RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES
Social Science Journal

Development of Trusted Human Framework for Mitigating Risks of Insider Threats

By

Muliati Sedek
Centre for Language Learning, Universiti Teknikal Malaysia Melaka

Rabiah Ahmads
Centre for Advanced Computing Technology, Faculty of Information Communication Technology, Universiti Teknikal Malaysia Melaka

Aliza Che Amran
Faculty of Electrical and Electronic Engineering Technology, Universiti Teknikal Malaysia Melaka

Siti Norfatihah Isnin
Faculty of Technology Management and Technopreneurship, Universiti Teknikal Malaysia Melaka

Nurdayana Izyan Ahmad Ahsan
Centre for Language Learning, Universiti Teknikal Malaysia Melaka

Abstract

This study is exploring insider threat which define as the potential for an individual who has or had authorized access to an organization's assets to use that access, either maliciously or unintentionally, to act in a way that could negatively affect the organization. However, the propensity for the organization to grant the system and physical accesses to an employee, contractor, or business partner (insider) is unavoidable and evidently, literature reviews put forward on the complexity and challenging tasks for organization to manage this insider threats. Beside a technical or technological perspective, a framework with the element of people, process and technology embedded in the Employee Life Cycle would be able to provide alternative for organization to mitigate risks of insider threats. The proposed framework developed using qualitative method and empirical study to organization fully implement cybersecurity control in Malaysia. Practitioners who responsible in strategizing security controls for organizations were interviewed. Our controls components inspired from the Common-sense Guide to Mitigating Insider Threats produced by the Software Engineering Institute of Carnegie Mellon University. Data retrieved from responders analysed using Delphi and results shows that Trusted Human Framework used to mitigate risks by identifying potential detect potential employees (insider) who bound to become a fraudster or perpetrator by violating the access or trust given by the company (employer). Three factors such as motive, opportunity and method are essential to be recognized, identified and suppressed within the organization boundary to stop the insider threats or attacks to happen. As a conclusion, the outcome of this study would be able to assist organization to understand further the general acceptance of the control practices and motivate the organization to strengthen the effort in mitigating insider threats. The suggested framework is also aimed to inspire more organizations to consider identifying insider threats as one of the risk in their company's enterprise risk management activities.

Introduction

Nowadays, the world is facing with the demand of effective services and productivity. In every business, quality of services and performance always a priority. Thus, to achieve target and increase productivity, organizations must make sure internal operations are functioning and be able to produce outcome as expected. The rapid growth of ICT and its components able to support productivity in the organizations. However, the advancement of ICT also put systems in the organization at risks. Risks of ICT has become major concern to employer in an organization.

Information Security is an area which introduce controls as protection mechanism to ICT systems. Risks to information security involve with threats identifications and what are the appropriate controls. Information Security Risks management start with identification of assets and threats associated with its. Threats can be divided into two accidental and deliberate. Risks associated with information security threats will be able to destroy internal system and finally lock all operations. Destruction of system will reduce productivity and finally reputation of organization. This study is about risks mitigations and the risks is caused by an internal threats or commonly known as insider threats.

Insider threats emerged and selected for the purpose of this study because of the necessity to explore and understand it further from the perspective of this country. It is essential, especially when the government of Malaysia acknowledge that insider threat pose significant danger to the organization (Malaysia Cyber Security Strategy, 2020). However, despite the recognition from the Malaysian government, there are still insufficient studies from this country perspective. This was pointed out in Figure 1.3 via search result of document and/or journal submission in the Elsevier's Scopus® online portal (last assessed on 31 March 2022).

Under the Malaysia Cyber Security Strategy (2020), the government has acknowledged that insider threats remain a significant cyber security risk to organizations. Insiders with access to critical information systems and data pose a significant threat to any organizations. There have been numerous cases of intellectual property theft and the leaking of sensitive information that have caused substantial financial and reputational damage (CDSE, 2020) and there were also incidents where these insiders, either employees or vendors, unknowingly became victims of elaborate cybercrime through watering hole attacks, social engineering ploys, malware and ransomware infections, propagation mechanism by inserting infected devices into the internal networks or randomly clicking on links found in emails or while browsing the Internet (Malaysia Cyber Security Strategy, 2020). Those occurrences could happen when someone ("the insider") had violated the employer's (organization) trust. This event of trust violation could be prevented or mitigated if the company practices certain controls which will be deliberated in this paper.

Research on insider threat detection, deterrence and mitigation comprises of focus areas such as the (i) "who" and "what", (ii) the "why" and (iii) the "how". The "who" is to identify the entities that have access to the organization and what asset they have access to. The "why" is referring to social and behavioral science research such as exploring the motivation behind the attack. The "how" is on mechanisms, capabilities, and pathways that insiders might utilize in an effort to cause harm (Claycomb et al., 2022).

This article is structured into five continuous sections. Section 2.0 brief related works on insider threats, section 3.0 described method used and section 4.0 presents results and

discussed Trusted Human Framework as mechanism to mitigate Insider Threats. The final section concludes by addressing real implementation of the proposed framework. The following section provides a review of previous studies on insider threats and risks mitigations.

Literature Review

Information Searching

Research on insider threat detection, deterrence and mitigation comprises of focus areas such as the (i) "who" and "what", (ii) the "why" and (iii) the "how". The "who" is to identify the entities that have access to the organization and what asset they have access to. The "why" is referring to social and behavioral science research such as exploring the motivation behind the attack. The "how" is on mechanisms, capabilities, and pathways that insiders might utilize in an effort to cause harm (Claycomb et al., 2022).

The keywords of "insider AND threat cyber AND security (insider threat + cybersecurity)" was used as the input search. Based on that entry, Scopus® online portal produced 797 results of document submission from fifty-three different countries. The result showed that the highest articles published at the United States of America (US) (29%) and followed by United Kingdom (UK), India, Australia, China, Canada and so on. Only one article published from Malaysia. Figure 1.1 shows distribution of articles published in journal associated to Insider threats from all countries.

