IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 15 January 2024, accepted 27 February 2024, date of publication 4 March 2024, date of current version 8 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3373265

TOPICAL REVIEW

A Review of the Insider Threat, a Practitioner Perspective Within the U.K. Financial Services

FINDLAY WHITELAW [1], JACKIE RILEY [2], AND NEBRASE ELMRABIT [2]
[1]Glasgow School for Business and Society, Glasgow Caledonian University, G4 0BA Glasgow, U.K.
[2]Department of Cyber Security and Networks, School of Computing, Engineering and Built Environment, Glasgow Caledonian University, Scotland, G4 0BA Glasgow, U.K.

Corresponding author: Nebrase Elmrabit (nebrase.elmrabit@gcu.ac.uk)

This work was supported by Glasgow Caledonian University.

ABSTRACT The insider threat within organisational cybersecurity continues to be of great concern globally. The current insider threat detection strategies are acknowledged as ineffective, evidenced by the increased reported events in high-profile insider threats and cyber data loss cases borne from insider and privilege misuse. The impact of insider incidents on Financial Service (FS) organisations is vast, operationally disruptive, and costly from a regulatory, financial, and reputational perspective. Many United Kingdom (UK) FS organisations have invested in insider risk programmes, but there is no sign of the insider threat diminishing. This paper will address the following research questions: 1) What factors influence employees to become malicious insider threats and apply this to employees working within the UK? 2) What preventative measures could be effectively operationalised within UK FS organisations to prevent malicious insider attacks? A literature review was conducted, reviewing 54 articles in peer-reviewed journals. Additional and relevant articles were incorporated to enrich the review, further substantiating the academic currency and context of the study. The review reveals five primary emerging insider threat themes, subsequently discussed and including behavioural indicators, information security behaviours, technical controls, insider threat strategies, and regulation. Throughout the literature review, one primary challenge highlighted the lack of articles published concerning the FS industry; however, the studies reviewed were relevant, appropriate, and applied across this review. Furthermore, the review also considers outcomes from a practitioner's perspective, offering insights into the limitations of insider threat approaches and strategies and offering potential recommendations.

INDEX TERMS Financial services, insider threat, insider threat strategies.

I. INTRODUCTION

The insider threat continues to be of great concern to organisations globally [1], [2], [3], [4], [5], with the FS industry being a persistent and lucrative target for inside threat actors [6]. Banks and FS organisations are seen as more attractive targets as criminals go to valuable assets, as cited in the Global Wealth Report [7]. Reigniting Radical Growth, conducted by Boston Consultancy Group, found that FS organisations are 300 times more likely to be a target of a cyber-attack [7]. Similarly, a Bank for International Settlements report found that financial and insurance companies were particularly targeted [8]. In addition, PWC's Fraud and Financial Crime Report 2022 found that fraud and economic crime have been at a record high over the past 20 years, with the top three themes cited as cybercrime, customer fraud and asset, with internal perpetrators accounting for 31% of fraudulent incidents [9]. Given the vast amount of digitised financial, data, and technological assets, these findings provide critical insights into understanding and developing insider threat strategies for FS organisations [8].

The associate editor coordinating the review of this manuscript and approving it for publication was Liang-Bi Chen.

Furthermore, the 2023 Insider Threat Report highlights the reality of insider threats for some organisations, which found that 74% surveyed feel moderately to extremely vulnerable to insider attacks, with 74% confirming insider attacks were becoming more frequent [10]. In addition, the report [10] revealed that 53% of organisations surveyed believe that detecting insider attacks has become increasingly challenging for them to discover in the cloud. Furthermore, 54% of organisations said that insiders already had credential access to the network and services, and 44% said an increase in the use of applications that leak data makes detection more complex [10]. The 2023 Insider Threat Report also suggests that the most significant risk to organisations is attributed to information technology (I.T.) privileged users (60%), with contingent workers, vendors, and suppliers (57%) posing a considerable threat to organisations [10]. The latest data breach investigation report [11] referenced that 78% of insider threat attacks modus operandi was driven by financial motivation, with incidents resulting in data loss, as it is easy to monetise. This trend has continued since 2019, when Insider Threat Report [12] found that organisations surveyed ascertained that fraud (57%), monetary gain (50%), and intellectual property (I.P.) theft (43%) were the driving forces. The report [12] also highlights a significant increase (28%) in data breaches and incidents from 2017, highlighting an increasing trend into 2019 and 2020, which is incongruent with the findings of the latest data breach report [12].

There have been several high-profile, financial services-related, cyber insider-driven incidents during recent years, with the Capital One incident of July 2019 being one of the highest profile within the UK FS industry. The Capital One case highlighted the risks that trusted parties (contractors and third-party vendors) could cause to FS organisations, where legitimate access to data and systems can be utilised for malicious intent [13]. In a similar insider-motivated case in 2018, a former JP Morgan & Chase Co. employee received a four-year sentence for selling customer's personal information [14]. Further afield and outwith the UK, insights and learnings from global insider incidents can be taken; for example, a Russian bank (Sberbank) uncovered 60 million credit card records for sale online. Sberbank publicly reported its suspicions, which subsequently led to an admission of an insider attack [15]; this attack was cited as motivated by financial gain. Similarly, in 2011, Bank of America was also a victim of an insider attack where a bank employee leaked hundreds of customer records to scammers, resulting in estimated losses of $10 million [16]. However, one of the most financially damaging insider-related incidents within the FS industry was related to the unauthorised access of passwords to payment systems within Punjab National Bank (PNB), which resulted in $1.8 billion of fraudulent transactions [17] and a loss of $43 million, to PNB [18]. Also, Absa, a South African bank, warned customers of a data breach caused by a rouge employee selling personal data to an external third party, reflecting a broader trend of cyber insider-related attacks [19]. More recently, a former Penn South Cooperative Federal Credit Union employee was sentenced to three years' probation for deliberately deleting thousands of files as an act of revenge for being dismissed [20].

The current recommendation for insider threat detection programmes aims to employ prevention, detection and response practices and technologies for insider threats [21]. However, despite the vast amount of guidance and information from security vendors and security experts relating to designing and developing insider threat programmes, the insider threat persists within FS organisations. There is an acceptance within the working practice that there is no silver bullet to addressing this threat, nor is there a one-size-fits-all solution to tackle the insider threat phenomenon, as evidenced in the current insider threat landscape and recent high profile insider cases. Nevertheless, this review will highlight several key areas. Section II explains the Insider Threat definition and the methodological approach to the review undertaken by the researcher in response to investigating the research questions.

1) What factors influence employees to become malicious insider threats and apply this to employees working within the UK FS organisations?
2) What preventative measures could be effectively operationalised within UK FS organisations to prevent malicious insider attacks?

Furthermore, Section II will introduce the five emerging research insider threat themes borne from the literature review, which include:

1) Behavioural Studies
2) Information Security Behaviours
3) Technical Controls
4) Insider Threat Strategies
5) Regulation

Section III will discuss and critically evaluate the five emerging insider threat research themes. Section IV will propose recommendations that FS sectors can adopt to help mitigate the malicious insider threat, addressing these five emerging insider threat research themes and concluding with a summary. Lastly, Section V of the paper proposes further research topics and future works.

II. LITERATURE REVIEW

A. DEFINITION'S

This study will define the insider threat to include the National Protective Security Authority (NPSA) definition in line with the UK FS organisation's maturity assessments [21]. The term insider will relate to an individual /person (s), also called employee (s). The term includes current and former employees, contractors, and trusted third-party suppliers. Furthermore, an individual, person, employee, contractor, or former employee who, by virtue of their role, function and or seniority, have or previously have had legitimate access to systems, sensitive data, and financial assets, which could cause severe or material harm to the FS organisations, will also be defined as the insider threat. Also, trusted third-party suppliers (an individual, company or organisation that has entered a contractual business relationship, providing services or employed to undertake commercial transactions on behalf of the FS) with legitimate access, as aforementioned, can be defined as an outsider insider.

B. APPROACH

A PRISMA framework [22] was applied to support the literature review, with 44 articles initially selected relating to Insider Threat or Insider Risk within the search terms. All articles were scholarly, chosen from three research databases, peer-reviewed, printed in English, and published between October 2017 and October 2020. An additional ten articles were identified to address the research question and help shape, influence and present similarities, differences, or gaps. We expanded the scope of the literature review by integrating additional and current articles, reinforcing the scholarly foundation and contextual significance of this investigation.

The articles were assessed for effectiveness, and a structured set of questions formed an assessment framework, which was developed and applied to assessing the qualitative, quantitative, and mixed-method studies by addressing the following questions:

1) Did the article address a focused question?
2) Are the articles relevant to this research question?
3) What was the methodology of the articles?
4) What are the key outcomes/findings of the article?
5) Are the outcomes/findings applicable to the population or research question?

A PICO acronym [22] was adopted to establish the criteria of the studies; please refer to Table 1. This structured format supported finding the best evidence available and assessing the research relevance and validity to address the research question. The simplistic review method outlined above was adopted to ensure the best evidence is collected due to the limitations of resources and timescales.

The literature review addressed each question and synthesised findings. Five main insider threat research themes emerged from the review process: behavioural indicators, information security behaviours, technical controls, insider threat strategies and regulation.

Despite insider threat being recognised as a significant threat across the UK based FS organisations. More research is needed in practice to understand insider threat behaviours, adequate technical controls, and best practice approaches to insider threat strategies.

This section will analyse and synthesise previous research views and findings to uncover potential themes, thought leadership, gaps or limitations in previous research, which will establish the significance of this review.

C. BEHAVIOURAL STUDIES

Extensive studies have been undertaken to understand better behavioural indicators, including human traits and characteristics of threat actors [23], [24], [25], [26], [27], [28], [29], [30]. Knowledge and awareness of past research studies relating to potential insider personality traits, characteristics and behavioural approaches will also assist the development of proactive organisational insider threat strategies.

