hardening as a preventive measure. Some interviewees referred to that as a part of the deterrence mechanism, a component of zero-trust and according to In3, implementing of system hardening is a "…part of the basic security hygiene" .

4.2.3 Monitoring and Logging

Monitoring and logging has been discussed in detail with all the interviewees and there seems to be a consensus on the importance of the monitoring between all the experts. Most experts have made a distinction between a data or transaction monitoring and a monitoring of individuals.

Data or transaction monitoring and logging is being seen as one of the most important security controls. According to In3 "if you put measures in place you need to monitor (...) you need to close the loop and monitor if your implementations are working". It is important, as per In5 to "… look at what's normal in [the] network versus what is not normal in [the] network. So, looking at telemetry collections, data flows transfers, what is normal for an employee during their work day and what is abnormal. For example, downloading many gigabits of files and sending them to cloud. "

Some interviewees have raised legal and ethical concerns of monitoring. According to In2 surveillance has a big downside as it presents a "huge breach of a privacy of people" taking into account that "most people come to work to do a good job" and "if you are recording all the people, you have 99.99% of people you are bothering with your control". And hence the question is "… is it a wise thing to do?".

Additionally, the importance to have a monitoring policy in place has been raised by many. It is crucial to be specific about what is being logged and monitored, for what purpose, how long the data is kept. It is important to involve legal to ensure that whatever is monitored and logged is not breaching the laws. According to In8 it is also important to disclose this information to the employees as otherwise people will "…totally lose trust".

4.2.4. NDA and a legal clause

Majority of the interviewees see NDA mainly as a mean to prove a malicious intent when an adversary has been committed.

Majority, like In4 has "never witnessed or seen or had experience with an NDA being successful, as according to In1, NDAs are "… only effective with honest and integral people. Those who are determined to damage an organisation, it is having no effect whatsoever ". NDA is considered to be a legal instrument that provides a better ground when looking for legal actions against a perpetrator and, as per In3 it "does not help to prevent somebody who has a bad intent."

4.2.5 Pre-employment vetting and profiling and in-employment screening

When discussing vetting and profiling, we see more or less the same slightly different between the interviewees. Although most of the experts agreed that this control should be put in place to check the basics – is the new employee fit the company's culture and if he or she is trustworthy – some experts were more optimistic about effectiveness of this control than others.

Consensus was on the fact that, as per In3 vetting "…can be essential to some organisations, like military but is not very useful for all". Also, vetting is, per In1, "only as effective as the analysis that's done on the information that is received". It can help to build a risk profile of an employee when, for example, a credit check is conducted In1 "… it gives you a better understanding of the risks of that individual from a financial crime perspective (…) build a picture of where blackmail could exist".

Almost all interviewees said that they will never hire a person who has lied on the job application or received negative references, however, as per In6, "…[although] it is important to understand what (…) manager in the past thought about you", one needs to understand the context as well, as one could have been fired from "an abusive organisation". It is also important to understand that the pre-employment vetting is very limited and should not be seen as a proof that a screened person can be trusted. As per In2, one of the few documents that is being used for screening in most of the EU countries only shows that a person in question "did not commit a recorded crime" …in the current country, indicating only that "we don't know if a person has committed any crime…" as "…absence of evidence does not prove anything".

Even if screening comes back entirely spotless it should not be used as an indicator that an employee will not commit any adversary. According to In6 "…because a person can kill also, if he never killed before. (…) there is always the first time". Interviewees also had a consensus on that, per In1 that "a determined attacker will have an extremely good vetting profile."

Some interviewees see this control in a less tented light. According to In5, "… it's very critical to know who our people are when we hire them and who are people are when they work for us. During the entire process, right, because people's lives, people's situations, they change over overtime, people change, right? So, the person you hire at the beginning may not be the person after five years."

When discussing in-employment screening, some experts raised the concern of trust. According to In2, in-employment screening gives a message: "you don't trust me". Additionally, In8 believes that "…when you go too deep (…) you can cause more harm than [when] you don't screen at all" and as In6 stresses "So you need to be careful because there you can create frustration, or you can create [a] lack of trust."

