MALICIOUS INSIDER THREAT TYPES – AN EMPIRICAL ANALYSIS

MANFRED HOFMEIER, ISABELLE HAUNSCHILD,
ULRIKE LECHNER

Universität der Bundeswehr München, Department of Computer Science, Neubiberg, Germany
manfred.hofmeier@unibw.de, isabelle.haunschild@unibw.de, ulrike.lechner@unibw.de

Malicious insider threats represent a particular challenge not only for defense, but also for research, as it is estimated there is a high number of unreported cases. Current taxonomies and typologies usually focus on specific aspects, such as goal or motivation, and tend to have tight boundaries. A number of malicious insider threat attack scenarios were identified in our research through qualitative interviews, enhanced with a game-based creative approach. The resulting data was used to develop a malicious insider threat typology in an empirical bottom-up approach. We developed an analysis scheme from existing taxonomies and typologies and used it in an empirical analysis of malicious insider roles and attack scenarios. We were able to identify eleven archetypes of malicious insider threats considering multiple facettes. This paper describes the analysis and the identified types.

Keywords:
insider threats,
typology,
information security,
Bled eConference,
research paper

University of Maribor Press

DOI https://doi.org/10.18690/um.fov.6.2023.8
ISBN 978-961-286-804-8

1 Introduction

The European Union Agency for Cybersecurity (ENISA) defines an insider threat as "an action that may result in an incident, performed by someone or a group of people affiliated with or working for the potential victim" (ENISA, 2020). Insider threats can also be distinguished as accidental or malicious (intentional). In this work we take a close look at malicious insider threats. These represent a particular challenge not only for actual protection, but also for research, as it is estimated there is a high number of unreported cases. Organizations tend not to disclose information on malicious insider threats (e.g., not to lose the trust of customers or partners), and typically only cases with news value become public. Thus, the cases examined in the research are not necessarily representing the current insider threat landscape. In general, information systems literature such as the UMISPC (Moody et al., 2018) addresses the field of insider threats primarily regarding accidental insider threats while the malicious type is usually not considered.

As we collected plenty of malicious insider threat attack scenarios in our research through an interview survey and a creative approach (using the serious game "Operation Digital Butterfly" (Hofmeier, 2021), which is designed to collect plausible insider roles and attacks), we use this data to develop a malicious insider threat typology.

Current taxonomies and typologies usually focus on specific aspects, such as goal or motivation, and tend to have tight boundaries. For example, the ENISA Threat Landscape Report distinguishes five types of insider threats by rationales and objectives (ENISA, 2020): *careless workers* mishandling data, violating policies or installing unauthorized applications; *inside agents* who steal information on behalf of outsiders; *disgruntled employees* who seek to harm their organization; *malicious insiders* who use existing privileges to steal data for personal gain; *third-parties* who compromise security through intelligence, misuse or malicious access to or use of an asset. Cappelli et al. distinguish three types of insider threats by objectives in the “CERT Guide to Insider Threats” (Cappelli et al., 2012): *theft* (e.g., of intellectual property or other data), *sabotage* (malicious manipulation of data or processes or causing reputational damage) and *fraud* (e.g., stealing financial goods). The German Insurance Association (GDV) defines four perpetrator types (Bundeskriminalamt, 2020): The *crisis perpetrator* who is triggered by crisis events in private or professional life that threaten status and lifestyle; the *inconspicuous* who takes advantage of an emerging opportunity; the *perpetrator with an economic-criminological disorder* who actively seeks or creates opportunities to commit a crime, and the *dependent* who is usually hierarchically subordinate to a main offender or owes the main offender a favor and fears repression in case of refusal to cooperate. Some taxonomies and typologies distinguish by insider position (Cole & Ring, 2005; Magklaras & Furnell, 2001; Bundesamt für Sicherheit in der Informationstechnik, 2018) or attack vector (Phyo & Furnell, 2004). Homoliak et al. (2019) provide a comprehensive taxonomy with multiple aspects.

However, there are only a few empirically based typologies of malicious insider threats in terms of comprehensive archetypes. Therefore, the aim of this research is to develop archetypes of malicious insider threats using our collected data in an empirical bottom-up approach.

2 Analytical Approach

We analyzed malicious insider threat roles and attack scenarios using scheme-based content analysis to develop the typology.

