Enhancing Cybersecurity Resilience in the Real Estate Industry: Mitigating Phishing and BEC Attacks

Oludolamu Onimole[1], Etinosa Imafidon[2], Denzel A. Pryor[3], Lucas Potter[4] and Xavier Palmer[4]

[1] Independent, Glasgow, UK
[2]Flexmore Tech Ltd, Edinburgh, UK
[3] Independent Researcher, Philadelphia, Pennsylvania, USA
[4]Biosview Labs, Dayton, Ohio, USA

oludolamuonimole@gmail.com
etinosahendrix@gmail.com
pryordlsa@gmail.com
BiosView1@proton.me

Abstract: As real estate transactions continue to shift toward fully digital workflows, the sector has become an attractive target for phishing and BEC attacks that exploit trust, time pressure, and fragmented communication channels. This paper contributes to cybersecurity research by moving beyond high level discussions of email fraud and focusing directly on the real estate industry as a primary domain of analysis rather than a peripheral use case. The study synthesizes existing academic and industry literature with a structured examination of multiple real-world incidents drawn from residential, commercial, and cross border property transactions. By analysing these cases collectively, the paper identifies recurring patterns in attacker techniques, Organizational weaknesses, and decision-making failures that enable financial loss. Attention is paid to how human behavior, process design, and informal verification practices interact with technical shortcomings to create exploitable conditions. A clearly defined methodology outlines the case selection criteria, temporal scope, and analytic approach, allowing the study to be replicated or extended by future researchers. This methodological transparency strengthens the academic value of the work while grounding the findings in observable evidence rather than assumptions. Based on the cross-case analysis, the paper proposes a practical, sector specific framework that aligns cybersecurity controls with the operational realities of property transactions, including third party coordination, legal timelines, and high value fund transfers. The findings offer practical relevance for cybersecurity professionals, real estate practitioners, and policymakers by translating incident analysis into concrete risk reduction strategies. At the same time, the paper advances scholarly understanding by presenting an industry focused model for addressing cyber enabled financial crime in trust-based transaction environments.

Keywords: BEC, Business email compromise, Phishing, Real estate cybersecurity, Social engineering, Wire fraud

1. Introduction

The real-estate sector has undergone a rapid digital transformation in recent years. Online escrow services, cloud-based e-signatures, and remote closing platforms are replacing paper-based closings and wet-ink signatures (PricewaterhouseCoopers, 2021). As Awofadeju et al. (2024) observe, this rapid digitalization of real estate has led to an industry that is increasingly threatened by cybersecurity challenges, more extensive than conventional ones. Business Email Compromise (BEC) attacks, first identified as an "emerging threat" by the FBI in 2013, have become a global problem due to their increasing sophistication (Bakarich and Baranek, 2020).

BEC continues to grow in threat, with complaints to the Internet Crime Complaint Center (IC3) totalling 19,954 in 2021, with losses up to $2.4 billion (ic3, 2021). The impact of BEC fraud is felt worldwide, with criminals having stolen over $26 billion through BEC scams since 2016 (Saud Al-Musib *et al.*, 2023). The real estate industry houses a trove of invaluable data coveted by cyber criminals, including confidential financial information and personal data. The most significant risk in this sector being the potential for wire fraud following email account compromise. Despite escalating losses, empirical cross-case analysis of BEC within real estate remains limited, and sector-specific resilience frameworks are underdeveloped

1.1 Research Problem, Contribution, and Objectives

The real estate sector's reliance on email for high-value transactions creates a critical vulnerability exploited by BEC attackers who leverage the complexity of the conveyancing process (Comora, 2019). U.S. authorities and FinCEN's 2023 research underscore that the numerous parties involved; buyer, seller, agents, and title/escrow officers and the high volume of document and payment instruction exchanges, particularly large wire transfers, make this industry a prime target. Specifically, sophisticated actors deploy cloned escrow agent emails to

disseminate fraudulent wiring instructions, successfully diverting closing funds to illicit overseas accounts or money mules (Federal Bureau of Investigation, 2022).

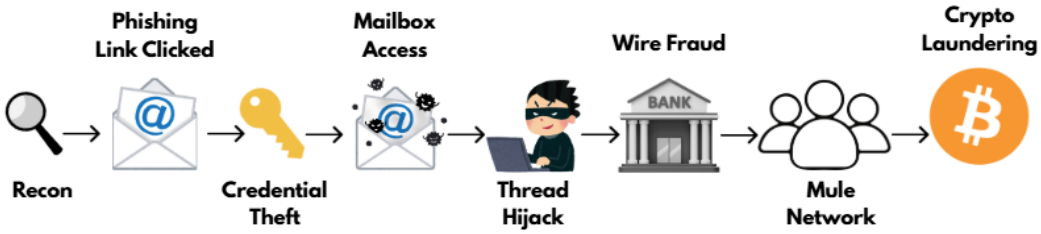

Figure 1: BEC Attack flow in Real Estate

This paper addresses the ensuing cybersecurity imperative: enhancing organizational resilience against phishing and BEC, which cause significant legal, financial, and reputational damage. Our core objectives are to: 1) Investigate BEC in the real estate sector, including criminal motivations; 2) Synthesize BEC attack typologies to inform tailored safeguards for industry stakeholders and policymakers; 3) Analyze the evolving threat landscape, focusing on actor tactics and motivations exploiting transaction vulnerabilities; and 4) Propose a sector-specific cybersecurity resilience framework integrating customized technical controls, governance, and best practices.

