Proceedings of the International Conference on Industrial Engineering and Operations Management

Publisher: IEOM Society International, USA DOI: 10.46254/BA08.20250193
Published: December 20, 2025

A Cognitive Operations Management (COM) Framework for Phishing Resilience: Quantifying User Decision Quality (UDQ) using Evidence Accumulation Modeling

Musfique-us-Salehin Arnob, Ovejite Saha and Md Anisuzzaman
Master of Science in Cyber Security
World University of Bangladesh
Dhaka, Bangladesh
26240340@student.wub.edu.bd, 26250445@student.wub.edu.bd,
26250446@student.wub.edu.bd, ovejites@gmail.com, musfique2@gmail.com

Abstract

Phishing has evolved into a major threat by leveraging AI-generated content and deepfakes to exploit human decision-making vulnerabilities. Traditional security measures fail to address the human element, a critical node in organizational defense. This paper introduces the Cognitive Operations Management (COM) Framework which quantifies human performance against phishing attacks through the User Decision Quality (UDQ) metric, encompassing Accuracy, Speed and Consistency. By applying the Drift-Diffusion Model (DDM), the framework mathematically links cognitive attack tactics to measurable UDQ degradation by enabling diagnostic insights into decision failures. Operational resilience is enhanced via Cognitive-Failure Modes and Effects Analysis (C-FMEA) for risk prioritization and Adaptive Cognitive Nudging (ACN) with Positive Friction interventions to dynamically steer users toward deliberate and accurate decisions. A hybrid modeling approach combining DDM and Agent-Based Modeling (ABM) simulates individual UDQ failures' systemic impact by allowing strategic allocation of security resources to high-risk users and optimizing organizational resilience metrics such as Mean Time to Compromise (MTTC). The COM Framework establishes a data-driven methodology for integrating cognitive risk management into cybersecurity operations, bridging human behavior modeling, operational strategy and ethical intervention design.

Keywords

Phishing Resilience, User Decision Quality, Cognitive Operations Management, Drift-Diffusion Model, Adaptive Cognitive Nudging

1. Introduction

The cybersecurity landscape faces a systemic crisis driven by the proliferation of sophisticated and highly personalized attacks designed to exploit the human decision node.

Phishing has escalated beyond opportunistic malware deployment to become a mainstream cybercrime which is characterized by AI-enhanced malicious content and deepfakes capable of creating "perfect messages" that blend seamlessly with everyday corporate communications (Kritika, 2025). This precision has driven a substantial 703% surge in credential phishing attacks (SlashNext, 2024) by confirming that traditional and reactive security models centered solely on technology are insufficient.

This report shows that the failure to detect and mitigate these cognitive attacks stems from treating the human user as an unpredictable liability rather than a critical and measurable component of the organizational security system.

Drawing inspiration from the reframing of industrial Advanced Persistent Threats (APTs) as a quantitative Operations Management (OM) problem focused on Overall Equipment Effectiveness (OEE) degradation (Rahman et al., 2020), this analysis adopts a rigorous OM perspective.

If Stuxnet demonstrated a successful attack that physically degraded machine performance (OEE Performance and Quality) (Rahman et al., 2020), modern phishing represents a Cognitive APT designed to degrade the performance of the human security "sensor."

This requires reframing the threat as a Cognitive Operations Management (COM) problem.
The core contribution of this paper is the introduction of the COM Framework which establishes User Decision Quality (UDQ) as the foundational measurable Key Performance Indicator (KPI) for the human element in cyber defense.
This framework moves beyond the binary "click/no-click" metric to define UDQ based on three components: Accuracy, Speed and Consistency.

To provide the necessary quantitative foundation, the framework proposes applying the Drift-Diffusion Model (DDM) which is a formal psychological model to mathematically quantify the precise relationship between cognitive attack tactics and the measurable degradation of UDQ parameters.
This quantitative modeling capability coupled with Industrial Engineering risk assessment tools enables the development of real-time and adaptive defense strategies known as Adaptive Cognitive Nudging (ACN).

1.1 Objectives

- To develop a framework for quantifying human decision-making in phishing scenarios.
- To measure User Decision Quality (UDQ) through Accuracy, Speed and Consistency.
- To model cognitive attack effects using the Drift-Diffusion Model (DDM).
- To design adaptive interventions to enhance organizational phishing resilience.

2. Literature Review

Effective defense against phishing necessitates a deep understanding of the adversarial approach which deliberately targets the innate architecture of human decision-making.