A recent review to develop a conceptual model for insider threat undertaken by Whitty [31] discusses employee motivations, suggesting employee disgruntlement, addiction, personal gain, financial hardship, relationship problems, legal matters, and conflicts at work are all indicators of insider threat. Similarly, Greitzer and Frincke [28] investigated combining traditional cybersecurity audit data with psychosocial data to develop a predictive model for insider threat mitigation. Greitzer and Frincke [28] proposed that the 12 overall psychosocial indicators and social factors inter-relate to individual thought and behaviour. A later study by Greitzer et al. [29] extended the development of a comprehensive insider threat taxonomy that includes over 300 behavioural and organisational factors and technical indicators. The volume of the indicators is vast, and the researchers [29] acknowledge the associated challenges of such a large data set. Therefore, they used an off-the-shelf ontology development tool to meet more straightforward design objectives. However, the scale of the indicators demonstrates the complexity of identifying and managing organisational threats.

A more recent enquiry [25] building on previous work researching personality, building on five constructs of:

1) Openness
2) Conscientiousness
3) Extraversion
4) Agreeableness
5) Neuroticism

The enquiry found that the big five personality factor descriptions are associated with cybersecurity behaviours and that conscientiousness and openness personality traits positively influence cybersecurity behaviours, which can also result in insider threat activity. Furthermore, some believe that psychopathy has a prominent effect on how individuals justify their malicious behaviours and suggest that the dark triad (i.e., psychopathy, Machiavellianism, and narcissism) of human behaviour comes into play as a critical driver of fraudulent or insider behaviour [26]. Nevertheless, little is known about the psychological mechanisms that may explain adverse workplace outcomes [32]. However, identifying these personality disorders in the workplace may raise ethical questions.

Despite ethical considerations, human and psychological drivers relating to understanding the insider threat need to be explored. Insider threats are not a new organisational problem [33]; with previously researched open-source insider cases, a documented list of psychological characteristics (representative of I.T. specialists) focused on traits of individuals who perpetrate insider threat activity. Six personal characteristics relating to insider activity included:

1) A history of personal or social frustrations
2) Computer dependency

TABLE 1. PICO.

PICO component	Description
P - Population	Colleagues (preferably) within financial service organisations who are malicious insider threats
I - Intervention	Preventative Insider Threat Programmes or Preventative Insider Threat Controls
C - Comparison	Colleagues within financial service organisations who do not become a malicious insider threat
O - Outcome	Development of Preventative Insider Threat Programmes or Controls

3) Ethical flexibility
4) Reduced loyalty
5) A sense of entitlement
6) Lack of empathy

Interestingly, an article on cyber hygiene and knowledge [34] reported that self-described cyber experts reported less secure behaviours and had less knowledge about cyber hygiene than other participants in an exploratory study of 268 participants. These works do not explicitly say that I.T. specialists or I.T. experts are not honest or trustworthy business professionals and partners. However, consideration should be given to those individuals who can cause severe or material harm to an organisation due to legitimate access and knowledge of systems, premises, and data.

Research looking at human behavioural factors supporting the development of an ontology highlights individual and organisational sociotechnical indicators of insider threat risk and other relevant indicators that can be defined based on personal history factors [24]. Personal historical factors can include (not exhaustive) financial risks, medical or health matters, unusual contact with foreign entities, radical beliefs, disloyalty and psychological or personality factors of concern. Further examination of case studies suggests that personal history events, personal predispositions, and psychological and personality characteristics can be used as markers or warning signs. These factors can indicate an increase in insider threat conduct, which the workplace or personal stressors could trigger. The Secret Service and the Computer Emergency Response Team (CERT) Division, based at Carnegie Mellon University, has determined that a problem in an employee's personal life can influence their actions in the workplace [35]. Notwithstanding this, there are ethical, employment law, and data privacy concerns about the processing, handling, and storing of this type of personal information about individuals within a working environment.

A review [36] did not look exclusively at behavioural indicators but focused on themes relating to environmental drivers; for example, a study found that an individual is less likely to perpetrate and partake in cybercrime activity (as well as participating in traditional crime) in years in which the individual is cohabiting with a partner, regardless if children are present within the household. The paper [36] also examined how private and professional lives and associated circumstances relate to cyber-offending (categorised as an insider threat). Other important factors were also uncovered, particularly when looking at the professional life of an individual. For example, it was established that individuals in employment and enrollment in education (although not statistically significantly related to cyber-offending or insider threat) reduce the likelihood of traditional offending. However, for these professional life circumstances, opposite effects are found to be more likely [36]. The increase in likelihood may be driven by increased opportunities in the workplace, where legitimate access to systems and data can provide opportunistic crime and insider activity, including insider fraud or other white-collar or employment-enabled crimes.

In examining the dynamics of insider threats within the FS industry, real-world cases, such as incidents at J.P Morgan Chase [37], where employees exploited their access for personal gain, echo findings from this study [36] regarding opportunistic misconduct due to having legitimate access to systems and data. Similarly, the Wells Fargo case [37], involving the creation of unauthorised accounts, parallels the discussion on employee behaviour [38], where perceived organisational conditions, expectations or unethical management practices may not deter unethical behaviour, including abusing access to computer and customer records, regardless of potential sanctions.

Opportunistic insider threats are two important considerations when exploring insider threat phenomena [39]. Padayachee [40] assessed opportunity-reducing techniques within information security, where the researcher believes that opportunity is more tangible than motive due to their evaluation of opportunity-reducing measures in information security. The researcher [40] suggests that the current detection strategies must be improved, and proactive mitigation strategies are more effective. The research [40] considers five categories of opportunity-reducing controls, categorised as 'increase effort', 'increase risks', 'reduce rewards', 'reduce provocation' and 'remove excuse', which attempts to conceptualise opportunity in terms of the insider threat phenomenon.

An examination to develop a framework for characterising attacks [41] proposed a conceptual framework from an in-depth analysis of case studies and published literature. The review [41] identifies the key elements that concentrate on the noteworthy events and indicators, the motivation behind malicious threats, and the human factors related to unintentional ones. The researchers [41] state that the motivation to attack can be driven by financial, political, revenge, curiosity or fun, power, competitive advantage, or peer recognition. A previous case study [35] highlighted

23 cases within the U.S. banking and finance industry, identifying that 27% of the perpetrators were experiencing financial difficulties in their private lives.

Also, an individual's current psychological frame of mind can significantly influence an attack, for example, disgruntlement [38]. The researchers [38] developed a framework that focused on what factors may motivate employees to commit information computer abuse. The study focused on disruptive and procedural organisational injustice. The purpose of the research was to understand what factors could either enhance or mitigate direct causal relationships. The research [38] was underpinned by behavioural theories of deterrence within information security. Furthermore, early work by Schultz [42] discusses several insider threat predictions and detection frameworks, including the generically termed CMO Model (Capability, Motivation and Opportunity); 'Capability', to make the attack, the 'Motive' to do so and the 'Opportunity' to commit the attack. However, despite several predictive models and frameworks, Schultz [42] concludes that there is "…no single clue sufficient for predicting and detecting insider attacks" [42]. According to some [35], deterrence research and deterrence theories relating to internal computer abuse underpin criminology theories.

Considering early work by Shaw and Stock [30], it is worth noting that it addressed the elevated level of organisational anxiety regarding the potential theft of intellectual property and critical sensitive or proprietary data. The report [30] provides an overview of human and organisational conditions, rather than technological factors, which contribute to insider threats from a clinical and forensic psychologist lens to support corporate security, law enforcement and government national security divisions, and a behavioural approach to this modus operandi. The paper [30] suggests that insider Intellectual Property (IP) or data thieves:

1) Often, technical positions within organisations with legitimate access to the data offer capability and opportunity. The perpetrators are male, aged on average 37 years.
2) Most perpetrators have signed IP or Non-Disclosure Agreements (NDA); trade secrets and business information are the most common IP and data stolen.
3) Typically, the perpetrators have already secured a new role external to the organisation, with 65% accepting positions with competitors or being used for their purposes (i.e., self-employment).
4) Most perpetrators use corporate networks such as email universal serial bus (USB) to transfer or exfiltrate the stolen data.

A more recent study [43] highlighted the rising concerns of insider cybersecurity breaches, proposing a cyber-security culture framework that evaluates behavioural and technical indicators to identify and mitigate insider threats, such as employee satisfaction, personality predispositions, access controls, policy violations, and awareness, to evaluate the insider threat risk. The framework applications are demonstrated through case studies, including malicious intentions, fraud, and espionage scenarios. This approach assessed individuals' and organisations' security culture to measure, analyse and identify potential insider threats. However, there are ethical and privacy concerns related to the psychological assessment used, and consideration of the complexity of implementing this framework will pose challenges to its universal applicability. Nonetheless, the framework emphasises the need for a proactive approach, including security training, to safeguard organisations and employees from insider threats.

The research and works mentioned above, with findings, highlight potential indicators and factors that can be used to shape preventative insider threat programmes of potential catalysts or triggers known in advance of an insider attack. Identifying possible employee motivations within these categories can support early intervention and insider threat prevention strategies ahead of a potential insider threat catalyst [39] or insider threat opportunities [36] for employees at a higher risk of becoming an insider threat.

D. INFORMATION SECURITY BEHAVIOUR

Analysis [44], looking at the impact of employment status on internet service provider (ISP) compliance, found that part-time or temporary employees and their organisational commitment to comply were lower than full-time permanent employees, as was their position held within the organisation. Therefore, [44] deemed this population a risker from an insider threat lens. Interestingly, a study in 2019 [45] identified that the role of leadership and leader power bases could also contribute to determining what factors influence employees to become a malicious insider threat, particularly around ISP compliance, social factors, and intrinsic motivators. The article [45] found that moderating leadership effects can differ, driven by varying factors, including how positive leadership is on employee relationships, reward, and legitimate leadership power. Similarly, research [46] was conducted looking at the impact of leadership on employees' intended information security behaviour and how and why different leadership styles enhance employees' intended information security behaviour. The research [46] found that transformational leaders had a positive impact, as they could directly influence employees on discretionary effort in-role and associated behaviour levels. Leadership influence is not only a contributory factor; personal attitude and behaviour should also be considered [46].

