Cybersecurity Intelligence: A Novel Information Security Threat Mitigation Approach

Patrick Offor
City University of Seattle, United States

I. Problem Statement

Despite technology and countermeasure investments worldwide, mandatory training and its repeated iterations in organizations, awareness, and education of the threats posed to critical information systems by trusted insiders globally, the exploits and havocs have continued to increase exponentially, rather than diminish. Trusted insiders have continued to threaten our networks and communication infrastructures, in spite of the availability of more capabilities for identifying the culprits, and the incessant prosecution and conviction of malicious actors. In addition, even with the exposure of non-malicious actors in organizations, training and education of employers and employees alike, analysis of costs to individuals and organizations due to cybersecurity losses, and the ubiquitous or plethora of defensive and offensive cybersecurity investments by governments and organizations in technical and non-technical measures, the issue of trusted insiders has continued to increase.

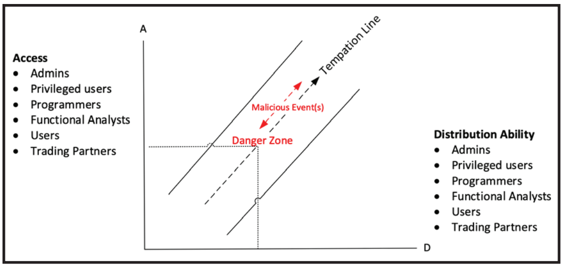
The main reason for such an unavoidable risk emanating from trusted insiders is not farfetched. Although anyone in an organization poses a risk to the organization's critical information, the cost is greater when it happen from those with authorized and privileged access. Organizations have personnel who have physical access to the organization's information systems, technical knowledge of the systems, undetectable distribution capacity of a stolen artifact (data, information, objects, intellectual property), and who understands the organization's cybersecurity mitigation strategy and plan. Therefore, having personnel in organization with such inevitable capacities pose even more significant risks and threats to the organization.

The practicality of insider threats is such that, at any given time, select employees would always have physical access and technical expertise of an organization's critical information systems or infrastructure, and non-suspecting distribution capacity of the compromised artifact as depicted in Figure 1. It is a known fact that information system professionals, depending on their positions, usually would have both the physical access to the systems and the systems' technical knowhow, including the systems' known vulnerabilities and the organization's risk management framework. Crossing the danger zone notation in Figure 1 indicates the point at which an employee, affected by one or more of the cybersecurity trigger indicators, has decided to become an insider malicious attacker, in part, because the opportunity of having access and distribution capacities had presented.

An insider attack originates from a trusted insider, regardless of whether the attack is malicious or non-malicious. Insider threats to organizations can generally be categorized as malicious (an attack by a criminal or malicious insider) or non-malicious (a careless, mistaken, negligent, or intentional but non-malicious attack by an employee, contractor, or otherwise) (Ponemon, 2018). People rather than technology or process, has shown to pose the greatest threat to organizations' critical information systems (IS), information security, or cybersecurity (Gelles & Mitchell, 2015; Greitzer & Hohimer, 2011) because they possess the two perilous elements to cybersecurity vulnerabilities, which are accessibility of the physical systems and technical knowledge of the systems (Archuleta, 2009). As such, the proposed study will conduct a theoretical evaluation of the phenomenon based human behavior theory underpinnings. In this context, people represent employees, contractors, and employers of a company who could otherwise be referred to as trusted insiders or actors

.

Figure 1: A Trusted Insider Becoming an Attacker (adapted from The Insider Threat, 2015)



The difficulty this problem poses to businesses, governments, institutions, and other entities is currently manifested in real-time and in the extant literature. In recent years, attacks by the trusted insiders have been very costly. In 2015, each incident's cost to organizations is estimated at over $144,000, and the resolution of the issues of insider actors cost organizations about $21,000 a day (Securonix, 2015). Out of the 3269 insider incidents in 2017 from 159 organizations in North America, Europe, Middle East and Africa, and Asia-Pacific, 64% were due to negligence by employees and contractors, 23% were from malicious or criminal insiders, and 13% were relating to user credential theft. On average, the total average cost of insider attack for the organizations was $8.76 million in 2017 (Ponemon, 2018). Ron Rockwell Hansen, a former Defense Intelligence Agency (DIA) officer, pleaded guilty to attempted espionage in March 2019 (Cyber Awareness Challenge, 2021).