2.1 The Architecture of Human Vulnerability

Human decision-making is characterized by a reliance on heuristics, or mental shortcuts which are typically advantageous but become critical vulnerabilities when exploited by malicious actors (Amos, 2023). Phishing campaigns are engineered to bypass the slow, deliberate and logical **System 2** cognitive process in favor of exploiting the fast, intuitive System 1 (Van Steen and De Busser, 2021). By preventing the user from engaging **System 2** which requires effort and attention to detail, the attacker heightens the user's susceptibility to manipulation (Amos, 2023).
Attacks leverage established principles of social influence such as those formalized by Cialdini which translate directly into effective phishing Tactics, Techniques and Procedures (TTPs) (Biswas, 2020). Examples include Reciprocity (promising confidential access in exchange for a click), Scarcity (exploiting the desire for what is difficult to obtain), Authority (exploiting the tendency to defer to perceived superiors such as impersonating HR or a CEO (Amos, 2023)) and Unity (exploiting shared social identities or interests) (Biswas, 2020).

2.2 Cataloging Cognitive Bias Exploitation

These social engineering TTPs are effective because they trigger specific cognitive biases.
Attackers strategically utilize both positive emotions (to enhance trust and compliance) and negative emotions (to activate stress hormones like cortisol and thereby accelerating decision speed) to adjust the target's judgment criteria and behavioral tendencies (Dong and Qian, 2021). Key biases exploited include the Urgency Effect which forces rapid, high-pressure decision-making (Dong and Qian, 2021) and Authority Bias (the tendency to be influenced by an authority figure) which has been demonstrated to be highly effective in compromising users (Goncalves and Ali, 2025). This systematic exploitation of mental frameworks converts organizational assets into vulnerabilities (Amos, 2023).

The Cognitive Attack Taxonomy (CAT) provides a formal academic structure for cataloging over 350 cognitive vulnerabilities, exploits and TTPs (Cognitive Attack Taxonomy, 2024). This formalization is essential for developing systematic risk assessment methodologies, such as the Cognitive-Failure Modes and Effects Analysis (C-FMEA) detailed in Section 5 (Cognitive Attack Taxonomy, 2024).

2.3 The Evolution to Adaptive Cognitive Warfare

The threat is evolving beyond passive baiting. The most advanced form termed Neuro-Phishing transforms the human interaction into a dynamic, cognitive feedback loop (Kritika, 2025). Attackers utilize generative AI models (such as WormGPT or FraudGPT) to produce highly customized contextually rich messages that mimic executive voices or internal communications by making them sound significantly more authentic (Kritika, 2025).

Crucially, this advanced approach integrates behavioral sensors (via browser extensions or compromised apps) to monitor minute user actions including micro-hesitation spikes, mouse attention and focus of the eyes (Kritika, 2025). These psycho-physiological indicators provide the attacker with real-time feedback and enabling them to dynamically tweak the campaign which is a process that transforms users into interactive targets (Kritika, 2025). This adaptive nature which aims to tweak memory, perception and emotion as they occur (Kritika, 2025), renders traditional and asynchronous defenses (like periodic security awareness training) increasingly obsolete.

The presence of a dynamic real-time threat demands that the defense mechanism operates on the same timescale by requiring a focus on adaptive Human-Computer Interaction (HCI) interventions to counteract the attacker's dynamic TTPs (Van Steen and De Busser, 2021).

3. The Cognitive Operations Management (COM) Framework and User Decision Quality

To address the cognitive APT, the COM Framework defines a necessary quantifiable measure of the human security performance by mirroring the necessity of OEE for measuring production efficacy (Rahman et al., 2020).

3.1 Formal Definition of User Decision Quality (UDQ)

User Decision Quality (UDQ) is the comprehensive metric used to assess human performance when confronted with security threats specifically phishing attempts.

It moves past simple click rates to quantify the efficiency and reliability of the human decision node which is essential for continuous risk assessment (Bederna, 2020).

3.2 Deconstructing UDQ Components

UDQ is a three-dimensional KPI:

- **Accuracy (A):** Defined as the probability of correct classification specifically the True Negative Rate (correctly identifying a phishing attempt as malicious). UDQ Accuracy is degraded by successful cognitive exploitation such as the Authority Bias (Goncalves and Ali, 2025) which leads to uncritical compliance.
- **Speed (Time-to-Decision, TTD):** The latency which is measured in time from the user's initial exposure to the suspicious link or email until their final action (clicking, ignoring, or reporting). TTD is often ignored in HCI security analysis but is critical as it is reduced by urgency-based exploits.
- **Consistency (C):** The stability and predictability of Accuracy and Speed across a diverse user population under various states of cognitive load (Anamalamudi et al., 2023) and across different phishing simulations. Consistency is vital for ensuring the reliability of the human sensor layer and mitigating the effects of alert fatigue (Anamalamudi et al., 2023).