In1 argues that screening should not be only a "snapshot in time", but "should be a continues process of a dialog", as "there are always people who determined to bypass that system and then (…) it's only effective as the holistic approach to screening". In this explanation, In 1 lead to the need for organisations to exercise a "duty of care", which will be elaborated further in this document.

4.2.6. Security awareness and training

At first, all the interviewees, without any hesitation, ranked security awareness and training to be one of the most effective security controls to prevent malicious insider adversaries. However, when discussing further many have adjusted their statement acknowledging that this control works the best to prevent a benign insider crime to, for example, according to In3 "…learning not to click on phishing emails …".

Nevertheless, this control is being seen as an important control for two reasons. First it introduces employees to the company's culture where security has a high priority and hence, it acts as deterrence. When regular security campaigns, trainings, awareness sessions take place employees become conscious that company is serious about security and hence will be less tempted to break that security

Through the awareness and training employees learn about security measures that are implemented in the company, like monitoring. As In4 stated "… if we talk about opportunistic crime, (…) you can feel that there is monitoring in place, you will definitely try to avoid it because you don't want to end up in jail. That's not your end goal. You're just trying catch what you can because (…) no one may notice it". The deterrence role is being stressed by In4: "…if they know there's some deterrence in place, they'd be less likely to do so".

Secondly, through security awareness and training people learn to understand what behaviour should be seen as insecure or suspicious and how to act upon it, which brings us to the last security control that has been discussed.

4.2.6. Confidential reporting procedure/whistleblowing

The importance, benefits and the downsides of this control has been seen differently by different interviewees. The implementation of this control and the responsibility for carrying it out are also seen very differently by the experts.

First of all, according to In1, "confidential reporting and whistleblowing process are incredibly important in the organisations" mainly "… Because the incident is extremely traumatic, however small, the group that is traumatized by this, with guilt and (…) court cases, if it goes to court, whether or not it ties people up for years and it's typologically damages people for a very long period of time. So if you can provide the whistleblowing to start with, to prevent [incidents and build a] system in place that people know they can go to after the incident takes place it can lessen the impact on an organization long term." In1 elaborated on how whistleblowing should be incorporated in the organizational culture in a positive way, which will be discussed further in this document.

In3 raised his concern that "there is a danger in there that some people will take this too seriously". When people are encouraged to pay attention to spot signs of malicious behaviour, they can make mistakes as "it is difficult to judge, and a regular person is not skilled enough to see the difference [between a normal and malicious behaviour]". In5 believes that although "it

would be helpful to the organisation (…) if employees would provide information (…) if they understood that there was a potential risk ….” it might not help the working relationship.

4.3. Additional thoughts: Supportive culture

At the end of each interview, practitioners was asked to share additional thoughts that were not covered throughout the interview questions, and the following insights were received.

When discussing malicious insiders, whether talking about preventive measure in general or zooming into the details of various controls, the concept of trust and open and supportive organisational culture was the common theme for all the interviewees. For many of the interviewees, preventing a malicious insider threat starts with removing the intent, as put by In2: “…Hard controls are great to prevent confusing by mistake, and soft controls are actually there to prevent a bad intent”.

In1elaborated the importance for organisations to exercise a “duty of care”, build a culture where people are free to talk about their issues in confidence and receiving a right support. “And you (…) should be able to say that to people. You should be able to say, yeah, you know what? I'm struggling for money at the moment. You know, the heating bills have gone up. I struggling to pay my bills. You should be able to say that in an organisation, you should be able to say that to people around you (…) without impacting on your professionally because people go through lights. Life is not. Life is not simple.” It is important to build a mutual trust between an organisation and employees.

In6 supported this argument stating that “we are not robots, we have our frustratons and we need to have a culture that recognises frustrations and addresse that, not only in a publishment bu also understanding that situation, understanding how to help the perons to overcome that or even to find alternative solution within the company or even outside the company if there are no other opportunities.”

Responsibilities of the employer are being further stressed by the In4 “if we genuinely care about staff, it reduces the probability to have inside threats. (…) obvious depending on the culture, but I do believe this point is important” and by In3 “it may sound simple, but having a good atmosphere in the company, treat people correctly” will help to minimise a malicious intent. “If you feel good in your company and you are supported and have a good management” should not make an employee feel the need to harm that organisation.

