Insider Cyber Threats In Ethiopian Telecom Security: Threats and Defense Strategies

Nebiyu Yohannes
MSc Candidate, Department of Software Engineering,
HiLCoE School of Computer Science and Technology
nebiyu.yohannesta@gmail.com

Seyoum Abebe
Lecturer, Department of Software Engineering, HiLCoE
School of Computer Science and Technology
seyumabebe13@gmail.com

Abstract

This study investigates insider cyber threats within the Ethiopian telecom, The study focuses on the motivations, behaviors, and security challenges faced by both intentional and unintentional insider threats. The study highlights the prevalence of insider threats such as data theft, system sabotage, and financial fraud, alongside those resulting from employee negligence or lack of security awareness. The findings showed that insufficient monitoring tools, inadequate employee awareness, and limited visibility into employee activities are significant challenges faced by telecom organizations. This paper also underscores the importance of a comprehensive, proactive defense strategy to mitigate these risks. The Key recommendations include the adoption of advanced behavioral monitoring tools, regular security awareness training for employees, and the implementation of stringent access control measures. On top of that, fostering a culture of transparency and trust, offering support mechanisms for employees, and conducting simulated insider threat exercises are essential steps toward creating a secure organizational environment. By focusing on these areas, organizations can improve their ability to avoid and respond to insider threats, thus protecting important assets and sensitive information. The research adds knowledge to cybersecurity studies in emerging economies by providing utility-based strategies that telecom companies in Ethiopia can use to boost their cybersecurity protections. Future research will benefit from the essential discoveries obtained from this study.

Keywords: Insider Threats, Cybersecurity, Telecom Security, ISO/IEC 27001, NIST CSF, Information Security

1. Introduction

The telecommunications sector plays a crucial role in keeping global communication intact. Telecom suppliers are responsible for constructing, operating, and overseeing the intricate network systems utilized for transmitting voice and data, as well as managing significant amounts of sensitive information. As a result, they are prime targets for various

types of cyber-attacks [9]. ICT is compressing the vast world into a more manageable space by enabling seamless information exchange and knowledge sharing, which enhances both business connections and social interactions. Whether in developed or developing nations, ICT is essential for driving economic growth and reducing poverty [15].

The telecom industry is undergoing a metamorphosis as it transitions from traditional business models to ones enabled by advanced technologies such as 5G [12]. 5G is a major change agent that demonstrates how technology and competition are revamping the state of play in the telecom industry [13]. This shift is necessary if telecom firms want to contend effectively with the threats of commoditization, intense competition, and fast-changing customer expectations. The digital transformation is reinforced by cloud computing, big data and analytics, the Internet of Things (IoT), robotics, and artificial intelligence (AI) is the most effective way for telecom firms to compete in an increasingly complex marketplace [12]. Success in the fast-paced, fiercely competitive corporate environment of today depends on innovation. Technology is one tool that executives may use to spur innovation and enhance their goods and services [14].

Nowadays, insider threats are a concern for many sectors and companies [8]. Insider threats are increasingly costly for organizations. According to research by the Ponemon Institute in 2020, insider threats incurred an average expense of $11.45 million, and 63% of these threats stemmed from employee carelessness [2]. Cyber security and Telecommunications generally go hand in hand. The telecom sector is one of the main targets of cybercrime. As telecom businesses' operations are altered by sophisticated technology, cyber security must also improve [1]. Insider threats represent a significant and evolving challenge for organizations. Understanding the most prevalent types of insider threats is essential to align defensive strategies and enhance threat management frameworks [21]. In the global telecom industry, insider cyber threats are increasingly recognized for undermining the confidentiality, integrity, and availability of critical systems and data. Both malicious and negligent insiders pose serious risks by exploiting authorized access to compromise organizational assets. According to the 2022 Global Insider Threats Cost Report, 67% of organizations experience a considerable number of insider-related incidents annually, underscoring the escalating nature of the threat [20]. Despite growing global awareness, limited research exists that specifically addresses insider threats within the Ethiopian telecom sector.

In Ethiopia, this issue is compounded by challenges such as the absence of local studies and a lack of context-specific defense strategies. While international research offers valuable guidance, the underlying motivations and behaviors of insiders in Ethiopia may vary due to socio-economic, organizational, and cultural differences. For instance, in the Ethiopian commercial banking sector, 66.6% of participants identified the lack of research as a major obstacle to mitigating insider threats [19]. This insight highlights a broader gap in contextual research, which likely extends to the telecom sector. Although various global studies focus on insider threat prevention, including the development of advanced

monitoring systems and behavioral models, Ethiopia's telecom industry remains underrepresented in this domain. Thus, this study seeks to fill the gap by analyzing insider threats in the Ethiopian telecom sector, identifying the motivations and behaviors of insiders, and proposing effective, context-aware defense strategies. The findings aim to contribute not only to academic discourse but also to practical applications in telecom security.

