MULTIDIMENSIONAL INSIDER THREAT DETECTION MODEL FOR ORGANIZATION

GANTHAN NARAYANA SAMY[1], NURAZEEN MAAROP[1], BHARANIDHARAN SHANMUGAM[2], MUGILRAJ RADHAKRISHNAN[3], SUNDRESAN PERUMAL[4] AND FIZA ABDUL RAHIM[1]

[1]Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Malaysia

[2]School of Engineering and Information Technology, Casuarina, Charles Darwin University, Australia

[3]Suruhanjaya Perkhidmatan Pelajaran Malaysia, Putrajaya, Malaysia

[4]Faculty of Science and Technology, Universiti Sains Islam Malaysia, Negeri Sembilan, Malaysia

ganthan.kl@utm.my, nurazean.kl@utm.my, fiza.abdulrahim@utm.my,
Bharanidharan.Shanmugam@cdu.edu.au,
mugilaj@spp.gov.my, sundresan.p@usim.edu.my

ABSTRACT

Insider threat is a most worrying threat that haunts many organizations today that cause enormous financial losses and damages. As a frontline, Information Technology (IT) organizations has to implement necessary countermeasures to protect critical infrastructure. Although, many approaches proposed before to detect and mitigate insider threat, significant rise of cases in past few years and unavailability of a widely accepted solution paves way to conduct more researches. Moreover, the pandemic situation has brought in a new challenge for IT organizations to review the existing safeguards. This paper aims to contribute an interdisciplinary approach at proposing a multidimensional model that scrutinize factors from multiple dimensions such as psychological, behavioral, technological, organizational and environmental dimension that triggers insider threat. The constructed model coordinates organizations to counter insider threat by addressing issues in more effective and efficient way by applying the multidimensional approach for mitigation.

Key words: *Insider Threat, Psychological Dimension, Behavioral Dimension, Technological Dimension, Organizational Dimension, Environmental Dimension*

1. INTRODUCTION

Generally, insiders are someone who attached to the organizations such as current or former employee, business partner or contractor who has or had legitimate access privileges to the critical infrastructure [1]h. Organizations intend to outsource system related services to experts from outside due to the lack of expertise, workload and job management [2]. Insiders categorized in detail to differentiate their role based on the level of access privileges. An employee of an organization is often regards as a pure insider who has access rights with passes, cards and tokens to enter the premises especially to the restricted location such as data center [3]. As a high-end insider, they have physical presence anywhere within the organization and knowledgeable about the physical and logical structure of the premises especially about critical infrastructure. When a pure insider initiate a threat, it is often disastrous since the abuse their access privileges and often labelled as malicious insider [4].

Meanwhile, insider associate is a type of insider who is not a direct employee to the organization with limited physical access to the premises. Furthermore, insider affiliate is a third party client related or closely connected to the insider such as spouse or a friend who enter the premise with the help of the insiders. Although they are restricted from accessing sensitive data, they might unintentionally expose the confidential data when handling the devices at premises. Indirectly, they are being a reason for the sensitive data exposed and often seen as a compromised insider for being a reason to harvest their login credentials through phishing attacks [4]. Finally, outside affiliate is the most crucial one because this type of attacker does not have any access privilege to the premises and not part of the organization. They labelled as insider since have a backdoor access to the company network due to the unprotected network and through social engineering attack [1]. Also known as low-level insiders, this type of attackers has a personal goal towards a premise and have patience to collect information about them before pursue an attack. Besides, they also could pose an attack by manipulating and persuading employee to expose the necessary information that might cause great consequences [4].

2. LITERATURE REVIEW

Most of the organizations are aware and well prepared to protect their essential information in order to maintain their competitive advantages, reputation and market position. As a first level strategy to mitigate external threat, Information Technology (IT) departments of many organizations endorse Information and Communications Technology (ICT) policies and procedures. As an advance treatment to mitigate cyber threat from external, many organizations have been working collaboratively to throw ideas onto reform and enhance countermeasures through cyber threat intelligence modelling based on their experiences with external attacks to protect their businesses from jeopardized by external forces. However, referring to the number of reported high-profile security incidents, surprisingly the threat to organization originated from within organizations [5].

Moreover, it is not always about the system vulnerabilities and weaknesses anymore but shifted to other internal factors that cause such security incidents. It was found that an act of insiders that are deliberately affect the system with an intention that negatively influence the security triad. Ironically, internal threats have a greater impact of losses compared to an external threat. While external attack executed by hackers from outside with least knowledge about the organizations, internal threat initiated within organization by an insider who might has a significant level of access to the critical infrastructure.

Cybercrime experts often highlights crimes initiated within the organization by the trusted parties who are also an asset of the organization are more severe than outsiders are since they hold important roles in organization [6]. Identifying the enemy hiding behind the enterprise boundary always considered as the hardest task and most critical threat in cybersecurity. Naturally, insiders are employees who have roles within organizations such as database administrators, information security officers, system administrators and cybercrime managers who could have authorized access to the assets and critical infrastructures exposed without other's knowledge. The in-depth knowledge that insiders possess are such as the existing organization framework, vulnerabilities, loopholes, backdoors, security controls, monitoring practices, and modus operandi [7].

2.1 Intentional Insider

Intentional insiders are employees or other stakeholders who are deliberately exploit critical infrastructure to cause damages by affecting the security aspects of system. Intentional insiders often known as malicious insiders since they are legitimate users with authorized access privileges and directly leak, exfiltration and destroy sensitive data [2]. Moreover, intentional insiders traditionally divided into traitors and masqueraders. Traitors usually are administrators who owns the direct access to the assets will use his own privilege to perform malicious activity. Meanwhile, masqueraders are someone does not own direct access to a system but eventually steals others access rights to causing information leakage for personal gains. In addition to that, change management will introduce new set of values into organization in order to increase efficiencies and effectiveness in operations.

Normally, changes related to the technological changes such as introduction of new system with new standard operating procedures to enhance the productivity. Besides, political changes also will introduce new regulations into organization, which could have an impact over the environment in organization [6]. The unpleasant feelings towards new changes in organization is because the employees found difficulties in leaving their comfort. Meanwhile, human often regards as the weakest link since all security incidents attributed by organizational insiders. Malicious insiders also want to continue to enjoy the benefit of malicious activity by keeping their corporate devices intentionally after leaving the job. In many cases, security aspects of the system is never changed leaving the trace for the intentional insider to have a continuous access to the network from outside [8].

Ironically, employees and other stakeholders are not malicious insiders at first but triggered to be an intentional insider in later stages. The organization need to identify reasons that causing employees to turn against them that would end up with costly loses to them [9]. In some cases, intentional insider exists at earliest stages of the employment whereby rivalry companies send their employees uses them to collect information and stealing knowledge. Besides, luring insiders in an organization is also a trend in economic and corporate espionage where many cases reported once executed.

2.2 Unintentional Insider

In contrast to intentional insider, unintentional insiders consist of employees and other stakeholders who are not deliberately leak the valuable information or accidentally manipulated data. Similar to intentional insiders, unintentional insider holds legitimate access privileges of critical infrastructure but however doesn't realize the amount of accountability towards the system in which their actions can directly compromise the attributes of security of the assets [10]. Insider threat researches considers employees as most dangerous attack vectors due to the lack of awareness and proper handling of the assets which can cause irreversible damages. This falls under inadvertent insiders since the attack initiated are without malicious intent and out of negligence but it still causes inadvertent disclosure of critical information. Most of the reported unintentional insider cases finds an insider does not aware that they are aiding a threat actor to initiate an unplanned incident. In other cases, a malicious outsider can also deceive an insider to leak out information through social engineering attack. In the perspective of IT, it is hard to differentiate between intentional and unintentional insiders because the impact of loses and damages to critical infrastructure are nearly equal [11].