3.3 UDQ Linkage to Organizational Security Resilience (MTTx)

Failures in UDQ translate directly into measurable degradations of system-level resilience that is quantified by time-based security metrics (MTTx). A significant drop in UDQ Accuracy correlates directly with an increased Phishing Success Rate (SlashNext, 2024). This means the initial compromise occurs sooner by increasing the average Mean Time to Compromise (MTTC) which measures the time between initial alert and containment of the threat (Arctic Wolf, 2024). Furthermore, substandard UDQ Speed (high TTD or hasty, low-α decisions as detailed in Section 4) negatively affects the incident response cycle. Slow decision initiation by the user increases the organizational Mean

Time to Detect (MTTD) which is the average time required to discover an incident that subsequently increases the Mean Time to Respond (MTTR) and contain the threat (Amazon Web Services, 2025). The strategy of optimizing TTD is, therefore, a direct lever for accelerating the organizational incident response velocity.

The COM Framework formalizes this linkage between behavioral performance and organizational resilience (Table 1 and Table 2).

Table 1. The Human Security Effectiveness (HSE) Metric: A UDQ Framework

UDQ Component	**Target Function**	**Primary Cognitive Bias Exploit**	**Organizational KPI Linkage**
Accuracy (A)	Maximizing True Negative Rate (correctly identifying phishing).	Cognitive Exploits (e.g., Authority, Scarcity).	Reduces overall Phishing Success Rate and subsequent MTTC.
Speed (TTD)	Optimal Time-to-Decision (avoiding hasty response).	Urgency Effect/Time Pressure.	Directly influences organizational MTTD and response initiation time.
Consistency (C)	Low variability in performance across user roles and tasks.	Alert Fatigue/Cognitive Load.	Predictability and reliability of the security human sensor layer, linked to user trust.

4. Quantitative Modeling: The Drift-Diffusion Model (DDM) for Phishing Decisions)

The strength of the COM Framework lies in its ability to translate qualitative cognitive exploits into quantitative parameters using Evidence Accumulation Models (EAMs) such as the Drift-Diffusion Model (DDM) (Shetty et al., 2024). DDM provides a formal mathematical structure for the decision process which statistical models often fail to capture comprehensively and particularly regarding response time behavior (Shetty et al., 2024).

4.1 The Evidence Accumulation Process

Phishing detection is modeled as a classic two-choice decision task: the user accumulates evidence for the "Phishing" option (e.g. suspicious URL structure, generic greeting (Harrison et al., 2016)) or the "Legitimate" option (e.g., convincing sender name, accurate company logo) (Sinha et al., 2024). The decision is made when the accumulated evidence crosses one of two decision boundaries ('Sequential sampling models...', 2019).

The DDM is defined by three key parameters where each corresponding to a point of cognitive attack or defense intervention:

- **Drift Rate (ν):** Represents the rate at which evidence is accumulated and the quality of that evidence.
- **Starting Point (z):** Represents the initial bias or prior probability the user has before accumulating evidence.
- **Boundary Separation (α)** Represents the user's caution level or the amount of evidence required before a decision is finalized.

The DDM provides a crucial mechanism to quantify the Speed-Accuracy Trade-off (SAT) by allowing managers to identify the optimal α that minimizes phishing failure (Accuracy) without excessive delay (Speed) ('Sequential sampling models...', 2019).

4.2 Mapping Attack Variables to DDM Parameters

Cognitive attack TTPs are quantitatively modeled by systematically altering the parameters of the DDM:

- **Impact on Drift Rate (ν):** Highly sophisticated, AI-generated and contextually aware messages (Kritika, 2025) increase the evidence accumulated towards the "Legitimate" boundary.

Simultaneously, users who perform poorly on phishing tasks often spend less time attending to diagnostic cues (e.g., URL details) (Harrison et al., 2016). This combination of high-quality deception and poor attention accumulation results in a misleadingly high positive drift rate (ν) towards compliance.
Improving UDQ Accuracy requires improving the quality of evidence accumulation such as increasing the salience of threat indicators in the interface design.

- **Impact on Starting Point (z):** Cognitive biases like the Authority Bias (Goncalves and Ali, 2025) or general pre-existing user trust (Keepnet Labs, 2024) shift the starting point (z) closer to the "Legitimate" decision boundary.

This means the user begins the decision process already biased toward compliance by requiring less additional evidence to click the malicious link.