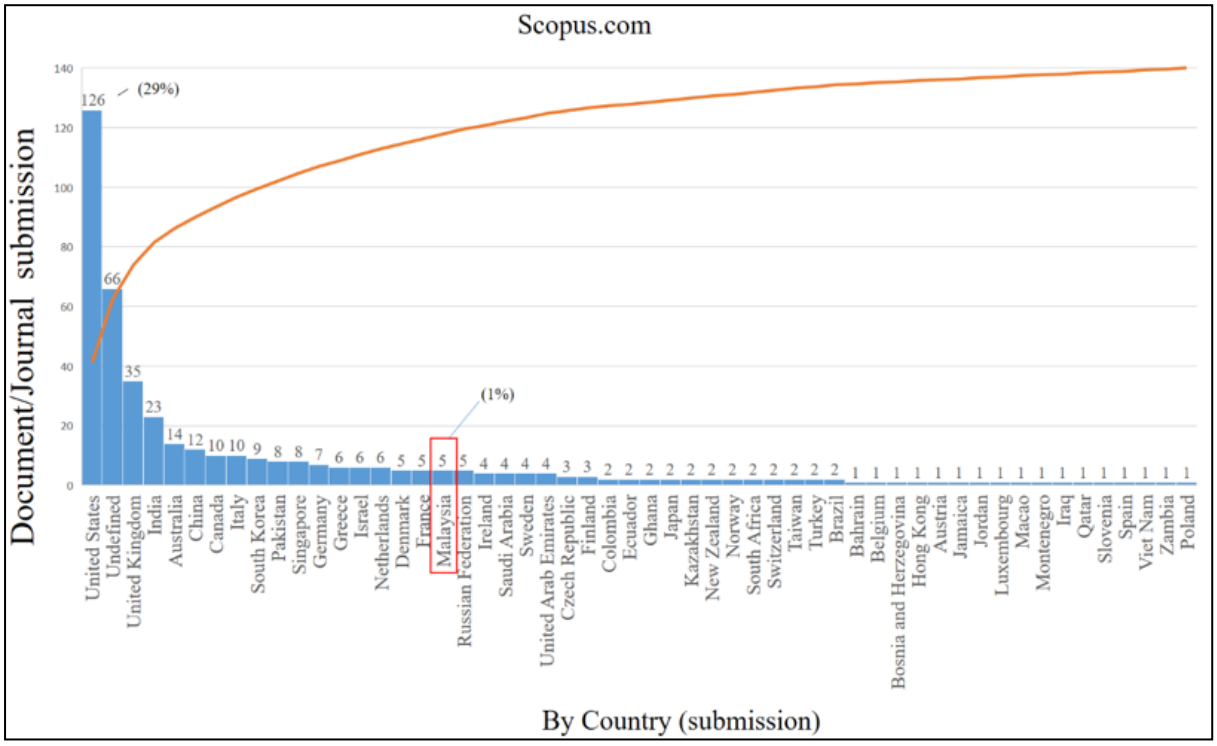

Figure 1.1. *Distribution of Article Published in Journal*

Definition

Theis et al. (2019) defined insider threat as, the potential for an individual who has or had authorized access to an organization's assets to use that access, either maliciously or unintentionally, to act in a way that could negatively affect the organization. Insider threats can be structured into four clusters i.e., actor, assets, action and impact (3A1I) further illustrated in Figure 1.2.

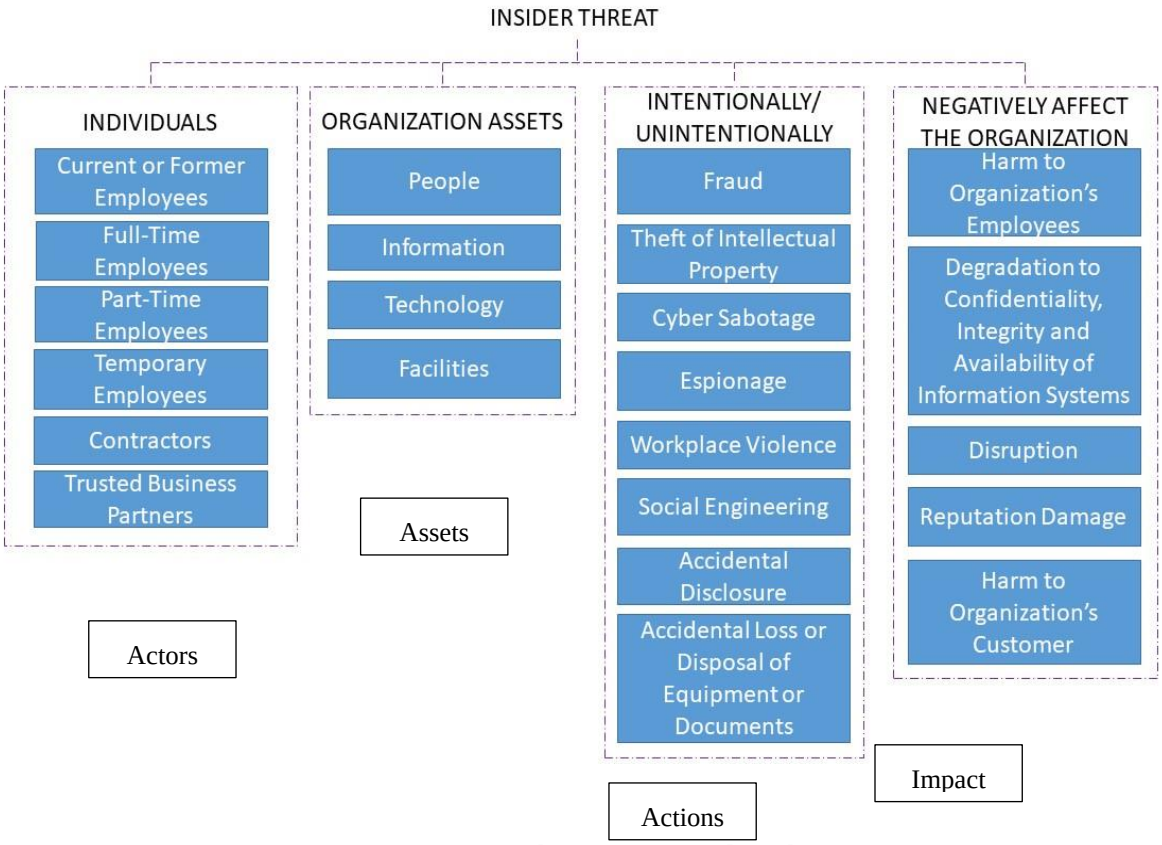

Figure 1.2 *Four Clusters on Insider Threats*

Roy et al. (2021) refers the insider as an active entity (person or software) who has valid authorization to assess the information asset of the organization insider attacks have higher rate of success, go undetected and pose higher risk than external enemies (Bakar et al., 2021). Also, Securonix (2020) discovers that many companies deploy additional monitoring controls like user and entity behavior analytics to supplement their primary tools such as data leak prevention system (DLPS) to detect insider threat actors.

However, Eberle and Holder (2009) state that technology devices such as intrusion detection system (IDS), intrusion prevention system (IPS), DLPS, anti-virus, anti-malware, firewalls, routers, and so on have been introduced and implemented within organizations to identify and prevent security breaches from outside perimeter and not the internal breaches from employees, contractors, and business partners. IBM Security (2021) reported that 40% of incidents were detected through alerts generated via internal monitoring tool, 100% of incidents that occurred were situation that insiders have administrative access and 40% of incidents, involved an employee with privilege access to the company assets

The total number of incidents recorded for the year 2021 were 10,016, where spam is at 102 (1.02%), intrusion at 1410 (14.08%), vulnerabilities report at 69 (0.69%), intrusion attempt at 159 (1.59%), denial of services at 22 (0.22%), malicious code at 648 (6.47%) and content related at 91 (0.91%). The highest reported case of each month is online fraud at 7098 (70.87%). Within organization, fraud cases can be propagated by the lack of awareness from insiders or employees when they tend to click phishing links which from groups of individuals and scammers. In particular, social engineering attacks continue to evolve due to a reliance on the Internet grows among users. This issue is not just a technological problem but require an understanding on human behavior toward cyber security (Ehizibue, 2022).

Insider threats occur in covertly manner, particularly by a person who is very familiar to his or her control environment. The attacks are not necessarily sophisticated where the tactics used are typically mundane and basic, hence did not raise alarm (ISACA, 2021). According to Hess and Cottrell (2015), most frauds cases committed by trusted employees because it is easy for them to steal from their employer and cover their transaction. Schulze (2016) discloses that privilege users who can access to sensitive information pose the biggest insider threat.