2. Related work

The European Electronic Communications Code (EECC) requires telecom providers to notify users of significant cyber threats, which aligns with best industry practices. However, studies show that too many warnings can desensitize users, while clear, specific alerts increase effective responses. Collaborative efforts in Italy and Belgium have successfully used coordinated communication to combat threats like SIM swap fraud and Flubot malware. The NIS2 proposal expands these approaches to other critical sectors with a flexible framework for timely threat communication. Cooperation among providers, national authorities, and CSIRTs is essential for effective threat mitigation. These efforts highlight that user outreach should complement technical measures, as users often lack the expertise to address complex cyber risks alone [6]. Telecom providers are encountering heightened cybersecurity risks as hackers employ advancing tools and methods with the main goal of stealing sensitive information such as credit card numbers and personal data. Given that telecom companies manage crucial infrastructure and deal with significant amounts of sensitive information, they are attractive targets for cyberattacks. Cybercriminals take advantage of weaknesses in software and hardware to infiltrate networks, frequently aiming to commit fraud or acquire customer data. Given the vital importance of telecom infrastructure, such attacks can result in extensive and serious repercussions [7].

In the United States, safeguarding critical infrastructure most of which is privately owned has been deemed a national priority. The National Strategy to Secure Cyberspace and the President's Critical Infrastructure Protection Board emphasize public–private partnerships to bolster defense against insider risks. The Department of Homeland Security (DHS) actively fosters collaboration with industry to raise awareness and share best practices. A cornerstone in understanding insider threats is the Insider Threat Study (ITS), a joint effort by the U.S. Secret Service's National Threat Assessment Center (NTAC) and Carnegie Mellon University's CERT Program. Launched in 2002, ITS analyzed 52 insider incidents in the IT and telecommunications sectors (1996–2002), covering IP theft, fraud, and sabotage. Key findings showed that both current and former employees many in technical roles and some with prior arrests, planned malicious acts in response to workplace events. The study highlighted behavioral and technical indicators that can precede insider attacks. Through its investigative and protective mandates, the Secret Service partners with DHS and CERT to coordinate research, incident response, and training establishing a model for cross-sector collaboration in insider threat mitigation [8].

Since telecommunications is a vital infrastructure, it must be safeguarded. The threat landscape demonstrates that can originate from a variety of sources and that vulnerabilities

exist on multiple levels: hardware, software, and human. It is imperative that telecom providers adopt a process-based approach to security, which includes threat prediction, prevention, detection, response, and investigation. A Page 6 crucial part of this is that they need a comprehensive, multi-layered security solution, yet this is insufficient on its own. It must be supplemented with shared intelligence, employee education, and teamwork. Numerous telecom providers currently have arrangements established for mutual sharing of network capability and capacity during disruptions, and this is the moment for them to begin leveraging the advantages of collective intelligence [9].

Early research on insider threats, though long established, has been revitalized by the rapid spread of IT systems and the internet, which greatly increase insiders' capacity to harm organizations. Serving as a key resource for those developing an Insider Threat Program (InTP), this study draws heavily on U.S. centric work especially Carnegie Mellon's CERT Division and supplements it with European guidance such as that from the Estonian Data Protection Inspectorate. It defines "insider" and "insider threat" through the intertwined dimensions of knowledge, access, and trust, and outlines five threat profiles: IT sabotage, intellectual property theft, fraud, espionage, and unintentional insider actions. The authors emphasize that successful InTP implementation often falters due to insufficient management support and inconsistent application of new measures, and they explore privacy and legal challenges via scenario-based analyses to guide practitioners through potential complications [10].

The research investigates the management of insider threats within the Ethiopian banking sector, concentrating on common threats, the motivational elements that lead to harmful actions, and the current strategies for mitigation. The study utilized a survey approach, using questionnaires to collect information from representatives of the nineteen commercial banks functioning in Ethiopia. The research used SPSS for conducting statistical analyses, implementing techniques like correlation, percentile, and mean [19].

Insider threats represent a serious danger to organizations, especially those involved in critical infrastructure. Recognizing these threats and their driving factors is crucial for developing effective mitigation strategies. This assessment uses the cyber kill chain model to analyze insider behavior, highlighting psychological factors behind malicious activities. Current defense techniques, including behavioral monitoring and access controls, are evaluated, with recommendations for stronger multi-layered defenses. The study identifies gaps in detection methods and emphasizes the need for advanced, proactive threat management. Future research should address emerging challenges and refine insider threat mitigation [16].

3. Method

The following research questions are addressed in this study: 1) what are the different types of insider threat in Ethiopian telecom sector and categories this threats in to intentional and unintentional threats? 2) What is the motivations and behavioral sign of potential insider in Ethio-telecom sectors? 3) What are the robust defense strategies against in insider threats

in Ethiopian Telecom sectors?