The issue is that most study on insider attack have if-x-then-y perspectives. They focused heavily on indicators, triggers, activity monitoring, and workplace reporting. They also focused on the attackers' character exhibitions, i.e., whether an attacker exhibits signs of having personality problem, mental disorder, ethical issue, personal or work-related issues, emotional issue, or overdependence (Liang et al., 2016). They also focus on whether the insider attacker has financial problem, is not rational, disgruntled or is socially isolated (Liang et al., 2016). Hence, we argue that although these factors play important roles in the characteristics of insider attacker, the choice of an attacker is more important because it consummates to an attack, as such, the second most critical part of the act other than the act. For that reason, the proposed study will focus more on the decisions or choices of insider attackers.

As the Chief Information Security Officer (CISO) of an organization, an Information Security or Cybersecurity Consultant, or Educator, imagine that you have the capacity to categorize the employees in your organization distinctively into four, based on a predetermine elements of data collected from the employees. And that you have the capacity to assess, identify, and determine the probability of employees' leanings or propensity to becoming insider attackers when affected by any of the already identified insider threat indicators based on the data. That is the kind of intelligence the proposed study could bring to bear. The presupposition is that such a study will support the operationalization of such capacity and would be a gold mine for cybersecurity professionals.

Therefore, the concept espoused in this note aims to provide a novel cybersecurity intelligence capability that can predictively and prescriptively help organizations to identify employees who may have the propensity to cross the danger zone on the temptation line, as illustrated in Figure 1, and become insider attackers or malicious actors when any one or more of the following insider threat indicators manifest itself: divided loyalties, identification, ideologies, revenge, anger tendencies, destructive behavior, adventure, thrilling tendencies, ego, self-image, ingratiation, compulsiveness and/or family problems (U.S. Department of Justice, 2014). It also aims to alert cybersecurity manager earlier for better deployment of mitigation measures and broaden cybersecurity skills and education.

II. Research Questions

The conceptual propositions for this proposed study is based on choice theory. The choice theory underlying principles would be adopted in the study because of its potential ability to illustrate the powerfulness of a substantive and reflective insight of proactiveness, prescriptiveness, and purposefulness in advancing cybersecurity intelligence. In assessing the reasonableness of using choice theory in examining the threat of trusted insiders to cybersecurity, we conducted a search of the relevancy of the theory in the extant literature and in other disciplines using "choice theory" as keyword since this is the first attempt to use it in a cybersecurity setting, at least, to the best of our knowledge. Therefore, the following is a delineation of the theory and a description of the expansiveness and usefulness of the theory to research and practice.

Choice theory "is an internal control psychology; it explains why and how we make the choices that determine the course of our lives" (Glasser, 1998, p. 7). It also explains that human beings are internally motivated to behave; although external stimuli (motivations) inform us, they do not control the specific choices we make or our responses to stimuli. Inherent in choice theory is the argument that all we do, from the beginning of our lives to the end, is to behave and relate (Glasser, 1998). Choice theory "is about making better choices, but we have to understand the reason for the bad choices before we can make good ones" (Glasser, 1998, p. 157).

In describing human behavior, Glasser suggested four inseparable components of each human behavior, i.e., activity, thinking, feeling, and physiology. Since these four components of each behavior work together simultaneously, he referred to it as a total behavior. In other words, Glasser further explained that when we are doing something, we are acting and thinking; that we are feeling something; and that we are breathing, our heart is beating, and our brain is working. Finally, he added that although the inner workings of these components are intertwined, (1) that we have direct control over our actions and thoughts, and (2) that we have indirect control over our feelings and physiology (Glasser, 1998). Therefore, the conceptual framework for the proposed study will anchor in the total behavior. Total behavior hinges on the idea that all behaviors are purposeful, and involve physiology, feeling, thought, and culminate in an act (Glasser, 1998).

Furthermore, choice theory is about human decisions; and how we relate to and gather information from one another, how we relate to or gather information from our organizations, and vice versa. This conception of choice theory is also relevant and suitable because people are the most significant cybersecurity threat. Choice theory will be relevant to gathering cybersecurity intelligence because behaving is relating and because of the need to understand the two relationships in an employer-employee relationship; how an employer behaves toward an employee and how an employee behaves and relates to the employer (Butorac, 2020).

Although choice theory or total behavior has not been used in cybersecurity intelligence literature—to our knowledge, it has been used in many other areas, including reality therapy, economics, sports, and education.

A Google Scholar search for "Choice Theory" indicates that Glasser (1998) has been cited 2,137 times since its publication. There were 724 citations of the theory from 1998 to 2010, and there were 1340 citations from 2011-2020, indicative of a trending interest on it. Equally important is that some of the books and articles that cited the choice theory have over 300-1,700 citations of their own.