2. Research Methodology

2.1 Methodology

This research employs an exploratory multiple case study design to investigate phishing and Business Email Compromise (BEC) incidents within the U.S. real estate sector. This approach is instrumental for exploring phenomena and generating new research avenues (Priya, 2021). Case study research involves the in-depth examination of specific real-world incidents or phenomena in their natural contexts, gathering information over a sustained period using diverse data collection methods (Asenahabi 2019; Priya 2021). An exploratory case study is warranted here because the motivations and triggers of the involved individuals are often unknown (Jain, 2021). Therefore, this qualitative multiple case study is the optimal methodology to examine BEC and investigate the underlying causes of criminal attacks (Helo and Hao 2022). This method excels at answering 'how' and 'why' questions and is particularly suited for cross-case comparisons (Urbinati et al. 2020). Given the limited empirical research on BEC in real estate, this design facilitates a deeper qualitative analysis of real-world incidents, encompassing their technical, organizational, legal, and financial dimensions, thus ensuring a nuanced understanding of attacker techniques and stakeholder responses.

2.2 Data Sources, Case Selection Criteria, Time Horizon, Data Collection, and Limitations

Cybersecurity resilience against phishing and BEC was assessed via evidence triangulation. Aggregate incident data from the FBI Internet Crime Complaint Center (IC3) and Anti-Phishing Working Group (APWG) established macro-level trends. Sector-specific risk profiles and best practices were synthesized from professional bodies such as the American Land Title Association (ALTA) and the National Association of Realtors (NAR). A purposive sampling strategy selected representative BEC incidents (2019-2026), focusing on evolving attacker sophistication, from simple spoofing to targeted campaigns. Selection prioritized critical real estate transaction workflows, specifically closing and wire transfer stages, encompassing residential and commercial deals verified through legal filings or law enforcement. Qualitative thematic analysis was applied to the structured case profiles to identify recurring attacker tactics, techniques, and procedures (TTPs), organizational vulnerabilities, and mitigation patterns. A cross-case comparative approach was used to detect recurring themes across incidents and derive sector-relevant insights that informed the proposed cybersecurity framework. This methodology has inherent limitations: reliance on publicly available data likely results in an understatement of BEC pervasiveness due to underreporting and the qualitative, exploratory nature precludes statistical generalization across the entire sector.

2.3 Search Strategy

A structured literature search was conducted to identify peer-reviewed studies addressing phishing, Business Email Compromise (BEC), financial transaction fraud, and sector-specific mitigation strategies. Scopus was

selected as the primary indexing database due to its broad coverage of cybersecurity, information systems, and interdisciplinary research.

Structured Boolean searches were executed using TITLE-ABS-KEY fields and limited to English-language publications between January 2019 -January 2026. Three focused query groups were developed to capture: (1) phishing and BEC in financial transaction contexts; (2) phishing and wire fraud within real estate transactions; and (3) mitigation and risk management strategies related to phishing-driven financial fraud. Boolean search strings are added below for methodological reproducibility and transparency as shown in table 1.

Table 1: Scopus Searches ((TITLE-ABS-KEY, English, 2019–2026)

Query Focus	Query String	Results	Year
Phishing / BEC in Financial Transactions	TITLE-ABS-KEY ((phishing OR "business email compromise" OR "email fraud" OR "wire fraud") AND ("financial transaction" OR "wire transfer" OR escrow OR "fund transfer")) AND PUBYEAR > 2018 AND (LIMIT-TO (LANGUAGE , "English"))	70	2019 - 2026
Phishing / Wire Fraud in Real Estate	TITLE-ABS-KEY((phishing OR "email fraud" OR "wire fraud") AND ("real estate" OR escrow OR realtor OR "property transaction")) AND PUBYEAR > 2018	9	2019 - 2026
Phishing Mitigation / Risk Management in Financial Context	TITLE-ABS-KEY((phishing OR "business email compromise") AND ("mitigation strategy" OR "risk management") AND ("financial transaction" OR "payment system")) AND PUBYEAR > 2018	11	2019 - 2026
	Total Initial Records	**90**	

After results in Table 1 were obtained, they were then exported and checked to remove duplicates and following duplicate removal, 79 results remained. Title and abstract screening further reduced the dataset to 51 studies directly relevant to phishing, BEC, and financial transaction security. Following full-text review, 46 peer-reviewed articles were included in the final thematic synthesis.