Table1: Question Summary

No	**Question Summary**
1	Encountered or observed insider threats?
2	Types of insider threats encountered?
3	Categorization of insider threats?
4	Common unintentional threats observed?
5	Departments with more unintentional threats?
6	Most frequent intentional threat types?
7	Departments with more intentional threats?
8	Most at-risk assets/data in telecom?
9	Primary motivations behind intentional threats?
10	Common causes of unintentional threats?
11	Behavioral signs of insider threats?
12	External factors influencing insider actions?
13	Personal/psychological susceptibility factors?
14	Key challenges in identifying insider threats?
15	Use of Data Loss Prevention (DLP) system?
16	Use of AI-driven behavior monitoring system?
17	Recommended defense strategies against insider threats?
18	Organizational considerations for insider threat defense?
19	Pre-hiring background checks and focus areas?
20	Methods used for background checks?
21	Re-screening during role changes or promotions?
22	Awareness/training programs to mitigate insider threats?
23	Suggested additional strategies or technologies for threat defense?

To address these questions, we followed a mixed-methods research approaches because it allows a comprehensive analysis by gathering both quantitative data and qualitative data, and it also provides a well-rounded understanding of insider threats. This study aimed to analyze insider cyber threats within Ethiopia's telecom sector and propose robust defense strategies. The research design outlined the methodological approach that was employed to achieve this objective.

3.1 Survey Development

To begin the questionnaire, a short overview was given regarding the purpose of the survey. Furthermore, participants were made aware of ethical and social concerns, and they were guaranteed that all gathered data would remain anonymous. Some of the survey questions are listed in table 1.The questions were organized into several sections, starting with demographic information. It then explored the activities respondents engage in when identifying insider threats, planning defense strategies, implementing security measures, and evaluating the effectiveness of those measures. At the end, participants were given the opportunity to share additional feedback or insights related to insider cyber threats in the

telecom sector.

3.2 Target Groups

The study sample was purposefully selected using purposive and snowball sampling. This approach ensures that the participants have the requisite knowledge and experience in cybersecurity, specifically in relation to cyber threats. These experts are critical to providing the insights needed for the study. Therefore, the focus was on selecting respondents with direct experience or involvement in managing cybersecurity within the telecom sector. This included IT managers and security officers in Ethiopian telecom companies, Cyber security professionals and experts working within the telecom industry, and other telecom staff.

3.3 Data collection

For the purpose of data collection in this research, interviews and surveys were conducted. Since the development of defense strategies required analysis of the telecom sector and its security practices, these methods were essential. The interviews were invaluable in extracting the necessary information from IT experts to formulate effective defense strategies against insider threats. Additionally, surveys was gathered quantitative and qualitative data from a broader sample of industry professionals to identify patterns and trends. The processes to be undertaken for data collection are discussed below.

I. Survey

Surveys are a common data collection method used in mixed methods research. Surveys involve the collection of standardized responses to a predefined set of questions from a sample of participants. Surveys can be implemented using online platforms or face-to-face methods [5]. This data helped identify patterns, trends, and the prevalence of insider threats. The participants in this case is a diverse group of employees, managers, and cyber security professionals within the Ethiopian telecom sector. A structured mixed-method questionnaire was developed, consisting of both closed-ended and Likert-scale questions. The questions was covered the topics to address the aims of the research targets.

II. Interview

Interviews are a qualitative data gathering strategy that involves asking open-ended questions to elicit detailed information about a participant's experiences, viewpoints, and opinions. Data may be collected in person, by phone, or online [5]. Interviews was helpful to gaining information about the nature of insider threats, the motivations behind such threats, and the effectiveness of current defense strategies from the perspective of key stakeholders.

During collecting the necessary data, face-to-face interviews was conducted using semi-structured interview questions. A semi-structured interview is a qualitative research method that combines open-ended questions to stimulate discussion with closed-ended questions, allowing the interviewer to delve deeper into specific topics or responses. The respondents' answer was recorded by taking detailed short notes. These interviews were very

important for gaining information about the existing threats and problems that emerge due to insiders.

4. Results and discussion

This part presents findings based on data from Ethio-Telecom and the insights obtained from the questionnaire and interview responses. The integrated analysis offers an in-depth view of the insider threat environment, concentrating on the various types of threats, underlying motivations, and behaviors, and proposes defense strategies.

A. Awareness of Insider Threats

One of the central components of this study was to assess the level of awareness among employees regarding insider threats. The findings revealed that an overwhelming majority of respondents (90.6%) were aware of what constitutes an insider threat, while only 9.4% admitted they were unaware. This high level of awareness may be attributed to increased global attention to cybersecurity and to internal capacity-building initiatives conducted within the organization. However, the presence of even a small percentage of unaware individuals highlights the ongoing need for comprehensive and inclusive training.