2.1 Material for Analysis

The data used in this analysis is interviews and serious game results. Interviews and games were part of LIONS and NutriSafe research projects.

The interviews were conducted from December 2021 to August 2022 with 13 experts from various organizations (table 1). The experts were selected from the LIONS project research network, while the selection criterion was the possibility of points of contact with the subject of malicious insiders. The interviews were structured using an interview guide, and topics were real-world cases, plausible scenarios, and assessments of malicious insider threats. The interviews were recorded, and summarized. Summaries were then sent to the respective interview partner(s) for a review regarding correctness (and anonymization). The interview study collected 21 instances or groups of attack scenarios, subject to the analysis presented in this paper.

Table 1: Interviews used in the analysis (anonymized)

Organization	Interview partner(s)
Consulting (logistics)	Director
Energy	Senior Expert Penetration Testing
Energy	Senior Expert Cyber Forensics Senior Expert Cyber Forensics Compliance Investigations
Energy	Information Security Manager
Civil engineering	Manager Software Development
Security technology	Information Security Officer
n.a.	Information Security Expert
n.a.	People Manager
Industrial software	Managing director
Public authority	Information Technology Manager
Security software	CEO

Table 2: Serious game iterations

Date	Game board	Players	Attack Scenarios
May 2020	Meat Production	6	2
Jul 2020	Meat Production	15	4
Oct 2020	Logistics Hub	7	3
Nov 2020	Logistics Hub	15	4
Mar 2021	Logistics Hub	12	3
Sep 2021	Travel Management	12	3
Feb 2022	Travel Management	10	6
Feb 2022	Travel Management	9	6
Feb 2022	Travel Management	9	6
Jul 2022	Logistics Hub	13	3

Because interviews have limited capabilities regarding the field of malicious insiders (e.g., typically, there is no knowledge of intentions or motivations of perpetrators), a creative game-based approach was also used. The serious game "Operation Digital Butterfly" (Hofmeier, 2021) – in an earlier version "Operation Digital Ant" (Hofmeier, 2020; Hofmeier & Lechner, 2021) – was developed – using a design science approach according to Hevner et al. (2004) – to generate fictional but realistic attack scenarios by malicious insiders. "Operation Digital Butterfly" is a tabletop game with a game board in the center, depicting an infrastructure of an organization. Three to four teams compete against each other in creating roles and attacks of malicious insiders, using role cards and scene cards. The game board describes the environment wherein insider threats take place. During our research, the game has been played with three different game boards: slaughterhouse and cutting plant, logistics hub with warehouse, and travel management in a public authority. Each team develops an insider role, an attack, and a security measure using a card deck. The cards structure the team discussion and the presentation of the attack vector and security measure developed in the team discussion. The teams are instructed to answer four questions on the role card to guide the creative design of attack measures:

- Who is the insider (position in the organization)?
- What does the insider want to achieve (intention)?
- Why does the insider want that (motivation)?
- How does the insider justify this to himself/herself (neutralization)?

The attack is developed using the scene cards. The filmmaking metaphor is used to make development and descriptions of attacks easy – also for players not used to formal notations. A threat is a sequence of scenes. This way, each team can tell their fictional insider attack by using a sequence of scenes.

To make the game more fun and to raise awareness about countermeasures to insider attacks, each team fills out a security measure card. Teams are instructed to anticipate possible attacks from the other teams (the roles are known) and develop an adequate countermeasure. This measure is valid for the attack plans of all teams and is then taken into account when rating the attacks. The winning team is determined through a rating system, in which the teams rate each other by three given categories: (1) Plausibility of role, (2) plausibility of the attack story, and (3) damage potential. Each team can give up to ten points for each category to the other teams. Note that the most important category for later analyses is "plausibility". This incentivizes that the developed attacks and roles are – to some extent – realistic and fit the profile of the role. The "damage potential" category makes the teams more likely to develop attacks that cause significant damage and therefore are of particular interest in security research. The game is also accompanied by a closing discussion, focusing on possible countermeasures regarding the attack scenarios developed in the game.