In8 adds a component of integrity and the need for each organisation to be open and integer: “you start as a company with (…) perspective, we're keeping integrity and (…) we are here to help then it should automatically be cascaded down to the people that work in your company so they [are also] honest and integer.”

Additional comments were made in relation to working from home culture, emphasizing the role of a social aspect in preventing a malicious insider threat. According to In4

“Remote working brings additional threats because few employees are able to have a dedicated office at home where there families can not see or hear what they do. And even without knowing it an employee can leak sensitive or critical informations. (…) Particularly post Covid, remote working risks really increase both opportunities to leak data and or bad actions from people [tat are] not in their usual state of mind (alcool, drugs, ...)”. This statement is fully supported by In6 “There is a kind of social disconnect. It's working like a [long distance] relation (…) cause you need to (…) keep alive that relation with the presents and being part of something big. If you think, OK, this is a normal job. I don't feel part of this organisation. I don't understand their mission. I'm just working here for the salary. I think that there is more chance that something bad happens when you have that organisation than if you have an organisation that puts together people”.

V. COMPARING INTERVIEWS AND LITERATURE

In this chapter we will look into the responses that were received through the interviews comparing them with the literature.

5.1. MALICIOUS INSIDER AND MALICIOUS INSIDER THREAT

Many researchers have tried to sketch a portrait of a malicious insider, specifying their personality traits, mental state and even predisposition and events that can lead to an insider crime. However, majority of the practitioners do not subscribe to this viewpoint; the general consensus amongst them was that life is not always easy and is not always predictable, sometimes horrible things happen to good people and therefore anyone can be pushed into the situation where he or she commits an insider crime. In addition to being pushed to commit a malicious crime from desperation, most of practitioners see the same types of malicious insiders as academia. They believe that people can become an insider threat for the reasons of financial gain, disgruntlement, ideology and if being hired by a nation state.

All interviewed cyber security experts acknowledged insider threat to be a serious danger to the organisations, for the same reasons as mentioned in the literature. Insider crime can cost company money, business, reputation, but it also can ruin a company’s culture, leaving people traumatised by the experience. Similarly to academia, cyber security practitioners believe that preventing malicious insider threat when presented by a determined actor or a nation state agent is close to impossible, hence, in this case, companies should be focused on timely detection.

5.2 SECURITY CONTROL

Further, when discussing the means to prevent the insider threat, we see that opinions of cyber security professionals tent to differ from those of academia. Moreover, we also see difference between experts that are employed by cyber security providers or threat intelligence companies, and the experts that have are responsible for designing, implementing and maintaining cyber security policy at corporates or other organisations. Further in this chapter, for the purpose of

consistency and simplicity, we will refer to them as security consultants and security responsibles respectively.

5.2.1 Hard Security controls

When discussing individual security controls, we can see a generic tendency amongst security consultant to be more optimistic about efficiency of the security controls, especially when speaking about hard security controls, than amongst the security responsibles. Security consultants named them to be the most effective ones, siding with the academia and official security bodies.

Security responsibles believe these controls to be effective but not necessarily as effective as the security bodies and academia presents them to be. Some security responsibles have seen these controls being breached, mainly due to the human factor, like trust, convenience, laziness and etc and hence have less confidence about successful functioning of these concerns.

In alignment with researchers, most of the security responsibles and some security consultants raised a concern of the need for balancing costs and work-efficiency with effectiveness of some hard controls. This has mainly been stated in relation to controls like IAM and especially the four-eye principle and the segregation of duties. Also, the question of legality and ethics when applying controls like monitoring and logging has been stressed by all. Interviewees were not able to go into the details, as none of them had a legal background, but many stated that laws, like GDPR, must be carefully consulted when designing and applying a monitoring process. Additionally, in alignment with academia, most were worried that extensive monitoring might breach the employees' trust.

5.2.2 Soft Security controls

First of all, when analysing the literature, we already see a difference in opinion between the academia and the official security bodies on the effectiveness of the soft security controls. Remarkably, the security consultants were more inclined to share the same opinion as the security bodies, while the practitioners were more aligned with the academia. However, when discussing the controls in depth we have witnessed a slight change in responses of the consultants, towards siding with the academia.