B. Classification of Insider Threats

Respondents were asked to identify the type of insider threats most commonly observed within their organization. The results showed that 56.2% believed unintentional insider threats were more prevalent, while 43.8% cited intentional threats as the primary concern. This suggests that while deliberate malicious activities are a critical risk, many threats arise from employee negligence, human error, or poor awareness. Hence, organizations must address both behavioral and procedural aspects of insider threat prevention.

C. *Primary Motivations behind Insider Threats*

Table 2: Primary Motivations behind Intentional Insider Threats

Motivations	**Percentage (%)**
Financial gain	64.86%
Personal Grievances	32.43%
External pressure	2.7%
Ideological beliefs	0%
Revenge or retaliation	0%
Other(Specified)	0%
Total	100%

Participants identified various motives behind insider threats. The most frequently cited motivation was financial gain, followed by Personal Grievances, External pressure, and the other coercion, Revenge or retaliation and negligence are not an effect for motivation. The prominence of financial gain aligns with global trends in insider threat cases, suggesting that socio-economic pressures might be influencing employee behavior. Understanding these motives can help organizations tailor their monitoring and mitigation strategies to detect risk

factors early.

D. Prevalence and Sources of Insider Threats

Respondents reported that departments most vulnerable to insider threats included customer service, IT, and sales. These departments typically have access to sensitive customer data and critical systems, making them attractive targets or points of vulnerability. The study found that 62.5% of participants had personally encountered or observed an insider threat incident during their tenure, indicating a relatively high prevalence. This statistic underscores the importance of proactive threat detection mechanisms and the need to cultivate a culture of cybersecurity accountability.

E. Most common causes of unintentional insider threats in Ethio-Telecom

Table 3: most common causes of unintentional insider threats

Cause	Frequency	Percentage (%)
Human Error (E.g, Accidental data leaks)	16	28.07%
Lack of awareness of security policies	18	31.57%
Mismanagement of privileged access	10	17.54%
Use of unsecured devices	13	22.8%
Other (specified)	0	0%
Total	57	100%

The research data demonstrates that insufficient employee understanding of security policies (31.57%) stands as the main cause of internal threats at Ethio-Telecom based on responses from 32 participants. Human errors leading to accidental data leaks proved to be the main contributor to internal security risks at 28.07% while lack of security policy awareness came next at 31.57% (data reveals). Both numbers underscore the necessity for additional staff training. Unprotected devices alongside mismanaged privileged access proved to be significant risks according to the respondents. No respondents specified other causes. These findings stress the importance of comprehensive security awareness programs, device restrictions, and privilege management practices.

F. Assets Most at Risk

The survey indicates that financial data (36.84%) and network infrastructure (36.84%) are perceived as the most at-risk assets, highlighting critical vulnerabilities in the organization's financial management and technical systems. Customer data (26.31%) also emerges as a significant concern, emphasizing the need to protect sensitive client information. Notably, intellectual property (0%) was not identified as at risk, suggesting either limited concerns in this area or a lack of awareness regarding its value. These results stress the importance of implementing robust security measures to protect financial systems, network infrastructure, and customer information.

G. Impact of Insider Threats

Participants were also asked to evaluate the impact of insider threats on the organization. Commonly reported consequences included data leakage, financial loss, reputational damage, and reduced employee morale. Data leakage was the most cited outcome, highlighting the potential for insider threats to compromise customer trust and regulatory compliance. These findings stress the need for stringent data governance frameworks and rapid incident response strategies.

H. Detection and Prevention Measures

The study explored existing measures for detecting and preventing insider threats. A significant portion of respondents acknowledged the presence of basic preventive mechanisms such as access controls, firewalls, and activity logging. However, only a few noted the existence of more advanced tools like behavior-based monitoring or Data Loss Prevention (DLP) systems. This gap suggests an urgent need to modernize insider threat defense capabilities, including the integration of AI-based monitoring and enhanced user behavior analytics.

I. Organizational Policy and Training

When asked about the adequacy of policies and training related to insider threat mitigation, only 40.6% of respondents believed that their organization had well-defined policies in place. Moreover, just over half (53.1%) reported receiving formal training on insider threats. These findings suggest that while awareness exists, institutional support mechanisms such as clear policies, periodic training, and top-down enforcement are still underdeveloped.