The game is scientifically validated (Hofmeier & Lechner, 2021) and designed to create plausible insider roles with intention, motivation, and neutralization (Sykes & Matza, 1957) combined with according attack paths. It also features plausibility checks (e.g., through team rating criteria and following external validation) of roles and scenarios. In ten game performances from May 2020 to July 2022 with participants from research institutions, companies, and public authorities, 40 attack scenarios – with at least medium plausibility each – were developed (table 2).

2.2 Analysis Scheme

To develop types that are as complete as possible, our aim was to look at as many aspects of malicious insider threats as possible. Therefore, we prepared an analysis scheme based on various existing taxonomies (see table 3), which partly follows the comprehensive taxonomy by Homoliak et al. (2019), who examined and combined various existing taxonomies. We grouped the different type aspects in six groups of characteristics: intention(s) or outcome, motivation, insider position, attack vector, timing, and psychosocial characteristics.

2.3 Analytical Procedure

Using this scheme as a two-dimensional category system following the qualitative content analysis methodology according to Mayring (2008), we analyzed the material in two iterations. In the first iteration, the cases (from the interviews as well as from the game results) were examined one by one. Each considered case was compared with the already extracted types. In case of similarity, it was assigned to the respective type, which is sometimes also accompanied by slight changes to the type (e.g. adding information to a category); in case of contrast with the existing types, a new type with the characteristics of the given case was created. In the second iteration, the cases were examined again by another researcher and in a different order to test whether each case had an adequate counterpart in the types. Among other things, this should prevent a sequence effect as well as minimize the effect of subjectivity.

Table 3: Taxonomy-based analysis scheme

Type characteristics	**Aspects**	**Source(s)**
Intentions / outcome	theft (of IP), sabotage, fraud, miscellaneous	Cappelli et al. (2012)
	espionage, IP theft, unauthorized disclosure, sabotage, fraud, workplace violence	MITRE (2022)
	information theft, harm to orgnization, personal gain	ENISA (2020)
Motivation	levels: self-motivated, planted, recruited	Cole & Ring (2005)
	motivation: financial, political, personal	Cole & Ring (2005)
	economic-criminological disorder, crisis, opportunity, dependency	BKA (2020)
Insider position	topology: pure insider, inside associate, inside affiliate, outside affiliate	Cole & Ring (2005)
	system role: system masters, advanced users, application users, none	Magklaras & Furnell (2001)
	physical access to control systems, privileged users, third-party employees	BSI (2018)
Attack vector	manifestation level: physical world, network, operating system, application, data	Phyo & Furnell (2004)
Timing	duration: long-term, short-term, one-time	Homoliak et al. (2019)
	point in time: before job termination, after job termination	Homoliak et al. (2019)
Psychosocial characteristics	levels: psychological, social, socioeconomic	-
	indicators: disregard for authority, disgruntlement, anger management issues, confrontational behavior, disengagement, not accepting criticism, absenteeism, self-centeredness, performance, lack of dependability, personal issues, stress	Greitzer et al. (2013)
	Personal vulnerabilities: introversion, social and personal frustrations, computer dependency, ethical "flexibility", reduced loyalty, entitlement, lack of empathy	Shaw et al. (1998)

3 Malicious Insider Threat Types

Based on the analysis of the interview results as well as the attack scenarios from the game, we identified eleven insider threat types. Below, the individual types are described according to the taxonomy-based analysis scheme.

3.1 Disgruntled Employee / Disgruntled Leaver

The disgruntled employee is motivated primarily by revenge and seeking "justice". This type is discuss in may insider threat studies – e.g., in the Insider Threat Study (Keeney et al., 2005). The wish for revenge can be based on different causes, such as being fired, having disputes with supervisors or management, a lack of recognition, unequal salary structures, or missed salary increases, which cause a - subjective - feeling of injustice. Here, we also discuss the disgruntled leaver as a subtype, which has the same characteristics except that it related to a job termination (either by the organization or the employee resulting from a perception of injustice). This insider type usually seeks to harm the organization, typically by sabotaging or causing reputational damage through physical sabotage (e.g., of products or machines) or data manipulation. A disgruntled employee is naturally an insider who has a contract with the organization, while he or she can have any position in any department within the organization. An incident is typically a one-time event at any time during employment or after job termination (disgruntled leaver).