Initially, most of the security consultants, almost instinctively, responded immediately that controls like screening and security awareness and training are very effective ones. However, when discussing it further, many have recognised limitations of these controls in the same way as described in the literature. At the end, almost all interviewees concluded that although important, pre-employment screening is a basic step in the recruitment to ensure that people that are hired have a fit with the company culture, as described by academia, and should not be seen as a test on trustworthiness, for the reasons that screening checks are very limited and people change over lifetime.

When discussing in-employment screening, almost all experts were in agreement with academia on the need to treat this process with great care, considering it can bring more harm than good, by breaking employees' trust and hence damaging the company's culture.

Security awareness and training was also seen as one of the most effective ones by all, however, further discussion illustrated that this controls is mostly effective to prevent a benign malicious insider incidents and only effective against malicious insiders as a form of deterrence. Additionally, it helps employees to recognise indications of compromise. These thoughts are aligned with academia.

Confidential reporting and whistleblowing are seen by most of the interviewees the same way as it is seen by academia. All recognise this to be very beneficial for an organisation, in theory, however, all raised a concern of practical execution of this control. Similarly to the researches, practitioners doubt if employees are sufficiently equipped with understanding and knowledge of what behaviour should be considered suspicious to feel comfortable to report it without worrying about possible negative consequences for co-workers. Working-from-home is seen as an additional complicating factor, the same was as it is seen by academia.

VI. Discussion/Conclusion

This chapter will provide an elaborate answer to the research question "Is there an alignment between academia and practitioners on effectiveness of the measures designed to prevent a malicious insider threat". We base our answer on the comparison made between the reviewed literature and the interviews that were conducted.

6.1 Interpretation of the Findings

The issue of a malicious insider has been identified as one of the key threats to organisations. Historically, companies have been focusing on putting measure in place to protect their infrastructure from an outside attack, paying less attention to potential insider threat, acting from an assumption of trust. History shows time and time again that this has been a naïve assumption. With the evolution of information technology, the means to commit an insider crime have also evolved and the number of the crimes committed by the insiders is keep on growing, leading to financial and reputation losses, losses of business, legal proceedings, and even human tragedies.

Considering the high number of malicious insider crime occurrences and the high costs associated with it, we believe it is important to understand if sufficient research has been done by the academia on the ways to prevent the insider crime and whether the outcome of their research has been sufficiently communicated to the practitioners for the alignment.

Through the literature review we have noticed that academia seems to be ambivalent when describing effectiveness of different preventive measures against malicious insiders. There is no consensus on effectiveness of security measures, and the benefits of controls described by one group of researchers are challenged by another group, by presenting a number of limitations and

flaws. Although the lack of conclusiveness might not look like a positive result, we believe it is as important, considering that understanding of benefits and limitations gives us a balanced view and prevents from overestimating effectiveness of one or another security control. Having a knowledge of the limitations of security controls caters for more thoughtful design of the security policy by the cyber security professionals.

When conducing the interviews, we initially assumed that there is a lack of alignment between the way academia views malicious insiders and the ways to prevent their crime and how it is being seen by practitioners, based on witnessed examples and the news. As it turned out, this assumption was not entirely correct and the majority of the cyber security practitioners seems to be aligned with the academia, with a very minor deviation on some topics. Similarly to academia, practitioners are also conscious of benefits and limitations security controls bring as preventive measures against malicious insiders. There seem to be no overestimation of the effect these controls have.

Moreover, an interesting new insight came forward as a result of these interviews. Practitioners believe that the best way to battel malicious insiders is to address the intent, and therefore for the employers to fully exercise their duty of care, to create a supportive culture where people feel welcomed and cared for. This supportive culture should be built by the leadership at the top and cascaded down to create an atmosphere of trust, openness, friendship, and loyalty. There is a general believe that organisations that build and promote such culture will significantly minimise the number of insider opportunistic crimes, crimes committed by disgruntled employees and out of desperation. It has also been said that socially engaged employees will likely recognise signs of persistent malicious insiders, like those who have been hired to harm an organisation. It is believed that the security culture is built when a supportive environment is created.

6.2 Relevance

Different reports have shown that the number of the insider threat incidents has grown significantly over the last years. Although malicious insider threat represents only about one third of all the crimes committed by internal people, the costs associated with it are very high.