Fortinet Insider Threat Report (2019) states that:

i. 68% of organizations feel moderately to extremely vulnerable to insider attacks,
ii. 68% of organizations confirm insider attacks are becoming more frequent,
iii. 56% believe detecting insider attacks has become significantly to somewhat harder since migrating to the cloud,
iv. 62% think that privileged IT users pose the biggest insider security risk to organizations.

Table 1.1 *shows source of insider threats obtained from Ponemon Institute (2022)*

Source of insider threat	Occurrences	%
Employee or Contractor	3,807	56%
Criminal or Malicious Insider	1,749	26%
Credential Theft (Imposter)	1,247	18%

Table 1.1: *Source of insider threats*

Related Work

Contos (2006) claimed that an organization considers their internal employees are the trusted people within the organizational boundary. But, whenever the offender is an insider, investigation process becomes tougher. People around them would also not prefer to admit that their co-worker is a malicious insider. Because of that, countermeasures and controls design for external threats continue as the companies' top priority and overlook the internal (insider) threats standpoint. The inability to handle the insider who happens to have accesses to sensitive and confidential information could cause loss of data and intellectual property, reduced data integrity, exposed personal or private information, and damaged or destroyed critical information assets.

Real Cases

This section discusses some sample of insider threats cases and demonstrates that the ITA is not only react to the personal or professional stressor, but they can also react toward other motivation and opportunity such as financial gain, grudge (disgruntle), and many more. Generally, ITA is once a trusted person who had been given an authorization, privilege, knowledge, and access to the company's asset and/or information systems. By having that privilege (example, benefit), the exact same person be able to violate or abuse the access given hence violating the company's trust. Table 1.0 depicts the real cases in relation to insider threats (www.cdse.org last accessed 01 march 2022).

Table 1.2: *Insider threat real cases*

Case	Individual	Who Have Or Had Authorized Access To	Organization's Asset	Use That Access	Intentionally Or Unintentionally	To Act In A Way That Could	Negative Affect The Organization
1	Abdul Majeed Airline Mechanic	Aircraft's computer system Aircraft's nose compartment Working site	People Information Technology Facilities	Access to aero plane's nose	Intentionally	Sabotage	Disruption Reputation damage Harm to organization's customers
2	Christopher Victor Grupe Senior Network Design Engineer	Computer Core switches Privilege network access	People Information Technology Facilities	Networking system Core switches	Intentionally	Sabotage	Disruption Reputation damage
3	Jason Needham Consultant	Limited access to client's email system FTP server	People Information Technology	Ex staff of the client and use the access to escalating privilege/hacking	Intentionally	Theft of intellectual property Social engineering	Reputation damage
4	Depanshu Kher Consultant	Privilege access to client's Microsoft O365	Technology	Delete client's document and folders	Intentionally	Sabotage	Degradation to CIA Disruption Reputation damage
5	Jean Patrice Delia Miguel Sernas Performance Engineers	Information/file servers contain trade secrets	People Information Technology Facilities	Download trade secret documents	Intentionally	Theft of intellectual property Social engineering	Degradation to CIA Reputation damage

6	Edward Lin Navy Officer	Government confidential information	People Information Technology Facilities	Transporting/ sharing confidential information with other (country) government official	Intentionally	espionage	Harm to the country National security issue Reputation damage
7	Henry Kyle Frese Former Defense Intelligence Agency (DIA)	Access to top secret information	People Information Technology	Orally disclose classified information to unauthorized person	Unintentionally (despite briefing on the "do's and don'ts briefing by the agency)	Classified information disclosure to unauthorized parties	Reputation damage National security concerns
8	Hongjin Tan Scientist	Information servers Email Trade secret	People Information Technology Facilities	Access escalation Copy information (without authorization)	intentionally	Theft of intellectual property	Degradation to CIA Disruption Reputation damage
9	Ivan A. Lopez Army Specialist	Physical access weapon	People Facilities	Harm others	Intentionally (depression)	Loss of lives Act of terrorist	Loss of lives Wounded innocent Disruption Reputation damage
10	Nghia Hoang Pho National Security Agency	Government confidential information	People Information Technology Facilities	Unauthorized removal of classified information (keeping it at his residence)	Intentionally (but putting excuse as wanted to work from home)	Unauthorized removal of secret information Putting the classified information at risk	Harm to the country Reputation damage

11	Christopher Paul Hasson US Coast Guard Lieutenant	Government information system Use his authorization/clearance to order Tramadol (steroids) from various illegal sources	People Information Technology Facilities	Email systems	Intentionally	Misuse the systems	Disruption Reputation damage
12	Shamai Leibowitz	Have access to classified information	People Information Technology	Wilfully disclosed 200 pages of classified documents and information relating to the intelligence communication activities	Intentionally	Espionage	Harm to the country National security issue Reputation damage
13	Shannon Stafford	Privilege access to most systems (as the system administrator)	People Information Technology	Intentionally Deleting files in the computer servers	Intentionally	Sabotage	Degradation to CIA Disruption Reputation damage
14	Sephen Kellog III	had access to classified information relating to operations and capabilities of the Navy's nuclear propulsion systems	People Information Technology Facilities	Transporting/ sharing confidential information with other Admitted to photographing areas containing sensitive information about the Navy's nuclear propulsion program on the ship	Intentionally	Espionage	Harm to the country Reputation damage

15	Sudhish Kasab Software Engineer	Possessed the access key for Cisco's WebEx Teams application that was maintained on servers hosted by Amazon Web Services (AWS).	People Information Technology Facilities	Deleted approximately 456 servers, resulting in the complete shutdown of the WebEx Teams application	Intentionally	Sabotage	Disruption Reputation damage Harm to organization's customers
16	Wei Sun	Computer Access to information directly related to sensitive defence technology during his employment	People Information Technology Facilities	Networking system Core switches	Intentionally	Putting classified information at risk being hijack	Reputation damage
17	Glen Omer Viau Former US Navy Contactor	Have access and authority to trade secret information	People Information Technology	Exported design (intellectual property) to China without license.	Intentionally	Potentially a theft of intellectual property	Reputation damage
18	Peter Zuccarelli	Privilege access to technology	Technology People	Illegally export the technology to China without authorization (collaborating with external)	intentionally	Theft of intellectual property Social engineering	Reputation damage

19	Bryan Underwood	Physical Access	People Information Technology Facilities	Took over 30 photographs of sensitive areas and created a schematic that listed all security upgrades to the consulate and locations of surveillance cameras.	Intentionally	Espionage	Harm to the country Reputation damage
20	Yuan Li	Company systems and database contain trade secret/intellectual property	People Information Technology Facilities	Accessed her employer's internal databases and downloaded sensitive company information to a removable device	Intentionally	Espionage Accessing Information without Need to Know Misuse of Information Systems	Harm to the country Reputation damage
21	Christopher Boyce	Had access to company valuable research program	People Information Technology Facilities	Access to steal and sell Soviet Embassy in Mexico City	Intentionally	Espionage	Harm to the country Reputation damage
22	Alireza Jalali	Technology – broadcast and microwave communications.	People Information Technology	Conceal unlawful destination of the goods Repackage and send to Iraq	Intentionally	Theft of intellectual property Social engineering	Reputation damage