3.2 Data Transfer to Competition

In this threat type, an insider takes data such as intellectual property (e.g., source code, blueprints) or other valuable information (e.g., customer data) with him or her when transferring to a competitor. The act is naturally a one-time event during job termination and typically based on an aim for personal gain. Still, it can also be additionally motivated by revenge or curiosity. Insiders of this type can be pure insiders or external contractors but are limited to persons with access to valuable data (e.g., files, applications, databases).

3.3 Industry Espionage

Insiders engaging in industrial espionage use given privileges to steal valuable information such as intellectual property while having any position with access to data (internal or external positions). They are typically recruited by external actors, typically using bribes. The willingness to accept bribes can be mediated by factors such as job satisfaction or financial situation. The act is usually a one-time event at any time during association with the organization.

3.4 State Espionage

Similar to the industry espionage type, insiders engaging in state espionage use given privileges to steal critical information while having any position with access to data. They are recruited by external agents, are bribed or blackmailed (e.g., after being compromised privately). The willingness to accept bribes or give in to blackmail can be mediated by additional factors such as job satisfaction, financial situation, or family circumstances. As with the industry espionage type, the act is usually a one-time event at any time.

3.5 Taking Advantage of Privileges for Personal Gain

When insiders take advantage of privileges to achieve personal gain, the motivations are manifold: in some cases, there are financial problems (e.g., through having too high lifestyle standards or depts), and others subjectively think they deserve the profit (which is not granted to them by the organization), and some are envious (e.g., of customers when it comes to expensive products or services). To achieve personal gain, these insiders either simply steal property (e.g., IT equipment) or use their access to IT systems to commit fraud. The actions (theft or fraud) often start small and then become more in case of success until the point where the actions become conspicuous. So, it is typically a series of events.

3.6 Unauthorized Inspection of Personal Data

Individuals who unauthorizedly inspect personal data are users or admins - typically pure insiders - with insights into databases (either directly or via applications). The act is usually short-term and motivated either by personal reasons (such as curiosity or having a crush on a person residing in the database) or by political agenda (e.g., looking up personal data of perceived enemies).

3.7 Intellectual Property Sale

When intellectual property is sold on black marketplaces (e.g., on the darknet), the perpetrators are usually people with technical skills, such as administrators or developers, and thus typically pure insiders. In this case, intellectual property can mean blueprints of products or source code of software products. When it comes to leaked source code, the risk of further cybersecurity incidents is also enhanced. The motivation resides in personal (financial) gain and opportunity through access to valuable data (e.g., repositories), supported by low commitment and ethical flexibility.

3.8 Whistleblowers

Whistleblowers follow their political or moral understanding and seek to publish critical data of the organization (e.g., data that are evidence immoral in the eyes of the perpetrator). These individuals identify themselves as whistleblowers - even if they aren't (according to the perceptions of the general society). They feel the organization deserves the harm and to act for the greater good. These views correspond with the neutralization techniques "denial of the victim" and "appeal to higher loyalties" (Sykes & Matza, 1957). In principle, this type of perpetrator can be anyone with access to relevant data, including third parties. In some cases, the insider might be encouraged by (external) parties. The act is usually a one-time event during affiliation with the organization.

3.9 Politically Motivated Sabotage

As with the whistleblower type, politically motivated saboteurs think that the victimized organization deserves the harm and that they act for the greater good (neutralization techniques "denial of victim" and "appeal to higher loyalties" (Sykes & Matza, 1957). But these individuals seek to actively harm the organization by (physical or digital) sabotage or causing reputational damage (e.g., by publishing compromising information) because they reject the organization. This primarily applies to public sector organizations or companies where the morality of the objectives or methods is in question. Perpetrators of this type can have any position in the organization, while the attack vector they choose depends on their position and the corresponding skills and opportunities.

3.10 Extortion

In the extortion type, insiders blackmail the organization with the help of their physical or digital access privileges. The target can be data (e.g., using ransomware) or physical goods (e.g., poisoning food in the supply chain).

These perpetrators are typically financially motivated, which can reside in financial problems. They also might have a criminal background or psychological issues. In general, they have low job commitment and might misjudge the consequences of their actions. They can have any position in the organization, while the attack vector they choose depends on their position and the corresponding skills and opportunities.

