ADRIAN NECAJ

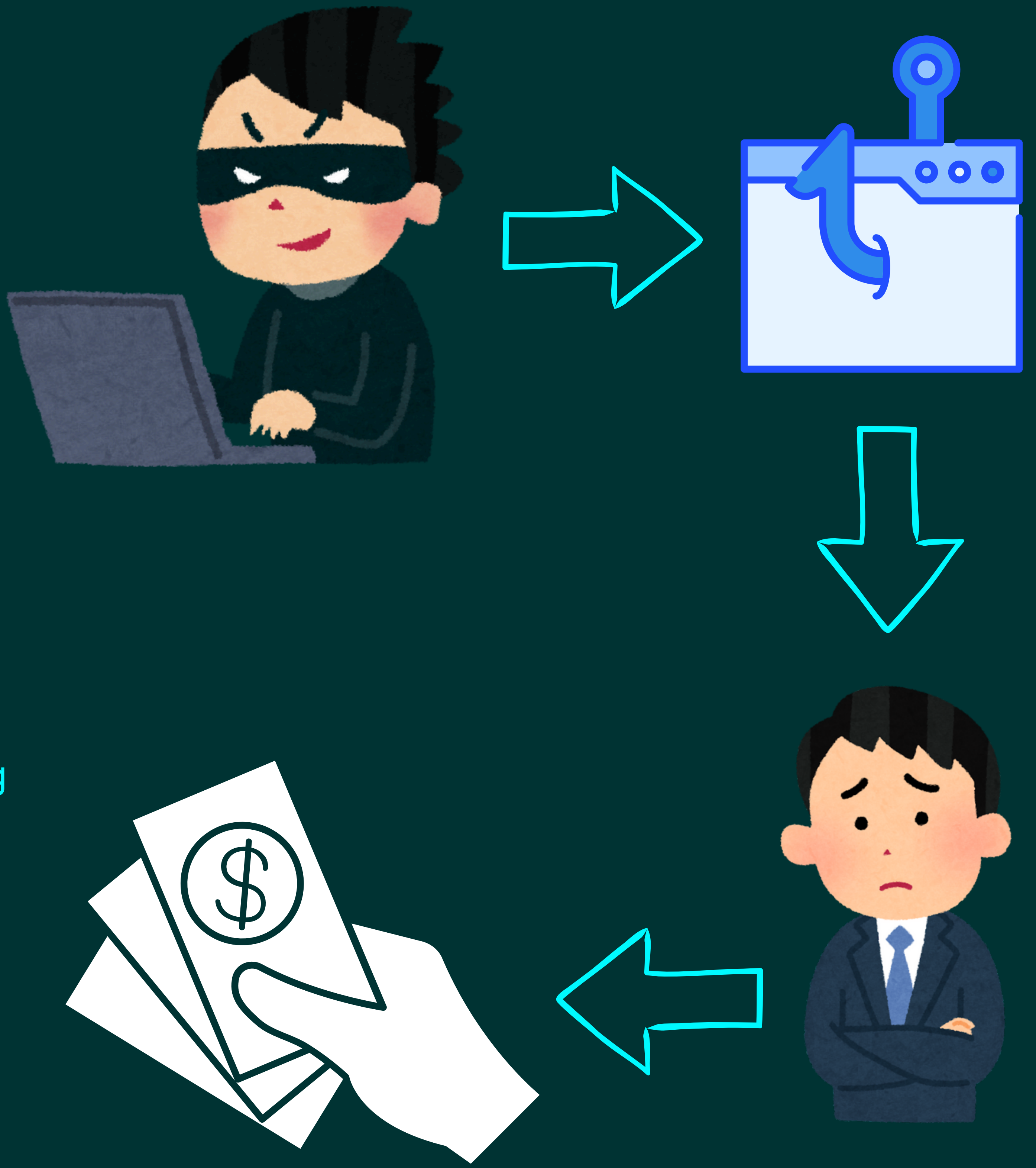
# Integrating Behavioral Risk Metrics into Governance, Risk, and Compliance Frameworks to Reduce Social Engineering Incidents

