ISSN:0975-9646

A Survey of Unintentional Medical Insider Threat Category

Jason Slaughter[#1], Dr. Kellep Charles, Ph.D.[#2]
Capitol Technology University
11301 Springfield Rd, Laurel, MD 20708, United States
[1]jslaughter@captechu.edu, [2]kacharles@captechu.edu

***Abstract*— Unintentional Insider Threat has the concept that an insider threat event may occur unintentionally versus maliciously. This survey proposes a new category of unintentional insider threat called the medical insider threat where the insider may be experiencing a medical problem causing their behavior. This article will be the first in a series of three articles on unintentional medical insider threats. Starting with a Qualtrics survey conducted over two months to perform a qualitative analysis if this additional type of unintentional insider threat should be added as a distinct sub-type under unintentional insider threat for the cyber security community.**

***Keywords*— insider, threat, detection, targeted, medical**

INTRODUCTION

Due to human behavioral factors not being well represented in structured models [1] detection of behavior changes caused by medical events has not been researched sufficiently in cybersecurity insider threat programs.

This study will provide additional insight into the detection of unintentional insider threats that have been or may be produced by a medical problem occurring.

While this study will focus on a medical condition causing an insider threat, the research can later be generalized to additional insider threat types and insider threat programs across government, academia, and industry.

The study will use me and my medical background as one example of a potential unintentional insider threat that is created due to a medical condition as opposed to a psychological condition or malicious intent. Additionally, two other Solider cases that can be found in open-source intelligence (OSINT) will be used to compare and contrast symptoms and outcomes.

Sentiment analysis is a type of natural language processing (NLP) that involves using computational techniques to identify and extract subjective information from text data. It is often used to determine the overall sentiment or emotion expressed in a piece of text, such as whether it is positive, negative, or neutral.

There is some evidence to suggest that sentiment analysis can be used to detect unintentional insider threats, as employees who are feeling stressed or overwhelmed may express negative sentiments in their communication that could indicate a potential risk. However, it is important to note that sentiment analysis is not a perfect solution and may not always be able to accurately identify every potential insider threat.

There are several research studies that have explored the use of sentiment analysis for detecting insider threats. For example, the following study [2] used sentiment analysis to identify potential insider threats in social media data.

Background

The background of this study starts with Soldiers who believe they were being targeted. In recent history, open-source intelligence (OSINT) reports of Soldiers who believe they are being targeted have been released in various news articles and on social media.

The intent of the study is to determine if there is a way to use natural language processing (NLP) such as sentiment analysis to detect if a Soldier feels they are being watched or targeted and to take appropriate action.

Following are three cases of Soldiers who felt they were being targeted or followed and the outcomes of those cases.

One high-profile report was of Major General Gregg F. Martin (Ret.) (https://ibpf.org/meet-your-bipolar-general/) who believed that due to where he had been and what he knew that he was being targeted by some unknown actors.

It was later determined that General Martin (Ret.) had bipolar and that he had exhibited symptoms of the condition for his entire career. They eventually came to a critical point when he called a previous commanding officer and began asking if he was being targeted.

The next Soldier in this study was Michael Froede (https://www.stripes.com/multimedia/podcasts/military_matters/2022-07-05/fast-take-michael-froede-podcast-6549018.html) who after returning from Vietnam on a mission believed he was being targeted. It was later determined that Michael Froede's problems began as a result of traumatic brain injury (TBI) that was untreated. The untreated TBI appears to eventually lead to paranoid hallucinations and eventually to the Soldier's suicide.

The next section of the background is my story and how this study began and why I chose this topic of study.

Looking back now, it was around July 2016 when I first started having paranoid thoughts and became sensitive to people speaking around me but not directly to me.

My wife and I were on a cruise to Roatan and then to Mexico for a small vacation while I was working for the Department of Veterans Affairs as a GS13. I had previously performed a lateral transfer as a GG13 from the DoD where I worked at Joint Interagency Taskforce South (JIATFS) supporting their mission.

While there, I received various training in counterintelligence. I was also a prior service member trained in combat arms and performed Short Range Air Defense (SHORAD) in support of U.S. Army missions.