Various researchers have been looking into the issue of malicious insiders, trying to understand their motives and hence finding the ways to prevent their crimes. Many reports and research papers have been issued over the years by cyber security academics as well as cyber security bodies, where insights on how to identify malicious insider and what measures needs to be taken to prevent and timely detect them have been shared. In addition, official cyber security bodies have mandated some of these measures to organisations operating critical infrastructure. Never the less, the number of cyber security incidents committed by malicious insiders is on the rise.

In this research we tried to understand whether the cyber security practitioners view security measures too optimistically, without taking into account all flaws and limitations, that are described by academia, which could potentially lead to an incident. The aim was to conclude if academia needs to share more of their findings with practitioners or the practitioners are sufficiently informed. We believe that this is an important step in addressing the issue of malicious insiders.

5.3 Limitations

When considering reliability of this research, several limitations should be considered.

First of all, one of the main limitations is the number of cyber security practitioners that have been interviewed that is too low from the statistical point of view to be reliable. Although we believe that, considering a good spread throughout different industries and cyber security domains, the data is sufficiently representative, additional responses could have given us a better insight.

Secondly, considering that the interview has been designed as semi-structured, it was conducted in a form of a dialog where not all the questions were elaborated to the same extent and the same depth by all the interviewees. This is partially due to the fact that not all the interviewees had the same level of knowledge and experience with all the topics they were asked to feedback on. Consequently, this might have created some level of bias.

Lastly, when analysing the interviews, we have noticed a difference in responses between cyber security responsibles and cyber security consultants. Although we refer to this group in the research, due to the limited sample we are not conclusive on this split. Having a larger interviewee group could have given a better indication if this split is coincidental or consistent.

6.3 Recommendation for the future study

We started this research suspecting that the main reason for the rise of the malicious insider threat is that the practitioners were not well informed by academia on all the limitations of the security controls. Though the analysis, we learned that cyber security practitioners have a balanced view on the effectiveness of the security controls. As the interviewees have been sharing their personal point of view and not the position of an organisation they are employed by, for the future research we recommend focussing on organisations, to understand whether security controls flaws and limitations are taking into account when security policy is being designed.

During the analysis of the conducted interviews, we have encountered an interesting insight on the role of a supportive culture or a duty of care in organisations as a preventive measure against malicious insider threat. When reviewing academic literature, we have not seen any research dedicated to understating how duty of care can impact malicious insider threat risk. Therefore, future research is encouraged to comprehend how organisational culture that is directed on wellbeing of an employee can benefit to the prevention of malicious insider crimes and whether organisations that have adopted such culture have less malicious insider incidents.

When conducting interviews, we have noticed a difference in opinions between practitioners employed by cyber security providers or threat intelligence companies and practitioners that are dealing with designing, implementing and maintaining cyber security policy in organisations. Considering the limited sample of interviewees, we were not able to conclude if the difference was coincidental or consistent. Therefore, we recommend to research whether there is a difference in how security professionals view preventive security controls against malicious

insiders based on their occupation or job function. This could create an opportunity for knowledge sharing should the difference be consistent.

5.5 Conclusion

The goal of this study was to determine whether there is an alignment between academia and cyber security practitioners on the effectiveness of the measures that are being put in place to prevent a malicious insider threat.

Prior to discussing the actual research question, we believe that it is important to understand whether academia and practitioners have the same opinion on the malicious insiders, their characteristics, and motivations. In the academic literature we see various research articles describing typical character and personality traits of someone who can become a malicious insider. Although not fully conclusive, academia in generally is inclined to believe that someone must have a specific predisposition wheatear a personality or a meatal condition in order to commit a malicious insider crime. This point of view is not shared by the practitioners, who, unanimously, believe that any person, regardless of his or her character or personality, under specific circumstances can become a malicious insider. We find this to be an important conclusion, considering that understanding of who your potential enemy is lays a foundation for the design of preventive measures, and hence the knowledge that it can be anyone should cater for more adequate response.

When analysing the conducted interviews, we see that the threat of malicious insiders is understood by the practitioners the same way as it is seen by academia and is not underestimated. When comparing the responses with the academic publications, we see that practitioners are aware of the benefits and limitations of the security controls as they are being described in the academic literature. Therefore, we can conclude that there is an alignment between these two. Hence the research question "*Is there an alignment between academia and practitioners on effectiveness of the measures designed to prevent a malicious insider threat?"* can be answered positively.