23	Alexander Fishenko	Information servers Trade secret/intellectual property	People Information Technology Facilities	illegally export millions of advanced microelectronics from manufacturers and suppliers located throughout the United States to the Russian Ministry of Defence	Intentionally	Theft of intellectual property Social engineering	Degradation to CIA Reputation damage
24	Candice Marie Claiborne	Held a Top-Secret security clearance since 1999	People Information Technology Facilities	Conspiracy, including cash, international travel and vacations, tuition at a Chinese fashion school, a fully furnished apartment, and a monthly stipend.	Intentionally	Conspiracy	Disruption Reputation damage National Security concerns
25	Jiaqiang Xu	Computer system Software code	People Information Technology Facilities	Stole proprietary software and source code information for his own profit	Intentionally	Theft of intellectual property Social engineering	Financial lost Reputation damage

26	Mozaffar Khazaee	Information related to US military Jets	Technology People System Facilities	Sold thousands of sensitive technical manuals, specification sheets, test results, technical data and other proprietary material relating to U.S. military jet engines	Intentionally	Theft of intellectual property Social engineering	Degradation to CIA Disruption Reputation damage National Security concerns
27	Gary Maziarz	Having access to intelligence analysts	People Information Technology Facilities	Leaking intelligence analysts	Intentionally	Conspirators	Harm to the country Reputation damage
28	Bryan Martin	Government confidential information	People Information Technology Facilities	Attempting to sell classified documents	Intentionally	espionage	Harm to the country Reputation damage
29	Walter Liew Research Engineer	Information servers Trade secret/intellectual property	People Information Technology Facilities	Conspired with former DuPont employees to steal chloride-route titanium dioxide production trade secrets and sell them in China	Intentionally	Theft of intellectual property Social engineering	Financial lost Reputation damage
30	Wen Chyu Liu Research Scientist	Access to trade secret	People Information Technology	Commit Trade Secret Theft	Intentionally	Theft of intellectual property Social engineering	Reputation damage

Table 1.3 *Previous Work People , Process and Technol*

No	Author	Contribution	People	Process	Tech	Mitigation Technique
1	(Alsowail and Al-Shehari, 2021). A Multi-tiered Framework for Insider Threat Prevention. MDPI Electronics 2021.	Unified framework that incorporates factors such as technical, psychological, behavioural, and cognitive for the "pre", "in", and "post" countermeasure.	Yes	Yes	Yes	Prevention: access control (biometrics & Asset metrics) "Pre"-counter measure, "in"-counter measure, and "post" countermeasure
2	(Kyle et al., 2020). USB-Watch: A Generalize Hardware-Assisted Insider Threat Detection Framework. Journal of Hardware System Security 2020.	Hardware based threat detection framework.	Yes	Yes	Yes	Human Interface device reports USB protocol Hardware
3	(Vasileious et al., 2018). A Framework for Data-Driven Physical Security and Insider Threat Detection. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM).	Physical Security Ontological (PS0) framework – provenance capability for improving physical security and insider threat detection. Supplementing for forensic investigation.	Yes	Yes	Yes	Data sources Log collection and aggregation Ontology (information about the environment)
4	(Angi et al., 2017). A Graph based Framework for Malicious Insider. Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS 2017)	Framework to isolate malicious users based on graph anomaly.	Yes	Yes	Yes	Isolate malicious users based on graph anomaly (compare against baseline) via Graphical Processing Unit (GPU) and Anomaly Detection Unit (ADU).
5	(Ionnis et al., 2017). Formalizing Policies for insider threat detection. A tripwire grammar. Journal of Wireless Mobile Network, Ubiquitous Computing and Depended able Application pp. 26-43.	- Information security policy review - policy violation - attack pattern	Yes	Yes	Yes	Review and formalising security policy Embed the policy in the tripwire (detect violation) Tripwire triggered in 2 ways: When policy is violated Evidence of known attack pattern is found.

Countermeasures

Previous work reported that cyber risks mitigations framework should include three major components i.e People, Process and Technology. Each component comprises several categories. Table 1.3 shares some view of others in relation to contribution and mitigation

techniques related to insider threat. A framework to deter and detect incident of insider threats is paramount especially when companies are still struggling to manage these threats and the associated risk. Deter is to discourage employees or staff to act negatively affecting the company while detect is to discover the insider or trusted employee who had become the perpetrator or potentially violating the trust.

This study attempts to comprehend and use set of best practices from CMU-SEI's mitigating insider threats guide and translated into the control statements. Based on the literature reviews, these control statements are deemed relevant to prevent and detect "insider" to become malicious (example, ITA). This study unable to discover any real cases or scenario happened in Malaysia to add on into the thirty cases showcased earlier. Nevertheless, the common pointers about the potential perpetrators such as espionage, illegally sharing information, misuse of information, mishandling information, unexplained affluence, anomalies behavior, gaining access to sensitive information, access without need to know, ego, and performance issues are something need to be understood. From the risk management standpoint, insider threats risk could not be totally eliminated but be able to be reduced or mitigated at acceptable level.

Methods

Overall this study follow research process as shown in figure 1.3. As shown in Figure 1.3, four phases involved in framework development. The first phase is about information gathering from literature review, real cases and initial interviews. The second phase was designing instruments. This phase required deep understanding of SEI-CMU which one of the major tools in setting the controls. At phase 2 Questions were developed and at phase 3 survey submitted o about 200 respondents based on direct and indirect contacts and personal references. We uses non-experimental research design and survey. Six focus groups (FG) namely Human Resource [HR], Legal [LG], Physical Security [PS], Data Owner [DO], Information Technology [IT] and Software Engineering [SE] in taking part for the activities suggested in Theis et al. (2019). Phase 3 also involved with the development of Trusted Human Framework.