Further insight can be gained from an exploratory study of cyber hygiene behaviours and knowledge. The researchers [34] surveyed 268 participants, looking at personal cyber hygiene factors. Although the study [34] did not focus on cyber hygiene and knowledge within an organisational setting, the participants' characteristic insights found no differences between behaviour and age. However, males were said to be more cyber-savvy than females. An investigation [47] examining human factors and data leakage suggested that organisational culture would be advantageous, operating within an ethical climate relating to a positive information-sharing culture. Despite the findings [47], the study found that incidents occurred due to personal greed, employees' jealousy, disgruntlement, and feeling vindictive which drove information leakage. All these drivers can be classified as insider activity. The researchers [47] proposed that human governance and being guided by a standard set of inherent human/employee principles and Organisational Embedded Culture (OEC) is positively beneficial. This is said to foster OEC to shape and guide employees' acceptable behaviour around information security culture, balancing a great working environment, progressive reward, and strict policies.

Similarly, an examination [38] of employee computer abuse intentions found that organisational or perceived distributive organisational injustice is not a significant motivator in forming computer abuse intentions when faced with the possibility of sanctions. Therefore, it may be feasible that employees do not see information security sanctions as an injustice due to their information security behaviour. Furthermore, employees may use a series of justifications and excuses to neutralise their actions as legitimate or acceptable [38]. In support of this, [36] argues that individuals do not perceive online behaviour as carrying the same weight or consequences of offline actions and behaviour. Furthermore, many studies have been undertaken to understand information security behaviour and better understand factors influencing employees to become insiders or mitigate insider threats. Behavioural science around information security studies incorporates multidisciplinary theories, including psychology, sociology, and criminology [48], including Deterrence Theory (DT), theory of planned behaviour (TPB), Social Bond Theory (SBT), Rational Decision-Making (RDM), Psychological Contract (PC), and Opportunity Theory (OT) [49]. Many studies and research articles on and around information security behaviour focus on factors that influence security behaviour, including policy compliance [50] and [51], factors that motivate employees to follow computer usage policies [52], and preventative measures [50]. These works are underpinned by behavioural theories, which look to provide more context around human cognition.

Research [51] looking at insider compliance with Information Security Policies (ISP) discussed the impact of DT, focusing on insiders' compliance with information security policies. The researchers [51] argue that the greater the sanctions, the more likely employees will adhere to ISP policies, particularly where there is malicious ISP non-compliance, suggesting that "…deterrence theory better predicts deviant behaviour in malicious contexts, cultures with a high degree of power distance, and cultures with a high uncertainty avoidance" [51]. The research [51] is also underpinned by a previous study [53], which argues that conventional training techniques are ineffective in reducing information security breaches and are driven by the reinforcement approach within organisations. However, it is worth noting that DT assumes employees know organisational policies and non-compliance consequences. Although it appears that regulating security behaviours and ISPs with sanctions deter negative insider behaviour, the researchers [53] also acknowledge that organisational culture can be instrumental when conceptualising deterrence theory in the ISP context.

Similarly, a recent study [52] looking at the impact of awareness of employee monitoring relating to computer usage policy compliance indicates that sanctions or penalties may only be effective based on organisational detection and monitoring capabilities. However, the researchers [52] agree with the study undertaken by Trang and Brendel [51] that perceived sanction severity and perceived sanction certainty have a statistically significant positive influence on compliance with computer usage policy. Notwithstanding, the study [51] did not expressly look at deliberate and malicious intent.

However, a study [54] undertaken across various industries, including financial services, exploring cybersecurity policies, and identifying common aspects and their applications to protect digital assets effectively suggests that further exploration of integrated security management and incident response operations should be considered as well as highlighting the importance of developing policies against diverse malicious cyber-attacks. A layered approach is required depending on their organisational risks.

In addition, Saffa et al. [50] present a novel conceptual framework to mitigate the risk of insiders using DT to understand better prevention approaches to the insider threat. Saffa et al. [50] claim that "…insider threats can be managed through psychological, managerial and technological aspects regarding information security". The researchers [50] suggest that perceived sanctions, certainty, and severity significantly influence employee attitudes and can deter ISPs. Their findings [50] also highlighted that increasing employee effort, heightening employee risk, and reducing employee rewards significantly influenced employees' attitudes towards not partaking in ISP misbehaviour. Conversely, [36] argue that individuals may be driven to partake in online criminal offences (cybercrime) in part due to individuals feeling disconnected from the offline real world [55] and individuals feeling that there are fewer negative social consequences committing offences related to cybercrime (compared to traditional crime). Another school of thought [56] suggests that psychological contract fulfilment can mitigate the negative effect of ISP compliance. It should also be considered a key driver that may influence employees to undertake insider activity.

D'Arcy and Lowry [57] argue that employee ISP compliance needs to be more active and suggest that cognitive factors alone do not fully explain ISP compliance, suggesting that organisational norms and affective factors such as colleague mood and feelings also influence ISP. However, other researchers [57] support the theory that deviant employee behaviour will have a low ISP. Furthermore, D'Arcy and Lowry [57] propose a multi-level model integrating affective factors with Rational Choice Theory (RCT) and TPB constructs. The research [57] findings highlighted that compliance attitudes, moral beliefs, organisational deviance, and descriptive norms were significantly associated with ISP compliance behaviour. However, causality was not established.

Aurigemma and Mattson [58] looked at the moderating effect of employee status on perceived behavioural control, underpinned by TPB, suggesting that positional or hierarchical power employees are more likely to get away with poor ISP. The researchers [58] believe that within hierarchical organisations, where rank and order or command and control structures are in place, this can impact any ISP non-compliance. Although the investigation [58] looked at ISP compliance from a physical security perspective, the same theories may apply and be relevant to ISP compliance relating to insider threat, including areas of misbehaviour or malicious intent within data loss and password hygiene. Aurigemma and Mattson [58] argues that organisational status is an important consideration, particularly relating to understanding the threats within an organisation. The lack of care could open opportunities and be an influencing factor associated with insider activity.

When investigating opportunistic employee behaviour concerning unauthorised access attempts on Iinformation Systems (IS), User Behaviour Analytics (UBA) examines the predictive validity of OT in the context of information systems. Thus, developing a model that considers and examines employee and department/organisational level opportunity circumstances [59]. The study [59] draws on previous work by [49], where an insider incident pinpoints the intersection of motivated offenders, suitable targets, and ineffective guardianship. By utilising the OT framework, researchers [59] found that the greater access to data, systems, and applications the individuals have, the more likely they are to make unauthorised access attempts. Similarly, [36] suggests an increased opportunity and likelihood of individuals engaging in cybercrime due to their knowledge and capability playing a part, mainly where individuals are employed within the I.T. sector. However, Malik [60] warns that technology is not currently or sufficiently advanced to effectively understand humans and make rational decisions, highlighting the complexity of preventing and detecting insider threat phenomena. However, strong social bonds, for example, family members, may reduce the likelihood of cyber-offending than traditional crimes [36].

Conversely, Slyke and Belanger [61] observed the interactions of humans and artefacts in insider security behaviours, concentrating on the mangle of practice perspective. The research [61] offers a counterargument to why security compliance is not a robust control for insider threats. More focus should be on socio-technical considerations, as ISP compliance needs to consider users' goals adequately. However, the paper did cite the same influencing factors as aforementioned, highlighting risky insider behaviours, including ISP violations, violating security policies, and writing down passwords. The mangled perspective may, however, support a deeper understanding of behaviours that emerge over time.

Another recent study [62], a theoretical model based on behaviour theories, assessed employees' intentions and behaviours regarding security information security. The findings highlighted the significant impact of psychological factors and facilitating conditions on employees' adopting information practices. However, the study [62] did not extensively examine contextual factors specific to organisations, such as organisational culture, leadership support, or resource availability. While the model suggests relationships between psychological factors, facilitating conditions, and information security behaviour, it does not prove causation. Nevertheless, the researcher recommends security awareness training to mitigate these risks.

E. TECHNICAL CONTROLS

The vast majority (90%) of the selected articles focused on predictive detection capability, where the emerging theme was technical controls, with [63] focusing on a sociotechnical approach, which looks to identify interactions between people and technology and strengthen existing cyber controls through Machine Learning (ML) However, most studies reviewed predictive technology that identifies malicious or anomalous behaviour, with mathematical algorithmic, ML, deep learning and Artificial Intelligence (AI) software being a popular methodology and approach. It should be noted that these technological capabilities are being explored and developed further and can be seen operationally within FS organisations by way of User and Entity Behavioural Analytics (UEBA) technologies.

UEBA can detect anomalies, highlight outliers' inactivity, and predict threats using ML capability, analysing substantial amounts of data from applications, devices, and network logs that would not be detected via traditional and siloed security tools. UEBA uses various AI and ML techniques, including supervised and unsupervised ML [64], Bayesian networks [2], and Deep Learning ML [65]. Notwithstanding UEBA technology, several other studies looked at narrower ML approaches within differing environments, with various capabilities and addressing several cases to approach the insider threat.

Schultz's early work [42] proposed a novel approach for predicting and detecting insider attacks based on the simple premise that no single clue is sufficient for predicting and detecting insider attacks, unlike the detection of externally initiated attacks. Schultz [42] suggested that multiple indicators and a mathematical representation of each indicator's contribution could indicate and detect insider attacks. This early seminal work [42] offered a framework, building on his previous work, defining relevant indicators, such as verbal behaviours, personality traits, and correlated usage patterns, which could be linked to predicting and detecting a potential insider attack.

A new way of predicting the risk of malicious insider threats before any insider activity occurs is seen in a developed framework [2]. The framework draws on 93 key insider threat indicators and data sources from a technical, organisational, and human perspective utilising a Bayesian network modelling and surveying organisations [2]. The outputs of the 93 key insider threat indicators were then used to estimate risk levels and can be duplicated and deployed within an organisational environment. Although many of the 93 indicators may be legitimate sources indicating the potential of insider threat (personal employee information, including employee work-related stress symptoms), these indicators can be subjective. Furthermore, data sources should be cautiously approached concerning the General Data Protection Regulation (GDPR) in handling and processing personal data within an organisational setting for security monitoring purposes.

A broader creative challenge was set by the Scientific Advances to Continuous Insider Threat Evaluation (SCITE) program, which was sponsored by the Intelligence Advanced Research Projects Activity (IARPA) [66]. The challenge posed was to detect a specific behaviour or identify individuals who belonged to a group from an incomplete data set. Throughout the series of challenges, one of the participating groups employed Multi-Model Inference Enterprise Modelling (MIEM) to conduct model averaging based on information criteria, which was deemed the most effective method above probabilistic relational models Bayesian network orientated predictions [66]. Despite this, the results of this challenge by SCITE are limited and based on one company data set, with no evidence of whether the outcomes were confirmed.