Additionally, through the interview we have gathered an interesting insight on the additional security measure, or rather a practice – duty of care – that has been seen by almost all security practitioners as the basis for all the other controls, as it addresses the intent. Considering this measure has not been outlined by the literature and therefore has not been discussed as a part of this research, understating of the role of duty of care is recommended for the future research.

BIBLIOGRAPHY

SOURCES

Almehmadi, A., & El-Khatib, K. (2017). On the Possibility of Insider Threat Prevention Using Intent-Based Access Control (IBAC). IEEE Systems Journal, 11(2), 373–384. https://doi.org/10.1109/JSYST.2015.2424677

Alsowail RA, Al-Shehari T. Techniques and countermeasures for preventing insider threats. PeerJ Comput Sci. 2022 Apr 1;8:e938. doi: 10.7717/peerj-cs.938. PMID: 35494800; PMCID: PMC9044369.

Lattal, Ashley. "The Hidden World of Unconscious Bias and Its Impact on the Neutral Workplace Investigator." Journal of Law and Policy, vol. 24, no. 2, 2016, pp. 411-466. HeinOnline, https://heinonline.org/HOL/P?h=hein.journals/jlawp24&i=427.

Becker, W. J., Belkin, L. Y., Conroy, S. A., & Tuskey, S. (2021). Killing Me Softly: Organizational E-mail Monitoring Expectations' Impact on Employee and Significant Other Well-Being. Journal of Management, 47(4), 1024–1052. https://doi.org/10.1177/0149206319890655
Bishop, Matt & Gates, Carrie. (2008). Defining the Insider Threat. 10.1145/1413140.1413158.
Bradbury, J. C. (2019). Monitoring and Employee Shirking: Evidence From MLB Umpires. Journal of Sports Economics, 20(6), 850–872. https://doi.org/10.1177/1527002518808350

Brafford, H. R. (2021). Preventing malicious insider threat using non-disclosure agreements (Order No. 28490866). Available from ProQuest Dissertations & Theses Global. (2566019952)

Brody, R. G. (2010). Beyond the basic background check: hiring the "right" employees. Management Research Review, 33(3), 210–223. https://doi.org/10.1108/01409171011030372

Caldwell, T. (2016). Making security awareness training work. Computer Fraud & Security, 2016(6), 8–14.

William Claycomb, Carly L. Huth, Lori Flynn, David McIntire, & Todd Lewellen. (2012). Chronological Examination of Insider Threat Sabotage: Preliminary Observations. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 3, 4–20.

CERT National Insider Threat Center Releases Sixth Edition of Common Sense Guide to Mitigating Insider Threats. (2019). Targeted News Service.

Contos, B. T. (2006). Enemy at the water cooler real-life stories of insider threats and Enterprise Security Management countermeasures (1st edition). Rockland, MA: Syngress.

Dennehy, M. (2021). Preventing Insider Cyberthreats in Organizations: A Qualitative Delphi Study. ProQuest Dissertations Publishing.

Delosreyes, G. C. (2017). Mitigating insider threat risk (Order No. 10686094). Available from ProQuest Dissertations & Theses Global. (1991511291).

Dupuis, Marc & Khadeer, Samreen. (2016). Curiosity Killed the Organization: A Psychological Comparison between Malicious and Non-Malicious Insiders and the Insider Threat. 35-40. 10.1145/2978178.2978185.

Eklund, M. C. (2019). Monitoring employees' e-mail correspondence and Internet use – A Finnish perspective – PART II. European Labour Law Journal, 10(2), 134–153. https://doi.org/10.1177/2031952519861478

Goffin, R. D., Jang, I., & Skinner, E. (2011). Forced-choice and conventional personality assessment: Each may have unique value in pre-employment testing. Personality and Individual Differences, 51(7), 840–844. https://doi.org/10.1016/j.paid.2011.07.012

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight Into Insiders and IT. ACM Computing Surveys, 52(2), 1–40. https://doi.org/10.1145/3303771

Hunker, J., & Probst, C. W. (2011). Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications, 2(1), 4–27.