3.11 Illegal Use of IT Infrastructure

In this type, individuals use the organization's IT infrastructure for their own illegal purposes for a long time, such as using storage devices for storing and providing illegal material or using infrastructure for illegal transactions (e.g., money laundering). Naturally, this type of perpetrator requires information technology skills and access to IT infrastructure. IT staff such as system administrators are typical for this insider threat actor.

4 Conclusion

We developed an analysis scheme from existing taxonomies and typologies for extracting malicious insider threat archetypes. We identified eleven types of malicious insider threats using this scheme in an empirical analysis of real-world and fictional but realistic (and plausible) adversarial insider roles and attack scenarios. These types consider multiple facets and thus exceed existing typologies.

However, there are some limitations. The types are based on the analyzed material and the subjectivity of an analyzing researcher. Therefore, the typology may not be complete, and new types may be identified by analyzing additional material using the developed analysis scheme.

The identified types are important for risk analysis in practice (e.g., scenario-based risk assessment) and a basis for further research. In addition, we found that a creative approach (here in the form of a serious game) could extend the results, particularly regarding intentions and motivations. In comparison with existing taxonomies and typologies, the typology presented in this paper features more dimensions (especially taxonomies are typically one-dimensional) and more types (e.g., politically motivated insiders are missing in other typologies). This way, our work enables a better understanding of malicious insider threats, a better understanding of the variety of malicious insider threats, more awareness of insider threats, and a better fit of security measures to the insider threat variety.

Acknowledgements

This work originates from the LIONS research project. LIONS is funded by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr, which we gratefully acknowledge. dtec.bw is funded by the European Union – NextGenerationEU. We would like to thank all game participants, all interview partners, and the LIONS project partners for fruitful discussions.

References

Bundesamt für Sicherheit in der Informationstechnik (2018). Industrial Control System Security – Innentäter. https://www.bsi.bund.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI- CS_061.html.

Bundeskriminalamt (2020). Monitoringbericht Innentäter in Unternehmen 2: Aktuelle inländische Forschungsbeiträge, wesentliche Ergebnisse und Handlungsempfehlungen. Technical Report.

Cappelli, D., Moore, A., Trzeciak, R. (2012). The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Addison Weseley.

Cole, E., Ring, S. (2005). Insider Threat: Protecting the Enterprise From Sabotage, Spying, and Theft. Syngress.

ENISA (2020). ENISA Threat Landscape 2020 - Insider Threat. Technical Report. ENISA.

Greitzer, F. L., Kangas, L. J., Noonan, C. F., Brown, C. R., Ferryman, T. (2013). Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis. e-Service Journal 9, 1.

Hevner, A. R., March, S. T., Park, J., Ram, S. (2004). Design Science in Information Systems Research. Design Science in IS Research MIS Quarterly, 28(1), 75–105.

Hofmeier, M. (2020). Operation Digital Ant. https://github.com/NutriSafe-DLT/operation-digital-ant.

Hofmeier, M. (2021). Operation Digital Butterfly. https://github.com/LIONS-DLT/operation-digital-butterfly.

Hofmeier, M., Lechner, U. (2021). Operation Digital Ant - A Serious Game Approach to Collect Insider Threat Scenarios and Raise Awareness. European Interdisciplinary Cybersecurity Conference (EICC). ACM, New York.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., Ochoa, M. (2019). Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. Comput. Surveys 52, 2.

Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., Rogers, S. (2005). Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. Technical Report. Carnegie Mellon University.

Magklaras, G. B., Furnell, S. M. (2001). Insider Threat Prediction Tool: Evaluating the Probability of IT Misuse. Computers and Security 21, 1, 62–73.

Mayring, P. (2008). Qualitative Inhaltsanalyse: Grundlagen und Techniken. 10th Ed., Weinheim/Basel.

MITRE (2022). MITRE's Human-Focused Insider Threat Types.
https: //insiderthreat.mitre.org/insider- types.

Moody, G. D., Siponen, M., Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance, MIS Quarterly, 42(1), pp. 285-311.

Phyo, A. H., Furnell, S. (2004). A detection-oriented classification of insider IT misuse. Proceedings of the 3rd Security Conference.

Shaw, E. D., Ruby, K., Post, J. (1998). The Insider Threat to Information Systems: The Psychology of the Dangerous Insider. Security Awareness Bulletin 2, 2–98.

Sykes, G. M., Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. American Sociological Review 22, 6, 664–670.