A Research Review

Countering Insider Threat:

Understanding the Bias Mindset While Determining a Response to an Insider Event

Jason Barnhart
ED 520
18 Apr 21

Summary

Biases in Insider Threat reporting and analysis, including cognitive, heuristic, and gender biases, affects how an incident is investigated, managed, and resolved. They can negatively affect an Insider Threat Program (InTP) and deterrence actions if the organization has incorporated perceived or unconscious bias into policy followed throughout the organization. Barnhart argues that while the overall tools and resources for InTPs have improved, bias still presents an area of concern for InT Professionals even when utilizing available tools and techniques. He provides readers with an overview of variations of bias in character or emotion, cognitive or intelligence ability, heuristics, and gender. Barnhart recommends that managers at all levels, especially those who oversee InTPs, understand and can identify bias to ensure that actions taken to mitigate Insider Threats are not thwarted.

Abstract

Understanding Insider Threat characteristics, behaviors, and the resulting effects is essential to any public organization or private agency. Security professionals, human resource personnel, legal departments, and organization management will more than likely be confronted with an insider threat incident, but not necessarily because incidents are on the rise. More so due to the business practices and operational awareness in society to 'prevent, detect, and respond to' (Cappelli, 2012) the insider threat. Countering the insider threat begins with the utilization of available tools and theories of analysis to manage actual incidents. An area of concern when utilizing such tools and techniques is to mitigate any bias when reviewing the data or investigation report. Bias has been identified, through perception and detected evidence, in how an incident is investigated, managed, and resolved based on bias from both the insider and the victim organization. Reviewing causes of bias, such as gender, heuristics, and intelligence, are necessary to further support efforts in improving InTPs and activities.

Contents

Section 1 - Introduction

Insiders, those who are employed by a company, organization, or agency, are considered a large and growing threat to the loss, compromise, theft, sabotage, or destruction of resources for employers (Cappelli, 2012). Insiders may also cover those who volunteer, assist, or collaborate through an agreement or common process with another organization, agency, or Government bureau. Realizing the threat to information, information systems, fiscal resources, or personal information is not the sole purpose of an InTP. Gaining insight, knowledge, and proactive policy to detect, prevent, and respond to insider threat activity in today's world has become a norm (Cappelli, 2012). Organizations have invested time and money into developing procedures, technology, and awareness to the whole of a company to mitigate an incident or potential incident from occurring. A slight sliver of this developing posture is understanding insider threat characteristics, behaviors, and the resulting effect to identify and implement useful tools in identifying insider activity or risk factors. These tools will help maintain normal operations and minimize the damage from an insider threat event.

Useful tools for a solid InTP are active and being further improved to assist corporations and Government agencies in providing information and data for analysis to prevent an insider threat. These same tools can be utilized to update policy, procedures, and training awareness to prevent insider threat actions after an incident occurs. Countering the insider threat also begins with utilizing available tools and theories of analysis to manage actual incidents.

An area of concern when utilizing such tools and techniques is to mitigate any bias when reviewing incident data, user activity, which may be the nexus of an insider threat event, or bias from practical methods when applied during an investigation. Bias can negatively affect an InTP and deterrence actions if the organization has incorporated perceived or unconscious bias into policy followed throughout the organization. This can hurt the employee by leading to false positive cases; have a shadowing effect to an investigation; hinder an organization's ability to fully implement insider threat prevention due to fear of discrimination for a myriad of reasons. Studying the causes of a bias nature in areas such as gender, heuristics, and intelligence are necessary to further support efforts in improving InTPs and activities. With this in mind, a review of insider threat data that is filtered, analyzed, and included for review must be aware of such bias to maintain program value.

Section 2 - Variations of Bias

When conducting the initial review of periodicals for understanding bias in analysis, one may think the search parameters would result in a small and similar set of comparisons or viewpoints. However, there are a multitude of ways bias is determined or identified, which has an equal effect on how insider threat is studied, analyzed, and countered. Consistent results returned to a small set of biases or risks to research or analysis techniques. This small set included bias, perceived or verified, in character or emotion, cognitive or intelligence ability, heuristics, and action or outcome based on gender.

Regardless, bias traits may be evident in how insider threat situation are detected and deterred. Knowing this aspect is key to making sure InTPs remain a viable solution in stopping damaging acts for every employer.