- **Impact on Boundary Separation (α):** Attacks leveraging the Urgency Effect often through negative emotional appeal or time pressure (Dong and Qian, 2021) to force the user to adopt low caution.

This decreases the Boundary Separation (α) by leading to a hasty decision that sacrifices Accuracy for speed ('Sequential sampling models...', 2019).
Critically, the Boundary Separation (α) represents the primary operational control point for defensive design as it can be actively manipulated by interface interventions.

The specific pattern of UDQ failure for instance, a high rate of errors coupled with a fast Time-to-Decision (low α) acts as a causal diagnostic tool.

This pattern indicates that the successful exploit was the Urgency Effect (a failure in choice architecture requiring physical intervention).

Conversely, a high error rate with normal TTD (high ν) suggests a failure in technical filtering and authentication against sophisticated message quality.

This distinction is vital for accurate resource allocation by directing investment either towards better technical filtering (to reduce ν) or ubiquitous interface controls (to increase α).

5. Operational Risk Quantification: Cognitive-Failure Modes and Effects Analysis

The rigorous quantification provided by DDM is integrated into a structured, proactive risk management process adapted from classic Industrial Engineering: the Failure Modes and Effects Analysis (FMEA) (ASQ, 2024). This adaptation, the **Cognitive-FMEA (C-FMEA),** moves cognitive risk analysis from qualitative assessment to quantitative, prioritized mitigation.

FMEA is designed to identify failures, assess their impact and prioritize actions based on the Risk Priority Number (RPN) (ASQ, 2024).

5.1 Structure of the C-FMEA

In the C-FMEA framework, the "failure modes" are defined by the specific cognitive attack TTPs cataloged in the Cognitive Attack Taxonomy (CAT) (Cognitive Attack Taxonomy, 2024). The potential "effects" are the quantifiable degradations of the three UDQ components (Accuracy, Speed, Consistency). The core of FMEA is the calculation of the RPN, defined as:

$$RPN = S \times O \times D$$

5.2 Recalibrating the Risk Priority Number (RPN) for Cognitive Risk

The COM Framework adapts the RPN parameters to the cognitive domain:

1. **Severity (S):** Unlike IT-centric severity scores, C-FMEA Severity is quantitatively tied to the resulting financial or operational impact of the breach enabled by the UDQ failure. This links the failure (e.g., "50% drop in Accuracy for high-privilege agent") directly to business consequence (e.g., total loss of high-value system control, assigned a score of 10). This methodology mirrors the strategic linking of APTs to OEE degradation and financial cost (Rahman et al., 2020).
2. **Occurrence (O):** The likelihood of the specific Cognitive Failure Mode (TTP) being successfully deployed against the organization that is informed by threat intelligence on frequently used tactics (SlashNext, 2024) and simulation data regarding environmental factors.
3. **Detection (D):** Traditionally, detection measures the ability to find the failure after it occurs.
4. In the C-FMEA, Detection is redefined as the likelihood that the real-time HCI intervention (the Nudge or Positive Friction control, detailed in Section 6) will fail to interrupt the cognitive shortcut and force the user into System 2 deliberation (Van Steen and De Busser, 2021). A high (D) score signifies a failure in the defense layer as the control is weak or easily dismissed while a low score signifies a highly effective intervention in mitigating the immediate cognitive shortcut.

This C-FMEA process translates cognitive risk into a standardized managerial format, allowing Chief Information Security Officers (CISOs) to prioritize investment in specific HCI controls based on their measurable ability to reduce the RPN associated with the highest-severity cognitive failure modes.

Table 2. Cognitive-Failure Modes and Effects Analysis (C-FMEA) Scoring

C-FMEA Parameter	**Cognitive Security Adaptation (COM)**	**Input Data Source**	**UDQ/DDM Linkage**
Failure Mode	Exploited Authority Bias (TTP: Executive Impersonation)	Cognitive Attack Taxonomy (CAT)	Shifts DDM Starting Point (z) toward "Legitimate" boundary.
Potential Effect	Uncritical compliance, 50% loss of Accuracy in high-privilege roles.	Empirical simulation data.	High error rate due to altered z.
Severity (S)	Critical (10): Total loss of high-value data/system control.	Organizational Risk Profile (e.g., financial/compliance cost).	High Severity justifies techno-regulation or mandatory friction.
Occurrence (O)	High (8): Tactic frequently used by targeted threat actors.	Threat Intelligence.	High Occurrence requires continuous monitoring.

Detection (D)	High (8): Real-Time Nudge (Control) is easily dismissed/vulnerable to fatigue.	HCI testing of control efficacy.	Detection measures the success of the Nudge in forcing deliberation (α).