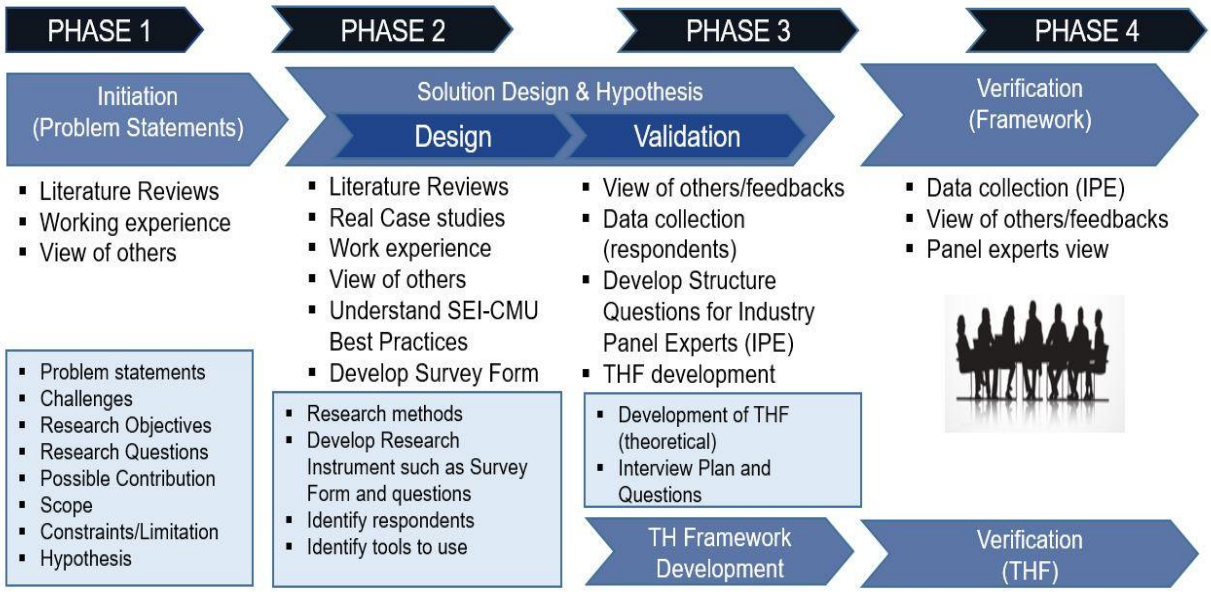

Figure 1.3. *Research Framework*

Phase 3 also explained structured of hypothesis as in Table 1.4

Development of Hypothesis

In order to find out the answers for the research questions and to accomplish the objectives, two main sets of hypotheses were formulated (such as, H_1 and H_0: Refer Table 1.4). The main data were collected from the respondents (R1 to R120: n=120) and industry panel experts (IPE 1…IPE 14: n=14). The independent variables (IV) refer to what were changed during the investigation (such as, respondents' and interview data), whereas dependent variables (DV) refer to what were measured (such as, controls inclination, acceptance, and effectiveness). The acceptance level (inclination) of the control statements toward mitigating insider threats came from the 120 respondents and fourteen industry panel experts, respectively. The results of both opinions were to be compared, and to see whether they are complementing (or supporting) each other.

Table 1.4 *Thirty Two (32) Statements of Hypothesis*

Set 1 hypothesis (H_1)		Set 2 hypothesis (H_0)	
H1	The recommended controls are applied (practiced) by the respondents' companies.	H17	The recommended controls are not applied (practiced) by the respondents' companies.
H2	The involvement of FGA provides inclination toward the control implementation by the respondents' companies.	H18	The involvement of FGA did not provide any inclination toward the control implementation by the respondents' companies.
H3	The involvement of FGB provides inclination toward the control implementation by the respondents' companies.	H19	The involvement of FGB did not provide any inclination toward the control implementation by the respondents' companies.
H4	The involvement of FGC provides inclination toward the control implementation by the respondents' companies.	H20	The involvement of FGC did not provide any inclination toward the control implementation by the respondents' companies.
H5	The involvement of FGD provides inclination toward the control implementation by the respondents' companies.	H21	The involvement of FGD did not provide any inclination toward the control implementation by the respondents' companies.
H6	The involvement of FGE provides inclination toward the control implementation by the respondents' companies.	H22	The involvement of FGE did not provide any inclination toward the control implementation by the respondents' companies.
H7	The involvement of FGF provides inclination toward the control implementation by the respondents' companies.	H23	The involvement of FGF did not provide any inclination toward the control implementation by the respondents' companies.
H8	The involvement of FGG provides inclination toward the control implementation by the respondents' companies	H24	The involvement of FGG did not provide any inclination toward the control implementation by the respondents' companies.
H9	The recommended controls could mitigate (reduce) the insider threats risk within the companies.	H25	The recommended controls could not mitigate (reduce) the insider threats risk within the companies.

H10	The involvement of FGA provides better assistance (support) toward the mitigation of insider threats risk.	H26	The involvement of FGA did not provide better assistance (support) toward the mitigation of insider threats risk
H11	The involvement of FGB provides better assistance (support) toward the mitigation of insider threats risk.	H27	The involvement of FGB did not provide better assistance (support) toward the mitigation of insider threats risk.
H12	The involvement of FGC provides better assistance (support) toward the mitigation of insider threats risk.	H28	The involvement of FGC did not provide better assistance (support) toward the mitigation of insider threats risk.
H13	The involvement of FGD provides better assistance (support) toward the mitigation of insider threats risk.	H29	The involvement of FGD did not provide better assistance (support) toward the mitigation of insider threats risk.
H4	The involvement of FGE provides better assistance (support) toward the mitigation of insider threats risk.	H30	The involvement of FGE did not provide better assistance (support) toward the mitigation of insider threats risk.
H15	The involvement of FGF provides better assistance (support) toward the mitigation of insider threats risk.	H31	The involvement of FGF did not provide better assistance (support) toward the mitigation of insider threats risk.
H16	The involvement of FGG provides better assistance (support) toward the mitigation of insider threats risk.	H32	The involvement of FGG did not provide better assistance (support) toward the mitigation of insider threats risk.

The qualitative Delphi process consisted of two or more round of consulting with panel expert (Keeney et al., 2011) and the sessions with the experts could be conducted either by email or online survey tools (Donohoe et al., 2012). In this study, qualitative Delphi study was used as the approach to ascertain whether recommended controls can mitigate insider threats risk and to be practiced among the companies in Malaysia. Fourteen industry panel experts were having two round interview sessions with guided questionnaire. Prior to that interviews, 120 respondents' data were gathered to gauge the implementation (or practiced) of the controls recommended in Malaysia. These controls are included to be part of the proposed Trusted Human Framework's activities. The final Phase provide panel experts view.

Panel of Experts

In order to strengthening the view that the control statements be able to mitigate insider threats, fourteen industry professionals were identified as the Industry Panel Experts (IPE). They were to provide feedbacks and opinion on the control statements implementation and agreeableness toward the ability of that controls in mitigating insider threats risk. Giannarou and Zervas (2014) provide their opinion that when constructing the expert's panel, it is important to consider their experience ("expertise") and knowledge ("knowledgeability") to determine the reliability and validity of the result. In this case, our experts are from the industry and leaders (C-level, Department Head, Section Head and Unit Head) in their respective areas. Table 1.5 provides list of IPE participated in this study.

Table 1.5: *List of Industry Panel Experts (IPE)*

Panel	Job Title/Designation	Company
Panel Expert 1	Chief Information Security Officer (CISO), Risk Management Department	State Owned Local Investment Bank
Panel Expert 2	Chief Information Security Officer (CISO), Risk Management Department	Leading Development Financial Institution (DFI) in Malaysia
Panel Expert 3	Chief Information Security (CISO) Risk Management Department	Leading Cooperation Bank in Malaysia
Panel Expert 4	Head, Core System and Enterprise System, Group IT Division	Leading Cooperation Bank in Malaysia
Panel Expert 5	Senior Manager, IT Change Management, IT Department	Leading Islamic Banking in Malaysia
Panel Expert 6	Assistant General Manager, Information Technology, IT Department	Leading Islamic Banking in Malaysia
Panel Expert 7	Head, Information Security, IT Department	Second Largest Islamic Banking in Malaysia
Panel Expert 8	Assistant Vice President, Group Internal Audit Department	Second Largest Islamic Banking in Malaysia
Panel Expert 9	Executive Director (Country Head), Information Security and Assurance Technology and Operations	Singaporean Bank (Operated in Kuala Lumpur)
Panel Expert 10	Director, Cybersecurity	Consulting Firm 1
Panel Expert 11	Director, Emerging Technology Risk and Cyber (ETRC)	Consulting Firm 2
Panel Expert 12	IT Manager, Group IT Department	Regulator for Financial Services (OFS)
Panel Expert 13	Section Head, Governance and Security, Digital Technology Division	Social Security Organization
Panel Expert 14	Section Head, Technology Risk, Risk Management Department	Social Security Organization

Results

The data from the survey and feedback from the panel experts help to identify, describe, and investigate the relationship between 55 the respective designed control statements against the companies' practices. A self-assessment exercise and analysis were conducted based on the design control statements, on whether those activities could mitigate insider threats risk by distorting either insider threat actors' method (M) of exploiting vulnerabilities, reduce the available window of opportunities (O) and deny the motives (m).