Sub-Section A - Emotional/Character/Behavioral Bias

The first bias aspect of analysis which may affect InTPs is geared to the emotion or character of an individual (Ho, 2008). How do we see the employee and the level to which they will comply with policy and procedures? Will they ensure to maintain proper practices to a proactive security environment? This may go for any employee, to include the victims (e.g., company, co-worker, and customer) or even those who work the problem (e.g., security, law enforcement, financial auditor, and lawyer). Basically, can anyone be trusted fully? This point confirms the need for an InTP, as well as oversight of the program. In the article *Behavioral Parameters of Trustworthiness for Countering Insider Threats,* Shuyuan Ho explains,

> 'To be able to tell if the employee is trustworthy is thus determined by the subjective perceptions from the individuals in his/her social network that have direct business functional connections, and thus the opportunity to repeatedly observe the correspondence between communication and behavior.' (Ho, 2008)

What Ho is verifying in this study falls in line with how the continuous evaluation process under Personnel Security utilizes an individual's social media information and connections, if such accounts are public, to validate a person's loyalty and trustworthiness to access sensitive or classified information. Same for an employee's social network (e.g., security investigation references, social references) being verified not only during a personnel security investigation, but also if an individual is suspected of being a potential insider threat requiring further threat analysis from key stakeholders (e.g., supervisor, security, human resources, and IT).

From a negative aspect, the concern is heavily reliant on one's social network for the basis of determining a level of trust. Security professionals and employers must rely on a much larger picture when assessing an individual's trust, as well as an individual who may be a wiling or unwilling insider. Employees who are unwilling insiders are merely doing their job when they unknowingly click on a link in an email or surf a website leaving a company's network open to attack. In this scenario, one's social network may or may not play a role in a threat event. However, HO provide validity to this point for those insiders who are willing participants.

> 'Thus, "insider threats" as an organizational problem gap is defined as executives or someone with authorized access, high social power and holding a critical job position, who is capable of inflicting high impact damage including psychological, managerial, or physical level, within an organization.'…'Behavior interpreted or perceived in one single observation / incident – or through multiple observations over time, to be applied in these multiple observations' (Ho, 2008).

This statement was related to the incident posed by 'Richard Hansen, a US counterintelligence agent,' (Ho, 2008). When looking at past insider threat activity, we learn how emotion may play into actions on both sides of the spectrum, from offender to victim. InTP leads may put emotion in front of an incident based on previous occurrences or perceptions of individuals passing their own type of judgement; bias character when dealing with an insider threat event degrades the organization's ability in countering the insider threat.

Sub-Section B - Cognitive Bias

Another bias identified in analysis, which may affect insider threat detection and prevention, is the overall cognitive ability, or intelligence, of all those involved and uninvolved in the insider threat matrix. Intelligence bias also may be applied by those who design software programs or algorithms to support Insider Threat Detection programs. Programs which can determine the size of data being transferred by a system user above the norm, file structure which verifies a user's need to know, or simply, technological advances which are easily understood by the system administrator.

There may also be cognitive bias between organizations or internal offices on the ability to understand policy, comprehend the measure or magnitude of the situation, or be interested in defeating the insider threat by easily and concisely explaining the requirements to employees. For instance, a Facility Security Officer (FSO) for a DOD-sponsored contract agency may have exceptional abilities. The same FSO switches to another company, or is selected for a Government position, and leaves the contractor agency with no back-fill or successor. The hired replacement is given the job based on the need to fill the seat and is not thoroughly vetted during the interview process. This damages the company or agency's ability to counter the insider threat effectively due to the new employee fitting into the cognitive bias aspect, 'biases can arise if the task at hand is not one for which the mind is designed' (Ho, 2008).

Another shortcoming within an agency or organization may be with policy interpretation due to lack of knowledge, lapse in training awareness, inability of staff to clearly perform their duties to properly report insider threat actions, or interpretation based on extreme circumstances. Personnel believe the system is either out to get them or can be used to their advantage, ‘Perception can vary if the observations (or interpretation) are from different observers, or if the target being studied is different, or the situation is different’ (Ho, 2008). Larger organizations may prevent or complicate insider threat activities based on an interest in pursuing fast pace advances before employees within the agency are ready or properly trained for the change; particular when it comes to new technology, 'people hold the general belief that new information technology is complex/difficult to understand' (Elsbach, 2019).