2.3 Insider Threat Challenges to IT Organizations

IT departments are the first line defense for any organizations both private and government as they implement security controls and counter measures to safeguard information systems that carries specific functions to support day-to-day operations. The current cybersecurity trend shows that top management are aware of external cyber-attack and are willing to invest in ICT security to help IT departments to protect organization's critical infrastructure in order to increase efficiency and productivity without disruption. However, in recent times, insider threat has emerged as the most challenging cybersecurity threat in which commonly employed security mechanisms and solutions are insufficient. Many IT organizations have failed to reverse the investigation of cybersecurity breaches towards inside because of the wrong understanding and perception about internal attacks [9]. Lack of understanding about the nature of insider threat is the root cause of the negligence hence the policymakers within IT organizations are focusing on strengthening the technology. In other word, they fail to deploy necessary protection, which is beyond technology to counter the compromised insiders [12].

Moreover, challenges to the security of information system have increased recently due to the pandemic-driven situation that force many organizations impose to work from home. Combatting insider threat during pandemic-driven environment is a new challenge to cybersecurity professional within IT organizations as malicious insider looks to capitalize the situation to attack on sensitive data. The urgency for remote access to the premises increased and privileges distributed accordingly to access from outside. In other word, the company network stretched to outside the office cloud until its user premises. The scope of security coverage increased drastically in a short period of time in which IT professionals does not have enough time to impose necessary countermeasures to mitigate any critical incident.

Meanwhile, many remote access service providers are taking advantage of the situation and has been actively promoting their tools and services to help on the situation [13]. Organization tend to subscribe those services to prolong business without disruption, as their primary motive is business continuity. IT professionals are under pressure, as they need to initiate a plan to mitigate any threat to their businesses initiated by insiders from outside of the company network. However, technological solution alone does not enough to counter the insider threat issues because of the nature of the threat. IT organizations should accept that insider threat is an issue, which is more than just technology.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.4 Insider Threat Ontologies

The wide variety use of information system by IT based organizations to present the services has also made them vulnerable for variety of cyber-attack including insider threat which is difficult to contrast and prevent [14]. Ironically, researches intend to find a suitable reference for investigating insider threat based on holistic approach. Ontological approach introduced by researchers to explain the insider threat scenario in a more approachable way. The idea of using a formal and standardized language for expressing knowledge about the insider threat domain facilitates information sharing across the organizations such as from SOFIT ontology as illustrated in Figure 1 and Figure 2 respectively [15].

Earlier, the ontological approach developed based on technical elements that contribute to insider threat incidents. However, the research expanded to include beyond the technical elements to a more complex approach. Insider threat ontology developed to give an effective way to scrutinize the factors and relating it to each other to find a solution based on human, technical and organizational factors. Ontologies were developed to narrow the relationship between human-technical in a structural way that help to investigate the defining aspect of human and technology interaction. Besides, it also developed based on human-organizational relationship factor which was transformed into ontology to help organizations to mitigate insider threat based on risk prioritization [16]. This research briefly explains the concerning behaviors of the employees by analyzing their job performances and violations as the measurement factor by linking with personal history. Those concerning behaviors linked and matched with the organizational and technical factor to represents the relationship in an ontological way using recognized ontology development methodology. The ontology hierarchy formalized and translated to a parent-child relationship of classes in ontology, which been derived from research literature.

3. PROBLEM STATEMENT

Researches that reviewed in this study were limited to human and organizational factors whereby insider threat has developed as an issue beyond those elements. There was lack of studies on different dimension and perspectives of insider threat based on real life surveys that focuses beyond sociotechnical elements such as environmental, psychological state, organizational influences and technological aspects. Meanwhile, conceptual study based on general frameworks and model may not relevant for some organization to adopt since the nature of business may vary to others. Meanwhile, tackling insider threat need to prove with the survey outcome from that particular organization to avoid biases in decisions, lack of real life cases and wrong implementations that does not improve the situation. Therefore, a multidimensional model that comprises all the dimensions needed in order to help organizations to provide an overall solution to insider threat.

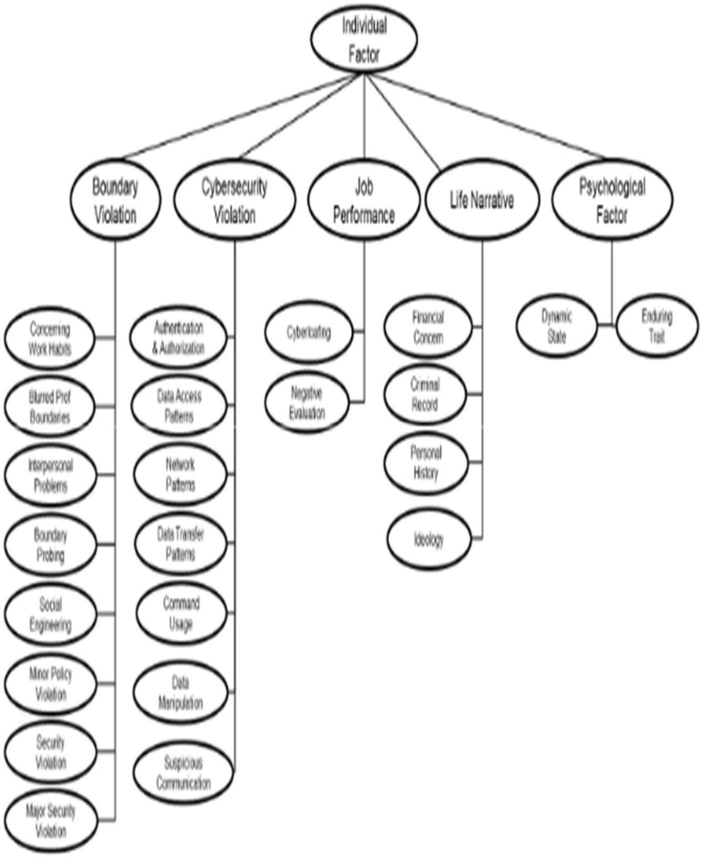

Figure 1: Individual Factor Branch of SOFIT ontology

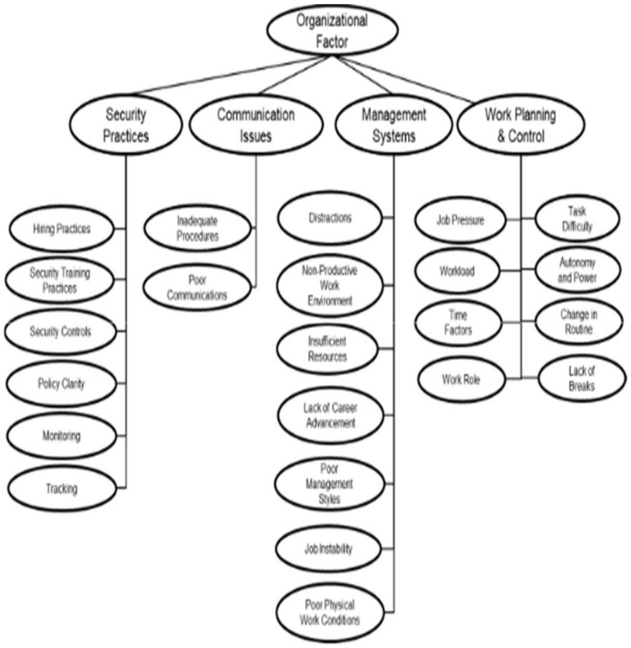

Figure 2: Organizational Factor Branch of SOFIT ontology

4. INSIDER THREAT DIMENSION

Insider threat researches has been actively conducted over the years to identify, analyze, apply and evaluate best approaches to build a foundation for decision makers to face the ever-growing threat. There were multiple reviews, suggestions, frameworks and models proposed to give essential ideas to the concept but integration of factors from multiple dimensions to give a broader knowledge for solution is still insufficient. Addressing the technological solution such as correcting vulnerabilities, enforcing policies and introducing defense in depth could only solve technical issues with insider threat [17]. Meanwhile, addressing the personality aspects of an employee such as survey on mental health, inspecting dissatisfaction and other social involvement could only address psychological traits of employees [18].