Additional targeted searches were carried out on reputable institutional platforms, such as the FBI Internet Crime Complaint Center (ic3), ENISA, and the National Association of Realtors (NAR), to contextualise industry impact and loss trends between 2019-2026. These reports were not part of the academic thematic coding procedure, but they were utilised for statistical background.

3. Literature Review

This study adopts a structured narrative literature review, using targeted database searches and thematic synthesis to identify key concepts, mitigation strategies, and research gaps related to phishing and BEC in financial transaction environments

3.1 Theoretical Framework

Routine Activity Theory (RAT) provides a systematic framework for understanding crime occurrence by integrating observations and offering structured answers (Connelly, 2014; Evans, Coon and Ume, 2011). Developed initially for US crime rates (Cohen and Felson, 1979), RAT now extends to cybercrime (Krishnakumar and Verma, 2021), positing that crime requires the convergence of three elements: motivated offenders, suitable targets, and the absence of capable guardians (Cohen and Felson, 1979). Financial or non-financial motives, a valuable victim, and inadequate technological, jurisdictional, or legislative guardianship elevate crime likelihood (Leukfeldt and Yar, 2016). Policy professionals utilize RAT for analysis, pattern examination, and generating crime prevention advice due to its analytical clarity (Leukfeldt and Yar, 2016). Motivated offenders, particularly BEC perpetrators, exploit electronic communication vulnerabilities. Applying rational choice theory, these social engineers prioritize the real estate sector for its high-value transactions, assessing risk versus reward

(Cohen and Felson, 1979; Nguyen, 2020). Objectives include diverting real estate funds or stealing Personally Identifiable Information (PII) (Leukfeldt and Yar, 2016). They deploy sophisticated social engineering, Phishing, Smishing, and vishing, often leveraging open-source intelligence to bypass IT security and manipulate recipients (Button et al., 2014; Christopher Hadnagy, 2018; Maimon et al., 2023). Target selection is predicated on potential gains outweighing penalties (Nguyen, 2020; Chen et al., 2023). Suitable targets, determined by the offender's motive, possess value, visibility, and accessibility (Turvey and Freeman, 2014). Prime targets include financial institutions, title companies, individuals in real estate transactions, and document repositories (Hutchings and Hayes, 2009). In phishing and BEC contexts, competent guardianship encompasses security controls, law enforcement (e.g., CERTs), financial institutions, or any entity capable of deterrence, as inadequate supervision increases vulnerability (Hutchings and Hayes, 2009; Nguyen, 2020). Deterring these attacks, which cost the real estate industry billions annually requires a comprehensive cybersecurity guardianship strategy. This necessitates investment in technology, establishing security processes, implementing controls like Multi-Factor Authentication (MFA) and Domain-based Message Authentication, Reporting, and Conformance (DMARC), and crucially, educating and training employees to serve as vigilant, competent guardians (Papathanasiou et al., 2023; Atlam and Oluwatimilehin, 2023).

3.2 Nature and Mechanics of Phishing and BEC

Phishing uses social engineering to criminally obtain sensitive data, often via deceptive electronic communications, such as fraudulent emails, texts, or websites (Bezerra et al. 2024). These attacks exploit user naiveté, frequently using a malicious URL to impersonate legitimate entities (Prasad and Dondeti, 2025). Variants include smishing (SMS), vishing (voice), whaling (targeting executives), and spear-phishing (highly tailored emails) (Birthriya et al. 2025; Prasad Panda, 2025). BEC is a sophisticated form of phishing where threat actors meticulously craft messages, often spoofing sender domains or leveraging compromised accounts, to steal private information or induce fraudulent financial transfers (Papathanasiou et al. 2023). In BEC, attackers impersonate trusted figures, like senior executives or business partners, to manipulate employees into divulging confidential data or wiring funds to fictitious accounts (Saqib et al. 2025). Practically, during real estate transactions, a compromised email account can be monitored by an attacker who then intercedes to request altered payment instructions, redirecting a wire transfer to a fraudulent account (Internet Crime Complaint Center (IC3), 2023).

3.3 Impacts Across Sectors, Existing Frameworks, and Identified Gaps

Phishing and BEC are a critical global financial threat, with FBI's IC3 documenting $2.4 billion in losses in 2021 (Federal Bureau of Investigation, 2021), and phishing as the primary vector for 85% of enterprise breaches (Reuben-Owoh and Haig, 2025). Real estate is acutely exposed, with BEC/EAC accounting for 35% of all recorded dollar losses in 2021 (American Land Title Association, 2022), and real estate-linked losses surging 72% between 2020 and 2022 (FBI Public Service Announcement, 2023; Federal Bureau of Investigation, 2022). While general frameworks like ISO/IEC 27001/27002 are adopted (Bibi et al. 2024; Bernardo et al. 2025; Hossain et al. 2024), their "one-size-fits-all" nature limits their application to specific scenarios (Aljumaiah et al. 2025; Bernardo et al. 2025). This creates a gap, as current standards are not tailored to integrate real estate's unique business practices (e.g., escrow, title transfer) with technical controls. Sector-specific resilience measures are thus essential but remain inadequately articulated in the literature.