Liang, N. (2017). Characteristics of malicious insiders and their relationships with different types of malicious attacks.

Preventing and Profiling Malicious Insider Attacks
Journal article·2012·Agata McCormac, Kathryn Parsons, Marcus Butavicius

McCormick H. (2015) The real effects of unconscious bias in the workplace. UNC Executive Development, Kenan-Flagler Business School. DIRECCIÓN.

McKinney, G. (2019). Understanding conditions which could improve department of defense contractor reporting of cyber insider threat pre-attack warning indicators in coworkers (Order No. 13899292). Available from ProQuest Dissertations & Theses Global. (2625996237).

Prabhu, sunitha, & Thompson, N. (2020). A Unified Classification Model of Insider Threats to Information Security.

Saxena N, Hayes E, Bertino E, Ojo P, Choo K-KR, Burnap P. Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. *Electronics*. 2020; 9(9):1460. https://doi.org/10.3390/electronics9091460

Eric D. Shaw, Ph.D., Harley V. Stock, Ph.D., ABPP, Diplomate, American Board of Forensic Psychology Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall

Trivedi , S. ., & Patel, N. (2021). Virtual Employee Monitoring: A Review on Tools, Opportunities, Challenges, and Decision Factors. Empirical Quests for Management Essences, 1(1), 86–99.

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387. https://doi.org/10.1016/j.cose.2021.102387.

Vasileiou, I., & Furnell, S. (Eds.). (2019). Cybersecurity Education for Awareness and Compliance. Advances in Information Security, Privacy, and Ethics. https://doi.org/10.4018/978-1-5225-7847-5.

Ziegler, M., MacCann, C., and Roberts, R. D. (2012). Faking: Knowns, unknowns, and points of contention. In Ziegler, M., MacCann, C., and Roberts, R.D. (Eds.). New Perspectives on Faking in Personality Assessment. New York: Oxford University Press, pp. 3-16; p 8.

WEBSITES

www.bbc.com/news/world-europe-63395323

www.bellingcat.com/news/2022/08/25/socialite-widow-jeweller-spy-how-a-gru-agent-charmed-her-way-into-nato-circles-in-italy/

Carnegie Mellon University. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2019_005_001_540647.pdf.

www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf

https://www.cisa.gov/defining-insider-threats

www.collinsdictionary.com/dictionary/english/security-vetting

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

www2.dtexsystems.com/2022-insider-risk-report

www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

https://gdpr-info.eu/art-41-gdpr/

www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2015/volume-5/cybersecurity-detective-controls_joa_eng_0915

www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

www.ponemon.org/news-updates/blog/security/data-breaches-caused-by-insiders-increase-in-frequency-and-cost.html

www.sans.org/blog/cis-controls-v8/

www.schneier.com/blog/archives/2009/02/insiders.html

www.tessian.com/blog/insider-threat-statistics/

www.verizon.com/business/resources/executivebriefs/insider-threat-report-executive-summary.pdf

APPENDIX A

Named used in the research paper	Function	Industry
In1	Head of corporate security	Critical Infrastructure
In2	Head of Cyber Security Centre	Global Corporate
In3	Technical expert	Cyber security provider
In4	CISO	Financial Industry
In5	VP Global Business	Cyber security provider
In6	Lead Principal	Cyber security provider
In7	Head of IAM	Global Corporate
In8	Consultant	Cyber security provider

APPENDIX B

Interview questions

1. What is your current role?
2. Do you consider malicious insider threat to be a real danger to organisations?
3. How would you describe a malicious insider? What do you think are the best ways to identify a malicious insider?
4. Do you believe it is possible to prevent incidents/crimes committed by malicious insiders?
5. From your point of view what security controls are the most effective ones to deal with malicious insiders?
6. When looking at the malicious insider, what is your opinion, in terms of effectiveness, on the following security controls; what works well and what does not
    a. Identity and Access management
    b. System hardening
    c. Monitoring & Logging and Employee monitoring
    d. Security training and awareness
    e. Pre-employment vetting and profiling
    f. In-employment Employee screening
    g. Confidential reporting procedures
    h. Contractual clauses and NDA
7. What are the constrains, barriers or considerations in the implementation of these controls?
8. What would you like to add?