An ML bio-inspired algorithmic model to mitigate insider threats was developed to emulate nature and natural ways of solving complex real-life problems [67]. A model based on utilising an existing unsupervised ML algorithm, looking for anomaly detection, identifying outliers, and applying swarm intelligence algorithms to enhance performance, incorporating the big five personality traits using synthetic data to avoid privacy and legal considerations [68]. However, psychometric data may need to be gathered or gained to assess employees' personality traits, contractors, and third-party contingent workers due to ethical, privacy, and GDPR considerations when operationalising this approach within an FS environment.

Smyth [69] suggested that data virtualisation is an effective detection method to protect big data warehouses used within most FS organisations. Smyth [69] states that data visualisation techniques will provide a solution to detect insider activity by removing the need to create multiple copies of the data, ensuring more robust controls through a single point of access across an organisation's I.T. estate. Furthermore, data virtualisation facilitates live monitoring of audit logs, preventing malicious insider activity within the estate within seconds rather than days. The trade-off and considerations for FS organisations are moving their data to a cloud-based application. This will bring additional operational considerations and risks to facilitate data virtualisation and potential downstream complexities of integrating their current logging and monitoring on-prem systems. This approach is similar to the study [65], which looked at image-based feature representation through greyscale images for insider threat classification to predict insider threats. The greyscale images represent behavioural characteristics and attributes, using deep ML and neural networks, claiming to be more sensitive than other predictive ML techniques, for example, user behaviour analytics (UBA) or UEBA. This approach is an interesting and complex concept; however, it must still be proven or untested within FS organisations. In contrast, UBA and UEBA capabilities are already acknowledged as complex technologies to deploy operationally. Nevertheless, these technologies are proving to be a popular security technology currently being evaluated or deployed across several FS organisations to address the insider threat.

Sharghi and Sartipi [70] presents a model to describe the behaviour elements and their relationships to user behaviour characteristics, attributes, relationships, structures, and effects of a series of user actions in a specific application domain. The researchers propose a standard behaviour pattern language (BPL), modelling language to highlight behavioural attributes and patterns, representing a particular behaviour of user pattern, and correlating data using sequence association, proximity, separation, and causality. This contribution is now seen as a developing feature of the UEBA and UBA software and platforms, which offer a consistent language and approach to operationalising within FS organisations.

Distance measurement techniques measure the relative difference between objects within a problem environment [71]. A study [71] focused on three distance measurement techniques (Damerau–Levenshtein Distance, Cosine Distance, and Jaccard Distance) and found that none of the methods tested achieved 100% accuracy and suggested that all three techniques could be aggregated to provide better confidence levels, rather than using one. This approach may add additional complexity and generate more false positives when operationalised. However, the researchers [71] reported that distance measurement techniques are faster to process than other heavy ML algorithms. Recognising that developing ML can predict and detect insider threats [71] and look to build upon previous work, using CERT synthetic data set, focusing on distance measurement techniques, to detect changes in behaviours.

Park et al. [72] looked at detecting potential insider threats by analysing sentiment across social media platforms, analysing emotions as the primary indicator. Machine learning algorithms were applied to detect possible malicious insiders via classification of the emotions (negative, neutral, and positive), with the study citing a 99.7% accuracy level. Sentiment analysis using M.L. technologies is underexplored within the FS organisations and used primarily for marketing and customer sentiment analysis. However, this approach could prove valuable to detect and prevent an insider attack using the same technology across collaboration platforms (Yammer or Microsoft Teams, for example) or email traffic.

A more unexpected, unique experimental research measures individual mouse-cursor movements when undertaking a mock theft experiment through an electrodermal online screening questionnaire [73]. The study hypothesised that mouse-cursor movements differed from individuals telling the truth versus those trying to conceal the truth. Whilst the findings from this small experimental study demonstrated that there was a positive indication that individuals who were trying to hide the truth could be identified, it does, however, call into question the extremes and situations in which this type of investigative technique would be deployed within FS, notwithstanding implications of consent, privacy, and ethical considerations.

Another recent study [74] uses mouse movement patterns as behavioural biometrics to verify individuals with access to privileged information, aiming to predict user legitimacy for real-time monitoring and protection of sensitive data. However, obtaining substantial amounts of user data in real-life operational settings may not be practical.

The approaches mentioned above are diverse, complex, and sometimes controversial. However, it supports the idea that technological approaches must be tailored to the organisational environment and culture, specifically aligning used cases to organisational risk appetite.

Several studies focused on data loss prevention (DLP) as an approach, with one study and experiment [64] identifying the best ML technique to detect anomalous or malicious emails as an insider threat vector. The experiment [64] demonstrated that adaptive boosting (AdaBoost), a specific method of training a booster classifier, can achieve the best classification accuracy, with 98.3% achieved through their experiment. AdaBoost algorithms can be deployed to enhance the performance of ML algorithms and are used to create weak learners to become stronger for binary classification problems [75]. The researchers [64] suggest that this approach can be used as a predictive modelling tool to determine an employee's risk level and insider threat likelihood using linguistic analysis of email traffic. However, the binary emphasis of the algorithm may only be appropriate in some organisational use cases.

Another research project [76] explored utilising ML capabilities to predict the likelihood of data loss/theft in email DLP to reinforce a system's data loss detection capabilities. This novel approach used Decision Trees and Random Forest algorithms in various experimental scenarios, which reported a 90-95% accuracy in predicting legitimate data loss events. However, it needs to be clarified how the detection of human threats, such as disgruntlement and privileged access for malicious purposes, can be achieved. Another drawback is the complexity of managing and configuring existing DLP solutions and overlaying ML capabilities. Therefore, confidence levels in scalability and operationalising could be higher.

A significant concern for FS organisations when considering technological (detective and predictive) controls is their cost to build, maintain and operationalise. Furthermore, adding challenges to deploying these tools and technologies will exacerbate available skills within the industry, with a potential skills shortage already being cited within the information technology field [77].

F. INSIDER THREAT STRATEGIES

The CERT Division, part of Carnegie Mellon University's Software Engineering Institute, provides insider threat mitigation recommendations by releasing the "Common Sense Guide to Mitigating Insider Threats" based on research and analysis of previous insider threat cases [78]. The guide [78] is based on continued research and analysis of over 1,500 insider threat incidents within public and private sectors. The evolving report [78] includes and describes the practices organisations should implement to reduce their exposure to the insider threat problem, with the latest recommendations around providing positive incentives within the workplace environment and highlighting current standards and regulations.

A study [6] looked at insider threat response and recovery strategies locally and within the FS industry. The research [6] was limited to only five representatives of FS organisations. However, the purpose of the study was to understand how the FS approaches insider threat, understand their response approaches and know what means of recovery they employ. The study [6] found that most reported insider attacks were financially motivated and often involved data theft. The researchers advocated eight recommendations [6, p. 17]:

1) Establish clear insider threat management governance structures.
2) Devise, implement, follow, and periodically review dedicated insider threat management policies.
3) Co-ordinate, memorise and streamline response and recovery measures and consider employing relevant third parties – e.g., law enforcement agencies, more frequently.
4) Ensure transparent communication of response and recovery measures to relevant stakeholders and create a sense of ownership among them.
5) Formalise threat intelligence-sharing activities and leverage key lessons learned across organisations.
6) Provide staff with relevant insider threat education and development programmes and ensure regular programme effectiveness reviews.
7) Evaluate response and recovery practices and incorporate lessons learned into future activities.

8) Ensure senior management buy-in and award the right attention to insider threat management.

A checklist summarised from findings of the CERT (2014) report [78] highlights best practices and recommendations to support the Insider Threat Programme (ITP) or Insider Threat Strategies (ITS). One proposal suggests that there needs to be better collaboration between the I.T. management and the human resources (H.R.) department. However, there were no new insights or suggestions on how this improved interlock and relationship can be utilised to offer a more robust ITP. Collaboration between these departments is critical to establishing the core purpose of any ITS to deploy an ITP to operationalise, particularly at scale. Furthermore, consideration of roles, responsibilities, and accountabilities will need to be established; for example, H.R. may be responsible for the overall organisational people risk, including screening and vetting. Although I.T. Security would be responsible for technical controls, i.e., DLP, UBA, multi-factor authentication (MFA), etc., divisional management may view risk appetite. Even though collaboration is necessary, there needs to be a clear line of sight in the overall accountability of the IRS or potential IRP, nor is there any consideration from a data privacy or legal perspective. Collaboration between these departments is critical to establishing the core purpose of any ITS to deploy an ITP to operationalise.

Based on the cyber kill chain framework, a layered defence strategy and approach is recommended, utilising organisational policies, considering corporate culture, and understanding the technical environment to combat insider threat [79]. The researchers suggest that understanding human behaviour and psychosocial factors is also essential in shaping insider threat strategies, which is critical. More importantly, the authors considered the importance of considering the organisational insider threat landscape, including detecting, and preventing unauthorised access to corporate resources, including data, devices, and premises.

Similarly, Richardson [80], in his paper 'Is there a silver bullet to stop cybercrime?', discusses internal and external fraud drivers and recommends that objectively assessing security weaknesses and vulnerabilities is paramount in developing robust security strategies across businesses and banks. However, the paper does not recommend linking this to a threat landscape assessment to maintain currency and drive an intelligence-led operation. Nevertheless, from an insider perspective, the article references some areas of consideration, including technical and non-technical controls, such as deploying MFA and segregation of duties. Notwithstanding that the paper suggested segregating duties, the recommendations could have further understood the populations and presented further segmentation. For example, they know what populations have access to business or bank data or systems access, considering where toxic combinations do not apply and where individuals can still cause severe or material harm. Therefore, by understanding who has access, additional segmentation could be beneficial, offering an opportunity to wrap additional controls or heightened screening, including vetting, criminal and credit checks as an extra measure or enhanced control framework.