6. HCI and Behavioral Interventions: Designing Resilient Choice Architecture

The operational defense phase of the COM Framework is focused on optimizing the user interface to the "choice architecture" to stabilize and maximize UDQ by designing resilience into the system (Van Steen and De Busser, 2021).

6.1 Positive Friction: Increasing the Decision Boundary (α)

To counteract the urgency and emotional manipulation that drives low-α decisions, security systems must integrate Positive Friction (ThinkMind, 2024). Positive friction involves introducing small and deliberate barriers or mandatory confirmation steps at critical decision points such as requiring a mandatory click-and-hold before navigating to an external link or forcing the user to transcribe the target URL before proceeding.

The goal is to create friction that demands immediate attention and action without being overly intrusive (Anamalamudi et al., 2023).

In DDM terms, positive friction directly increases the Boundary Separation (α) ('Sequential sampling models...', 2019). This action forces the user to accumulate more evidence and actively transition from intuitive System 1 thinking to the careful deliberation of System 2 (Van Steen and De Busser, 2021). The use of strong visual affordances which is interactive elements that clearly signal their intended use (UXPin, n.d.) can be used to guide the user to review the diagnostic cues (sender, URL structure) (Harrison et al., 2016) and thereby enhancing the evidence quality and increasing the drift rate (ν) toward the "Phishing" decision boundary.
If the DDM analysis shows that UDQ failures are primarily caused by low α (hasty decisions), the primary investment should be in ubiquitous positive friction mechanisms.

6.2 Adaptive Cognitive Nudging (ACN): Context-Aware Intervention

Traditional, generic warnings often lead to alert fatigue by diminishing both compliance and security outcomes (Anamalamudi et al., 2023). **Adaptive Cognitive Nudging (ACN)** provides a mechanism for dynamic, personalized and timely prompts which are crucial because a nudge must be presented every time a user is faced with a security decision to maintain effectiveness (Keepnet Labs, 2024).

ACN systems integrate User Behavior Analytics (UBA) and Context-Aware AI (Anamalamudi et al., 2023) to predict when a user is operating under high cognitive load or when a specific cognitive bias is being activated.

The DDM model serves as the trigger mechanism: if the system detects user behavior that suggests a sudden shift in DDM parameters such as a micro-hesitation followed by immediate movement toward a click (indicative of System 1 haste (Kritika, 2025)), an ACN intervention is launched to temporarily increase α or shift χ.

The successful implementation of ACN relies on precise calibration. The frequency of prompts must be regulated to avoid saturation and reactance (Anamalamudi et al., 2023) while the intensity of the friction applied must be proportional to the predicted threat level and the severity of the cognitive bias being exploited (e.g., a high-severity threat exploiting a strong Authority Bias requires more friction than a low-severity generic phishing attempt).

6.3 Ethical and Transparency Mandates

As defense mechanisms move into the cognitive domain, ethical governance becomes non-negotiable. Nudging must adhere to the principle of proportionality (MDPI, 2024) by ensuring that controls are justified by the expected reduction in the Severe (S) risks identified in the C-FMEA. Furthermore, stakeholders must ensure that the nudging behavior is transparent to the user as studies show that the visibility of a nudge does not necessarily reduce its

effectiveness (Van Steen and De Busser, 2021). This adheres to the principle that controls should influence choice while respecting volitional autonomy (MDPI, 2024).

7. Strategic Modeling for Organizational Resilience

Understanding UDQ at the individual level (via DDM) must be integrated into a larger organizational model to assess systemic risk and strategic investment return.

Security risk is an emergent property of the network and not just the sum of individual failures ('Agent-based Modeling...', 2024). Therefore, the COM Framework requires a hybrid simulation approach that couples DDM with Agent-Based Modeling (ABM).

7.1 Agent-Based Modeling (ABM) for Systemic Risk

ABM is a bottom-up simulation technique that models complex systems based on the interactions of autonomous, heterogeneous agents ('Agent-based Modeling...', 2024). It is the ideal tool to model the emergent security posture resulting from varied individual UDQ performances ('Agent-based Modeling...', 2024).

In this framework, organizational employees are modeled as agents that is parameterized by heterogeneous attributes including unique DDM parameters (α, ν, τ) derived from C-FMEA analysis and potentially dynamic cognitive profiles (Conde and Whiskeyman, 2025). These agents also possess attributes representing network connectivity, asset access privileges and security software interactions ('Agent-based Modeling...', 2024).