While on the cruise, I heard an individual talking about how they had just retired after twenty years from the FBI and I found that odd and mentioned to my wife that normally you wouldn't hear someone say that to random strangers on a cruise ship. I became more alert after this happened.

My wife and I debarked from the cruise ship in Roatan and began walking around looking at the shops inside the fenced area. We decided to walk over to the mall that could be seen outside the fence.

Two things happened next. As we were leaving the fence a young male began to shadow us all the way into the mall area. I assumed he was a pickpocket and mostly ignored him until he got close to us. I told my wife I wasn't comfortable in the area and we left to walk back to the cruise liner.

As we were walking in the gate a current or prior service member looked at me and asked how it was out there. I mentioned that we had observed the young male shadowing us and I wasn't comfortable in the area. He related that he had been on a mission in the area years prior and looked at his wife and

told her they were getting back on the cruise. We didn't see or speak to them after that.

On arriving back at the Department of Veterans Affairs all seemed to be normal. However, I was much more tense and on alert to things happening around me.

I was on a phone call and the project manager at the time yelled at me in front of the entire team and customers about changing dates to timestamps for better security auditing.

Later my supervisor accused me of saying something to a contractor that was never said. At this point, I was under more work-related stress because of things that were said. I requested to be moved to a new supervisor and new project manager after working for them for over three years.

They said I was crazy and didn't know what I was talking about. These events could have been indicator one in an unintentional insider threat scenario.

I sent numerous emails during the timeline at the Department of Veterans Affairs between August 2014 and September 2017. These emails could have potentially been used to detect an anomaly using natural language processing techniques such as sentiment analysis.

Finally, in 2017 I began working for the Executive Director of VA's Office of Accountability and Whistle Blower Protection. While working for this office everything seemed to calm down. They had moved me to work full-time remotely and I couldn't hear what anyone was saying or at least what I thought they were saying. I went on to help create the Veteran Affairs (VA) Veteran Identity Card (VIC) software and helped to deploy it worldwide.

In September 2017 I applied for a new position in the U.S. government as a CG14 for the FDIC working as Sr. Enterprise Cybersecurity Architect.

When I started things seemed reasonably normal for any Federal agency but that quickly changed. I was sitting in my office when my supervisor came in to talk to me about a company I owned at the time.

I created a corporation with the intent of automating e-commerce activities. As a civil servant, I was required to disclose the purpose and scope of the company to the FDIC ethics team.

During the conversation regarding this, we heard loud banging in the pipes above our heads. The supervisor mentioned they were probably just dropping cables for connections.

My mind immediately went to they are putting in listening devices. The paranoia was back in full swing. I went to a local Target store with my wife a few weeks later and thought someone said that they had her phone.

I kept hearing conversations down the hallways in the FDIC that sounded like I was under investigation for something. Then everything got worse. I was convinced my family was being targeted.

At first, I thought it was someone saying I leaked classified material and then I thought it was worse and it was one of the country's various enemies targeting us because of my time working for the Department of Defense and the Intelligence Community. I asked a co-worker at the FDIC if there was any reason a Federal agency would tell me they were taking my family out the back and I should go to work as normal and leave through the front. This was one of the many other opportunities where an insider threat program could have detected an anomaly.

Eventually, while all of this was occurring over years, I finally had a full seizure at work. I woke up in the hospital thinking that five eyes (FVEY) were watching me and that one of my FDIC co-workers was a member of them. I thought another co-worker was a handler and I should be listening to him and that the needle they were using to do the spinal tap on me was to give me a lethal injection for something I had done.

I went home after the temporal lobe seizures at work and continued to have severe paranoia and what my wife called hypervigilance. I was convinced that my family was still being targeted.

I was still a full-time employee of the FDIC during this period. A couple of other odd events happened while I was on medical leave with the FDIC. The landlord mentioned that one of the other tenants worked for the Secret Service also just out of nowhere. I wasn't close with the landlord and found this very odd and it raised my threat awareness. The second event happened while my wife and I were walking on trails and an obviously military or law enforcement person walked past my wife and me and told his wife that "he's not one of mine". Which also raised my threat awareness.

During these events, I was on social media. I began posting messages on Twitter, Facebook, and LinkedIn stating that I thought I was being targeted and leaving what I thought at the time were keywords or trigger words that would have someone go look into what was happening. This would be at least the third time that an insider threat program using natural language processing (NLP) could be used to detect the anomaly in both the patterns of text and the content of what was being said.