4. Case Studies

To examine how phishing and BEC attacks impact real estate transactions, this study analyzes six representative cases drawn primarily from the U.S.. Each case reflects a distinct scenario: law firm system compromise, executive-level residential fraud, cross-border laundering, rapid institutional intervention, minor domain spoofing with limited recovery, and insider-level transaction mirroring. Collectively, these varied contexts enable structured cross-case comparison of technical, procedural, and behavioral vulnerabilities. Together, these cases provide a diverse evidence base for identifying recurring vulnerabilities and mitigation patterns across incidents. Their comparative characteristics are summarized in Table 2.

Case Study 1: Homebuyer loses $600,000 in BEC attack

In August 2024, Richard Bates, a homebuyer in Connecticut, became a victim of wire fraud during his property purchase (Mary K. Jacob, 2024). Hackers breached the email system of his law firm, Hastings, Cohan & Walsh, LLP, and accessed transaction details. Using this information, the attackers sent Bates a fraudulent email, seemingly from his attorney, with fake wire instructions (Mary K. Jacob, 2024).

This case reflects a failure of capable guardianship under RAT. The absence of enforced secondary verification procedures and secure email controls created an exploitable gap in procedural and technical defenses. The lack of mandatory call-back verification represents a process failure rather than purely a technical breakdown.

Case study 2: Silicon Valley executive defrauded of $400,000 in home purchase (USA,2024)

In July 2024, Rana Robillard, became a victim of wire fraud during a high-value residential real estate transaction in California (Bevan Hurley, 2024). This incident exploited a critical vulnerability: the reliance on unencrypted email for sharing sensitive financial instructions. Posing as the mortgage broker, criminals induced the victim to wire a $398,359.58 down payment to a fraudulent JPMorgan Chase account (Son, 2024). Despite rapid FBI intervention to freeze the funds, complex jurisdictional and procedural hurdles significantly delayed restitution (Son, 2024). Although rapid FBI involvement limited damage, the attack succeeded due to the absence of mandatory call-back verification and secure communication channels. It reinforces that organizational process design, rather than victim inexperience, determines susceptibility.

Case Study 3: South Australian Homebuyer Loses $813,000 in BEC Scam (Australia, 2024)

Case 3 exemplifies the sophisticated, cross-jurisdictional nature of BEC fraud targeting real estate conveyancing. In May 2023, a South Australian home purchaser was defrauded of $813,000-the entire property payment via an email impersonation scam (Glover, 2024). The perpetrator employed domain spoofing, utilizing an email address nearly identical to the legitimate conveyancer's, differing by only a single character. While recovery was substantial, the extended restitution timeline highlights the psychological and operational costs of delayed guardianship activation. The capable guardian element under RAT emerged reactively rather than preventively.

Case Study 4: Stamford Homebuyer Email Wire Fraud (USA, 2023)

In March 2023, a Connecticut homebuyer nearly lost $426,000 due to a sophisticated BEC scheme targeting a real estate transaction (Peter Yankowski, 2023). A fraudster interceded in the email exchange between the buyer and their agent, utilizing an email spoofing tactic to redirect the high-value wire transfer to a fraudulent account. While the initial spoofing attack succeeded in redirecting funds, rapid coordination between law enforcement and financial institutions enabled recovery. This suggests that resilience in real estate cybersecurity must incorporate both preventative and responsive guardianship mechanisms. Detection speed significantly influences financial outcome severity.

Case Study 5: Haines City Couple Wire Fraud (USA, 2025)

In Florida, Matthew Brock and his wife experienced a BEC attack while making a down payment on their new home. Cybercriminals intercepted their transaction by impersonating the couple’s title company, changing a single letter in the email address to create a fraudulent account. The altered email allowed the attackers to gain access to the wiring instructions, which they modified by substituting the legitimate bank, routing, and account numbers with their own (Louis Bolden 2025).

This incident shows how minimal technical deception in the form of alteration of a single email character can bypass informal verification habits. The failure occurred primarily at the procedural layer, where no enforced independent confirmation protocol existed prior to fund release.

Case Study 6: Millennial Buyer Wire Fraud (USA, 2024)

In Tennessee, real estate investor, Regina Smith, fell victim to a sophisticated BEC scheme during the acquisition of her fourth property. Preparing a $60,000 down payment for a $280,000 property, Smith received fraudulent wire transfer instructions a day before closing which appeared to originate from the title company. Attackers had achieved system compromise, enabling them to perfectly mirror prior correspondence, including specific transaction variables like the closing date, costs, and personnel names (Pandy, 2024). The success of this attack demonstrates the interaction between technical infiltration and behavioral manipulation as social engineering is combined with contextual transaction knowledge.