The attacker is modeled as a malicious agent defined by its strategic goals and TTP repertoire (CAT) (Padur et al., 2025). The ABM simulates the attacker's ability to propagate through the simulated network by utilizing the highest-risk TTPs identified by C-FMEA and adapting its deployment strategy based on the simulated organizational UDQ failure rates.

7.2 Modeling Emergent Organizational Risk and Strategic Investment

The hybrid model simulates how individual UDQ failures (decisions governed by the DDM) lead to network compromise and subsequent lateral movement by the attacker (Padur et al., 2025). The macro-level output of the ABM is a probabilistic distribution of the system-wide **Mean Time to Compromise (MTTC).**

This approach addresses a critical question of scale that micro-level models cannot face the UDQ failure of a single high-privilege agent (characterized by high C-FMEA Severity) and can lead to rapid, cascading system failure (Padur et al., 2025) and potentially outweighing numerous low-severity failures by agents with limited access.

The ABM simulation allows management to focus security hardening efforts on the agents who pose the greatest probabilistic risk to organizational MTTC and MTTR and thereby maximizing the return on investment (ROI) for defense resources.

For example, by simulating the effects of rolling out a universal Positive Friction mechanism (which increases every agent's α) versus investing in role-specific training to counter Authority Bias (which adjusts the τ parameter for only high-privilege agents), the CISO can quantitatively evaluate which strategy yields the greatest statistical reduction in system-level MTTC.

This capability enables data-driven and strategic resilience planning.

8. Conclusion

8.1 Summary of Contributions

This report introduced the Cognitive Operations Management (COM) Framework to address the systemic crisis of AI-enhanced phishing by quantitatively managing the human decision node. The framework establishes User Decision Quality (UDQ) which is a three-dimensional KPI measuring Accuracy, Speed (TTD) and Consistency as the operational metric for human cybersecurity.

This was supported by two primary contributions:

1. **Quantitative Modeling:** The framework mapped cognitive attack TTPs (cataloged via the Cognitive Attack Taxonomy) to the mathematically verifiable parameters (α, ν, τ) of the Drift-Diffusion Model (DDM). This established a rigorous causal link between behavioral exploitation and measurable UDQ degradation by providing a diagnostic tool for resource allocation.
2. **Operationalization and Resilience:** The framework proposed operationalizing risk assessment using Cognitive-Failure Modes and Effects Analysis (C-FMEA) which recalibrates Severity and Detection based on UDQ impact and HCI control efficacy. Defense is executed through Adaptive Cognitive Nudging (ACN) and Positive Friction interfaces designed to dynamically manipulate the DDM Boundary Separation (α) to force System 2 deliberation. Finally, system-level risk is measured using hybrid DDM-ABM simulations to quantify the impact of UDQ failures on organizational resilience metrics like Mean Time to Compromise (MTTC).

8.2 Future Research Agenda

The COM Framework opens several critical avenues for future research at the intersection of cognitive science and cybersecurity operations:

- **Empirical DDM Parameterization:** The conceptual framework must be rigorously validated through extensive empirical studies. Future work should focus on leveraging neuro-physiological indicators (Kritika, 2025) and HCI metrics (e.g., error rates, response time) (Anamalamudi et al., 2023) in controlled settings to obtain precise, statistically valid distributions for DDM parameters (α, ν, τ) across various organizational roles, cultural contexts and stress conditions.
- **Financial and Supply Chain Integration:** The COM framework currently links APTs to UDQ. The next logical extension is the explicit integration of UDQ degradation with financial cost models (e.g., calculating Cost Per Compromise) and System Dynamics (SD) modeling (Rahman et al., 2020). This would allow researchers to assess the long-term macroeconomic supply chain ripple effects resulting from a UDQ-based organizational compromise especially in industrial or critical infrastructure sectors.
- **AI-Driven Cognitive Profiling and Ethics:** Research is required to safely develop and validate AI systems that construct adaptive and dynamic user security profiles (often termed cognitive black boxes (Conde and Whiskeyman, 2025)). Such profiles are essential for continuous amd personalized security hardening via ACN. This development must proceed under strict ethical mandates by ensuring that any manipulation of choice architecture is transparent and proportionate to the quantifiable, high-severity risks being mitigated (MDPI, 2024).

References

AI-Assisted Security Warnings., AI-Assisted Security Warnings: Reducing Cognitive Load While Maintaining Cybersecurity, *Proceedings of the International Conference on Industrial Engineering and Operations Management*, 2024.

Arctic Wolf., Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), Mean Time to Contain (MTTC), Available: https://arcticwolf.com/resources/glossary/mttd-mttr/, 2024.