Finally, after several more visits to the hospital, they determined that I was having temporal lobe seizures. Most likely brought on by the underlying issue of idiopathic hypersomnia and the various sleep issues that I still have today. Although they are now controlled with medications.

Once everything was medically under control, I was able to look back at the events and understand the root cause. If an insider threat detection tool had existed to detect these anomalies and medical intervention had been performed sooner, the risk to the organizations would have been greatly reduced. As it stands, I didn't end up being an unintentional insider threat. But that is mainly because of training and my mentality. Outside detection and responses did not limit the chance for unintentional disclosures. In fact, my family and friends were primarily responsible for making sure there really wasn't a threat.

Purpose of the Study

According to [1] the study of unintentional insider threats is an important area of research that aims to understand and identify the risks associated with employees who may accidentally or unintentionally expose an organization to security risks. This can include employees who may be unaware of the potential consequences of their actions, who may be overwhelmed by their workload or personal stress, or who may simply make a mistake due to a lack of training or awareness.

Unintentional insider threats can be difficult to identify and prevent, as they may not be motivated by malicious intent. However, they can still pose a significant risk to an organization, as they can potentially expose sensitive information, disrupt operations, or compromise the security of the organization.

The purpose of the article is to contribute original research into a potentially new type of insider threat called the medical insider threat type.

This insider threat type will be defined as an unintentional insider threat who has a medical condition that causes alterations in their behavior or cognitive abilities.

A future article will use a subset of medical conditions to create a sample of possible medical problems that could lead to this unintentional insider threat scenario.

Original handwritten journals, social media (OSINT), email, and text messages will be used for the sample data in future articles.

Theoretical Framework

Employees and other insiders may exhibit changes in behavior, language, or communication patterns that indicate a potential

risk of unintentional insider threat. These changes may be caused by factors such as stress, burnout, or other psychological or social issues or medical issues.

Sentiment analysis is a method of extracting and analyzing the emotional or evaluative content of text or speech data. It can be used to identify patterns of sentiment or emotion in large datasets of communication, such as emails, chat logs, or social media posts.

The use of sentiment analysis in the detection of unintentional insider threats can be guided by theories or models of human emotion and cognition, such as the appraisal theory of emotion or the cognitive load theory. These theories can provide a framework for understanding how employees' emotions and cognitive processes may influence their behavior and decision-making, and how these factors may be related to the risk of unintentional insider threat.

To detect unintentional insider threats using sentiment analysis, organizations may need to develop appropriate data collection and analysis processes, such as designing and implementing sentiment analysis algorithms or choosing appropriate data sources and sampling methods. These processes should be guided by considerations such as data quality, ethical and legal considerations, and the need to protect employees' privacy.

To validate the effectiveness of sentiment analysis as a means of detecting unintentional insider threats, organizations may need to conduct empirical studies or experiments to assess the accuracy and reliability of the methods and tools used. These studies may involve using real or simulated data or may involve collecting data from employees or other insiders through surveys or other methods.

Research Questions

Definition of a medical insider threat: A trusted employee who has had for example a seizure or significant health event that leads to out-of-character behavior or decline in cognitive abilities both in and out of the workplace.

The following research questions will guide the study:

1. RQ1: Should a new type of insider threat be added to the common model of types currently existing? The medical insider threat.
2. RQ2: Is a combination of cyber threat intelligence and sentiment analysis sufficient to detect insider threat types defined in academic literature and industry?
3. RQ3: Given a medical insider threat should psychology or medical professionals be added to the insider threat response and mitigation team?

Nature of the Study

A literature review was conducted using a selection of keywords around sentiment analysis, insider threat, and targeting for each of the articles in the series.

Additionally, keywords around behavior detection and insider threat were researched.

A qualitative analysis was conducted using three research questions and control questions created in a Qualtrics survey instrument. The questions were submitted to the cybersecurity community through Qualtrics and the responses were anonymous to include removing the IPs of the respondents.

A qualitative analysis of the responses was conducted to determine if the cybersecurity community believes a medical insider threat should be added to the known threats for an insider threat program. Results are provided in both graphical and written formats.