A study on behavioral aspects of an employee, which includes the changes in behavior, addressing current motivation and attitude towards particular situation could clarity the associated behavior of an employee [1][12]. In addition to that, organization and work environment factors also triggers inadvertent insiders. Although, insider threat factors are interrelated to each other in contributing to the insider threat, categorizing them separately based on its respective dimensions is necessary. Each dimension analyzed in depth to scrutinize the most contributing factors in that particular dimension to understand its effect on employees. The base understanding can enrich the threat detection whereby effective countermeasures can accommodate to reduce the number of cases. Based on findings above, it is obvious that there are five different dimension of insider threat such as psychological, behavioral, technological, organizational and environmental is needed as illustrated in Figure 3 for detection purposes.

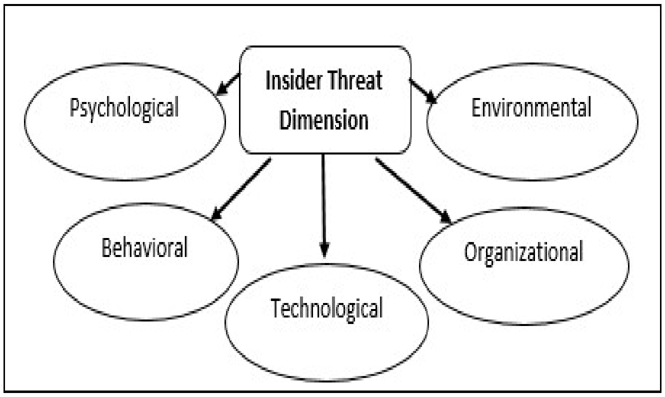

Figure 3: Insider Threat Dimensions

4.1. Psychological Dimension

Psychological dimension projected as the current mental state of an employee, which is a strong predictor of behavior among insiders also affects their external characteristics. Most of the time, employees are not behaving according to their own intention because intention is associated with their cognitive process whereas the behavior is about the spontaneous impulsive response towards a situation [14]. Psychological state of an employee often invisible to management but their actions is visible and creates a perception on them. There are many factors identified as the contributor to the negative psychological traits among which organizational politics are external factor that affect the mentality of an employee. Enforcement of new policies, beliefs, set of rules and changes in environment could give impact to employees.

Change management should implement in a more formal way from the beginning to encourage employees to grow together with the organization. This is important to avoid any gap between management and employees as many could disagree or unhappy with the new process of work execution. Constant communication regarding changes on the processes is crucial to avoid such differences. Researchers introduce psychological traits that could affect employees in both positive and negative in which negative psychology inspire workplace violence, maladaptive behavior and other unpleasant emotions towards management. This could influence employees to make emotional decision that could impose with justice and revenge towards management. Considering the negative emotion plays an important role in convincing an insider to turn as malicious and discordant to organization's policies, this research will focus on the widely accepted negative personality traits such as Dark Triad model and Big Five-Personality Model [18] as depicted in Figure 4 and Figure 5 respectively. For a more transparent research purposes, the most relevant element among others under each personality traits analyzed for its impact on employees.

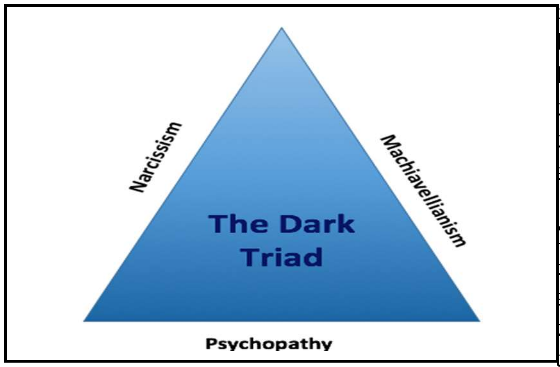

Figure 4: Dark Triad model

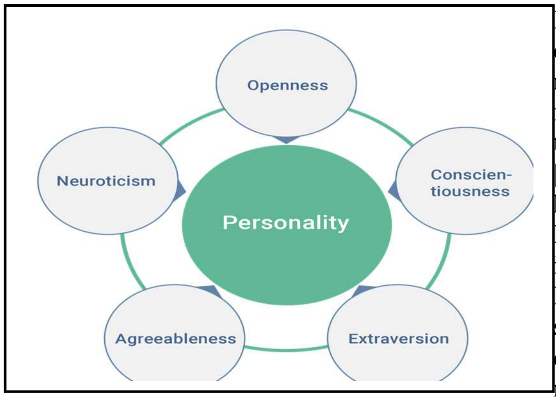

Figure 5: Big Five-Personality Model

4.1.1 Narcissism

Narcissism is one of the underlying psychological aspects under dark triad personality traits that represents malevolent qualities and extreme selfishness in a collaborative situation o act unethically for personal gain [19]. An employee who is egocentric about their own qualities and capabilities could demonstrate negative attributes and relationship with other employees. A narcissist is someone who is willing to take vengeance on others by changing perception towards an issue according to their needs at that moment. They also love to be acquainted with important people for their own benefit and easily get bored with the same routine job. A narcissist expects them to be center of attention and always self-claim as a natural leader of the team in which team activities could not succeed without their involvement [20]. A narcissist also carries a dominance over others in organizations and tend to find weaknesses in others to expose at the right time to overcome any challenges from them. They are extremely proud of their way of thinking and behaving while shows the sense of entitlement and grandiosity in any involvement, which develops negative relationship with others in organization. Usually, they are good at attracting others in their first interaction to gain trust and may recruit others to follow their belief and ideology [21]. Most of the time, narcissist will never admit their mistakes and may accuse others in the process.

Moreover, a narcissist also shows poor financial behavior which can be related to their aggressiveness during an ego clash during decision-making task in management. Most of the time, a narcissist willing to justify their malicious act to ensure they not judged wrongly and to gain the trust of management. According to Narcissist Personality Inventory (NPI), self-sufficiency and exhibitionism is a common characteristic of a narcissist since they possess the underlying feeling of knowing everything and do not hesitate to exploit themselves when an opportunity arises [19]. Besides, the motivation to act unethically to have a strong need for validation is the result of lack of socialization. Lack of socialization and interactions since childhood cause them to have lack of empathy towards others even in critical stage. Therefore, narcissism is a malevolent quality that triggers an insider to become malicious and bring costly damages to IT organizations.