Additionally, using "Choice Theory" as a keyword/phrase and selecting "Peer-reviewed (scholarly) journals," "Full Text," and "2015-2020" as limiters or criteria in the Academic Search Premier database, we found 10,069 articles relating to the theory, indicative of the relevancy and the amount of interest in the theory in recent times. Minimizing the criteria will provide greater number of academic journals with choice theory as well.

III. Contribution

First, the outcome of the proposed study will add to the body of knowledge because it will help in answering the question of whether a predictive or prescriptive analysis could foretell an employee's cybersecurity tendencies or behaviors? An information security manager that is armed with employees' cybersecurity tendency intelligence will be better prepared in instituting surgical and appropriate countermeasures to insider threats, risks, and vulnerabilities.

Secondly, the outcome of the proposed study will help in answering the question of the degree to which a predictive or prescriptive analysis would foretell an employee's cybersecurity tendencies or behaviors? Here, the question is whether the juice is worth the squeeze—the proposed study will provide the magnitude of or the significance of such employee's cybersecurity tendencies.

Thirdly, the outcome of the proposed study will assess whether an organization could reasonably minimize its cybersecurity risk and threat exposures when the findings are operationalized. In order words, it will demonstrate that the development of such proposed cybersecurity intelligence is not only theoretical but has applicability and generalization.

Furthermore, if the findings in the proposed study were to come to fruition, it will usher a new dimension to applied research because of its rich real-world application potentials and will further academic inquiry in cybersecurity because of its social science implications. The potential contribution to the body of knowledge would be (1) to confirm or disconfirm the essence of total behavior or the falsifiability of the concept of total behavior, (2) would help in determining whether personnel in organizations could be categorized such that their cybersecurity leanings when faced with insider threat triggers could be determined, and (3) provide statistical answers to insider threat research problem or the phenomenon of interest.

Typically, some middle to large organizations have over 1,000 employees, as such it is not logical, in fact, it will not be reasonable to individualize each person's total behavior. Hence, the first iteration of the study will categorize the sample subjects in four so that it can be manageable. Each category will be measured against each of the insider threat indicator or triggers in order to extrapolate cybersecurity intelligence. The categorization would be exploratory in nature and will be based on the data collected using a survey instrument.

IV. Rationale

The rationale for this concept is to provide researchers and practitioners with an essential and actionable cybersecurity intelligence since the issue of insider threat has not diminished despite current technical and non-technical solutions available in the market. Secondly, the importance of advancing this concept is because in spite of the rapidity of technology innovation and creativity, and despite the technological capabilities available to organizations, government, and institutions of learning, the issues of trusted insiders have continued to ravage industries around the world.

Additionally, the provision of such intelligence is in line with the Cybersecurity Workforce Framework stipulated in the National Initiative for Cybersecurity Education (NICE). Although the concept that effective cybersecurity or information security risk management (RSK), data administration (DTA), and knowledge management (KMG) are complex schemes, especially in the middle to large organizations, is not novel, there is a need for the establishment of a continuum of efforts toward a better cybersecurity mitigation approach. Moreover, an organization's ability to manage cybersecurity threat and risk largely depends on its capacity to formulate, articulate, and enforce the provisions stipulated in the NICE Framework categories relating, but not limited to Secure Provision (SP), Oversee and Govern (OV), Protect and Defend (PR), and Investigate (IN), among others (NIST SP 800-181).

V. Investigative Approach

We will use exploratory and quantitative research approaches for the study—see research contribution. Discernment and categorization of personnel based on the total behavior can only be achieved based on exploratory inquiry because will be the first of its kind. Furthermore, quantitative approach will be used because of its capacity to determine relationships among variables or constructs and the phenomenon of interest, and because it is predictive in nature. A survey instrument will be used to gather data from subjects among the working population in the U.S. The development of variables or constructs for the study will be based on the total behavior's core principles. Following the initial theoretical investigation, depending on the result, a longitudinal examination may ensue for generalization and further affirmation of the result.

In addition, quantitative analysis tends to explore attitudes and behaviors (Offor, 2016). The first iteration of this study would test the falsifiability of the theory. In other words, the initial objective is to establish that all actions/activities are based on total behavior. In identifying our total behavior categories, we will assess their correlations to provide cybersecurity intelligence. We will then assess how insider threat triggers moderate each total behavior category in relation to insider threat behaviors.