CS-GY 6233
Introduction to Operating Systems
December 2025

# THE SOCIAL ENGINEERING PROBLEM

## UNDERSTANDING THE BASICS

- 60% of security breaches involve social engineering
- $4.45M average cost per data breach (2023)
- Technical defenses ≠ Human defenses



# THE GRC FRAMEWORK GAP

## COMMON THREATS AND THEIR IMPACT

NIST Cybersecurity Framework
ISO/IEC 27001
FAIR (Factor Analysis of Information Risk)

✓ Firewall configurations
✓ Patch management
✓ Access control policies
✗ Human susceptibility
✗ Behavioral risk
✗ Social engineering vulnerability

# RESEARCH HYPOTHESIS

## MAIN HYPOTHESIS

"Integrating behavioral risk metrics into GRC frameworks will reduce successful social engineering incidents by at least 25% compared to traditional technical-focused approaches."

- CONTINUOUS BEHAVIORAL SIMULATIONS
- OPERATING SYSTEM-LEVEL MONITORING
- MACHINE LEARNING RISK SCORING
- DYNAMIC ACCESS CONTROLS

Traditional GRC Incidents

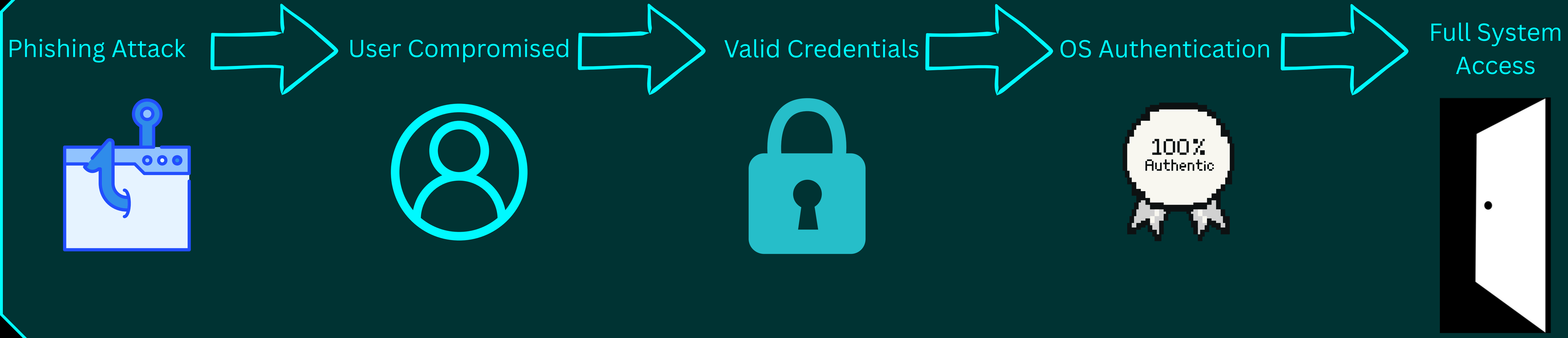
40% →

Human Integrated GRC

# RESEARCH HYPOTHESIS PT 2.

## WHY THIS MATTERS FOR OPERATING SYSTEMS

- OS GRANTS ACCESS BASED ON AUTHENTICATION ✓
- OS CANNOT DISTINGUISH LEGITIMATE USER FROM COMPROMISED CREDENTIAL ×
- HUMAN BEHAVIOR = OS SECURITY PERIMETER

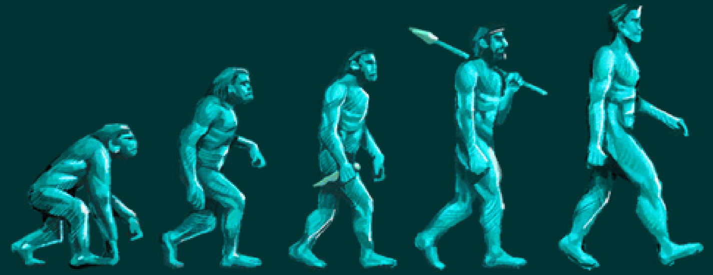


Phishing Attack → User Compromised → Valid Credentials → OS Authentication → Full System Access