J. Common Behavioral Signs of Potential Insider Threats

Table 4: Common Behavioral Signs of Potential Insider Threats

Behavioral Indicator	**Frequency (n)**	**Percentage (%)**
Unusual interest in sensitive data	17	29.31%
Disgruntled attitude or low morale	4	6.89%
Unexplained changes in behavior	10	17.24%
Lack of compliance with security protocols	13	22.41%
Isolation from coworkers	6	10.34%
Increased personal internet usage during work	8	13.79%
Other(Specified)	0	0%
Unanswered	1	1.72%
Total	58	100%

Respondents were allowed to select multiple indicators for potential insider threats. The most frequently cited behavioral sign was unusual interest in sensitive data, reported by 29.31% of respondents. This was followed by lack of compliance with security protocols (22.41%) and unexplained changes in behavior, such as erratic work patterns (17.24%). Additionally, increased personal internet usage during work (13.79%), isolation from coworkers (10.34%), and disgruntled attitudes or low morale (6.89%) were identified as potential indicators. No respondents specified other indicators, and 1.72% left the question

unanswered.

Interview

In this section, we explore the thematic analysis of the semi-structured interviews conducted with key informants in the Ethiopian telecom sector. Thematic analysis was utilized to uncover patterns and themes from the interviews that illustrate the difficulties, strategies, and shortcomings in handling insider threats within the sector. The analysis aims to align with the research objectives and provide actionable insights.

By addressing these different themes, the interview findings provide a comprehensive view of the insider threat landscape and serve as a valuable complement to the survey data. They also inform the development of effective and context-specific defense mechanisms for enhancing cybersecurity resilience. Based on the interviews, the main themes are:

A. Employee Vetting and Background Checks

Employee vetting and background checks emerged as a significant theme during the interviews. While most participants confirmed that their organizations conduct background checks during the pre-employment phase to evaluate potential risks, there was a consensus that ongoing or post-employment background checks are not standard practice. This lack of continuous monitoring poses a critical vulnerability in the hiring process, as employee circumstances, motivations, and behaviors can change over time, potentially introducing new risks that were not evident at the time of hiring. The absence of post-employment background checks means employees with access to sensitive systems and data could become a growing insider threat, particularly if emerging risks go unnoticed. This gap highlights the need for dynamic, continuous vetting mechanisms to strengthen insider threat prevention efforts.

B. Challenges in Implementing Insider Threat Prevention

Organizations face significant challenges in effectively addressing insider threats, including resource constraints, privacy concerns, and organizational resistance to change. Many respondents identified insufficient budgets and a lack of dedicated resources as major obstacles to implementing comprehensive insider threat defense strategies. This often results in inadequate personnel and financial support needed to establish robust prevention programs. Privacy concerns were also highlighted, as interviewees emphasized the need to balance employee rights with the necessity of monitoring and surveillance tools. The fear of infringing on employee privacy rights has led many organizations to adopt a cautious approach, limiting the scope of monitoring solutions and hindering effective threat detection.

C. Use of External Devices

During the interviews, a significant concern that emerged was the utilization of external devices, including USB drives and other forms of external storage, in the systems of telecom companies. While the cybersecurity team is aware of the associated risks, respondents

indicated that various departments, excluding the cybersecurity team, frequently use these devices, leading to potential security vulnerabilities. The absence of a stringent device management policy creates a gap in security measures, allowing external devices to be used freely without proper oversight.

D. Job Rotation and Knowledge Loss

Another critical issue highlighted in the interviews was the absence of job rotation practices within the telecom sector. A number of respondents voiced worries that the introduction of job rotation might result in the departure of seasoned employees, potentially leading to significant financial setbacks for the organization. As a result, employees often remain in the same roles for extended periods, increasing the risk of insider threats. The lack of job rotation poses a significant challenge, as it allows individuals prolonged access to sensitive systems, which can be exploited over time.

E. Inadequate Frequency and Customization of Employee Training

A key issue highlighted during the interviews was the infrequency and lack of customization in the employee training program on insider threats. While the organization has an existing training program in place, it is conducted only once every few years, which presents several challenges. The long intervals between training sessions fail to address the constantly evolving nature of insider threats and do not adequately manage the integration of new employees or role transitions within the organization. This gap means that during the time between training sessions, new employees may be hired, and existing employees may transition to different roles, both of which require role-specific, up-to-date training. Without regular updates or continuous training programs, these employees may not be aware of emerging threats or changes in security policies, which increases the likelihood of inadvertent insider threats.

F. Need for Broader Collaboration and Partnership

During the interviews, it was revealed that the organizations current partnership and collaboration efforts are limited to a single external entity NSAs. However, these collaborations primarily focus on defending against external cyberattacks. There is a significant gap in collaboration and knowledge-sharing when it comes to managing and preventing insider threats. Enhancing collaborations to encompass a wider variety of organizations, such as telecommunications and cybersecurity firms, may yield important knowledge on effective strategies for identifying and addressing insider threats.

G. Lack of AI and ML Integration for Insider Threat Detection

During the interviews, it was revealed that the organization currently does not utilize Artificial Intelligence (AI) or Machine Learning (ML) solutions to detect or prevent insider threats. When asked if there were any plans to implement such technologies in the future, the response was that the organization had no current plans or strategies for AI/ML

integration. However, they recognized the possible advantages of these technologies, indicating that AI and ML could significantly contribute to enhancing the identification and management of insider threats moving forward.