Security professionals must understand the complexity of insider threat events in a holistic sense from the actual event, the leading factors which manifested or were present, noticed or unnoticed, before the event, and how far and wide the damage may be from such an event. For instance, a simple event where malware is identified after a system parameter alerted the IT professional to the file anomaly. InTP personnel must have the cognitive ability to look beyond just a simple file. There must be a full review to determine how far the file intruded. Was the event intentional? How much data or files were breached? Is this an attack or an initial attempt? Will there be further vulnerabilities from this one incident? These are examples of the understanding one must have to prevent or respond to insider threat incidents. In reflection, this may be viewed as bias per se, 'understanding how mindset and biases play a role in strategies, tactics and vital decisions that may ultimately prevent an attack from being successful' (Haselton, 2015). Another foundation of cognitive bias is,

> 'By cognitive bias, we mean cases in which human cognition reliably produces representations that are systematically distorted compared to some aspect of objective reality'
> 'As an evolutionary psychological perspective predicts that the mind is equipped with function-specific mechanisms adapted for special purposes-mechanisms with special design for solving problems.' (Haselton, 2015)

Sub-Section C - Heuristic Bias

Problem solving, or coming quickly to a solution to prevent or respond to insider threat activities may not be ideal, coherent, or exact, but the end result is adequate to the current situation. This is a heuristic approach to countering insider threats; how quickly can we identify, verify, and deal with the problem to prevent or deter the next event in a simplified manner? In review of *The Evolution of Cognitive Bias,* the analysis provided a clearer understanding of heuristics.

> 'There may also be costs in real time, since decisions using complex algorithms will often take longer or require more attentional resources than decisions using simpler alternatives. Adaptive decisions often need to be made fast, and this may well constrain the type of strategies that are optimal. Evidence from a variety of sources demonstrates that people do indeed solve problems differently when under time pressure or when their motivations to be accurate are reduced.' (Haselton, 2015).

Heuristic bias is further identified in how people perceive others, to include all employees of an organization at lower levels, 'Those higher in power are more likely to endorse stereotypes about others than to attend to individuating information specific to the target' (Haselton, 2015). Approaching an insider threat event or even managing a program with this aperture limits the ability to prevent incidents when the bulk of the time is spent on putting employees into categories long before actually having factual data. This comes into play when first hearing of an insider threat incident and basing the issue without fully understanding the circumstance. An example may be when a manager or company executive passes responsibility onto a subordinate who may not have a higher education and blames the individual when something goes wrong with the system when the actual situation resulted from a programming error or system deficiency. Specifically, an employee is repeatedly identified as causing intrusion detection faults in an electronic security system for several days. Organization personnel and technical teams review system parameters and initially determine the alarm anomalies are due to the employee not properly securing the facility. This is the quick and easy solution to the problem, assign blame to the individual with the least understanding of electronic security systems. The actual issue is later identified to be with how the system was designed improperly, as well as defective items internal to the control components to the facility.

Another example of heuristic bias can be applied to initial assessments or investigations into high profile insider threat events, particularly active shooter events. The media is often quick to assign stereotypical nomenclature to individuals without allowing law enforcement or investigators to fully review all the circumstances leading to the event. Specifically, a sailor, Fireman Romero, on 4 December 2019 fatally shot two shipyard workers, wounded another shipyard worker, and then shot himself (DOD, 2020). Even though the investigation determined the incident could not have been detected or that anyone would have known Romero would do such an act, there were still points along the way which were potentially missed. Those being mental health issues Romero was dealing with, past medical history which contributed to his ability to adapt to his overall responsibilities and qualification requirements, lack of support to understand Romero's entire situation, or even the command's medical team collaborating with the local military treatment facility to get a clear picture of Romero (DOD, 2020). Findings did discover other weaknesses in not just the main command Romero was assigned, but other organization or agency issues to prevent, detect, and respond to an insider threat.

Sub-Section D - Gender Bias

Another bias to understand when countering insider threat is related to gender. Gender bias is identified as an issue in the research or analysis of many topics. Gender plays a determining factor in how the justice system applies sentencing, how society perceives the role of men and women, or even the perception of how men are more likely to commit insider threat incidents over women (Meaux et al., 2018). Several studies addressed this area of bias through situations research. Participants were given a scenario and a name of the offender. In one side of the situation, the pronoun 'he' was used to describe the actor while in the other situation, 'she' was used to describe the actor. The study discovered participants viewed men more likely to have truly committed the event and held men to a higher standard in relation to judgement and punishment.