A table was used to document human behavior associated with a medical insider threat. The table is based on known behavior from medical conditions selected for the research.

Significance of the Study

This study furthers the research on insider threats and proposes a new type of insider threat known as a medical insider threat. The study looks at the insider threat from a behavioral standpoint versus a network activity standpoint.

The research contributes to behavioral theory in cybersecurity by providing research into a medical event such as an altered mental state from a seizure, traumatic brain injury, or diabetes and how insider threat programs detect these events.

LITERATURE REVIEW

There have been many authors who have contributed to the study of unintentional insider threats in the field of cybersecurity.

Richard A. Clarke and Robert Knake, authors of the book "Cyber War: The Next Threat to National Security and What to Do About It" (2010) [3], discuss the risks and consequences of unintentional insider threats in the context of cyber warfare.

The concept of using machine learning such as sentiment analysis has also been widely discussed and researched.

[5] This paper concludes that sentiment analysis can be used to detect anomalies in social media data. The proposed method is tested on tweet data and the results demonstrate its capabilities for anomaly detection through sentiment analysis. Additionally, this study surveys existing methods of both anomaly detection and sentiment analysis, as well as their limitations and challenges.

[6] This paper concludes that RBEM-Emo is a promising approach for emotion detection. It advances the current state-of-the-art in sentiment analysis beyond polarity and uses Plutchik's wheel of emotions model to detect such emotions from human written messages. The performance of this algorithm was evaluated on two different datasets, compared with existing techniques like a recursive autoencoder, and found to be better than them.

[7] This paper proposes a constraint optimization framework for detecting emotion from the text. The proposed model is linear in the input size and hence suitable for large datasets. It can be easily configured to add new features as well as incorporate refined emotion lexicons, which helps improve its performance further. This inference algorithm solves multi-label classification problems i.e., it allows documents to have multiple emotions assigned at once or pick one single most dominant emotion category per document; additionally, categories are also assigned to words that help expand existing emotional lexicon databases used by our system. Promising empirical results on three diverse datasets after testing the model's accuracy with different constraints such as topic correlations, specialized features suggested by prior work, and established emotional lexicons like NRC Emotion Lexicon, etc.

[8] This paper proposes a novel idea for solving the problem of identification of emotion intensity from social media data. It suggests that algorithms can be used to identify the strength/intensity of emotions expressed in informal and short text messages on sites such as social networking, blogs, etc. The proposed method could help us understand how strongly people feel about certain topics or towards their friends by analysis of these texts.

[9] This paper concludes that a text-mining model can be used to detect emotions in texts. The dataset used was the best-worst scaling technique, which has been classified by previous researchers into four emotional categories: anger, fear, joy, and sadness. Naive Bayes classifiers were employed as the method

optimized by particle swarm optimization for this research project. Results showed high accuracy when compared with other types of research projects on similar datasets; it also provided good classification performance even though its characters differed from most datasets tested before.

[10] This paper concludes that the amount and variety of data generated through social media sites have increased significantly. Personal information is included in this data, making it important to process the data for meaningful insights. An example application was developed using Twitter as a platform to classify crimes according to Turkish Statistical Institute criminal records and keywords were defined accordingly. A total of 150,000 tweet data from Turkey was collected between specified dates which revealed 56% of people talking about terrorist attacks or bombing incidents on those days with words like "bomb", "terror", etc having 24%, 12%, and 8% respectively among them. Correlations are found between different situations by expanding keyword groups so bigger masses can be accessed easily for a better understanding of the real situation at hand.

Table 1 describes a sample of medical conditions that this study will use to detect Unintentional Medical Insider Threats. These conditions could lead to possible Unintentional Medical Insider Threats and may be detectable using sentiment analysis of changes in the sentiment or patterns of writing the individual is producing.

TABLE I
TABLE OF MEDICAL PROBLEMS OF UNINTENTIONAL MEDICAL INSIDER THREATS

Medical Condition	Description
Epilepsy	A neurological disorder characterized by recurring seizures.
Encephalitis	Inflammation of the brain can cause seizures and other neurological symptoms.
Meningitis	Inflammation of the membranes surrounding the brain and spinal cord, which can cause seizures and other neurological symptoms
Stroke	A disruption of blood flow to the brain can cause seizures and other neurological symptoms.
Traumatic Brain Injury	An injury to the brain caused by an external force can cause seizures and other neurological symptoms.
Alcohol Withdrawal	Abrupt cessation of alcohol consumption can cause seizures and other neurological symptoms.
Brain Tumors	Abnormal growths in the brain can cause seizures and other neurological symptoms.