H. Lack of Safe Reporting Mechanism for Suspected Insider Threats

During the interview, it has come to light that the organization presently lacks a secure method for employees to report suspicious activities or possible insider threats. This highlights a critical gap in the company's approach to insider threat management. In the absence of a structured and secure reporting system, workers might be reluctant to bring forward issues of concern, whether because of fears of backlash, lack of confidence in the procedure, or confusion about how to move forward.

I. Employee Support Programs (Transportation and Other Benefits)

It was revealed during the interviews that the company currently does not offer any significant employee support programs, such as free transportation or other benefits. This absence of support programs, which could enhance employee well-being and job satisfaction, highlights a gap in the organization's approach to employee engagement. Programs that offer support to employees, such as transportation services, wellness initiatives, or childcare aid, can enhance morale and job satisfaction, resulting in increased productivity and a greater dedication to the organization's objectives. While these programs are not directly related to insider threat prevention, their absence can lead to disengagement and dissatisfaction, which may have indirect consequences for security efforts. Employees who feel unsupported or undervalued may be less motivated to participate in security initiatives or report suspicious activities. In contrast, providing such benefits can create a more positive work environment, fostering loyalty and trust, which may also improve security efforts by encouraging employees to be more engaged in safeguarding the organization.

J. Motivation and Behavior of Insiders

The problem of insider threats in the telecom sector is complex and driven by multiple underlying motivations and behaviors. According to the interviews, financial pressure is a key reason that drives employees to partake in harmful behaviors. For instance, Employees experiencing financial struggles might exploit their access to sensitive information for personal benefit, including selling confidential data or enabling fraud. This financial vulnerability creates a risk where desperate employees might compromise security in exchange for quick monetary rewards.

5. Discussion

The discussion section of this study aims to utilize the findings from the data analysis

to answer the research questions. Provide insights into the factors contributing to insider cyber threats in the Ethiopian telecom sector.

5.1 Discussions Related to Research Question 1

What are the different types of insider threats in the telecom sector, and how can they be distinguished between intentional and unintentional threats?

Insider threats can be classified as either intentional or unintentional [3]. In the telecom sector, this classification remains relevant, as both types pose significant security risks. Intentional threats involve conscious actions executed by insiders, including data theft, system sabotage, or financial fraud, typically driven by motives such as financial gain or personal grievances. These types of threats may involve employees stealing sensitive data, manipulating systems for financial gain, or intentionally damaging network infrastructure. On the other hand, unintentional insider threats are typically the result of human error, negligence, or a lack of awareness, such as misconfiguring systems, sharing passwords, or inadvertently exposing sensitive information. These threats are not malicious but still pose significant risks due to carelessness or lack of training.

The difference between these two categories of threats is rooted in the reasons for their occurrence. Intentional insiders are individuals who deliberately misuse their access to an organization's resources to cause harm [11]. This action can involve changing data or inserting malware or other pieces of offensive software to disrupt systems and networks [3], whereas a non-intentional insider is someone who unintentionally hurts the company via carelessness, ignorance, or unintentional activities. Non-intentional insider is exposure of an organization’s IT infrastructure, systems, and data that causes unintended harm to an organization. Examples include phishing emails, rogue software, and “malvertising” (embedding malicious content into legitimate online advertising) [3]. To address these risks, telecom organizations must implement extensive security protocols, such as continuously monitoring employee actions. Furthermore, Continuous training and security awareness programs are essential for reducing unintentional insider threats and enhancing employees’ ability to recognize potential security risks. By efficiently handling both intentional and unintentional insider threats, telecom companies can enhance the protection of their confidential information and preserve the reliability of their operations.

5.2 Discussions Related to Research Question 2

What are the motivations and behaviors of individuals who pose insider threats in the telecom sector?

There will always be individuals within an organization or country who act against it intentionally. These actions can be driven by prosocial motivations (e.g., helping an external group), asocial motivations (e.g., personal gain), or antisocial motivations (e.g., retribution) [4]. The motivations of individuals who pose insider threats in the telecom sector primarily revolve around personal and financial factors. Financial gain is the most significant

motivation, with individuals engaging in insider threats to profit from stealing sensitive data or manipulating systems for monetary benefits. Another common motivation is personal grievances, which may include dissatisfaction with job conditions, conflicts with management, or frustration with organizational policies. Interestingly, motivations like external pressure, ideological beliefs, and revenge were not significant factors, highlighting that financial and personal motivations are more dominant in driving insider threats within the telecom sector.