Hypotheses 1: Narcissism is positively influence malicious intent in an insider threat incident

4.1.2 Neuroticism

Neuroticism is a one of the psychology traits from a widely accepted big five personality traits that relates to emotional instability. An insider who is affected with neuroticism often falls into mental disorders such as mood and anxiety disorders that triggers them to be self-isolating without mingling with others [21]. Those who are self-isolated often find sources outside from organization to communicate and share information. Insiders who were extremely sensitive are likely get affected by neuroticism whereby they often find an ordinary situation as more challenging and threatening while minor frustrations in job felt as unusual and hopelessly difficult. Meanwhile, an insider who scores high for neuroticism will be most likely have high tendency to complain about everything. They simply have a poor ability to control emotions towards a decision and often have poor tendency to detect lies while overestimate the response of others in an organization. They tend to believe others blindly with the perception that everyone is truthful and may fail to detect lies [22]. The likelihood of these insiders to fall for phishing attacks through social engineering are very high and become as a source of information provider for outsiders [23]. Employees affected with neuroticism also tend to get upset with other employees who does not believe in their perception and often prefer to work alone. Loneliness is a way for them to avoid disappointments, which is highly detected among female employees. Their internet behavior is a concern for management since those who prefer to work alone or isolating themselves from others could spend more time on the internet. Therefore, it is common for them to become an online fraud victim. Organization finds difficulties in managing them if their personality not thoroughly explored since they are vulnerable for multiple online threats. Studies shows they are vulnerable to different addictions, which could cause a harm to organization. Therefore, probability of an insider with high score on neuroticism more likely can engage with an insider threat incident within organization.

Hypotheses 2: Neuroticism is positively influence malicious intent in an insider threat incident

4.1.3 Extraversion

In contrast to the neuroticism, extraversion, which is opposite to introversion relates to an active and enthusiastic individual. Unlike other big five personality traits, extraversion explains the positive side of an insider. An insider who is an extravert is someone who likes to work with people and has good interpersonal communication skills [24]. They always have straightforward attitude towards fellow colleagues, job assignments and top management. An extrovert does not feel lonely as they are friendly to everyone and open minded when it comes to find a common solution. They often does not hide their true feelings and action behind them, as they tend to be sociable [12]. Most of the time, positive psychological aspects contribute well to the organization but somehow in many cases it indirectly causes trouble to the organization. Extraversion reflects negatively towards malicious intent but somehow there are facts about extrovert that could possibly related to insider threat. Extrovert are excitement and thrill seekers, as they tend to experiment their recklessness with opportunities that are available. Meanwhile, an employee with higher extravert usually unable to work in a team even if they believe doing so. The focus of a team could possibly biased with an extrovert in a team [18]. This is because extrovert often have difficulties with concentration on task, which is on a timeline, and tend to show impatient towards other teammates who are behind schedule. This often leads to conflict among the teammates and loss of the sense of togetherness among teammates. In this case, an extrovert either can finish his tasks earlier or postpone it to some other time by blaming other teammates for the decision. Management of finds difficulties in finding agreeableness within team about tasks they carried on. Besides, they also can possibly be a victim of social engineering attack since they are always being expressive towards everyone and easily are connected. This might lead to lack of extra-cautious in social networks activities that could victimize them to phishing vulnerability and possible attacks [25]. IT organizations need to investigate insiders for extraversion, as it is often going unnoticed and the fact that an extravert can possibly neutralize their actions. The act of neutralization is to maintain their reputation within organization and to justify their mistakes by giving appropriate reasons for the damages created which believed and accepted by organization as genuine. Hiding behind justification and rationalizing wrong actions seen as malicious since they are hiding the real incident that happened.

Hypotheses 3: Extraversion is positively influence malicious intent in an insider threat incident

4.2 Behavioral Dimension

In the context of IT organization, behavior of an employee interpreted as system related activities, which also known as an insider's security behavior. Generally, behavior is an attribute of an employee that influenced by many aspects such as personal belief, cultural background, political stand, and emotional attitude depends on the legitimate and accidental insider [23]. Cyber counterproductive work behavior is commonly a negative aspect of behavior such as fraud, theft, workplace aggression, cyberstalking and infrastructure abuses that against legitimate interest of an organization. It may cause disharmony among employees due to interpersonal conflicts and increasing workplace deviance by colluding with peers. Meanwhile, accidental insider are being a cause of threat due to lack of security awareness, lack of technical skills and techno-stresses [1]. This research will investigate the impact of behavioral aspects of an employee such as motivation and capability based on commonly discussed theories such as situational crime prevention theory, CMO model and Innovative behavior traits as an independent theory as illustrated in Figure 6 and Figure 7 respectively.

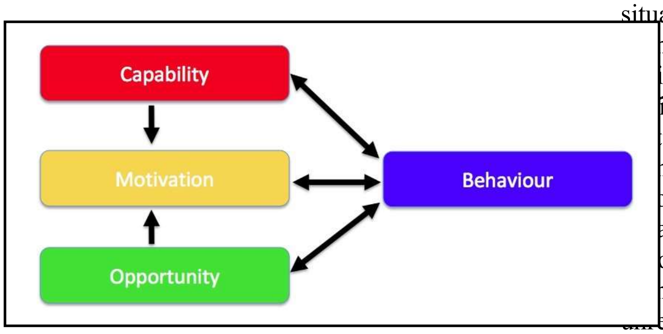

Figure 6: CMO model

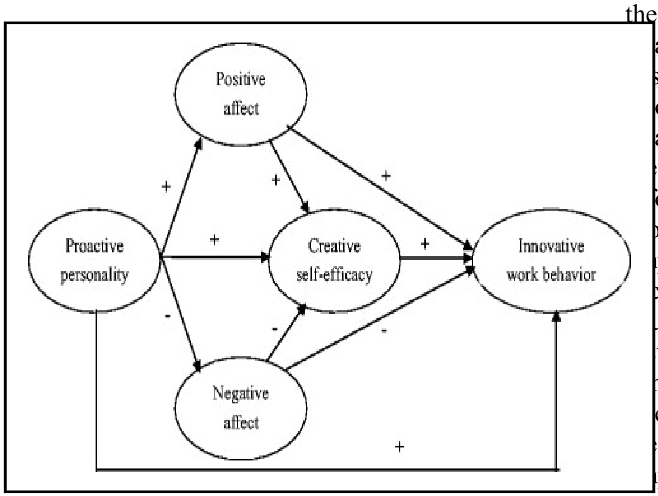

Figure 7: Innovative Behavior Traits

4.2.1 Motivation

Previous researches found motivation is the root cause of behavioral changes among intentional insiders who influenced by personal gain, revenge, political, cyberbullying, skill set, reputation and information theft. Most of the time, motivation is not carried at the beginning when an employee joins the organization but later intention changes due to variety of reasons [4]. High-end insiders are employees who are motivated with malicious mission and execute them in a long term without a trace. Motivation to engage in a destructive behavior often triggered due to both internal and external changes that influence an insider from losing their dedication. Internal changes related to underlying psychological disorder due to personal problem and stressful lifestyle that carried from outside into organization whereas external changes are surroundings of workplace that is challenging and uncomfortable to them [7]. IT organizations consists of frontlines who manages and illicit access to the critical infrastructure all the time from office or remotely. During the pandemic situation, many organizations are working from he accessing the office network and managing ical information. Most of the organization are icult to predict the current state of employee's ivation since there is less interaction at the mises. Meanwhile, there are concerning cases orted regarding employees who joining the anization with malicious intent to cause trouble organization. Corporate crimes often exists hin white-collar community and goes eported due to the reluctance to reveal those incidents and their losses due to the damages to their business and reputation [26]. They sent by al companies with motivation to attack at any st to damage the reputation from within. It may o because of financial gain besides revenge on al company. Industrial espionage is a type of thod used by competitors to steal physical ormation, corporate secrets, pattern and totypes using individuals in the form of ployee who is an insider with certain level of cess privileges. Criminals in the form of insiders uld have free access to corporate facilities, tricted files and electronic system access which nply their tasks [27]. Since the impact of insider eat is still at worrying state, a proper chanism to address the motivation of the ployees should be in place.