Table 2: Summary of Real Estate BEC Case studies

Case	Scenario Type	Attack Vector	Estimated Loss	Key Parties Involved	Outcome
Case 1	Law firm system compromise	Email account compromise / wire instruction manipulation	$726,000	Homebuyer, law firm, bank	$129,000 recovered
Case 2	Executive-level residential fraud	Spoofed email impersonating transaction party	$398,359.58	Buyer, title company	Partial recovery
Case 3	Conveyancer system compromise	Compromised email thread and payment redirection	$813,000	Buyer, bank, international actors	$272,000 recovered. Investigation ongoing
Case 4	Realtor account compromise	Email interception during escrow transfer	$426,000	Buyer, bank, FBI task force	$425,000 recovered
Case 5	Title Email / Domain spoofing attack	Single-character domain spoof of title company	$38,000	Homebuyer, title company, bank	$5,000 recovered
Case 6	Insider-level transaction mirroring	Fraudulent email with detailed transaction data	$60,000	Buyer, title company	$60,000 recovered but property lost

5. Thematic Synthesis and Cross-case Analysis

Thematic synthesis is a technique for finding, examining, and summarising patterns or themes in data. It makes it easier to compare similarities and differences between the events, actions, and procedures that serve as the case study's analytical units (Cruzes et al. 2015). In this body of work, we will combine thematic synthesis with cross-case analysis which systemically evaluates information from individual case studies and identifies patterns across cases (Mynott and Kager 2024). To address recurring vulnerabilities across the six case studies, a structured thematic synthesis was conducted. Each case was coded according to theme / attack vector and control failure. Cross-case comparison was then used to identify patterns that consistently contributed to successful fund diversion.

5.1 Common Attack Vectors and Organizational Vulnerabilities

Cross-case evaluation reveals that email-based impersonation was present in all six incidents and summarized in table 3. Attackers either altered a single character within a legitimate domain, hijacked active email threads, or leveraged compromised accounts to inject fraudulent wiring instructions. This uniform recurrence confirms that email remains the dominant operational attack surface in real estate transactions. A second consistent pattern was the absence of mandatory secondary verification prior to high-value wire transfers. In all six cases, funds were transmitted without independent confirmation through voice call or authenticated secure platform. This procedural deficiency significantly increased transaction suitability under RAT by weakening capable guardianship at the approval stage. Organizational vulnerabilities were further observed in technical control inconsistencies. MFA or secure email configuration deficiencies were identifiable in four of six cases. However, technical weakness alone did not determine loss magnitude. Instead, outcomes were influenced by the presence or absence of structured verification and institutional response coordination. Additionally, limited inter-organizational coordination, particularly between banks and real estate professionals, exacerbates the difficulty in timely detection of suspicious transfers.

Table 3: Thematic patterns identified across all six Cases

Theme	Cases Observed	Primary Failure Type
Email Spoofing / Thread Hijacking	6 / 6	Technical
Absence of Secondary Verification	6 / 6	Procedural
MFA / Email Security Deficiency	4 / 6	Technical
Delayed Detection and Response	3 / 6	Organizational

5.2 Technical vs. Human Factors - Comparative Synthesis Across all Cases

BEC attacks fundamentally succeed by merging technical compromise with sophisticated social engineering (Table 2). While technical vulnerabilities like inadequate identity verification and compromised accounts are contributory factors, human elements are equally significant. Human error, often attributed to insider threats, accounts for a substantial portion of security risks and successful cyberattacks (Alsharif et al. 2021; Rahman et al. 2021). Attackers exploit human factors negligence, lack of awareness, deadline pressure, and routine communication familiarity to influence victims (Kadena and Gupi 2021). Subtle email spoofing is effective even against experienced parties relying on visual cues. The synthesis confirms that BEC attacks, initiated by technical compromise, are ultimately resolved by human decision-making. From a theoretical perspective, motivated offenders target high-value, time-sensitive transactions whose fragmented communication reduces guardianship visibility, exploiting the sector's reliance on large payments and inconsistent security practices. Suitable targets are defined by workflow complexity and coordination gaps, not just financial magnitude. Financial outcome severity is influenced by response speed, with rapid reporting demonstrating partial or substantial recovery, suggesting resilience operates both preventively and reactively. This convergence of technical compromise, procedural gaps, and behavioral susceptibility creates the conditions for successful exploitation, directly informing the layered resilience framework in Section 6.

6. Proposed Framework for Real Estate Cybersecurity Resilience

The cross-case synthesis and findings in Section 5 identified four recurring vulnerabilities: email impersonation as the dominant attack vector, absence of secondary verification, inconsistent technical safeguards, and exploitation of closing-stage urgency. The proposed framework directly responds to these patterns through a structured four-layer model: People, Processes, Technology, and Governance.