Men are perceived to be more involved in insider threat events related to IT systems. However, overtime, analysis has determined women are beginning to be just as likely to commit insider threat actions similar in numbers as men. Is this due to greater ability to detect and report such occurrences, or is it due to men and women equally becoming bolder in executing IT system attacks?

> 'Our findings contribute to information system security research by utilizing the chivalry hypothesis and gendered stereotypes to theorize about issues detecting and evaluating possible malicious insider threats. This study extends current research on chivalry hypothesis research by linking gendered criminal and computer stereotypes to bias in evaluating information system security threats. Overall, our findings are consistent with tenets underlying chivalry hypothesis (Goethals et al., 1997) that when men and women who commit the same crime are treated differently in that women receive more lenient treatment (Chesney-Lind 1978).' (Giddens et al., 2020)

Section 3 – Recommendations

In review of the articles, periodicals, and studies, there is sufficient information and evidence to verify there is an ability of bias to become embedded into any organization's InTP. Managers at all levels, and those who oversee insider threat analysis, must understand and be knowledgeable of bias to ensure their abilities to counter harmful actions are not thwarted. Bias aspect in gender, cognitive abilities, heuristics, and emotion are just a few examples covered. Other bias analysis which are of concern include data collection bias, procedural bias, publication bias, design bias, participation bias, and bias reporting to name a few more. Having a clear understanding of how bias can infiltrate a program is indispensable in countering insider threat activities.

Section 3 - Conclusion

Insider threats may be subject to bias analysis and actions by victims, offenders, and others. As long as it is known, understood, and managed, the risks of bias hindering program effectiveness can be minimized. Throughout this review, the focus was to identify the various bias present in analysis and research, confirm or verify how it may play a part in incident outcome, and more importantly, how to recognize the potential for bias to reduce program operations. Anyone who has been assigned responsibilities associated to investigations develop their own perceptions or bias to similar situations overtime, even if the offender is a different person. Each situation or scenario must be treated differently, but through the same general process.

Throughout history, there have been many cases of insider threat. What initiates the event, how it is dealt with, and later prevented from reoccurring is necessary for any InTP. It is important to be alert to program deficiencies – like bias analysis or perceptions – and manage issues which may arise to lower a company, organization, or agency's ability to prevent, detect, and respond to insider threats.

References

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

Carnegie Mellon University, 2018
CERT: Low Cost Technical Solutions to Jump Start an Insider Threat Program
Software Engineering Institute

Department of the Navy, 2020
Investigation Into Fatal Shooting Incident on Pearl Harbor Naval Shipyard of 4 December 2019

Elsbach and Stigliani et al., 2019 KD Elsbach, I Stigliani
New Information Technology and Implicit Bias
Academy of Management Perspectives. Vol. 33, No. 2, 185-206

Haselton et al., 2015 M. Haselton, D. Nettle, and D. Murray
The Evolution of Cognitive Bias
Wiley Online Library Part VII. Interfaces with Traditional Psychology Disciplines

Ho, 2008 S. Ho
Behavioral Parameters of Trustworthiness for Countering Insider Threats
Syracuse University

Giddens et al., 2020 L. Giddens, L. Amo, and D. Cichocks
Gender Bias and the Impact On Managerial Evaluation of Insider Security Threats
Vol. 99. Sciencedirect.com

Meaux et al., 2018 L. Meaux, J. Cox, and M. Kopkin
Saving damsels, sentencing deviants and selective chivalry decisions: juror decision-making in an ambiguous assault case
Psychiatr Psychol Law, 2018; 25(5): 724-736

Pfleeger, Shari, S.L. Pfleeger
Insiders Behaving Badly
Rand Corporation – Infrastructure, Safety, and Enviroment

Sarniak, 2015 R. Sarniak
9 Types of Research Bias and How to Avoid Them
GAPf!SH, Article 20150825-2

Tversky, et al., 1973 A. Tversky

Judgement Under Uncertainty: Heuristics and Biases
Office of Naval Research Advanced Research Projects Agency AD-767 425