Hypotheses 4: Motivation is positively influence malicious intent in an insider threat incident

4.2.2 Capability

IT organizations consists of professionals, administrators, system owners, programmers, network administrators and operations heads who owns necessary skill sets and access privileges to perform daily tasks. Access privilege is a key for an insider that make them capable to access sensitive data that is critical for organization's business and reputation can be accessed anywhere from world. Most of the high-end insiders are IT professionals that have knowledge, experience and technical skills compared to others in the organization and capable to use the intelligence to create an opportunity to execute fraudulent. In some organizations, they are the decision makers who develops and execute the policies and procedures on handling critical assets. The primary weaknesses of the execution of policies are the unavailability of mechanisms monitor the activities of the content developer instead of users. The top management trust the content developers blindly and always fail to introduce a mechanism to monitor their ICT activities as well. The capability of malicious insider who is technically good will rapidly gather data, accurately process information and strategically sabotage them [28]. Moreover, capability also gives insiders an advantage to neutralize and justify their fraudulent activities using neutralization techniques and reasoning structures, which were unable to doubt by others. Meanwhile, the feeling of superiority over others also could trigger them to use their system capability to engage in malicious activities. Some of the high-end insiders tend to use their role and capacity to persuade others to engage in a threat [29]. Meanwhile, most of the employees are using the opportunity arise within organization to develop capability such as knowledge on weaknesses and strengths of operations, policies and procedures. Insiders that capable to gain access beyond their restrictions are engaging in untraceable activities using their skill sets. There are also malicious insiders who uses another employee without his knowledge to perform threat against organization. User credentials theft is a way to misuse other's account to steal valuable information from organization. In some cases, surprisingly some working colleagues still sharing credentials among themselves to execute daily tasks, in which a malicious insider would take advantage to misuse the opportunity. Advanced Persistent Threat (APT) is a type of threat used by capable insiders to use a compromised host as an agent to collect critical information without noticed by anyone. The host will listen and grab all the information that the system transacts. Usually, they hide behind the legitimate activities and rapidly changing malicious domain names that used to collect information. Insiders who involve in APT constantly changes the domain names and leaving limited evidence, which made others difficult to detect. Most of the time, a little number of temporal evidence were left after the successful attack which leave any form of forensic investigation is difficult to conduct. Therefore, capability is malicious insider's key to execute a threat incident successfully.

Hypotheses 5: Capability is positively influence malicious intent in an insider threat incident

4.2.3 Innovation

The rapid pace of cyber technology innovation leads many organizations to invest on upgrading and evolving from the current solution to a more productive solution. IT organizations are the center of the innovation as the cyber technology continues to evolve and will need to hire innovative people to make changes and support the cyber workforce [30]. Innovators has been hired from outside to introduce a new method, product and solution as part of creativity and to lead innovation in IT organization. Besides, innovative work behavior theory explains characteristics of innovators have the propensity to behave in isolation since they believe they are superior to others in the team and could destroy the innovative nature of an organization. Similar to psychological personality traits, Innovative personality traits explains the characteristics and features that found among innovators [31]. Trait of concern found in innovative traits that has similarities to insider threat personality, which an organization should eliminate during the hiring process [32]. Meanwhile, innovative behaviors posed by innovators often seen as risk takers, disruptors, impractical and works under unstructured environment that could develop a gap between existing less or non-innovators. Moreover, active employees who known as innovative thinkers among organization would proactively seek for new opportunities within organization to seek for new work processes and knowledge. Frustration built when they failed to fulfill their intention could lead to affective valence. Besides that, concerns raised over innovators as only they could thoroughly understand and operate the new invention over others. The pattern and framework of the new invention is solely depending on innovators rather than management. Any changes, updates and maintenance work will refer to the innovators or lead by innovators. It will definitely put them in a special place and felt superior to others in organization. They also claim an unmovable spot in organization and felt untouchable by anyone. Indirectly this will give them more courage and confidence in their action and even do not hesitate to go against the policies and procedures. Eventually, their position will negatively influence innovators to involve in malicious activities that could harm the resources. Therefore, innovative behavior considered as triggering an insider to involve in malicious activity against IT organization,

Hypotheses 6: Innovative behavior is positively influence malicious intent in an insider threat incident

4.3 Technological Dimension

Technological advancement and innovation increase the chaos among IT professionals who concerns about information leakage, fraudulent, and internal sabotage of critical information. It is a realistic threat, which comes from insiders who are intentionally and unintentionally produce disastrous damages. Naturally, IT professionals have mechanisms to identify possible threat, trace back the source of threat and pre-planned countermeasures to mitigate potential threat. However, violation towards the mechanism imposed is common among the authorized personal. IT professionals may intentionally skip technical procedures to simplify the process for personal benefit, which leads to intentional violation. These violations may trigger insiders to make one-step further to intentionally execute immoral activities digitally or physically towards valuable assets [33]. Although, many organizations adopted defense-in-depth methodology to counter the attack, lack of awareness among unintentional insiders could pave ways for malicious people to go beyond the boundary.

4.3.1 Cybersecurity Violation

Cybersecurity violation describes digital security breaches and violation such as abusing access privileges that produces devastating implications on system. During the pandemic situation, employees working from home by remotely accessing to office assets, which may increase the risk of cybersecurity violation because of lack of control over employees who is away from organization [34]. Most of the organizations does not prepare for sudden changes to the operations that accessed and conducted remotely. There was not enough time for organizations to explore the secure mechanisms and right tools to connect to office remotely. Decisions made on at quickest as possible to maintain operations running without any disruptions by adopting and subscribing remote devices and tools which may not familiar among employees. Organizations also does not have ample of time to train the employees about the new norm of work to ensure save working environment. Meanwhile, IT literate employees may use unauthorized tools to access office assets remotely could increase the risk of data manipulation and information leakage. Lack of monitoring over users away from office premise since their access does not fall under organization's surveillance, which could increase anonymity. Malicious insiders can be both with and without access privileges. Insiders who hold genuine authorization and authentication could misuse it for intentional exploit and personal benefit. Moreover, intentional insiders deliberately involve themselves in sequence of action that violate the ICT security policies such as unauthorized command line usage and other suspicious communications over internet [15]. Principles of least access privileges practiced by most of the IT organization to limit the access only to authorized personal to perform modification but somehow the trusted party has betrayed the trust with their delinquent behavior. Inadequate separation of privileges causes both intentional and unintentional insider to freely access internal resources without filtration. Insiders who do not own access privileges will probe and attempt to steal information from others using social engineering attack to gain access to the system. Illiterate employees on ICT devices could be a victim of remote access whereby they can be a victim of man in middle attack. Employees with lack of awareness or training on ICT security would be a liability who could unintentionally violate cybersecurity policies and accidently leak company secrets online. Therefore, cybersecurity violation whether intentionally or unintentionally will trigger insider threat incident.