ASQ., What is FMEA?, Available: https://asq.org/quality-resources/fmea, 2024.

AWS., Mean time to contain, Available: https://docs.aws.amazon.com/security-ir/latest/userguide/mean-time-to-contain.html, 2025.

Bederna, Z. (2020). Components of Security Awareness and Their Measurement, Part 1, *ISACA Journal*, vol. 5, 2020.

CMS., Guidance for Failure Mode and Effects Analysis (FMEA), Available: https://www.cms.gov/medicare/provider-enrollment-and-certification/qapi/downloads/guidanceforfmea.pdf, 2024.

Cook, V. and Ali, A., End-of-line inspection for annoying noises in automobiles: trends and perspectives, *Applied Acoustic*, vol. 73, no. 3, pp. 265-275, 2012.

Cybersecurity Dive. (2024). Social engineering campaigns highlight the ability to exploit human behavior, Available: https://www.cybersecuritydive.com/news/social-engineering-campaigns-highlight-the-ability-to-exploit-human-behavio/760747/, 2024.

Defense/MDPI. (2024). These profiles offer a comprehensive view of an individual's mental processes, decision-making patterns, emotional tendencies, psychological resilience, and potential future behaviors, Available: https://www.tandfonline.com/doi/full/10.1080/08850607.2025.2571497, 2024.

Goncalves, D. and Ali, A. (2025). The influence of cognitive biases on human decision making in phishing email detection, *Proceedings of the 5th North American International Conference on Industrial Engineering and Operations Management*, Detroit, Michigan, USA, August 10-14, 2025.

Harrison, B., Svetieva, E. and Vishwanath, A. (2016). Individual processing of phishing emails: how attention and elaboration protect against phishing, *Online Information Review*, vol. 40, no. 2, pp. 265–281, 2016.

IEEE. (2023). Subjective Time Estimation to Measure the Cognitive Load of Interactive Mobile User Interfaces, *Proceedings of the 2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS)*, 2023.

JASSS. (2025). Towards a Model with Which to Study the Behaviour of Malicious Agents with Hybrid Attack Capabilities in Social Cyber-Physical Systems, *Journal of Artificial Societies and Social Simulation*, vol. 28, no. 1, 2025.

Keepnet Labs. (2024). What is the Nudge Theory for Security Awareness?, Available: https://keepnetlabs.com/blog/what-is-the-nudge-theory-for-security-awareness, 2024.

MDPI. (2024). Ethical analysis of nudging in cybersecurity: A systematic review, *MDPI*, 2024.

NCC Group. (2024). Psychology of the Phish: Leveraging the Seven Principles of Influence, Available: https://www.nccgroup.com/psychology-of-the-phish-leveraging-the-seven-principles-of-influence/, 2024.

NCSC. (2021). Security by Behavioural Design: A Short Summary, Available:(https://www.ncsc.nl/binaries/ncsc/documenten/rapporten/2021/september/14/security-by-behavioural-design-een-korte-samenvatting/Security+by+Behavioural+Design+%28Leiden+University%29.pdf), 2021.

NexGenAM. (2024). Understanding Failure Mode and Effects Analysis (FMEA) Scores, Available: https://www.nexgenam.com/blog/failure-mode-and-effects-analysis-fmea/, 2024.

Rahman, M. A., Ali, A. and Reimer, D. (2020). Modeling the impact of APTs on smart factory performance: an operations management perspective, *Proceedings of the International Conference on Industrial Engineering and Operations Management*, Dhaka, Bangladesh, December 20, 2020.

Rahman, M. A., et al. (2024). From phishing to neuro-phishing: a new frontier in cognitive tech warfare, Available: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/from-phishing-to-neuro-phishing-a-new-frontier-in-cognitive-tech-warfare, 2024.

Reimer, D. and Ali, A. (2023). Friction and affordance in cybersecurity interfaces, *Proceedings of the 12th Annual International Conference on Industrial Engineering and Operations Management*, Istanbul, Turkey, March 7-10, 2023.

Reimer, D., et al. (2021). Nudging towards security: developing an application for wireless network selection for android phones, *Proceedings of the 2015 British HCI conference*, ACM, pp. 193–201, 2021.

Rouse, M. (2020). Cognitive biases explained, Available: https://ridgesecurity.ai/blog/how-phishing-uses-your-cognitive-biases-against-you/, 2020.

Rouse, M. and Ali, A. (2020). Interpreting the Cognitive Attack Taxonomy, Available:(https://cognitiveattacktaxonomy.org/index.php/Interpreting_the_Cognitive_Attack_Taxonomy), 2020.