Research Methodology

The research method will be a qualitative analysis using a Qualtrics survey to collect the responses of the cybersecurity community on the research questions and control questions. The qualitative analysis will be on the question responses.

Population

The participants of the research will be anonymous members of the cybersecurity community. Control questions will be administered as a verification step to determine the level of cybersecurity expert the respondent is.

Additional members of the study include three Soldier's cases developed from OSINT data, journals, emails, and text messages over the selected time period.

Sample

The following images contain the output of the Qualtrics survey.

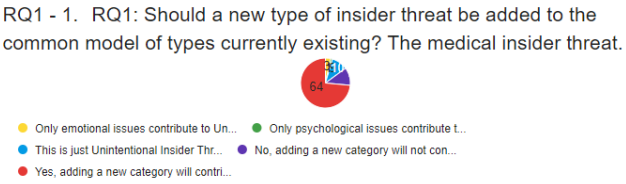

Image 1
RQ 1

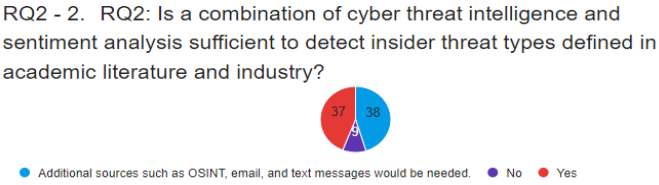

Image 2
RQ 2

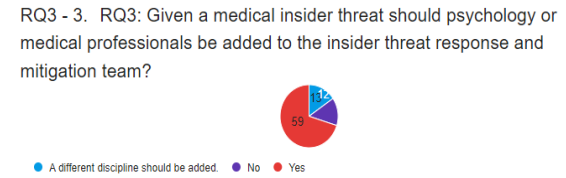

Image 3
RQ 3

Image 4
Control Question 7

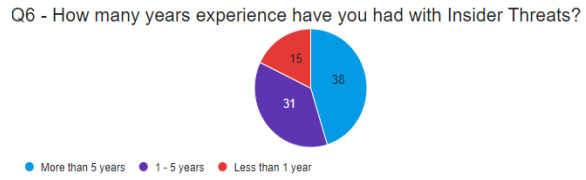

Image 5
Control Question 6

Materials/Instruments

A Qualtrics survey was conducted over a two-month period to collect responses from the cybersecurity community. The Qualtrics company was engaged to provide the survey with greater reach and improved metrics. The Qualtrics company put together a sample board to review the research questions and answer them using qualitative responses.

Additionally, fourteen responses were received from social media and direct outreach to individuals within the cybersecurity community who were interested in contributing and answering the survey. Qualtrics was paid three thousand dollars to validate that they could get sixty-seven responses based on the criteria of the survey. Qualtrics was paid an additional thousand dollars for the license they were required to have a support contract attached to it.

Data Collection and Data Analysis

Data was collected over a two-month time period. Some of the data were collected using the Qualtrics paid services and a small portion of the data was collected using social media links to LinkedIn, Facebook, and Twitter.

The total number of those surveyed was 91 respondents who met or exceeded the control question criteria.

The survey takers were cybersecurity professionals with between one to greater than five years of experience. The survey indicates that the majority of the community sampled falls in the greater than five years of experience in cybersecurity. Further, the survey indicates that the majority of those surveyed have greater than five years of experience with insider threats.

The results of the RQ1 indicate that a new category is needed. And further research should be conducted into how this category should be added to the existing categories of intentional and unintentional insider threats.

The results of RQ2 indicate that cyber threat intelligence (CTI) and sentiment analysis may be sufficient to detect an unintentional insider threat but the results are split with thirty-seven for yes and thirty-eight for additional data is required.

The results of RQ3 indicate that medical and psychological staff should be added to insider threat programs to assist with the detection and response of unintentional insider threats.