The *People* layer is foundational, mandating recurring education from property managers to executives on threats like phishing and social engineering to mitigate human error, a primary attack vector. It targets behavioral susceptibility, particularly urgency exploitation during closing phases. Structured awareness training must emphasize transaction-stage risk, spoof detection, and emotional manipulation tactics. The cases demonstrate that even experienced buyers and professionals are vulnerable when deadline pressure overrides verification discipline. The *Processes* layer formalizes the operational response, establishing clear, sector-specific protocols for risk assessment, business continuity, and disaster recovery, vital for high-value transactions and sensitive tenant data. It mitigates the universal absence *problem* of secondary verification across cases. A non-negotiable, documented call-back verification protocol for all wiring instructions is essential. Wire details must be confirmed through pre-established, independently sourced contact information rather than email correspondence. This procedural control directly addresses the recurrent guardianship gap identified in Section 5. *Technology*, the third pillar, addresses the consistent use of email spoofing and compromised accounts observed in all six cases. Mandatory phish-resistant MFA, enforced DMARC/SPF email authentication, secure client portals for transaction communication, and encrypted document exchange platforms are required to reduce exposure at the primary attack surface. These controls directly mitigate the technical deficiencies identified in Cases 1, 3, and 6. Finally, the *Governance* layer ensures oversight and accountability. Board-level reporting on transaction fraud attempts, periodic audit of wire verification compliance, and integration of cybersecurity risk into fiduciary responsibility frameworks institutionalize capable guardianship. This layer sets in stone the protective and educative role of intermediaries such as law firms, escrow agents, and brokers.

Collectively, this framework operationalizes RAT within the real estate sector by strengthening guardianship mechanisms at technical, procedural, behavioral, and institutional levels. Rather than treating BEC as isolated fraud events, the model addresses systemic transaction design weaknesses. By aligning defensive controls with empirically identified cross-case vulnerabilities, the framework provides a sector-specific roadmap for reducing the probability and impact of BEC attacks in high-value property transactions.

6.1 Next Steps for Empirical Validation

While the People–Process–Technology–Governance framework addresses empirically identified vulnerabilities, its academic contribution can be further strengthened through formal validation. To move beyond the current conceptual model, we propose a large-scale, international survey to validate the framework's effectiveness across different market segments and quantify its real-world utility. Additionally, future research should incorporate the analysis of non-public incident reports to offer a richer, more granular understanding of emerging threats that may be underrepresented in public filings due to reputational concerns. These steps are necessary to transition the framework from a descriptive model to a statistically validated resilience standard.

7. Conclusion

To identify recurrent technological, procedural, and behavioural weaknesses, this study looked at six incidents of phishing and business email compromise on real estate transactions. It was shown through cross-case analysis and thematic synthesis that weakened *guardianship* in time-sensitive transaction procedures is what drives BEC success. Empirical findings are made into practical controls that are suited to the operational reality of real estate using the proposed four-layer framework. The methodology provides an organised way to improve sector-specific resilience by matching defensive actions with patterns of exploitation that have been detected. To conclude, motivated offenders will continue to target the real estate industry for a fast payday, thus, enhancing oversight and resilience in technological, procedural, and institutional areas is critical to reducing the probability of successful BEC attacks.

Ethics Statement: No additional ethical considerations were needed as no experimental subjects were taken.

AI Ethics Statement: AI tools within Grammarly and Google Docs were used for organizing the paper, including grammar and spelling checks.

References

Alsharif, M., Mishra, S., & AlShehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science and Engineering*, *40*(3), 1153–1166. https://doi.org/10.32604/csse.2022.019938

American Land Title Association. (2021). *Cyber Losses Hit $6.9B in 2021*. ALTA.Org. https://www.alta.org/blog/post/cyber-losses-hit-69b-in-2021

Asenahabi, B. (2019). *Basics of Research Design: A Guide to selecting appropriate research design*. *6*, 76–89.

Atlam, H. F., & Oluwatimilehin, O. (2022). Business Email Compromise Phishing Detection Based on Machine Learning: A Systematic Literature Review. *Electronics*, *12*(1), 42. https://doi.org/10.3390/electronics12010042

Bakarich, K., & Baranek, D. (2020). Repeat offenders: Examining cases of multiple years of internal control weaknesses. *Managerial Auditing Journal*, *35*(4), 499–520. https://doi.org/10.1108/MAJ-05-2019-2302

Bernardo, L., Malta, S., & Magalhães, J. (2025). An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF. *Electronics*, *14*(7), 1364. https://doi.org/10.3390/electronics14071364

Bezerra, A., Pereira, I., Rebelo, M. Â., Coelho, D., Oliveira, D. A. D., Costa, J. F. P., & Cruz, R. P. M. (2025). A case study on phishing detection with a machine learning net. *International Journal of Data Science and Analytics*, *20*(3), 2001–2020. https://doi.org/10.1007/s41060-024-00579-w

Bibi, S., Azam, F., & Anwar, M. W. (2024). Implementing ISO 27001 Security Measures in Educational Open-Source ERP Systems. *2024 14th International Conference on Software Technology and Engineering (ICSTE)*, 35–39. https://doi.org/10.1109/ICSTE63875.2024.00014