During the early stage of data collection phase, follow up calls were made to at least ten prospects (potential respondents) to understand the reasons for their unreturned forms. Further to that, the respondents came from the following sectors/industry (refer Table 1.5) where majority of them were from the Financial Sectors (32%) followed by Government and its related companies (28%) and Manufacturing (10%).

Table 1.5: *Respondents' sectors/industry*

	Sectors/Industry	(n=120)	(%)
1.	Construction	4	3%
2.	Consultancy Services	4	3%
3.	Educational Sector	11	9%
4.	Energy – Oil & Gas	4	3%
5.	Financial Sector – Banking	32	27%
6.	Financial sector – Insurance	6	5%
7.	Government/Agencies/Statutory Body	12	10%
8.	Government Link Investment Companies (GLIC)	13	11%
9.	Government Owned Companies (GOC)	8	7%
10.	Manufacturing	12	10%
11.	Technology Companies	5	4%
12.	Telecommunication Providers	7	6%
13.	Transportation & Logistics	2	2%

Focus Group study is developed as mechanism to test hypothesis and it the results show that

i. Overall, the recommended controls are generally practiced by the respondents' companies,
ii. Focus Group (FG) involvement in the control activities provides inclination toward the control implementation by the respondents' companies,
iii. Panel experts agree that the recommended controls could mitigate insider threats risk within the companies, and
iv. Focus Group (FG) involvement in the control activities provides support to the organization toward mitigating of insider threats risk.

Trusted Tunnel to Trusted Human Framework

The idea to have this framework is to ensure all respective employees who have gone through (or being assessed by) the THF's cyclic processes are always perceived as the trusted human being. This is due to the rigorous processes that imposed to are obeyed (or complied with) by these employees, contractors, business partners, etc. The idea is simplified in Figure 1.4 to illustrate the THF Tunnel.

Figure 1.4: *Trusted Human Framework (THF) Tunnel*

Trusted Human Framework is considered as the approach contains set of activities to be conducted within organization to manage insider threats risk. The idea of the framework is to ensure the respective employees who have gone through the THF's cyclic processes are constantly perceived as the trusted human being. This is due to the fact gathered from the survey and panel expert interviews' discovery, where majority of activities suggested in the THF can suppress at least one of the perpetrators' method, opportunity or motive to violate the given trust.

Example of trust violations are espionage, illegally sharing information, misuse of information, mishandling information, gaining access to sensitive information, access without need know, sold information to competitors, and many more. A trusted person or insider who potentially turns out to be perpetrator can be stopped when M (method) O (opportunities) m (motives) factors are not presence simultaneous. When at least one of these factors are denied (absence), it could deform the threats or attacks. Figure 1.5 provides general overview of the overall THF processes and components.

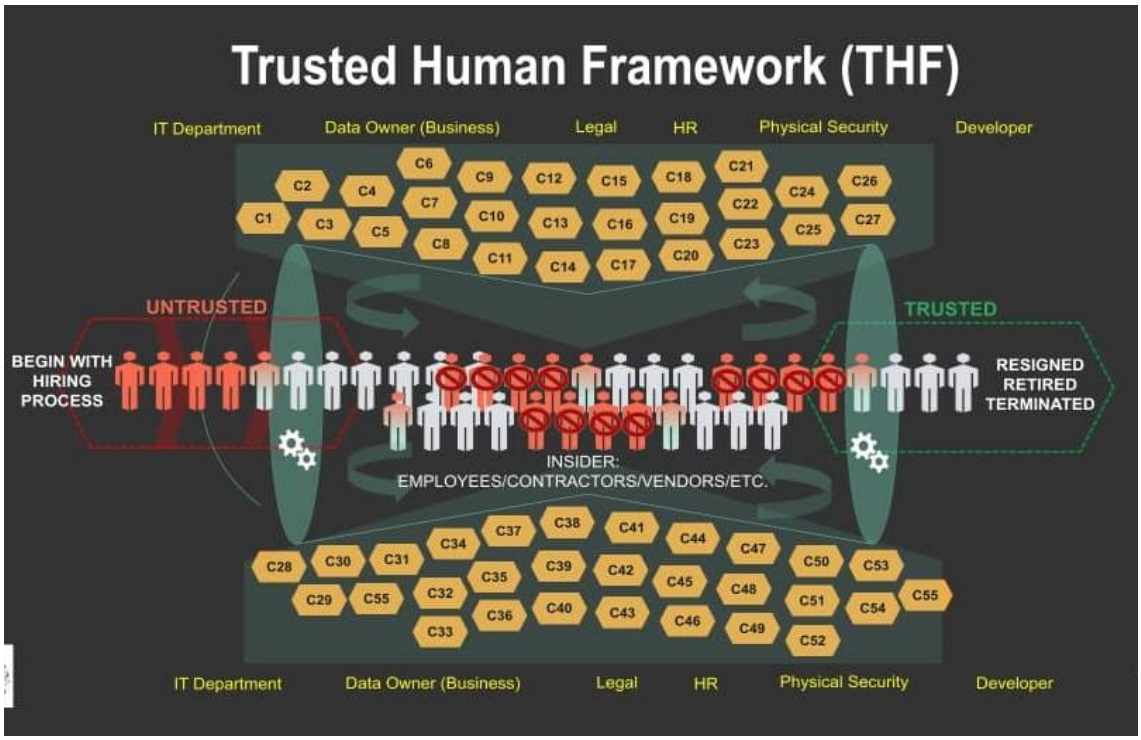

Figure 1.5: *The overall trusted human framework processes*

Conclusion

As a conclusion, the outcome of this study would be able to assist organization to understand further the general acceptance of the control practices and motivate the organization to strengthen the effort in mitigating insider threats. The suggested framework is also aimed to inspire more organizations to consider identifying insider threats as one of the risks in their company's enterprise risk management activities. Trusted Human Framework able to mitigate risks of insider threats. We developed survey and focus group discussion to test our hypothesis. The 55 design controls verified by panel of expert were then incorporated to build trusted tunnel. We finally explored controls statements (best practices) with example of real case study on mitigating insider threat incidents.

Acknowledgement

Research Funded by Ministry of Higher Education Malaysia under TRGS Grant Scheme, Universiti Teknikal Malaysia Melaka give full support on this research.

References

Amidei, J., Piwek, P. and Willis, A., 2019. The use of rating and Likert scales in Natural Language Generation human evaluation tasks: A review and some recommendations. In: Proceedings of the 12th International Conference on Natural Language Generation, pp. 1-7.