Ki-Aries and Fairy [81] highlight the importance of maintaining information security, protecting organisational assets, and not using information security training and awareness programmes as a compliance measure. The research looks to advance security training and awareness effectiveness by presenting a persona-centred training and awareness approach. The authors suggest that the personas should be reflective and an archetype of the organisational users and training and awareness programmes, have top-level organisational sponsorship and ensure that the content engages and supports a collaborative security culture.

Fimin [82] discusses the risks that individuals who intend to leave an organisation can pose an increased risk of becoming an insider threat, for example, taking I.P. or data on exiting the organisation and recommends five areas that could help detect or prevent increasing the risk. However, an opportunity for I.P. theft or data loss to have occurred before the employee resignation may have already occurred. Therefore, these recommendations and practices should be reinforced throughout the employee lifecycle:

1) Codes of conduct, expectations of role and policy requirements through regular effective communication, and training and awareness programmes.
2) Consider gardening leave, depending on the impact that the individual can potentially cause.
3) Disable external, email, web, and printing rights.
4) Put enhanced controls, i.e., on a watch list if email or web access remains so this can be triaged as a priority or block all access to unapproved email domains.
5) Consider deploying UBA technology as a detective and predictive control measure.

Jalil and Hassan [83] also looked at strategies for protecting trade secrets from theft, highlighting the importance of legal and administrative measures in this digital age. The authors [83] recommend several information security measures but expand the benefits of NDAs in more depth, drawing attention to having a clear definition of trade secrets or confidential information to enforce the NDA. Furthermore, emphasis was placed on organisations demonstrating that they have taken appropriate measures to protect the data in the first instance [83]. An example of this was seen in the recent case of Morrison's Plc, where Morrison's was found to be vicariously liable for a deliberate and malicious data breach from a former employee [84]. Jalil and Hassan [83] also recommend the benefits of having an end-to-end control environment wrapped around from onboarding, including appropriate vetting checks and a robust leavers checklist. The leaves checklist would ensure that an exit interview is conducted, the obligations of NDA are reiterated, and all data is wiped or destroyed from Bring Your Own Device (BYOD) or Bring Your Own Cloud (BYOC). Even with this approach, operational controls are essential, such as information security training and awareness, codes of conduct policy reinforcement, and cyber monitoring controls to monitor information security compliance.

A comprehensive overview of a fraud matrix is outlined [85]. The paper [86] has significance in understanding the insider threat, as internal fraud can be categorised as an insider threat due to trusted employees or third-party contingent workers having legitimate access to systems and data assets and abusing this for malicious purposes. Although several types of fraud were identified from an internal and external perspective, the framework can understand how they are committed, particularly from an internal perspective. Examples of internal fraud included privileged access abuse and financial misappropriation, which align with previously outlined insider threat cases. This taxonomy can identify internal fraud to deploy controls, such as MFA and cybersecurity monitoring, as a mitigation strategy.

Another example of how internal fraud is intrinsically linked to insider threat is a recent study investigating weaknesses of internal controls within work expense claims procedures [86]. Despite the survey [86] conducted, it should be acknowledged that the study narrowly focused on expense fraud as an insider attack. The study [86] highlighted that weak internal controls drive the internal abuse of expense claims. Recommendations include enhancing the control environment (including tighter controls within the finance department), standardising policy, and improving colleague satisfaction. This can lead to a better working environment, thus reducing the opportunity or motivation to abuse expenses [86]. However, in practice and seen within one large FS organisation, detected expense claims abuse can account for circa 3-5 % of investigations (pre-COVID-19 levels) [87]. Pre-employment screening, competitive salary packages, and transparent policies and procedures around financial expense claims reflect the Nations' Report on Occupational Fraud and Abuse (2016) by the Association of Certified Fraud Examiners. They conclude that 14% of fraud is expense-related [88]. The significant difference between investigations in practice could be an area for further research. However, within FS and in practice, effective training and education, policy controls to ensure compliance to mitigate this threat, and delegated authority to sign off expenses are devolved at a local management level, which may account for the lower reported levels of internal expense fraud.

Finally, research [89] that presents a more obscure strategy for tackling the insider threat suggests that the wrong ambient room temperature can cause temporary and residual stress on individuals, introducing two categories of insider threats for blue and white collar workers. The central premise of the argument [89] is centred around the thermal stress in the working environment, citing that the wrong temperature, in particular temperature above 38-40 degrees, can cause short-term and extra stress in individuals. Stress impacts productivity levels and biological reactions; for example, the body produces more adrenaline. The temperature is said to cause discomfort, resulting in health-related matters, occupational stress, and disgruntlement. The paper [89] proposes several measures to adapt working conditions to minimise insider threats, including working conditions, nutrition, and psychological traits. The goal is to be used as a preventive strategy against malicious behaviour, preventing counterproductive behaviour. There was no consideration of external working environments and how this could impact an individual's mood and subsequent behaviour. However, acknowledging that the working environment is essential, including recognising that employers have a duty of care to provide a safe working environment for their employees. To my knowledge, there have not been any insider risk cases that have been cited as a root cause as a direct result of environmental working temperature. Nevertheless, reviewing the working environment and stress levels could be explored more deeply to understand a direct correlation.

G. REGULATION

Only a few articles emerged from the literature search parameters relating to law or regulation [83] and [90]. Reid's [90] study was based on U.S. policy and regulation. The author advocated reforming the current legal U.S. framework to provide assurance and reliability in code for organisations, including enforcement and exploring U.S. laws governing employment relationships. Despite the study's limitations, primarily not relating to UK laws and regulations nor FS focused, some insights can be drawn with some similarities; for example, the review calls for simplifying enforcement surrounding the insider threat within organisations. There are low reporting and conviction rates within the practice and throughout the FS industry, driven by perceived reputational damage and high enforcement criteria thresholds; therefore, organisations are not keen to prosecute [90]. Jalil and Hassan [83] highlight the importance of protecting organisational trade secrets from theft, misuse, abuse, and misappropriation and suggest that protection can be gained via legal and internal control and governance measures. The legal measures include confidentiality, NDA and communication, multimedia, and computer crime laws. However, detection and evidence must be proven before any criminal prosecution. The UK law and regulation [91] and [92] specifically:

1) General Data Protection Regulation (GDPR), 2018
2) Criminal Justice Act, 1993
3) Computer Misuse Act (CMA), 1990
4) Trade Secret Enforcement of 2018

The UK law and regulation can all be reviewed to support deterring insider threats and proactively loading insider or internal fraud cases onto the UK. National Credit Industry Fraud Avoidance System (CIFAS). The exam question remains: is there an organisational risk appetite from FS institutions to pursue and publicly prosecute malicious insider activity despite any potential insider incident stemming from a potential operational failure? Risk appetite can be defined as the amount of risk an organisation is willing to take to deliver its strategic objectives [93]. Therefore, the publication of these potential operational failures could generate greater financial losses, reputational damage due to inadequate or failed internal processes, people or systems, or external events [94] and take years to recover from [80].

III. DISCUSSION

Limited studies have been undertaken within the insider threat field within the FS industry, despite FS being a primary target for data theft and financial fraud resulting in damage to the brand, reputation, customer trust, and the bottom line [95]. However, this review reveals five primary emerging insider threat research themes:

1) Behavioural
2) Information Security Behaviour
3) Technical Controls
4) Insider Threat Strategies
5) Regulation

The review highlighted several articles and studies that focused on behavioural studies within Section, II-C, with indicators and factors that could potentially influence or be contributing factors to malicious insider threats:

1) Insider personality traits
2) Insider characteristics
3) Insider behavioural approaches and motivations
4) Psychosocial
5) Social indicators
6) Sociotechnical indicators
7) Psychopathy

However, identifying behavioural indicators (as aforementioned above) has ethical implications under GDPR, considering employee privacy and UK employment law, which would consider potential mental health or learning difficulties. Notwithstanding this, implementing behavioural monitoring needs to be purposeful, proportionate, and lawful. Furthermore, behavioural monitoring may not consider the employee working environment within a FS environment and personal circumstances. Also, personality testing may not be a true-to-life representation of how an individual portrays themselves or intends to be represented to an employer.

Information Security Behaviour (ISB) within Section II-B highlights that there has been considerable focus on ISB, identifying factors associated with ISB compliance. Studies include examining:

1) Employment status
2) Employee demographics
3) Leadership relationships
4) Organisational structures and cultures
5) Theoretical models liking ISB, including employee psychological contracts, deterrence theory, theory of planned behaviour, social bond theory and opportunity theory
6) Information security compliance, sanctions, and perceived consequence

Understanding ISB is a critical layer of defence against insider threats, with humans being widely acknowledged as the weakest link in any security posture, including within an FS environment. Nevertheless, limitations from a security monitoring operational perspective should be considered, similar to the considerations highlighted in behavioural studies. In addition, individuals within the FS organisation may feel that security monitoring within their workplace infringes on their data privacy rights. Any information security sanctions may lead to employee disgruntlement. Furthermore, security sanctions such as retraining may be ineffective in tackling opportunistic employee behaviours.

Technical Controls, within Section Section II-E, brings into sharp focus the vast number of studies within this area, with over 90% focusing on predictive technical capabilities to tackle organisational insider threats. The studies covered a plethora of technical proposals, including:

1) Machine Learning and Artificial Intelligence
2) Socio-Technical Controls
3) Bayesian Networks
4) Distance Measurement
5) Data Visualisation Techniques (Greyscale)
6) Sentiment Analysis
7) Data Loss Prevention

The scale of studies in this field can represent FS practice with many cyber security or insider threat programmes deploying at least one technical detection capability. Some technical approaches, such as UEBA and Sentiment Analysis, may be too complex and costly to deploy. Furthermore, some technologies still need to be considered mature, for example, sentiment analysis and greyscale. Therefore, adoption rates may need to be faster across FS organisations. Lastly, some of the studies were exploratory. They would not be fit for purpose as a viable consideration to deploy across an FS working environment, for example, elector dermal screening or monitoring of cursor movements. Like behavioural and ISB studies, technical controls also need to consider using employee personal information for organisational monitoring purposes, which must be within jurisdictional boundaries for ethical, legal and data privacy considerations.