Hypotheses 7: Cybersecurity violation is positively influence malicious intent in an insider threat incident

4.3.2 Boundary Violation

In the perspective of IT organization, boundary violation related to an employee breaking or crossing his/her predefined responsibility, functions, positions and attributes in the organization. Each individual in an organization has certain level of limitations that related to job scope, regulations, and behaviors [2][7]. When an employee intended to go beyond the limitations, it can be categorized as a concerning work habits and should addressed immediately. It happens because the employee has an unclear vision towards personal/professional boundaries whereby personal issues often mixed up with profession. This may increase threats such as attendance issues, threatening and intimidating behavior towards others and minor policy violations. In addition to that, security violation that recorded by an employee who crosses his/her boundary should give immediate warning to prevent any further risks to the system. Sometimes, the concern with boundary violation are non-technical issues such as unauthorized foreign travel and travel policy violation, which could affect their system behavior. Most of the IT organization considers boundary probing as an underlying issue and accepts it as long as it does not affect the operations. However, in later stages it might harm the policies that causes security violations [2]. Social engineering also considered as boundary violation as sensitive information about organization should not discussed or shared publicly. Boundary can also be physical aspect in which each employee has a limitation to have a physical presence within organizations. Sensitive areas such as data center is a limited access area and usually breaches were related with unauthorized access. Entering without permission using others credentials or breaking into sensitive areas often related to malicious intention. Besides that, take ownership on others responsibility without their consent is also an act of breaching their positions and responsibility. In that case, an employee who breaching their boundary at workplace is consider as influencing threat incident.

Hypotheses 8: Boundary violation is positively influence malicious intent in an insider threat incident

4.4 Organizational Dimension

Most of the employees are motivated, committed and dedicated towards job at the point of joining organizations. However, multiple reasons caused them to lose their dedication towards work and became a threat to organization. Organization is one of root cause that triggers an insider to act against the them since they were affected by unpleasant feelings due to uneven workload and poor separation of duties [4][35]. Organization often blames an individual for his/her malicious behavior, errors and unintentional threat and refuse to review their management system but intend to overlook the root cause of the problem [6]. Organization consists of set of people works together to produce common outcome using technology that defined by set of policies and operating procedure. IT organizations implement information security policies as a guideline for employees on the do's and don'ts to preserve the confidentiality, availability and integrity of information assets. However, compliance issues among insiders have been an alarming factor since organizational culture overwrites information security policies [36]. This is because the security decision made often influenced by work culture that affect mentality and decision-making.

4.4.1 Time Pressure

Time plays an important role in IT organization in decision-making strategies and to employees on their cybersecurity behavior. Employees demonstrate non-secure cybersecurity behavior because unable to cope up with the time pressure due to catching up with the datelines with excessive workload. Top management often set a timeframe for project to meet completion in the concept of need-it-fast at any cost triggers work stress among IT professionals. This is because of the pervasiveness of technology that increase the complexity of infrastructure often interrupts tasks from completed on time [37]. Besides, unrealistic timeframe to meet the deadline of project added with poor matches of workers to skillset will engage more pressure and confusion to employees that might lose motivation to work. Studies on human cybersecurity behavior also shows employees that work on multiple projects often meet with severe time constraints, as they need to multitask by finishing both primary and additional tasks. Driven by the high expectations from management and time constraints, IT professionals can have detrimental effects to their cognitive and affective process and outcomes [36]. Sometimes, an individual's perception and attitude towards changes in deadline and time pressure also influence their decision-making activities. Adding to that, some IT professionals able to cop up with the time pressure and accepts the nature of work but some views it as a burden to them. Besides, due to time constraints many organizations neglect secure behavior while running a project. The priorities are to race towards finishing the project soonest due to time pressure and care less about cybersecurity behavior [23]. This will indirectly promote non-secure behavior, which may cause harm to the critical assets. Under time pressure, even security experts also became a victim of social engineering traps in which they became a victim by phishing emails. As time pressure grows, general employees also tend to get frustrated with security requirements and willing to bypass it in order to simplify the process. Each employee has varying opinion about the security in general and their approach would be different from others. Some of them may attempt to misinform others with their perception about security and influence them negatively. This is because security perceived as least priority under time pressure. Bypassing and breaching security intentionally will open door for accidental leakage of critical information.

Hypotheses 9: Time pressure is positively influence malicious intent in an insider threat incident

4.4.2 Management Systems

IT organization should implement effective management systems to reduce the opportunity of insider threat proactively and.to ensure stability, productivity and show commitment to employees. Even though management system in place, some IT organization does not practice it due to lack of awareness on employee welfare concerns. Poor management styles of running organization will lead to dissatisfaction, disgruntlement and lack passion towards work [2][11]. Meanwhile, improper organization policies and assurance that cause instability may influence uncertainty among employees and unhealthy working environment. Meanwhile, employees need to be free from external distractions such as pressures from superiors, unrealistic work schedule, insufficient remunerations and uneven job separations. Employers must ensure employees have an unbreakable trust and commitment towards organizations with providing salary hike, promotion, remunerations, bonuses and other wellbeing. Besides, insufficient resources such as also force employees to work in a disharmony, which affects their job performances and their motivation. Lack of career advancement also force employees to take drastic actions by involving in destructive actions that disrupts the operation [7]. Moreover, during pandemic situation, many employees face difficulties to sustain their job and face retrenchment due to mismanagement or does not have suitable employee management system to help them. Employees would react negatively towards such disastrous news and might take revenge back by engaging in internal attack to demolish critical assets.

Hypotheses 10: Improper management system is positively influence malicious intent in an insider threat incident

4.4.3 Security Practices

Although IT organization implements security controls and countermeasures to prevent any kind of threat towards critical infrastructure, the importance of security awareness and practices often overlooked or given less importance in the application. Security training given to employees at the beginning of hiring into organization and assume employees are aware of the security practices in place at IT organization [38]. Due to growing security concerns, organization introduce new security controls to counter new threat patterns but the awareness only limited to IT professionals who are managing it. Instead, policy clarity should spread to everyone in organization with proper training. In other cases, many organizations reluctant to upgrade themselves with new technology update because it involves cost. They often opt to renewing the current solution which they feel enough to counter the basic problem. Cybersecurity concerns grows often and new solution may need to counter new types of threat to organization. Loopholes due to the old solutions could be a vulnerability that exposed by employees from within. Meanwhile, monitoring and tracking of any kind of security concerns such as cyber-attack, policy violations and data forgery should plan periodically and proactively. Besides, many organizations consider the knowledge and skills of an employee during job hiring process and give less concern about background of employee related to ICT security concerns. A proper background check about previous employment and records should also take into account to avoid hiring potential problematic employee [23].

Hypotheses 11: Improper security practice is positively influence malicious intent in an insider threat incident

4.5 Environmental Dimension

Working environment is crucial to create a good healthy atmosphere that boost the motivation and dedication of employees to complete assigned tasks. Commitment is associated with good leadership that ensures the safety environment with sufficient resources to help simplify the job [18]. Management also should ensure employees motivation is in good condition by frequent check on mental and physical health. Mental health check is crucial to ensure employees stay positive about their organization's mission. Constant communication with employees to find out their concerns about job is a proactive step to identify and rectify at early stages to avoid insiders turn malicious [39] Job satisfaction survey can help management to find out the current level of motivation with those employees who are reserved to express their feelings.