Based on the survey responses, the results were interesting in that RQ1 indicates there is a need for a new category. Given greater categorization of the topic, further research could be applied to this specific area and the correct resources with the correct skill sets could more effectively be assigned for detection.

RQ2 was very limited in that it only states that CTI and sentiment analysis alone is not enough to detect an unintentional medical insider threat. Future research will use the ALIAS technology for both sentiment and topic analysis to further explore how correct this response is.

RQ3 is the most interesting in that it indicates additional resources should be added to the insider threat response team. Given a panel of experts in psychology and medicine, it may be effective to pass portions of the detection process to this team. For instance, if an individual has had a seizure, both groups will understand the ramifications and the potential issues versus the cybersecurity experts having to become proficient in psychology and medicine on top of their current expertise in cybersecurity.

Assumptions

The data collected provides a sample of how cybersecurity feels about adding an additional category to unintentional insider threats called the medical insider threat.

It is assumed that all answers provided were in good faith and to the best of the knowledge of the individuals submitting the responses.

This article assumes that unintentional insider threat is too broad of a category given the nuances involved in insider threat and seeks to further refine the discussion on the topic to the root cause of the unintentional insider threat, which in this case is a medical problem.

Limitations

The survey was limited in size due to time constraints and monetary constraints on the researcher. The survey could be expanded to reach a wider audience given more time and resources.

Ethical Assurances

The survey did not collect any identifying information about the respondents. All survey takers are anonymous. No publicly identifiable information (PII) has been captured or produced by this article beyond the names present in the acknowledgments section.

SUMMARY

Insider threat whether intentional or unintentional is a significant issue for all organizations that seek to protect their information.

The proposed category of unintentional medical insider threat is meant to add an additional area of research to the topic and to further focus on the detection and response to this type of threat.

This article is meant to both propose the new category of unintentional insider threat and to contribute to new research on the category.

Future articles will focus on the detection of the unintentional medical insider threat using tools and techniques such as sentiment and topic analysis using software known as ALIAS to perform an analysis on open-source intelligence such as Twitter feeds and handwritten accounts of potential unintentional medical insider threats who thought they were being targeted.

Acknowledgment

Jason Slaughter wishes to acknowledge the following individuals:

- Dr. Kellep Charles Ph.D.
- Dr. Carole E. Chaski Ph.D.
- Supporting family.
- Supporting team members at MITRE. - *The author's affiliation with The MITRE Corporation is provided for identification purposes only and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.*
- Brian Seborg
- Jay Fultz

REFERENCES

[1] F. L. Greitzer et al., "Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies," 2014 47th Hawaii International Conference on System Sciences, 2014, pp. 2025-2034, doi: 10.1109/HICSS.2014.256.

[2] Kim, J., Lee, H., & Kim, D. (2018). Insider threat detection using sentiment analysis on social media data. International Journal of Information Management, 41, 15-23.

[3] Clarke, R.A., & Knake, R. (2010). Cyber War: The Next Threat to National Security and What to Do About It.

[4] Zhaoxia, Wang., Victor, Joo., Chuan, Tong., Xin, Xin., Hoong, Chor, Chin. (2014). Anomaly Detection through Enhanced Sentiment Analysis on Social Media Data. 917-922. doi: 10.1109/CLOUDCOM.2014.69

[5] Erik, Tromp., Mykola, Pechenizkiy. (2014). Rule-based Emotion Detection on Social Media: Putting Tweets on Plutchik's Wheel. arXiv: Computation and Language

[6] Yichen, Wang., Aditya, Pal. (2015). Detecting emotions in social media: a constrained optimization approach. 996-1002.

[7] Sonia, Xylina, Mashal., Kavita, Asnani. (2017). Emotion intensity detection for social media data. 155-158. doi: 10.1109/ICCMC.2017.8282664

[8] Erfian, Junianto., Rizal, Rachman. (2019). Implementation of Text Mining Model to Emotions Detection on Social Media Comments Using Particle Swarm Optimization and Naive Bayes Classifier. doi: 10.1109/CITSM47753.2019.8965382

[9] Serkan, Savaş., Nurettin, Topaloğlu. (2019). Data analysis through social media according to the classified crime. Turkish Journal of Electrical Engineering and Computer Sciences, 27(1):407-420. doi: 10.3906/ELK-1712-17.