Insider Threat Strategies outlined in Section II-F found comprehensive reports and studies recommending best practices, although these were not explicitly focused within a UK based FS environment. However, several studies provided a checklist of recommendations for implementing an insider threat programme, and insights can be applied within an FS environment, which will be discussed further below in FS Sector Recommendations. Suggestions of cross-functional collaboration were also proposed, which would help break down silos and support a unified approach to tackling the insider threat reputational, people, and technology risks, which are applicable in FS organisational structures. Insights from studies looking at internal fraud taxonomies can provide meaningfully used cases to help build detective and preventive insider threat controls. Consideration and acknowledgement that there is no silver bullet to tackle the insider threat problems within a UK based FS environment needs to consider an up-to-date assessment of the FS organisational threat landscape and insider threat maturity assessment.

Regulation, outlined within Section II-G, primarily focused on U.S.-based policy and regulation, as no studies were identified to be UK based, and none related to FS industries. However, similarities in approach to UK regulation and policy can be drawn. For example, UK enforcement law could be simplified to support a positive increase in the reporting of insider threat cases. Regulations and UK law enforcement may be controlled by enforcing FS organisational NDA and Trade Secret Act agreements.

IV. RECOMMENDATIONS FOR UK BASED FS SECTOR

The following recommendations provide valuable insights and guidance for the UK based FS organisations and synthesise potential UK based FSsector recommendations that offer practical advice, which can be explored or deployed in an operational environment. These recommendations draw insights from the literature review.

Behavioural Studies: Understanding behaviour and insights from behavioural studies informs organisational policy, ensures safe working conditions, and embeds a security-conscious and positive culture. Reinforcing or prioritising the following recommendations will create a people-centric security culture, reducing insider and security threats while improving employee satisfaction, engagement, and productivity. UK FS organisations should:

1) Create a positive cybersecurity culture and working environment.
2) Establish free and accessible Employee Assist Programmes, including health, wellbeing, and financial support.
3) The Principle of Least Privilege Access within FS organisations should be adopted.
4) Understand and identify who has access to systems, segment and enhance control environment if applicable.
5) Offer safe, confidential Speak Up or Whistleblowing services.
6) Robust compliance and governance frameworks linking Privacy and UK Employment Law.

Information Security Behaviour: understanding ISB is crucial in reducing insider threats, as these promote a culture of vigilance. By adopting the following recommendations and measures, UK FS organisations will strengthen their ability to achieve a sustainable long-term people-centric security culture:

1) Ensure deployment of robust, effective, regular mandatory Education and Awareness Programmes and re-training modules.
2) Set out clear Information Security Policies (i.e., Acceptable Usage, Data Privacy Policies).
3) Be transparent and inform individuals of internal security monitoring.
4) Establish clear and transparent colleague treatment strategies and appropriate consequences or sanctions if policy violations occur.
5) Utilise NDA documents.
6) Promote a positive organisational and leadership culture.
7) Deploy multi-layered detective controls (i.e., UBA and DLP) and assess holistic security culture behaviours.

Technical Controls: Tailoring technological approaches to the organisational environment will enhance the effectiveness of insider threat detection, which can complement existing security monitoring and detection tools, improving overall security measures. The following recommendations should be considered, assessing, and prioritising the general insider threat risks in line with organisational budgets:

1) Technological approaches must be tailored to the organisational environment; consider UBA ML technologies to complement other technological detection tools.
2) Consider early adoption of detection capabilities, i.e., Sentiment Analysis, Deception and Denial tools.
3) Deploy bespoke phishing tests to support insider threat training and awareness programmes.
4) Consider social media scanning as part of pre-employment vetting.
5) Consider introducing cloud unique threats to access, abuse of legitimate access, data loss, supply chain compromise, etc.)
6) Understand and identify who has access to systems, segment and enhance control environment if applicable.
7) The Principle of Least Privilege Access within the UK FS organisations should be adopted.

Insider Threat Strategies: These strategies promote proactive identification and mitigation efforts of insider threats while ensuring alignment with industry standards, enabling risk reduction strategies, and fostering a positive, security-conscious working environment. Recommendations are noted below:

1) Ensure executive sponsorship for insider threat programmes, with joint ownership of people and technology insider threat risks for the FS organisation.
2) Insider threat programmes to be based on risk reduction principles.
3) Conduct regular Insider Threat landscape assessments against FS and other industries (i.e., oil, gas, mining)
4) Review internal security control playbooks against published insider threat cases to assess control gaps in operations and processes.
5) Consider segmentation of workforce population and applying additional control framework to those populations who can cause severe or material harm by virtue of role, access to data, premises, leavers, employee type, etc. This could include consideration of gardening leave, removal of external email access, additional internet restrictions, or enhanced email monitoring.

6) Conduct employment vetting over and above pre-employment vetting in line with the segmentation of populations who can cause severe or material harm by virtue of role, access to data, premises, leavers, and employee type. Consider annual or three-yearly vetting attestations.
7) Conduct regular benchmarking and maturity assessments to assess the insider threat programme risk reduction journey.
8) Ensuring a safe and positive working environment is a hygiene factor.

Regulation: Highly regulated environments of UK FS organisations will benefit from proactive security monitoring measures to strengthen their fraud prevention efforts, as well as acting as a deterrent, while promoting the importance of a culture of trust within its organisation, underpinned by regulatory frameworks and principles, for example:

1) Proactive loading of known and identified UK fraud onto the national Credit Industry Fraud Avoidance System (CIFAS).
2) Regular CIFAS checks as part of enhanced in-role vetting checks for individuals identified as part of a population who can cause severe or material harm by role, access to data, premises, leavers, employee type, etc.
3) UK FS organisations need to leverage the powers of law enforcement regulation and consider loading insider incidents onto the CIFAS database to act as a deterrent and to act as an employee integrity check within and across UK FS organisations and better collaboration leading to the sharing of best practice across UK banks and FS to reduce instances of insider threats.
4) Utilise GDPR to develop a robust privacy impact assessment to ensure no bias, subjectivity, or illegal monitoring.

There is an acknowledgement that malicious insider threat indicators, including personality traits, personality characteristics, personality disorders and historic personal factors, pose ethical and regulatory constraints and are unqualified assessments and should not be used as a basis when considering organisational insider threat monitoring.

However, understanding and monitoring information security behaviour can also help identify riskier populations and function as a preventative tool to mitigate insider threats. Nonetheless, intervention tactics, technological controls and current insider threat strategies are acknowledged as ineffective, evidenced by the increase in reported events, high-profile insider threats and cyber data loss cases borne from insider and privilege misuse. Furthermore, insider threat detection programmes currently employ prevention, detection and response practices and technologies for insider threats. However, despite the vast number of technologies, guidance, information and strategies, there is no operational reduction in the threat landscape and the acceptance within the UK FS industry. There is no silver bullet in practice, which is a negligent attitude.

V. FUTURE WORKS

Considering the limited studies on understanding malicious insider threats within the UK FS, coupled with evolving technologies and regulatory and ethical scrutiny, there is further opportunity to explore insider threat detection and mitigation strategies. From a practitioner's perspective, one engaging topic of discussion and a great understanding of how insider threats manifest in different professional landscapes, identifying common patterns that transcend industry boundaries but also understand the unique elements that individual industries grapple with. Future research can also look at insider threat strategies in other FS organisations, out with the UK. Reviewing and comparing these strategies could provide a valuable perspective on what works best in the unique setting of financial services or highly regulated working environments. In addition, further research could investigate the relationship between organisational culture and insider threat behaviours, exploring how perceived organisational injustice and pressure (despite the presence of sanctions), to inform insider threat mitigating strategies.

Furthermore, advanced technologies like ML, UEBA, Sentiment Analysis, and Deception and Denial tools have significantly improved our early detection capabilities. However, a deeper dive into their impact and effectiveness in the real world and understanding the return on investment versus threat mitigation would be insightful.

Next, the strategic effectiveness of segmentation-based control frameworks for monitoring high-risk populations is an interesting subject, given that internal security controls such as Privileged Access Management and Zero Trust principles should minimise the opportunity for insider threat incidents. However, these controls do not consider external factors, such as psychosocial indicators, disgruntlement, or financial hardship, which could catalyse an insider attack. Would such a framework help limit potential insider threats, and how successful would this be in practical application? Then, the ethical dimensions of assessing psychological characteristics for insider threat detection purposes is also a compelling discourse. The potential benefits must be weighed against ethical considerations, not to mention the implications of using such sensitive data.

The extensive nature of the recommendations presented within the review, offers a comprehensive foundation for future research, providing detailed guidance and practical application of these recommendations within real world UK FS environments. In addition, future research can also examine insider threat strategies in other FS organisations beyond the UK This exploration could include a comprehensive comparative analysis of strategies across different industries. Reviewing and comparing these strategies across various geographical and regulatory contexts with a focus on the applicability within the FS industry globally

Lastly, developing an Insider Threat Maturity Model to assess and enhance insider threat programme strategies within UK financial services organisations could be an exciting avenue to pursue. This could provide UK FS organisations with a structured way to improve or strengthen their controls, identify potential gaps in their insider threat detection and prevention controls and programmes, and thereby limit insider threats.

These are the broad areas that future works could delve into, with each offering a wealth of insight into managing and mitigating insider threats. What is appealing about these topics is that they encompass a range of issues, from technical aspects of threat detection to the human and organisational elements of managing insider threats from a practitioner perspective.

REFERENCES

[1] J. Mills, J. Dever, and S. Stuban, "Using regression to predict potential insider threats," *Defense Acquisition Res. J.*, vol. 25, no. 2, pp. 122–157, Jul. 2018.

[2] N. Elmrabit, S.-H. Yang, L. Yang, and H. Zhou, "Insider threat risk prediction based on Bayesian network," *Comput. Secur.*, vol. 96, Sep. 2020, Art. no. 101908.

[3] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, and M. Ochoa, "Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures," *ACM Comput. Surv.*, vol. 52, no. 2, pp. 1–40, Mar. 2020.

[4] J. Carson, "The evolution of the digital insider trader," *Comput. Fraud Secur.*, vol. 2017, no. 8, pp. 12–15, Aug. 2017.

[5] M. G. Gelles, "Introduction–Insider threat today," in *Insider Threat*. Boston, MA, USA: Butterworth-Heinemann, 2016, ch. 1, pp. 1–18.