4.5.1 Non-productive

Non-productive work environment could pave ways for inadvertent insider turns into disgruntled insider and transform into malicious insider [40]. Bullying at work is an incident at a non-productive environment in which an employee could turn to revenge another employee by exploiting him for personal satisfaction. Meanwhile, working environment that does not follow standard and recognition could distract insiders. Usually, companies that does not follow the standard in practice should have not follow a proper operating procedure. During the current pandemic situation, many organizations have to adapt in a new norm of working whereby many works process executed and monitored remotely. There was new operating procedure introduced for those who working onsite that organization should follow. However, those organizations that not adapting to new norm, forcing employees to work as normal as before and risking the employee's life. This could pave ways for employees to show their dissatisfaction through internal threat. Moreover, employees often demonstrate their competitive advantage among each other to expect for appreciation from colleagues. When expectation does not fulfill communication, issues arise among employees that will even worsen the situation. Communication among employees are crucial to complete tasks since most of the IT projects needed a collaborative effort to complete [36]. When healthy communication does not exist, employees with malicious intention to get revenge can arise that will affect the overall motivation of the organization.

Hypotheses 12: Non-productive environment is positively influence malicious intent in an insider threat incident

4.5.2 Rationalization

Rationalization exists in an unproductive work environment among irresponsible employees and human tendency to rationalize certain behavior. Rationalization is a neutralizing techniques used by insiders to justify their suspicious activities with almost perfect reason to convince management to escape from any further punishments [36]. Denial of responsibility is a type of neutralization technique in which, an act of violation is justified as a victim of circumstances or they forced to act such in desperate situation. They also tend to use another technique called denial of injury by justifying their act does not cause damages to any organizational asset. As part of an organization, insiders are well verse of the work environment with loopholes in system and vulnerabilities in security. That backdoor access to the system used by insiders to use for cyber loafing and policy-breaking activities. They pretend to perform legitimate work and managed to convince organizations if any doubts raised against them. Organizations also have introduced sanctions to combat the deviant behavior of employees but somehow it does not work since the neutralization techniques often stronger than sanctions in influencing intentions to continue to violate. Organization should realize neutralization techniques are strong predictors of IT security policy violation. Moreover, non-compliance towards security policies that practiced by some could create loopholes in work environment which can spread across organization. Organizations that failed to inspect the environment will give indirect opportunity to perform unethical activities. However, insider denies his malicious intention by manipulating the intention by giving acceptable reasons [29]. Instead, they blame weakly controlled environment and unclear code of conduct for breaching the policies such as unavailability of physical control at the premises [17].

Hypotheses 13: Rationalization is positively influence malicious intent in an insider threat incident

5. PROPOSED MODEL

The proposed solution is a model that gives a holistic approach to insider threat detection whereby the constructed model based on most contributing factors that gathered from multiple dimensions. IT professionals can implement the proposed model as a guide for further investigation among insiders to inspect the existence of recommended in their organization. Therefore, Figure 8 illustrate the proposed model.

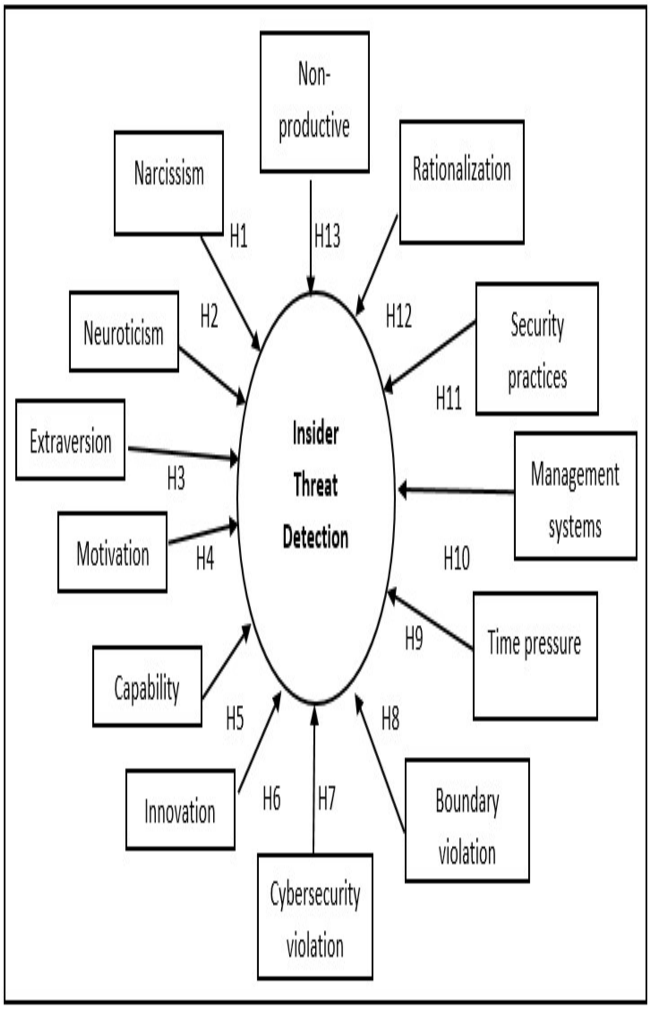

Figure 8: Proposed Multidimensional Insider Threat Detection Model

6. CONCLUSION

Organizations should give continues concern and learn from current trend since insider threat is an issue that will exist throughout employment. The proposed model gives an overall solution to insider threat since it addresses multidimensional aspects of an organization to counter insider threat. It achieves the objectives of the research by scrutinizing factors from every dimension of insider threat and the area of concern that an organization should continuously improve to ensure the integrity, confidentiality and availability of critical information. The research is limited to the research investigation based on recognized dimensions and on review of existing models. Attributes that found as most relevant under each dimension in contributing to insider threat gathered under a model to rectify the understanding and view of organization towards insider threat. However, there may have dimensions that newly added to mitigate insider threat in a more effective way. In future, the proposed model will get enhance to address the insider threat issue at the hiring process of an employee. The model also will be tested and upgraded after a brief survey among IT professional and in depth analysis of result to enrich the model.

7. ACKNOWLEDGEMENT

The authors would like to thank Universiti Teknologi Malaysia (UTM) for their assistance and support for this work through the Tier 2 Grant Scheme under vote number Q.K130000.2656.16J43.

REFERENCES

[1] A. J. C. Bell, M. B. Rogers, and J. M. Pearce, “The insider threat: Behavioral indicators and factors influencing likelihood of intervention,” *International Journal of Critical Infrastructure Protection*, Vol. 24, 2019, pp. 166–176.

[2] Frank L. Greitzer, “Insider threats: It’s the Human, Stupid!,” *Proceedings of the Northwest Cybersecurity Symposium (NCS’19)*, April 8, 2019, pp.1-8.

[3] Sixuan Zhang and Dorothy Leidner, “From Improper to Acceptable: How Perpetrators Neutralize Workplace Bullying Behaviors in the Cyber World,” *Information & Management*, Volume 55, Issue 7, 2018, pp. 850-865

[4] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K. K. R. Choo, and P. Burnap, “Impact and key challenges of insider threats on organizations and critical businesses,” *Electron.*, Vol. 9, No. 9, 2020, pp. 1-29.

[5] H. Habibzadeh et al., “A data analytical approach for assessing the efficacy of Operational Technology active defenses against insider threats,” Procedia Comput. Sci., Vol. 153, 2019, pp. 100–107.

[6] S. Wilson *et al.*, “Cognitive security: A comprehensive study of cognitive science in cybersecurity,” *Futur. Gener. Comput. Syst.*, Vol. 48, 2018, pp. 1–6, 2018.

[7] S. Quarter, “Positioning Your Organization to Respond to Insider Threats,” Vol. 47, No. 2, 2019, pp. 75–83.

[8] M. N. Apau, M. Sedek, and R. Ahmad, “A Theoretical Review: Risk Mitigation Through Trusted Human Framework for Insider Threats,” *2019 Int. Conf. Cybersecurity, ICoCSec 2019*, 25-26 September, 2019, pp. 37-42.