Shetty, D., et al., Crowdsourcing with the drift-diffusion model of decision making, *Frontiers in Big Data*, vol. 7, 2024.

Sinha, A., et al. (2024). Cognitive biases in phishing detection and prevention, *Proceedings of the 2024 IEEE International Conference for Convergence in Engineering (ICCE)*, 2024.

SlashNext. (2024). 2024 Phishing Intelligence Report, Available: https://www.infosecurity-magazine.com/news/2024-phishing-attacks-double/, 2024.

ThinkMind. (2024). The Positive Friction Model: A Novel Behavioral Approach to Enhancing HCI Design, *SECURWARE 2025: The Nineteenth International Conference on Emerging Security Information, Systems and Technologies*, 2024.

UWF. (2024). Agent-based Modeling of Entity Behavior in Cyber Space, Available:(https://ircommons.uwf.edu/esploro/outputs/bookChapter/Agent-based-Modeling-of-Entity-Behavior-in/99380557595706600), 2024.

UXPin. (2024). Affordances: User Interaction, Available: https://www.uxpin.com/studio/blog/affordances-user-interaction/, 2024.

vmPFC/mOFC. (2019). Sequential sampling models as a framework for understanding inter-temporal and risky choice, *PLOS Computational Biology*, 2019.

Wang, X., et al., The influence of cognitive load and time pressure on fraud decision-making, *Proceedings of the 23rd national psychological academic conference (Volume I)*, 2020.

Biographies

Musfique-us-Salehin Arnob is a Graduate Assistant in the Department of Computer Science and Engineering at the World University of Bangladesh. He specializes in AI, information systems and cybersecurity by focusing on deep learning–based vulnerability detection and AI-driven security automation. In his role, he coordinates academic and research activities, supervises undergraduate projects, supports course accreditation and mentors students in AI and cybersecurity research. He guided student teams at the BTRC Telecom & Digital Innovation Fair 2025 by assisting with project development, documentation and technical presentations. Mr. Arnob earned his BSc in Computer Science and Engineering at the World University of Bangladesh where his thesis, "Identifying and Detecting Backdoor Attacks using Deep Neural Networks," achieved over 99% accuracy in detecting malicious URLs and backdoor vulnerabilities using NLP and LSTM models. His research interests include NLP, Large Language Models, Machine Learning, Program Analysis and Secure Software Systems by aiming to advance AI-enabled, autonomous and privacy-preserving cybersecurity solutions.

Ovejite Saha is a Network Engineer specializing in network design, cybersecurity and industrial network systems. He holds a Master's degree in Cyber Security from the World University of Bangladesh, a Bachelor of Science in Computer Science and Engineering from Sonargaon University and a Diploma in Environmental Engineering from Sherpur Polytechnic Institute. He has extensive professional experience at Nextech Limited and the Public Works Department (PWD), MIS Division-2 where he designed and deployed scalable LAN/WAN infrastructures supporting over 800 endpoints. His work included configuring Cisco and Fortinet devices by implementing VPNs and network access controls and monitoring network performance using tools such as SolarWinds, PRTG and Wireshark. As a System Support Engineer at Nextech Limited, he optimized network performance, migrated legacy systems to modern infrastructure and ensured high network availability. His research interests focus on networking and industrial network systems, with expertise in routing protocols, VLANs, firewalls, VPNs and security mechanisms. He holds certifications in IT Support, Mikrotik Networking and Faronics Expertise. Driven by a commitment to secure and resilient network infrastructures, Mr. Saha aspires to advance as a Network and Security Administrator by contributing to reliable and high-performance industrial networks.

Mr. Md Anisuzzaman is the Head of Cloud Operations at MeghnaCloud (BDCCL) and bringing over 20 years of experience in IT project management and architecture. He specializes in leading complex cloud and infrastructure projects and in his current role, he architects Opensource-based private cloud environments, drives cloud strategy and leads cross-functional teams across Cloud, NOC, SOC and DevOps. Prior to joining MeghnaCloud, he spent over 12 years at GETCO Telecommunications Limited where he served as Head of IT & Billing by managing telecom BSS infrastructure and large-scale billing implementations. His earlier career included roles as an Application Development Manager for International Turnkey Systems (ITS) in Lagos, Nigeria. Mr. Anisuzzaman holds a BSc in Computer Science from East West University and currently completing an MSc in Cyber Security from World University of Bangladesh and holds professional certifications including the Six Sigma (DMAIC) Black Belt, Red Hat Virtualization, OCA Cloud Infra, GCP Cloud Certification and ITIL® Foundation.