Unintentional insider threats are often caused by employee's lack of knowledge, prioritization of convenience over security [17] [18]. The most common causes involve in telecom is misuse of technology, human error and a lack of awareness of security policies. These causes point to the fact that employees may unintentionally expose sensitive information or mishandle security procedures due to insufficient training or inadequate security awareness. Other significant causes include mismanagement of privileged access and use of unsecured devices, which reflect potential vulnerabilities in day-to-day operations. The behaviors associated with insider threats also provide insight into their motivations and actions. For example, unusual interest in sensitive data was identified as a key behavioral indicator, suggesting a strong focus on confidential or restricted information. Other signs include a lack of compliance with security protocols and increased personal internet usage during work, which may indicate disengagement or an intention to bypass security measures. These behavioral patterns, combined with the motivations, help organizations detect and mitigate potential insider threats more effectively.

5.3 Discussions Related to Research Question 3

What robust defense strategies can be proposed to mitigate insider threats in the telecom sector?

Ethio-Telecom needs to adopt a comprehensive and proactive defense strategy to mitigate the risk of insider threats. Drawing from interviews and research findings, the following strategies have been recognized as effective methods to enhance internal security and decrease vulnerabilities:

1. Implement Comprehensive Employee Training Programs

Educating employees about security policies, social engineering tactics, data protection responsibilities, and potential consequences of insider threats enhances organizational resilience. Well-informed staff are less likely to unknowingly participate in harmful activities and are better prepared to recognize and report suspicious behavior.

2. Periodic / Continuous Background Checks

Conducting background checks before and during employment helps identify individuals with risky behavior patterns or criminal records. Ongoing screening ensures early detection of potential threats, especially for employees in sensitive positions.

3. Endpoint Restrictions for Insider Threat Defense

Limiting the use of external devices (e.g., USB drives), disabling unauthorized

applications, and restricting internet access on specific endpoints minimizes the risk of data exfiltration and unauthorized access to critical systems.

4. Partnerships and Collaborations

Collaborating with cybersecurity experts, telecom regulatory bodies, law enforcement, and international partners can provide access to threat intelligence, best practices, and incident response support. These partnerships help organizations stay ahead of evolving insider threat tactics.

5. Adoption of AI and Machine Learning for Insider Threat Defense

Using AI and ML algorithms enables organizations to detect abnormal patterns in user behavior, such as unusual login times or unexpected data transfers. These technologies improve threat detection accuracy and reduce response times.

6. Periodic Access Review

Consistently assessing employee access permissions guarantees that individuals have access solely to the systems and information pertinent to their current positions. This minimizes the risk of privilege misuse and thwart unauthorized access by former employees or individuals who have transitioned to different roles.

7. Simulated Attacks

Running simulated phishing attacks or internal threat exercises helps evaluate employee readiness, identify weaknesses, and improve incident response strategies. It also encourages a proactive security culture within the organization.

8. Job Rotation

Rotating employees between different roles or departments limits the opportunity for malicious insiders to exploit long-term access to sensitive resources. It also allows organizations to detect inconsistencies and potential fraud that may go unnoticed in fixed-role settings.

9. Whistleblower Channels

Establishing secure and anonymous channels for reporting suspicious behavior encourages employees to come forward without fear of retaliation. This helps uncover potential threats early and promotes a culture of accountability.

10. Addressing Employee Concerns

Unresolved complaints, dissatisfaction with jobs, and stress in the workplace often drive insider threats. Companies that take the time to hear and address employee issues are more inclined to foster trust and lessen the risk of deliberate harm.

11. Time-Based Access Control (TBAC)

TBAC restricts system or data access to designated periods according to operational requirements. For instance, employees might be permitted to access sensitive databases solely during business hours. This minimizes the chance for unauthorized access during off-hours or times when supervision is not present.

6. Conclusion

This study has discussed insider cyber threats in the Ethiopian telecom industry, focusing on the driving factors, actions, and classification of the threats. The study found that both significant intentional and unintentional threats are posed to critical organizational assets, including sensitive customer information, financial data, and network infrastructure. Intentional threats typically occur in familiar ways: data breaches, financial fraud, and disruptions to systems. In contrast, unintentional threats often stemmed from negligence or insufficient security awareness among employees.

Some of the key challenges identified were a lack of visibility over employee activities, limited monitoring tools available, and employees not being aware of cybersecurity risks. The report concludes that the fight against insider threats requires a proactive multi-layered approach combining technological solutions with employee engagement and continuous assessment of threats. The strategies of Mitigation need to go beyond technological defenses in fostering a culture of security awareness and vigilance among employees.

Moreover, the research pointed out that organizations need continuous oversight of their security approaches and investment in modern technologies, including artificial intelligence-based behavioral monitoring tools. These tools significantly enhance the detection and prevention of insider threats through the identification of anomalies in employee behavior.

Defending against insider threats is complex and requires more than just technical solutions. It involves access control, monitoring, and system hardening to prevent both accidental and intentional harm.

Based on the study's findings, the following key strategies are recommended:

Employee Training: Offer role-specific security awareness programs covering insider threats, data protection, and how to report suspicious activity.