Bailey, T., Kolo, B., Rajagopalan, K. and Ware, D., 2018. Insider threat: The human element of cyberrisk. McKinsey Quarterly, pp.1-8.

Bakar, R.A., Rahmatullah, B., Munastiwi, E. and Dheyab, O., 2021. A confirmatory analysis of the prevention insider threat in organization information system. Journal of Technology and Humanities, 2(1), pp.20-30.

Bilusich, D., Chim, L., Nunes-Vaz, R.A. and Lord, S., 2018. There is no single solution to the 'insider'problem but there is a valuable way forward. WIT Transactions on Engineering Sciences, 121, pp.135-146.

Bishop, M. and Gates, C., 2008. Defining the insider threat. In Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead, pp. 1-3.

Bishop, M., Conboy, H.M., Phan, H., Simidchieva, B.I., Avrunin, G.S., Clarke, L.A., Osterweil, L.J. and Peisert, S., 2014. Insider Threat Identification by Process Analysis. IEEE Security and Privacy Workshops, pp. 251-264.

BNM, 2018. Risk Management in Technology (RMiT). [online] Available at: https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+(RMiT).pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078 [Accessed on 21 May 2022]

CA Technologies, 2019. Insider Threat Report [online] Available at: https://ca-security.inforisktoday.com/whitepapers [Accessed on 15 June 2019]

Callahan, C.J., 2013. Security Information and Event Management Tools and Insider Threat Detection. [online] Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a589914.pdf [Accessed on 07 April 2019].

Cattermole, G., 2019. Developing the employee lifecycle to keep top talent. Strategic HR Review, 18(6), pp. 258-262.

CDSE, 2020. The Cases. [online] Available at: https://securityawareness.usalearning.gov/cdse/case-studies/cases.html [Accessed on 02 February 2022].

Cherry, K., 2020. The Hawthorne Effect and Behavioral Studies. [online] Available at: https://www.verywellmind.com/what-is-the-hawthorne-effect-2795234 [Accessed on 15 April 2021]

Claycomb, B., Greitzer, F., Jaros, S.L. and Gardner, C., 2022. Introduction to the Special Issue on Insider Threats. Digit. Threat.: Res. Pract, 3(1), pp. 1-3.

Claycomb, W.R., Huth, C.L., Flynn, L., McIntire, D.M., Lewellen, T.B. and Center, C.I.T., 2012. Chronological examination of insider threat sabotage: Preliminary observations. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 3(4), pp.4-20.

Code42 Software Inc., 2022. Annual Data Exposure Report. [online] Available at: https://www.code42.com/resources/reports/2022-data-exposure#main-content [Accessed on 21 February 2022]

Contos, B.T., 2006. Enemy at the water cooler: True stories of insider threats and enterprise security management countermeasures. Elsevier.

Covey, S. M. R., 2014. The speed of trust: The one thing that changes everything. Simon & Schuster.

Cresswell, J.W., 2014. Concise Introduction to Mixed Methods Research. Sage Publishing, pp. 3-19.

Computer Emergency Response Team | Software Engineering Institute | Carnegie Mellon University. 2018. [online] Available at: CERT Definition of 'Insider Threat' - Updated (cmu.edu) [Accessed on 03 February 2021]

Donohoe, H., Stellefson, M. and Tennant, B., 2012. Advantages and limitations of the e-Delphi technique: Implications for health education researchers. American Journal of Health Education, 43(1), pp.38-46.

Eberle, W. and Holder, L., 2009. Graph-based approaches to insider threat detection. In Proceedings of the 5th annual workshop on cyber security and information intelligence research: cyber security and information intelligence challenges and strategies, pp. 1-4.

Ehizibue, D., 2022. Investigation of individuals' behavior towards phishing attacks using the health belief model. Bachelor's Thesis of University of Twente.

Ernst and Young, 2013. Bring your own device Security and risk considerations for your mobile device program. [online] Available at: https://www.ey.com/Publication/vwLUAssets/EY_Bring_your_own_device:_mobile_security_and_risk/%24FILE/Bring_your_own_device.pdf [Accessed on 05 February 2019].

Fortinet Insider Threat Report, 2019. Insider Threat Report. [online] Available at: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/insider-threat-report.pdf [Accessed on 15 February 2022]

Farquhar, J., Michels, N. and Robson, J., 2020. Triangulation in industrial qualitative case study research: Widening the scope. Industrial Marketing Management, 87, pp.160-170.

Farrokhi, F. and Mahmoudi-Hamidabad, A., 2012. Rethinking convenience sampling: Defining quality criteria. Theory & Practice in Language Studies, 2(4), pp. 784-792.

Freund, J. and Jones, J., 2014. Measuring and managing information risk: a FAIR approach. Butterworth-Heinemann.

Goswami, S. and Agarwal, R., 2015. A study on employer branding and its impacts on employee's attraction and retention. International Journal of Management and Social Sciences Research, 4(6), pp.9-15.

Greitzer, F.L., 2019, April. Insider Threats: It's the HUMAN, Stupid!. In Proceedings of the Northwest Cybersecurity Symposium, pp. 1-8.

Greitzer, F.L. and Frincke, D.A., 2010. Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. In Insider threats in cyber security, Springer, Boston, MA, pp. 85-113.

G. Mazzarolo and A.D Jurcut, 2019. Insider threats in Cyber Security: The enemy within the gates. [online] Available at: https://arxiv.org/ftp/arxiv/papers/1911/1911.09575.pdf [Accessed on 08 August 2022].

Harpe, S.E., 2015. How to analyze Likert and other rating scale data. Currents in pharmacy teaching and learning, 7(6), pp.836-850.

Hess, M.F. and Cottrell J.H., 2016. Fraud risk management: A small business perspective. Business Horizons, 59(1), pp.13-18.

IBM Security, 2021. IBM Security X-Force Insider Threat Report. 2021. Special Intelleginent Report. [online] Available at: https://www.ibm.com/downloads/cas/YNAPDA6B [Accessed on 21.02.2022]

IBM Security and Ponemon Institute, 2020. Cost of Insider Threat: Global Report. [online]

Available at: https://www.ibm.com/downloads/cas/LQZ4RONE [Accessed on 20 April 2021]

Intelligent and National Security Alliance (INSA). 2017. Assessing the mind of the malicious insider: using a behavioral model and data analytics to improve continuous evaluation. [online] Available at: https://www.insaonline.org/wpcontent/uploads/2017/04/INSA_WP_Mind_Insider_FIN.pdf [Accessed on 02 January 2022]

ISACA, 2021. A Holistic Approach to Mitigating Harm from Insider Threats. [online] Available at: https://isaca.org [Accessed on 01 January 2022]

Jonathan, M., Akshay, A., Aishwarya, Z., Aditya, K., Anshuma, N. and Hemant, T., 2016. An approach towards automated employee resignation system. International Journal of Computer Science and Mobile Computing, 5(3), pp. 395-402.

Keeney, S., McKenna, H. and Hasson, F., 2011. The Delphi technique in nursing and health research. John Wiley & Sons.

Kim, A., Oh, J., Ryu, J., Lee, J., Kwon, K. and Lee, K., 2019. SoK: A Systematic Review of Insider Threat Detection. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 10(4), pp.46-67.

Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L. and Osula, A.M., 2015. Insider threat detection study. NATO CCD COE, Tallinn.

Leftkothea Giannarou and Efthimious Zervas. 2014. Using Delphi technique to build consensus in practice. [online] Available at: https:// business-and-management.org/library/2014/9_2--65-82-Giannarou,Zervas.pdf [Accessed on 03 January 2022].

Malaysia Cyber Security Strategy 2020-2024. [online] Available at: https://asset.mkn.gov.my/wp content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf [Accessed on 03 January 2022].

Massey, A., Lindsay, S., Seow, D., Gordon, J. and Lowe, D.J., 2021. Bubble concept for sporting tournaments during the COVID-19 pandemic: Football Club World Cup. BMJ open sport & exercise medicine, 7(2), pp. 1-5.

MIA, 2009. Malaysian Institute of Accountants Using Malaysian Standards on Auditing in the Audits of Small and Medium-sized Entities Malaysian Auditing Manual. [online] Available at: https://www.mia.org.my/v2/downloads/ppt/auditing/publications/2009/07/15/MIA_Malaysian_Auditing_Manual_15_Julai_2009.pdf [Accessed on 01 January 2019].

Moon, M.D., 2019. Triangulation: A method to increase validity, reliability, and legitimation in clinical research. Journal of Emergency Nursing, 45(1), pp.103-105.

Morgan, A. and Wilk, V., 2021. Social media users' crisis response: A lexical exploration of social media content in an international sport crisis. Public Relations Review, 47(4), pp. 1-14.

Mundie, D.A., Perl, S.J. and JD, C.H., 2014. Insider Threat Defined: Discovering the Prototypical Case. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 5(2), pp.7-23.

Mundie, D.A., Perl, S. and Huth, C.L., 2013. Toward an ontology for insider threat research: Varieties of insider threat definitions. In 2013 third workshop on socio-technical aspects in security and trust, pp. 26-36.

National Defense Authorization Act, 2018. Department of Defense. [online] Available at: https://sgp.fas.org/news/2018/03/dod-insider.html. [Accessed on 05 May 2021]

Nemoto, T. and Beglar, D., 2014. Likert-scale questionnaires. In JALT 2013 conference proceedings, Tokyo: Jalt, pp. 1-8.

NIST, 2021. Security and Privacy Controls for Federal Information Systems and Organization. [online] Available at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf [Accessed on 23 September 2021]

Ophoff, J., Jensen, A., Sanderson-Smith, J., Porter, M. and Johnston, K., 2014. A descriptive literature review and classification of insider threat research. Proceedings of Informing Science & IT Education Conference, pp. 211-223.

Pfleeger, S.L., Predd, J.B., Hunker, J. and Bulford, C., 2009. Insiders behaving badly: Addressing bad actors and their actions. IEEE transactions on information forensics and security, 5(1), pp.169-179.

Piaw, C.Y., 2013. Mastering research statistics. Malaysia: McGraw Hill Education, New York, United States.

Ponemon Institute, 2022. Ponemon Cost of Insider Threats Global Report. [online] Available at https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats [Accessed on 21 May 2022]

Purbasari, T. and Abadi, F., 2022. The Influence of Organizational Culture, Leadership Style on Employee Experience has an Impact on Retention. Fair Value: Jurnal Ilmiah Akuntansi dan Keuangan, 4(3), pp.1254-1266.

Probst, C.W., Hunker, J., Gollmann, D. and Bishop, M., 2010. Aspects of insider threats. In Insider threats in cyber security, Springer, Boston, MA, pp. 1-15.

Rehman, S., Ali, S., Sajjad Hussain, M. and Zamir Kamboh, A., 2019. The role of physiological contract breach on employee reactions: Moderating role of organizational trust. Pakistan Journal of Humanities and Social Sciences, 7(2), pp.233-244.

Roessing, V., 2010. The business model for information security. ISACA.

Roger, C.M., David, S.F. and James, H.D., 2007. An Integrative Model of Organizational Trust: Past, Present, and Future. Academy of Management Review, 32(2), pp. 344-354.

Roy, P., Sengupta, A. and Mazumdar, C., 2021. A structured control selection methodology for insider threat mitigation. Procedia Computer Science, Elsevier B.V., 181, pp. 1187–1195.

Scarfone, K., 2018. A Comprehensive Guide to SIEM Products. [online] Available at: https://searchsecurity.techtarget.com/feature/Introduction-to-SIEM-services-and-products [Accessed on 05 March 2019].

Schulze, H., 2016. Insider Threat Spotlight Report. [online] available at: https://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2016.pdf [accessed on 05 April 2020]

Securonix, 2022. Justifying Your Insider Threat – 7 Real-word Examples To Help Measure ROI. [online] Available at: https://pages.securonix.com/rs/179-DJP-142/images/Justifying-Your-Insider-Threat-Program-Securonix.pdf [Accessed on 05 March 2022]

Stefano, F., 2016. Implementing Segregation of Duties (SoD). [online] Available at: https://www.isaca.org/Journal/archives/2016/volume-3/Documents/Implementing-Segregation-of-Duties_joa_Eng_0516.pdf. [Accessed on 05 March 2019].

Sutton, M., 2018. Routine Activity Theory:“Mindless” Chemistry Meme Masquerades as a Theory of Crime Causation. Internet Journal of Criminology. pp. 1-34.

Tessema, M., Ready, K. and Embaye, A., 2013. The Effects of Employee Recognition, Pay and Benefits on Job Satisfaction: Cross Country Evidence. Journal of Business and Economics, 4(1), 1-13.

Theis, M., Trzeciak, R.F., Costa, D.L., Moore, A.P., Miller, S., Cassidy, T. and Claycomb, W.R., 2019. Common sense guide to mitigating insider threats. Technical Report, Carnegie Mellon University, Software Engineering Institute.

Thompson, N., 2020. A Unified Classification Model of Insider Threats to Information

Security. In 31st Australasian Conference on Information Systems, pp. 1-12.

Trusted advisor, 2010. Improving Trust – A Deeper Look into The Trusted Advisor Trust Quotient. [online] Available at: https://trustedadvisor.com/public/TrustEquationSpecial Ebook.pdf. [Accessed on 09 April 2022]

Van Ruitenbeek, E., Keefe, K., Sanders, W.H. and Muehrcke, C., 2010. Characterizing the behavior of cyber adversaries: The means, motive, and opportunity of cyberattacks. In 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Supplemental (DSN 2010), pp. 17-18.

Veriato, 2022. Steps to Protect Your Data During The High Risk Exit Period. [online] Available at https://www.veriato.com/resources/whitepapers/3-steps-to-protect-your-data [Accessed on 20 February 2022]

Wells, G.L., Kovera, M.B., Douglass, A.B., Brewer, N., Meissner, C.A. and Wixted, J.T., 2020. Policy and procedure recommendations for the collection and preservation of eyewitness identification evidence. Law and Human Behavior, 44(1), pp. 1-3.

Willits, F.K., Theodori, G.L. and Luloff, A.E., 2016. Another Look at Liker Scale. [online] Available at: https://egrove.olemiss.edu/jrss/vol31/iss3/6 [Accessed on 20 March 2021]