Birthriya, S. K., Ahlawat, P., & Jain, A. K. (2025). Detection and prevention of spear phishing attacks: A comprehensive survey. *Computers & Security*, *151*, 104317. https://doi.org/10.1016/j.cose.2025.104317

Bolden, L. (2025, February 20). *Haines City couple falls victim to wire fraud during home purchase*. WKMG. https://www.clickorlando.com/news/local/2025/02/20/haines-city-couple-falls-victim-to-wire-fraud-during-home-purchase/

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, *47*(3), 391–408. https://doi.org/10.1177/0004865814521224

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588. https://doi.org/10.2307/2094589

Comora, E. (2019). *A Profile on Threat Actors Targeting Real Estate Transactions through Email Account Compromise,*. Utica College.

Connelly, L. M. (2014). Use of theoretical frameworks in research. *Medsurg Nursing: Official Journal of the Academy of Medical-Surgical Nurses*, *23*(3), 187–188.

Cruzes, D. S., Dybå, T., Runeson, P., & Höst, M. (2015). Case studies synthesis: A thematic, cross-case, and narrative synthesis worked example. *Empirical Software Engineering*, *20*(6), 1634–1665. https://doi.org/10.1007/s10664-014-9326-8

Evans, B. C., Coon, D. W., & Ume, E. (2011). Use of Theoretical Frameworks as a Pragmatic Guide for Mixed Methods Studies: A Methodological Necessity? *Journal of Mixed Methods Research*, *5*(4), 276–292. https://doi.org/10.1177/1558689811412972

Federal Bureau of Investigation. (2022). *FBI 2022 Congressional Report on BEC and Real Estate Wire Fraud*. https://www.fbi.gov/file-repository/reports-and-publications/fy-2022-fbi-congressional-report-business-email-compromise-and-real-estate-wire-fraud-111422.pdf/view

Federal Bureau of Investigations. (2021). *FBI Internet Crime Report 2021*. ic3.gov. https://www.ic3.gov/AnnualReport/Reports/2021_ic3report.pdf

FinCEN. (2023, March 30). *FinCEN Analysis of Business Email Compromise in the Real Estate Sector Reveals Threat Patterns and Trends | FinCEN.gov*. https://www.fincen.gov/news/news-releases/fincen-analysis-business-email-compromise-real-estate-sector-reveals-threat

Glover, A. (2024, October 1). *Aussie home buyer loses $813k in horror email scam*. 9News. https://www.9news.com.au/national/south-australian-woman-scammed-out-of-800k-during-house-sale-cybercrime/f815d8c8-c337-43ba-8d31-e5b34b1f5c74

Hadnagy, C. (2011). *Social engineering: The art of human hacking*. Wiley Pub.

Hasan, M. N. (2022). Applicability of Routine Activity Theory: An analysis based on cybercrime in Bangladesh. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4265385

Helo, P., & Hao, Y. (2022). Artificial intelligence in operations management and supply chain management: An exploratory case study. *Production Planning & Control*, *33*(16), 1573–1590. https://doi.org/10.1080/09537287.2021.1882690

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Understanding Local Government Cybersecurity Policy: A Concept Map and Framework. *Information*, *15*(6), 342. https://doi.org/10.3390/info15060342

Hurley, B. (2024, July 25). *Tech executive falls for $400,000 scam while buying 'cursed' house*. https://www.thetimes.com/world/us-world/article/tech-executive-scam-buying-house-dtmk5qn3w

Hutchings, A., & Hayes, H. (2009). Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the 'Net'? *Current Issues in Criminal Justice*, *20*(3), 433–452. https://doi.org/10.1080/10345329.2009.12035821

Jacob, M. K. (2024, August 5). *Connecticut homebuyer loses $600K to hacker theft | New York Post*. https://nypost.com/2024/08/05/real-estate/connecticut-homebuyer-loses-600k-to-hacker-theft/

Jain, N. (2021). Survey Versus Interviews: Comparing Data Collection Tools for Exploratory Research. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2021.4492

Kadena, E., & Gupi, M. (2021). Human Factors in Cybersecurity: Risks and Impacts. *Security Science Journal*, *2*(2), 51–64. https://doi.org/10.37458/ssj.2.2.3

King Faisal University, Aljumaiah, O., Jiang, W., Beijing University of Posts and Telecommunications, Reddy Addula, S., University of the Cumberlands, Amin Almaiah, M., & The University of Jordan. (2025). Analyzing Cybersecurity Risks and Threats in IT Infrastructure based on NIST Framework. *Journal of Cyber Security and Risk Auditing*, *2025*(2), 12–26. https://doi.org/10.63180/jcsra.thestap.2025.2.2

Krishnakumar, A., & Verma, S. (2021). Understanding Domestic Violence in India During COVID-19: A Routine Activity Approach. *Asian Journal of Criminology*, *16*(1), 19–35. https://doi.org/10.1007/s11417-020-09340-1