[9] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, and M. Ochoa, “Insight Into Insiders and IT,” *ACM Comput. Surv.*, Vol. 52, No. 2, 2019, pp. 1-40.

[10] I. A. Gheyas and A. E. Abdallah, “Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis,” *Big Data Analytics*, Vol. 1, No. 6, 2016, pp. 1-29.

[11] S. N. Isnin *et al.*, “Cognitive security: A comprehensive study of cognitive science in cybersecurity,” *Procedia Comput. Sci.*, Vol. 153, No. 10, 2019, pp. 100–107.

[12] Pletzer, Jan Luca & Oostrom, Janneke & Bentvelzen, Margriet & de Vries, Reinout. “Comparing domain-and facet-level relations of the HEXACO personality model with workplace deviance: A meta-analysis. Personality and Individual Differences”, *Journal of Vocational Behavior*, 2019, pp.1-48.

[13] S. Shunmuganathan, R. D. Saravanan, and Y. Palanichamy, “Securing VPN from insider and outsider bandwidth flooding attack,” *Microprocess and Microsystems.*, vol. 79, 2020, pp. 1-10.

[14] Shappie, A. T., Dawson, C. A., and Debb, S. M., “Personality as a Predictor of Cybersecurity Behavior”, *Psychology of Popular Media Culture*, 2019, pp. 1-6.

[15] F. L. Greitzer, J. Purl, Y. M. Leong, and D. E. S. Becker, “SOFIT: Sociotechnical and organizational factors for insider threat,” *Proc. - 2018 IEEE Symp. Secur. Priv. Work. SPW 2018*, February, 2018, pp. 197–206.

[16] Greitzer, FL, M Imran, J Purl, ET Axelrad, YM Leong, DE Becker, KB Laskey, and PJ Sticha. (2016). “Developing an ontology for individual and organizational sociotechnical indicators of insider threat risk.” *The Eleventh International Conference on Semantic Technology for Intelligence, Defense, and Security (STIDS 2016)*, Fairfax, VA, November 15-16, 2016, pp.1-9.

[17] Tesleem Fagade and Theo Tryfonas, “Malicious Insider Threat Detection: A Conceptual Model,” *Secur. Prot. Inf. 2017*, 2017, pp. 31-44.

[18] Alistair Raymond Bryce Soutter, Timothy C. Bates, and René Mõttus, “Big Five and HEXACO Personality Traits, Proenvironmental Attitudes, and Behaviors: A Meta-Analysis”, *Perspectives on Psychological Science*, Vol.15(4), 2020, pp. 913-941.

[19] P. Muris, H. Merckelbach, H. Otgaar, and E. Meijer, “The Malevolent Side of Human Nature: A Meta-Analysis and Critical Review of the Literature on the Dark Triad (Narcissism, Machiavellianism, and Psychopathy),” *Perspect. Psychol. Sci.*, Vol. 12, No. 2, 2017, pp. 183–204.

[20] C. Sedikides, “In Search of Narcissus,” *Trends Cogn. Sci.*, Vol. 25, No. 1, 2021, pp. 67–80.

[21] Srinivasan S., Ananthapadmanaban K.R. (2020) Intelligent Agent-Based Organization for Studying the Big Five Personality Traits. In: Peng SL., Son L., Suseendran G., Balaganesh D. (eds) Intelligent Computing and Innovation on Data Science. *Lecture Notes in Networks and Systems*, Vol 118, 2020, pp.81-89.

[22] S. Yuan and X. Wu, “Deep Learning for Insider Threat Detection: Review, Challenges and Opportunities,” *Computers & Security,* Volume 104, 2021.

[23] S. Eftimie, C. Racuciu, R. Moinescu, and D. Glavan, Insider "Threats and thermal stress in the working environment,” vol. XXIII, No. 1, 2020.

[24] Bouabre Jean Baptiste Koffi, “Inferring Big Five Personality Factors using Text Analysis Its Assessment and Impact on Prosocial Behavior and IS Security Compliance”, *The University of Texas at Arlington*, Phd Dissertation, May 2020.

[25] K. M. T. Tianwei V. Du, Alison E. Yardley, “Mapping
Big Five Personality Traits Within and Across Domains of
Interpersonal Functioning”, *Assessment*, 28(5), 2021, pp.
1358-1375.

[26] T. Hou and V. Wang, “Industrial espionage-A systematic literature review (SLR),” *Computers & Security,* Vol. 98, 2020, pp.1-12.

[27] M. Button, “Editorial: economic and industrial espionage,” *Secur. J.*, Vol. 33, No. 1, 2020, pp. 1-5.

[28] D. Y. Kao, “Cybercrime Countermeasure of Insider Threat Investigation,” *Int. Conf. Adv. Commun. Technol. ICACT*, February, 2019, pp. 413-418.

[29] M. Radhakrishnan *et al.*, "Proposed Insider Threat Detection Model For Malaysian Government Agencies," *Open Int. J. Informatics*, Vol. 6, No. 4, 2018, pp. 54–67.

[30] N. A. N. Mohammad, W. M. Yassin, R. Ahmad, A. Hassan, and M. N. A. Al Mhiqani, An Insider Threat Categorization Framework for Automated Manufacturing Execution System," Int. J. Innov. Enterp. Syst., Vol. 3, No. 02, 2019, pp. 31–41.

[31] M. Li, Y. Liu, L. Liu, and Z. Wang, "Proactive Personality and Innovative Work Behavior: the Mediating Effects of Affective States and Creative Self-Efficacy in Teachers," *Curr. Psychol.*, Vol. 36, No. 4, 2017, pp. 697–706.

[32] Adam Humphrey, "Do Innovative Thinkers Pose An Increased Insider Threat?: A Preliminary Analysis," *Masters Thesis*, Naval Postgraduate School, Monterey, California, June 2019.

[33] L. Ren, Xueshuang and Wang, "A Hybrid Intelligent System for Insider Threat Detection Using Iterative Attention," *Proceedings of 2020 the 6th International Conference on Computing and Data Engineering (ICCDE)*, January 2020, pp. 189-194.

[34] M. N. Al-Mhiqani *et al.*, "A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations," *Appl. Sci.*, Vol. 10, No. 15, 2020.

[35] L. Xiangyu, L. Qiuyang, and S. Chandel, "Social Engineering and Insider Threats," *2017 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov.*, Vol. 1, 2017, pp. 25-34.

[36] A. Vedadi and M. Warkentin, "Can Secure Behaviors Be Contagious ? A Two-Stage Investigation of the Influence of Herd Behavior on Security Decisions," Vol. 21, 2020, pp. 428–459.

[37] N. H. Chowdhury, M. T. P. Adam, and G. Skinner, "The impact of time pressure on human cybersecurity behavior: An integrative framework," *26th International Conference on Systems Engineering (ICSEng),* December 2018, pp. 1-10.

[38] B. Alotaibi and H. Almagwashi, "A Review of BYOD Security Challenges, Solutions and Policy Best Practices," *1st International Conference on Computer Applications & Information Security (ICCAIS)*, 4-6 April 2018, 2018, pp. 1-6.

[39] R. Zimmerman et al., "Modeling Insider Threat From the Inside and Outside : Individual and Environmental Factors Examined Using Event History Analysis", Defense Personnel and Security Research Center, Seaside, CA, Technical Report, August 2018.

[40] S. R. de S. N. Cardoso et al., "Human Factors In Information Leakage: Mitigation Strategies For Information Sharing Integrity," Vol. 3, No. 1, 2017, p. 87.