[6] J. Eggenschwiler, I. Agrafiotis, and J. R. Nurse, "Insider threat response and recovery strategies in financial services firms," *Comput. Fraud Secur.*, vol. 2016, no. 11, pp. 12–19, Nov. 2016.

[7] A. Zakrzewski, T. Tang, G. Appell, R. Fages, A. Hardie, N. Hildebrandt, M. Kahlich, and M. Mende, "Global wealth 2019," Boston Consultancy Group, Boston, MA, USA, Tech. Rep., 2019. [Online]. Available: https://web-assets.bcg.com/img-src/BCG-Reigniting-Radical-Growth-June-2019_tcm9-222638.pdf

[8] I. Aldasoro, L. Gambacorta, P. Giudici, and T. Leach. (2020). *The Drivers of Cyber Risk*. Centre Econ. Policy Res. Accessed: Jan. 3, 2024. [Online]. Available: https://www.bis.org/publ/work865.pdf

[9] PWC. (2022). *Pwc's Global Economic Crime and Fraud Survey*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

[10] Cyber security Insiders. (2607). *Cyber Security Insider Threat Report 2023*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.cybersecurity-insiders.com/portfolio/2023-insider-threat-report

[11] Verizon. (2608). *Data Breach Investigations Report*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.verizon.com/business/en-gb/resources/reports/dbir

[12] Verizon. (2018). *Ransomware Still a Top Cybersecurity Threat, Warns Verizon 2018 Data Breach Investigations Report*. SyndiGate Media Inc. Accessed: Jan. 3, 2024. [Online]. Available: https://www.verizon.com/about/news/ransomware-still-top-cybersecurity-threat-warns-verizon-2018-data-breach-investigations-report

[13] K. Quach. (Aug. 7, 2020). *Capital One Fined $80 M for Shoddy Public Cloud Security. Yeah, Same Bank in That 106 M Customer-Record Hack*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.theregister.com/2020/08/07/capital_one_fine/

[14] United States Dept. of Justice. (Aug. 10, 2018). *Former JP Chase Bank Employee Sentenced to Four Years in Prison*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.justice.gov/usao-edny/pr/former-jp-morgan-chase-bank-employee-sentenced-four-years-prison-selling-customer

[15] A. Hamilton. (2019). *Sberbank Data Leak May Have Exposed 60 M Customer Accounts*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.fintechfutures.com/2019/10/sberbank-data-leak-may-have-exposed-60m-customer-accounts/

[16] D. Lazurus. (May 24, 2011). *Bank of America Data Leak Destroys Trust*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.latimes.com/business/la-xpm-2011-may-24-la-fi-lazarus-20110524-story.html

[17] S. Goswami. (Feb. 21, 2018). *Mitigating the Insider Threat: Lessons From PNB Fraud Case*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.bankinfosecurity.com/mitigating-insider-threat-lessons-from-indian-fraud-case-a-10674

[18] D. Tripathy. (Feb. 26, 2019). *How PNB Says it Fell Victim to India's Biggest Loan Fraud*. Accessed: Jan. 3, 2024. [Online]. Available: https://uk.reuters.com/article/uk-punjab-natl-bank-fraud-explainer/how-pnb-says-it-fell-victim-to-indias-biggest-loan-fraud-idUKKCN1GA0WE

[19] Finextra. (Dec. 4, 2020). *Absa Warns of Data Leak by Rogue Employee*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.finextra.com/newsarticle/37090/absa-warns-of-data-leak-by-rogue-employee

[20] P. Strozniak. (Jan. 13, 2023). *Former CU Employee Sentenced in IT Revenge Case*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.cutimes.com/2023/01/13/former-cu-employee-sentenced-in-it-revenge-case/?slreturn=20230629141341

[21] U.K. Government National Protective Security Authority. (Nov. 10, 2023). *Introduction to Insider Risk*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.npsa.gov.uk/introduction-insider-risk

[22] CASP. (Dec. 2020). *Critical Appraisal Skills Programme*. Accessed: Jan. 3, 2024. [Online]. Available: https://casp-uk.net/

[23] U.K. Government National Protective Security Authority. (Apr. 2013). *Insider Data Collection Study*. National Protective Security Authority. Accessed: Jan. 3, 2024. [Online]. Available: https://www.cpni.gov.uk/system/files/documents/63/29/insider-data-collection-study-report-of-main-findings.pdf

[24] F. L. Greitzer, M. Imran, J. Purl, E. T. Axelrad, Y. M. Leong, D. E. Becker, K. B. Laskey, and P. J. Sticha, "Developing an ontology for individual and organizational sociotechnical indicators of insider threat risk," in *Proc. CEUR Workshop*, vol. 1788, 2016, pp. 19–27.

[25] A. T. Shappie, C. A. Dawson, and S. M. Debb, "Personality as a predictor of cybersecurity behavior," *Psychol. Popular Media*, vol. 9, no. 4, pp. 475–480, Oct. 2020.

[26] A. Harrison, J. Summers, and B. Mennecke, "The effects of the dark triad on unethical behavior," *J. Bus. Ethics*, vol. 153, no. 1, pp. 53–77, Nov. 2018.

[27] N. Liang and D. Biros, "Validating common characteristics of malicious insiders: Proof of concept study," in *Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2016, pp. 3716–3726.

[28] F. L. Greitzer and D. A. Frincke, "Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation," in *Insider Threats in Cyber Security*, vol. 49. Boston, MA, USA: Springer, 2010.

[29] F. L. Greitzer, J. D. Lee, J. Purl, and A. K. Zaidi, "Design and implementation of a comprehensive insider threat ontology," *Proc. Comput. Sci.*, vol. 153, pp. 361–369, Jan. 1987.

[30] E. Shaw and H. Stock. (2011). *White Paper*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.symantec.com/content/en/us/about/media/pdfs/symc_malicious_insider_whitepaper_Dec_2011.pdf

[31] M. T. Whitty, "Developing a conceptual model for insider threat," *J. Manage. Org.*, vol. 27, no. 5, pp. 911–929, Sep. 2021.

[32] V. Zeigler-Hill and A. Besser, "Dark personality features and workplace outcomes: The mediating role of difficulties in personality functioning," *Current Psychol.*, vol. 40, no. 11, pp. 5430–5444, Nov. 2021.

[33] E. D. Shaw, J. M. Post, and K. G. Ruby, "Inside the mind of the insider," *Secur. Manage.*, vol. 43, no. 12, p. 34, 1999.

[34] A. A. Cain, M. E. Edwards, and J. D. Still, "An exploratory study of cyber hygiene behaviors and knowledge," *J. Inf. Secur. Appl.*, vol. 42, pp. 36–45, Oct. 2018.

[35] R. Willison, P. B. Lowry, R. Paternoster, and V. Tech, "A tale of two deterrents: Considering the role of absolute and restrictive deterrence to inspire new directions in behavioral and organizational security research," *J. Assoc. Inf. Syst.*, vol. 19, no. 12, pp. 1187–1216, 2018.

[36] M. W. Kranenbarg, S. Ruiter, J.-L. van Gelder, and W. Bernasco, "Cyber-offending and traditional offending over the life-course: An empirical comparison," *J. Develop. Life-Course Criminol.*, vol. 4, no. 3, pp. 343–364, Sep. 2018.

[37] T. Eliyahu. (May 14, 2019). *Financial Cyber Threats: 10 Cases of Insider Bank Attacks*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.sentinelone.com/blog/financial-cyber-threats-10-cases-of-insider-bank-attacks/

[38] R. Willison, M. Warkentin, and A. C. Johnston, "Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives," *Inf. Syst. J.*, vol. 28, no. 2, pp. 266–293, Mar. 2018.

[39] N. S. Safa, C. Maple, T. Watson, and R. Von Solms, "Motivation and opportunity based model to reduce information security insider threats in organisations," *J. Inf. Secur. Appl.*, vol. 40, pp. 247–257, Jun. 2018.

[40] K. Padayachee, "An assessment of opportunity-reducing techniques in information security: An insider threat perspective," *Decis. Support Syst.*, vol. 92, pp. 47–56, Dec. 2016.

[41] J. R. C. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. T. Wright, and M. Whitty, "Understanding insider threat: A framework for characterising attacks," in *Proc. IEEE Secur. Privacy Workshops*, May 2014, pp. 214–228.

[42] E. E. Schultz, "A framework for understanding and predicting insider attacks," *Comput. Secur.*, vol. 21, no. 6, pp. 526–531, Oct. 2002, doi: 10.1016/s0167-4048(02)01009-x.

[43] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Detecting insider threat via a cyber-security culture framework," *J. Comput. Inf. Syst.*, vol. 62, no. 4, pp. 706–716, Jul. 2022.

[44] S. Sharma and M. Warkentin, "Do I really belong? Impact of employment status on information security policy compliance," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101397.

[45] H. L. Kim, H. S. Choi, and J. Han, "Leader power and employees' information security policy compliance," *Secur. J.*, vol. 32, no. 4, pp. 391–409, Dec. 2019.

[46] N. Guhr, B. Lebek, and M. H. Breitner, "The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory," *Inf. Syst. J.*, vol. 29, no. 2, pp. 340–362, Mar. 2019.

[47] W. P. Wong, H. C. Tan, K. H. Tan, and M.-L. Tseng, "Human factors in information leakage: Mitigation strategies for information sharing integrity," *Ind. Manage. Data Syst.*, vol. 119, no. 6, pp. 1242–1267, Jul. 2019.

[48] B. Lebek, J. Uffen, M. Neumann, B. Hohler, and M. H. Breitner, "Information security awareness and behavior: A theory-based literature review," *Manage. Res. Rev.*, vol. 37, no. 12, pp. 1049–1092, Nov. 2014.

[49] P. Wilcox, K. Land, and S. Hunt, *Criminal Circumstances: A Dynamic Multicontextual Criminal Opportunity Theory*. New York, NY, USA: Aldine De Gruyter, 2570.

[50] N. S. Safa, C. Maple, S. Furnell, M. A. Azad, C. Perera, M. Dabbagh, and M. Sookhak, "Deterrence and prevention-based model to mitigate information security insider threats in organisations," *Future Gener. Comput. Syst.*, vol. 97, pp. 587–597, Aug. 2019.