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Maimon, D., Howell, C. J., Perkins, R. C., Muniz, C. N., & Berenblum, T. (2023). A Routine Activities Approach to Evidence-Based Risk Assessment: Findings From Two Simulated Phishing Attacks. *Social Science Computer Review*, *41*(1), 286–304. https://doi.org/10.1177/08944393211046339

Martins Awofadeju, Beryl Fonkem, Omolola Akinola, Odunayo Rofiyat Olaniyan, Afolayan Ayokunle Fadeke, & Toyosi Motilola Olola. (2024). Strategies for mitigating cybersecurity challenges to fund management in the digitalized real estate industry. *Magna Scientia Advanced Research and Reviews*, *11*(1), 385–398. https://doi.org/10.30574/msarr.2024.11.1.0061

Mynott, J. P., & Kager, K. (2024). Usability testing of a conceptual model through retrospective cross-case analysis. *MethodsX*, *13*, 102950. https://doi.org/10.1016/j.mex.2024.102950

Pandy, J. (2024, March 20). *A millennial who'd bought 3 houses got scammed out of $60,000 buying her fourth—And it's more common than you might think*. Business Insider. https://www.businessinsider.com/millennial-buying-home-got-scammed-by-real-estate-wire-fraud-2024-3

Papathanasiou, A., Liontos, G., Liagkou, V., & Glavas, E. (2023). Business Email Compromise (BEC) Attacks: Threats, Vulnerabilities and Countermeasures—A Perspective on the Greek Landscape. *Journal of Cybersecurity and Privacy*, *3*(3), 610–637. https://doi.org/10.3390/jcp3030029

Peter Yankowski. 2023. *Police: Stamford homebuyer nearly lost $426K in email wire fraud scam*. Available at: https://www.stamfordadvocate.com/news/article/stamford-real-estate-email-wire-fraud-scam-17849100.php [Accessed: 25 November 2025].

Prasad Panda, S. (2025). The Evolution and Defense Against Social Engineering and Phishing Attacks. *International Journal of Science and Research (IJSR)*, *14*(5), 397–408. https://doi.org/10.21275/SR25504223645

Prasad, Y. B., & Dondeti, V. (2025). PDSMV3-DCRNN: A novel ensemble deep learning framework for enhancing phishing detection and URL extraction. *Computers & Security*, *148*, 104123. https://doi.org/10.1016/j.cose.2024.104123

PricewaterhouseCoopers. (2021). *Understanding cyber risks in real estate*. PwC. https://www.pwc.com/ca/en/industries/real-estate/understanding-cyber-risks-in-real-estate.html

Priya, A. (2021). Case Study Methodology of Qualitative Research: Key Attributes and Navigating the Conundrums in Its Application. *Sociological Bulletin*, *70*(1), 94–110. https://doi.org/10.1177/0038022920970318

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021). Human Factors in Cybersecurity: A Scoping Review. *The 12th International Conference on Advances in Information Technology*, 1–11. https://doi.org/10.1145/3468784.3468789

Reuben-Owoh, B., & Haig, E. (2025). A Systematic Review of Voluntary Cybersecurity Standards and Frameworks. *International Journal of Information Security*, *24*(5), 206. https://doi.org/10.1007/s10207-025-01121-0

Saqib, N. A., AlMuraihel, Z. A., AlMustafa, R. Z., AlRuwaili, F. A., AlQahtani, J. M., Aodah Alahmadi, A., Alqahtani, D., Alharthi, S. A., Chabani, S., & Al Kubaisy, D. A. (2025). OFF-The-Hook: A Tool to Detect Zero-Font and Traditional Phishing Attacks in Real Time. *Applied System Innovation*, *8*(4), 93. https://doi.org/10.3390/asi8040093

Saud Al-Musib, N., Mohammad Al-Serhani, F., Humayun, M., & Jhanjhi, N. Z. (2023). Business email compromise (BEC) attacks. *Materials Today: Proceedings*, *81*, 497–503. https://doi.org/10.1016/j.matpr.2021.03.647

Son, H. (2024, July 23). *A Silicon Valley executive had $400,000 stolen by cybercriminals while buying a home. Here's her warning*. CNBC. https://www.cnbc.com/2024/07/23/wire-fraud-in-real-estate-silicon-valley-executive-warning.html

Turvey, B. E., & Freeman, J. (2014). Victim Lifestyle Exposure. In *Forensic Victimology* (pp. 143–176). Elsevier. https://doi.org/10.1016/B978-0-12-408084-3.00006-5

Urbinati, A., Chiaroni, D., Chiesa, V., & Frattini, F. (2020). The role of digital technologies in open innovation processes: An exploratory multiple case study analysis. *R&D Management*, *50*(1), 136–160. https://doi.org/10.1111/radm.12313

Van Nguyen, T. (2020). *Cybercrime in Vietnam: An Analysis based on Routine Activity Theory*. https://doi.org/10.5281/ZENODO.3747516