VI. Lesson Learned

The currency of the following observations or lessons learned is one of the motivations for this conceptualization and proposal for a new innovative and creative examination of the phenomenon:

- Cybersecurity education is still evolving because cybersecurity threats are still evolving.
- As our cyber presence increases, governments and organizations alike must advance cybersecurity technical and non-technical solutions and be zealous in crafting the right mix of regulation.
- That our cyber environment will outgrow our physical environment because the

Internet has no boundaries; as such, the need for a safer cyber environment cannot be overstated.

VII. Implication for Practice

The results of the study will indicate that organizations can be better served when they could make reasonable assessments and judgments or have reasonable sets of expectations of their employees' information security or cybersecurity propensities or postures in order to take appropriate mitigation countermeasures. It will help organizations in taking preventative measures to cybersecurity rather than relying on reactive measures.

A successful result will advance cybersecurity intelligence capabilities and provide cybersecurity managers, across the globe, with predictability in their mitigation strategies, plans, and efforts. In addition, a successful result will advance interests in the psychology community, especially for practitioners in the reality therapy.

VIII. Implication for Research

The result of the study will ignite a new frontier in theoretical examinations of the phenomenon of an insider threat since "a theoretical framework is a set of related concepts or constructs formulated based on a given theory to analyze, explain, predict, prescribe, and understand a phenomenon" (Offor, 2016). In addition, a theoretical examination of a trusted insider's issue requires the formulation of a translatable, observable, and empirically testable theory (Offor, 2016). The benefits of a successful outcome from the proposed study will enrich academic research cybersecurity, psychology, and other academic domains because understanding human behaviors is the core to understanding cybersecurity issues emanating from trusted insiders.

IX. Call for Action

We are open to and are looking for research partners, sponsors, and/or participating organizations in order to advance this proposed study.

References

Aldhizer III, G. R. (2008). The Insider threat. *Internal Auditor,* 65(2), 71–73.

Butorac, D. (2020). Choice theory vs. common sense: Relationships. *International Journal of Choice Theory & Reality Therapy, 39*(2), 17–21.

Center for Development of Security Excellence. (2019). Insider threat: Potential risk indicators. Retrieved from https://www.cdse.edu/documents/toolkits-insider/INTJ0181-insider-threat-indicators-job-aid.pdf

Cyber Awareness Challenge. (2021). Retrieved from https://public.cyber.mil/training/cyber-awareness-challenge/

Gelles, M. G., & Mitchell, K. (2015). Top 10 considerations for building an insider threat mitigation program. *Journal of Threat Assessment and Management, 2*(3-4), 255-257.

Glasser, M. D. (1998). Choice theory: A new psychology of personal freedom. New York, NY: HarperCollins.

Greitzer, F.L., & Hohimer, R. E. (2011). Modelling human behavior to anticipate insider attacks. *Journal of Strategic Security, 4*(2), 25-48.

Haystax. (2019). Insider threat report. Retrieved from https://haystax.com/wp-content/uploads/2019/07/Haystax-Insider-Threat-Report-2019.pdf

InfoSecurity. (2018). Top ten cases of insider threat. https://www.infosecurity-magazine.com/magazine-features/top-ten-insider-threat/

Moghaddam, F. M., & Studer, C. (1998). Illusions of control: Striving for control in our personal and professional lives. WestPoint, CT: Praeger.

Liang, N., Biros, D. P., & Luse, A. (2016). An Empirical Validation of Malicious Insider Characteristics. *Journal of Management Information Systems, 33*(2), 361–392.

Offor, P. I. (2016). Examining consumers' selective information privacy disclosure behaviors in an organization's secure e-commerce systems (Doctoral dissertation, Nova Southeastern University).

Ponemon Institute. (2018). 2018 cost of insider threats: Global. Retrieved from https://153j3ttjub71nfe89mc7r5gb-wpengine.netdna-ssl.com/wp-content/uploads/2018/04/ObserveIT-Insider-Threat-Global-Report-FINAL.pdf

Puhakainen, P., & Siponen, M.T. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly,* 34, 757-778.

The Insider Threat—The human aspect: It's emotional. (2015). Retrieved from https://youtu.be/XT1TmxE5NfY

U.S. Department of Homeland Security (DHS). (n.d). Insider threat. Retrieved from https://www.dhs.gov/science-and-technology/cybersecurity-insider-threat

U.S. Department of Justice Security Federal Bureau of Investigation (FBI). (2014). The insider threat. Retrieved from https://web.archive.org/web/20140803163734/http://www.fbi.gov/ about-us/investigate/counterintelligence/insider_threat_brochure