[51] S. Trang and B. Brendel, "A meta-analysis of deterrence theory in information security policy compliance research," *Inf. Syst. Frontiers*, vol. 21, no. 6, pp. 1265–1284, Dec. 2019.

[52] N. I. Raddatz, K. Marett, and B. S. Trinkle, "The impact of awareness of being monitored on computer usage policy compliance: An agency view," *J. Inf. Syst.*, vol. 34, no. 1, pp. 135–149, Mar. 2020.

[53] E. N. Ceesay, K. Myers, and P. A. Watters, "Human-centered strategies for cyber-physical systems security," *ICST Trans. Secur. Saf.*, vol. 4, no. 14, May 2018, Art. no. 154773.

[54] A. Mishra, Y. I. Alzoubi, A. Q. Gill, and M. J. Anwar, "Cybersecurity enterprises policies: A comparative study," *Sensors*, vol. 22, no. 2, p. 538, Jan. 2022.

[55] J. Suler, "The online disinhibition effect," *CyberPsychol. Behav.*, vol. 7, no. 3, pp. 321–326, Jun. 2004.

[56] J. Han, Y. J. Kim, and H. Kim, "An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective," *Comput. Secur.*, vol. 66, pp. 52–65, May 2017.

[57] J. D'Arcy and P. B. Lowry, "Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study," *Inf. Syst. J.*, vol. 29, no. 1, pp. 43–69, Jan. 2019.

[58] S. Aurigemma and T. Mattson, "Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls," *Comput. Secur.*, vol. 66, pp. 218–234, May 2017.

[59] J. Wang, Z. Shan, M. Gupta, H. R. Rao, and M. University, "A longitudinal study of unauthorized access attempts on information systems: The role of opportunity contexts," *MIS Quart.*, vol. 43, no. 2, pp. 601–622, Jan. 2019.

[60] J. Malik, "Making sense of human threats and errors," *Comput. Fraud Secur.*, vol. 2020, no. 3, pp. 6–10, Jan. 2020.

[61] C. Van Slyke and F. Belanger, "Explaining the interactions of humans and artifacts in insider security behaviors: The mangle of practice perspective," *Comput. Secur.*, vol. 99, Dec. 2020, Art. no. 102064.

[62] A.-S. I, W. Yassin, N. Tabook, R. Ismail, and A. Ismail, "Determinants of information security awareness and behaviour strategies in public sector organizations among employees," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 8, pp. 479–490, 2022.

[63] C. W. Probst, F. Kammüller, and R. R. Hansen, *Formal Modelling and Analysis of Socio-Technical Systems*. Cham, Switzerland: Springer, 2015.

[64] F. Janjua, A. Masood, H. Abbas, and I. Rashid, "Handling insider threat through supervised machine learning techniques," *Proc. Comput. Sci.*, vol. 177, pp. 64–71, Jan. 1975.

[65] R. G. Gayathri, A. Sajjanhar, and Y. Xiang, "Image-based feature representation for insider threat classification," *Appl. Sci.*, vol. 10, no. 14, p. 4945, Jul. 2020.

[66] D. P. Brown, D. Buede, and S. D. Vermillion, "Improving insider threat detection through multi-modelling/data fusion," *Proc. Comput. Sci.*, vol. 153, pp. 100–107, Jan. 2019.

[67] A. Nicolaou, S. Shiaeles, and N. Savage, "Mitigating insider threats using bio-inspired models," *Appl. Sci.*, vol. 10, no. 15, p. 5046, Jul. 2020.

[68] A. Y. Alanis, N. Arana-Daniel, and C. Lopez-Franco, *Bio-Inspired Algorithms for Engineering*. Oxford, U.K.: Butterworth-Heinemann, 2018.

[69] G. Smyth, "Using data virtualisation to detect an insider breach," *Comput. Fraud Secur.*, vol. 2017, no. 8, pp. 5–7, Aug. 2017.

[70] H. Sharghi and K. Sartipi, "An expressive event-based language for representing user behavior patterns," *J. Intell. Inf. Syst.*, vol. 49, no. 3, pp. 435–459, Dec. 2017.

[71] O. Lo, W. J. Buchanan, P. Griffiths, and R. Macfarlane, "Distance measurement methods for improved insider threat detection," *Secur. Commun. Netw.*, vol. 2018, pp. 1–18, Jan. 2018.

[72] W. Park, Y. You, and K. Lee, "Detecting potential insider threat: Analyzing insiders' sentiment exposed in social media," *Secur. Commun. Netw.*, vol. 2018, pp. 1–8, Jul. 2018.

[73] J. L. Jenkins, J. G. Proudfoot, J. S. Valacich, G. M. Grimes, and J. F. J. Nunamaker Jr., "Sleight of hand: Identifying concealed information by monitoring mouse-cursor movements," *J. Assoc. Inf. Syst.*, vol. 20, no. 1, pp. 1–32, 2019.

[74] M. Yildirim and E. Anarim, "Mitigating insider threat by profiling users based on mouse usage pattern: Ensemble learning and frequency domain analysis," *Int. J. Inf. Secur.*, vol. 21, no. 2, pp. 239–251, Apr. 2022.

[75] P. Pedamkar. (2020). *Adaboost Algorithm*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.educba.com/adaboost-algorithm/

[76] M. F. Faiz, J. Arshad, M. Alazab, and A. Shalaginov, "Predicting likelihood of legitimate data loss in email DLP," *Future Gener. Comput. Syst.*, vol. 110, pp. 744–757, Sep. 2020.

[77] B. Bracken. (2020). *Survey: Cybersecurity Skills Shortage is 'Bad,' but There's Hope*. Accessed: Jan. 3, 2024. [Online]. Available: https://threatpost.com/cybersecurity-skills-shortage-survey/160866/

[78] M. Theis, R. Trzeciak, D. Costa, A. Moore, S. Miller, T. Cassidy, and W. Claycomb. (2022). *Common Sense Guide to Mitigating Insider Threats*. Carnagie Mellon Univ. Accessed: Jan. 3, 2024. [Online]. Available: https://insights.sei.cmu.edu/library/common-sense-guide-to-mitigating-insider-threats-seventh-edition/

[79] 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," *Electronics*, vol. 9, no. 9, p. 1460, Sep. 2020.

[80] J. Richardson, "Is there a silver bullet to stop cybercrime?" *Comput. Fraud Secur.*, vol. 2020, no. 5, pp. 6–8, Jan. 2020.

[81] D. Ki-Aries and S. Faily, "Persona-centred information security awareness," *Comput. Secur.*, vol. 70, pp. 663–674, Sep. 2017.

[82] M. Fimin, "Five steps to protect confidential data when employees leave," *Comput. Fraud Secur.*, vol. 2017, no. 9, pp. 10–13, Sep. 2017.

[83] J. A. Jalil and H. Hassan, "Protecting trade secret from theft and corporate espionage: Some legal and administrative measures," *Int. J. Bus. Soc.*, vol. 21, no. S1, pp. 205–218, 2020.

[84] P. Muncaster. (Oct. 20, 2018). *Morrison's Loses Insider Breach Liability Appeal*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.infosecurity-magazine.com/news/morrisons-loses-insider-breach/

[85] C. Onwubiko, "Fraud matrix: A morphological and analysis-based classification and taxonomy of fraud," *Comput. Secur.*, vol. 96, Sep. 2020, Art. no. 101900.

[86] A. Nawawi and A. S. A. P. Salin, "Internal control and employees' occupational fraud on expenditure claims," *J. Financial Crime*, vol. 25, no. 3, pp. 891–906, Jul. 2018.

[87] F. Whitelaw, "Expense claim fraud FS 2021," Lloyds Banking Group, Edinburgh, U.K., Tech. Rep., 2021.

[88] Association of Certified Fraud Examiners (ACFE). (2016). *2016 Report to the Nations, on Occupational Fraud & Abuse—Global Fraud Report*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf

[89] S. Eftimie, C. Racuciu, R. Moinescu, and D. Glavan, "Insider threats and thermal stress in the working environment," *Sci. Bull. Mircea Cel Batran Naval Acad.*, vol. 23, no. 1, pp. 271A–276A, 2020.

[90] D. J. Reid, "Combating the enemy within: Regulating employee misappropriation of business information," *Vanderbilt Law Rev.*, vol. 71, no. 3, pp. 1033–1069, 2018.

[91] U.K. Govornment. (Feb. 2020). *U.K. Legislation*. Accessed: Jan. 3, 2024. [Online]. Available: http://www.legislation.gov.uk/

[92] U. Government. (2021). *The Trade Secrets (Enforcement, etc.) Regulations 2018*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.legislation.gov.uk/uksi/2018/597/made

[93] A. Chapelle, *Operational Risk Management: Best Practices in the Financial Services Industry*. West Sussex, U.K.: Wiley, 2019.

[94] R. Gillet, G. Hübner, and S. Plunus, "Operational risk and reputation in the financial industry," *J. Banking Finance*, vol. 34, no. 1, pp. 224–235, Jan. 2010.

[95] S. Chavali. (Oct. 14, 2020). *How Insider Threat Impact the Financial Services Industry*. Accessed: Jan. 3, 2024. [Online]. Available: https://www.proofpoint.com/uk/blog/insider-threat-management/how-insider-threats-impact-financial-services-industry

FINDLAY WHITELAW was born in Scotland, U.K. She received the Master of Business Administration (M.B.A.) degree from Strathclyde University, Glasgow, in 2015. She is currently pursuing the Ph.D. degree with Glasgow Caledonian University, Glasgow. Her current research interest includes malicious insider threats within a financial service organizational setting.

JACKIE RILEY received the M.Sc. degree in operational research from Strathclyde University, and the Ph.D. degree from Glasgow Caledonian University, in 2001. She is currently the Head of the Cyber Security and Networks Department, Glasgow Caledonian University. Her current research interests include insider threat prevention, cybersecurity education, and awareness.

NEBRASE ELMRABIT received the M.Sc. degree in computer and network security from Middlesex University, London, and the Ph.D. degree in computer science from Loughborough University, in 2019. He is currently a Cybersecurity and Digital Forensics Lecturer with the Department of Cyber Security and Networks, Glasgow Caledonian University. His research interests include insider threat prevention, cybersecurity architecture, privacy, digital forensics, and intelligent grid cybersecurity.