Employee Well-being: Address staff concerns through performance-based rewards, financial advice, and open communication to reduce risk factors.

Behavior Monitoring: Use AI-driven tools to detect unusual behavior while maintaining trust.

Background Checks: Conduct periodic checks to identify financial or personal risks that may lead to insider behavior.

Access Control: Apply least-privilege principles and regular access reviews. Implement Time-Based Access Control (TBAC) to restrict access outside working hours.

Whistleblower Channels: Establish safe, anonymous reporting systems to encourage alerts without fear of retaliation.

Simulated Attacks: Run insider threat simulations to test response and improve protocols.

Job Rotation: Rotate roles to prevent any one person from gaining excessive control,

especially when paired with TBAC.

These strategies collectively create a strong, proactive defense against insider threats, fostering a secure and aware organizational culture.

References

[1] M. Sneps-Sneppe1, D. Namiot2, R. Pauliks1," information system cyber threats and telecommunications engineering courses", latvian journal of physics and technical sciences 2020, n 1-2 doi: 10.2478/lpts-2020-0007

[2] Eden Teklemariam, "user behavior-based insider threats detection using few shot learning", AAU School of Electrical And Computer Engineering

[3] Fortinet,https://www.fortinet.com/resources/cyberglossary/insider-threats

[4] Multiple Approach Paths to Insider Threat (MAP-IT): Intentional, Ambivalent and Unintentional Insider Threats "https://citrap.scholasticahq.com/article/37117-multiple-approach-paths-to-insider-threat-map-it-intentional-ambivalent-and-unintentional-insider-threat "

[5] Mixed Methods Research – Types & Analysis Mixed Methods Research - Types & Analysis - Research Method

[6] Georgia Bafoutsou, Slawomir Bryska, Marnix Dekker, " CYBER THREATS OUTREACH IN TELECOM", ENISA (European Union Agency for Cyber security) March 2022.

[7] E. M. Onyema, A. E. Dinar, S. Ghouali, B. Merabet, R. Merzougui, and M. Feham," Cyber Threats, Attack Strategy, and Ethical Hacking in Telecommunications System, " August 2022, https://www.researchgate.net/publication/363061476

[8] U.S Department of Homeland Security (United States Secret Service, CERT, "Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector," January 2008

[9] Kaspersky security intelligence, "Threat Intelligence Report for the Telecommunications Industry"

[10] Markus Kont, Mauno Pihelgas, Jesse Wojtkowiak, Lorena Trinberg, Anna-Maria Osula,"Insider Threat Detection Study", CCDCOE, NATO Cooperative Cyber Defense Center of Excellence Tialilinn, Estonia, www.ccdcoe.org, publications@ccdcoe.org

[11] Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.

[12] Infosys Knowledge Institute," assuring digital- trust in telecommunication", www.infosys.com/services/cyber-security/insights/cybersecurity-telecom.pdf

[13] Lisa Schwarz-, Oracle NetSuite, "Top 24 Challenges Facing the Telecom Industry Today", June 11, 2024, www.netsuite.com/portal/resource/articles/erp/telecom-industry-challenges.shtml

[14] Forbs, "15 Ways Technology Can Drive Innovation and Improve Your Offerings", www.forbes.com/councils/forbesbusinesscouncil/2023/04/10/15-ways-technology-can-drive-innovation-and-improve-your-offerings/

[15] Leyew, Bewketu, "A Liberalized Telecommunications Sector for Ethiopia: the Regulatory Frame work and Its Prospect", Addis Ababa, 2007-06, www.etd.aau.edu.et/items/1922232f-b291-4160-8bc6-4ba358f07099

[16] Neetesh Saxena, Emma Hayes, Elisa Bertino, Patrick Ojo, Kim-Kwang Raymond Choo and Pete Burnap, "Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses", 7 September 2020

[17] Zac Amos, "Common Insider Threat Motivations and Prevention Tactics", Thetek, www.thetek.com/common-insider-threat-motivations-and-prevention-tactics/, 04/29/22

[18]Proofpoint, "The Primary Factors Motivating Insider Threats", www.proofpoint.com/us/blog/insider-threat-management/primary-factors-motivating-insider-threats , September 17, 2019

[19] Behabtu Amare, "Assessment of Insider Threat in Ethiopian Banking Industry", Addis ababa university school Of graduate studies school of Information science. Workshet Lamenew (Phd), JUNE, 2015

[20] Ponemon Institute, "2022 Cost of Insider Threats Global Report", 2022 Cost of Insider Threats Global Report, Accessed: 30-10-2022.

[21] Holger Schulze, "New Report reveals insider threats trends , challenges and solutions ",New Report Reveals Insider Threat Trends, Challenges, and Solutions - Cybersecurity Insiders , email: info@www.cybersecurity-insiders.com