*** No comprehensive framework integrating behavioral metrics into GRC processes ***

# RELATED RESEARCH

## WHAT OTHERS HAVE DONE



### HUMAN FACTORS RESEARCH:

- Khadka & Ullah (2025): Human error dominates cyber incidents
- Schaltegger et al. (2025): Cognitive bias predicts phishing susceptibility

### TECHNICAL APPROACHES:

- Pearman & Brooks (2024): Human-centric risk scoring models
- Nguyen & Ortiz (2024): ML prediction (87% accuracy)

### GRC LIMITATIONS:

- Thompson & Chen (2024): Weak correlation between compliance and breach resistance
- Colabianchi (2025): Gap between theory and implementation

# IMPLEMENTATION - PART 1: OVERVIEW

## EXPERIMENTAL DESIGN

Study Parameters:

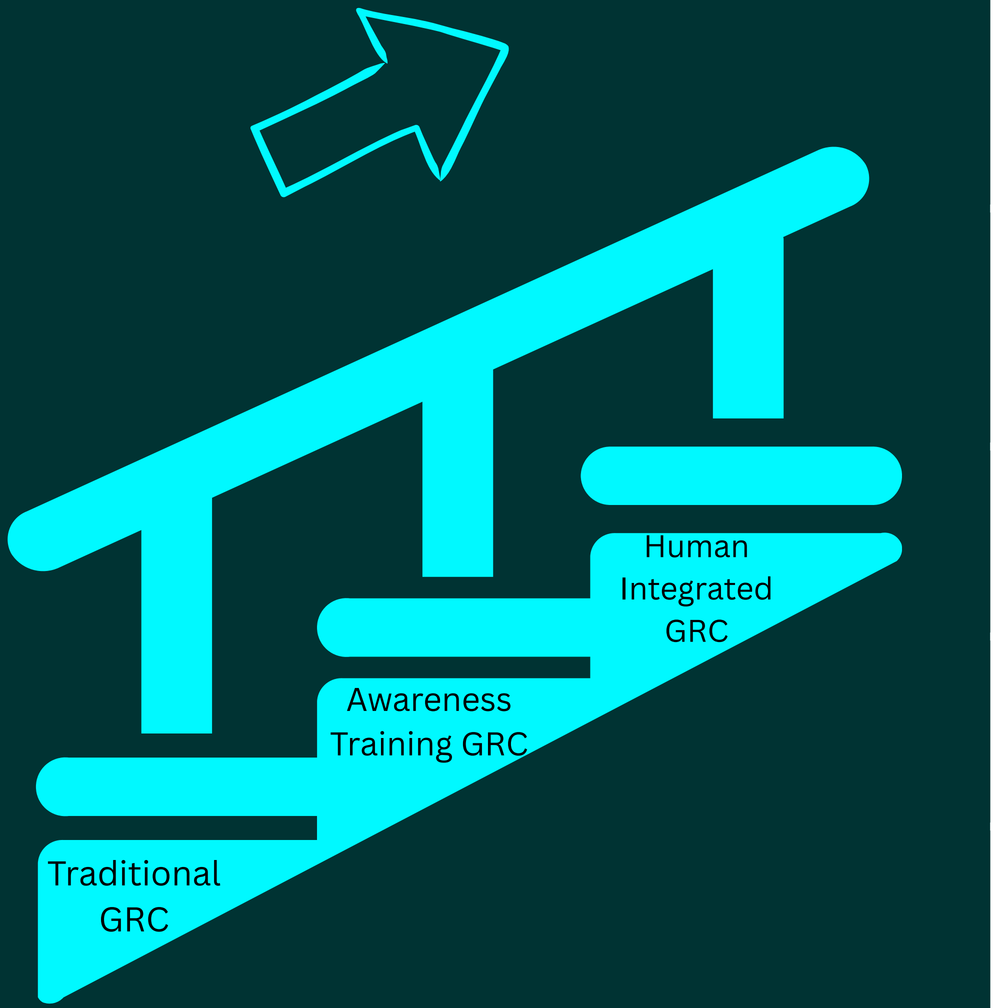
- Environment: Simulated enterprise with 200 users
- Infrastructure: Mixed Windows Server / Linux domain
- Duration: 30 days
- Attacks: 1,000 controlled social engineering attempts

Three Models Tested:

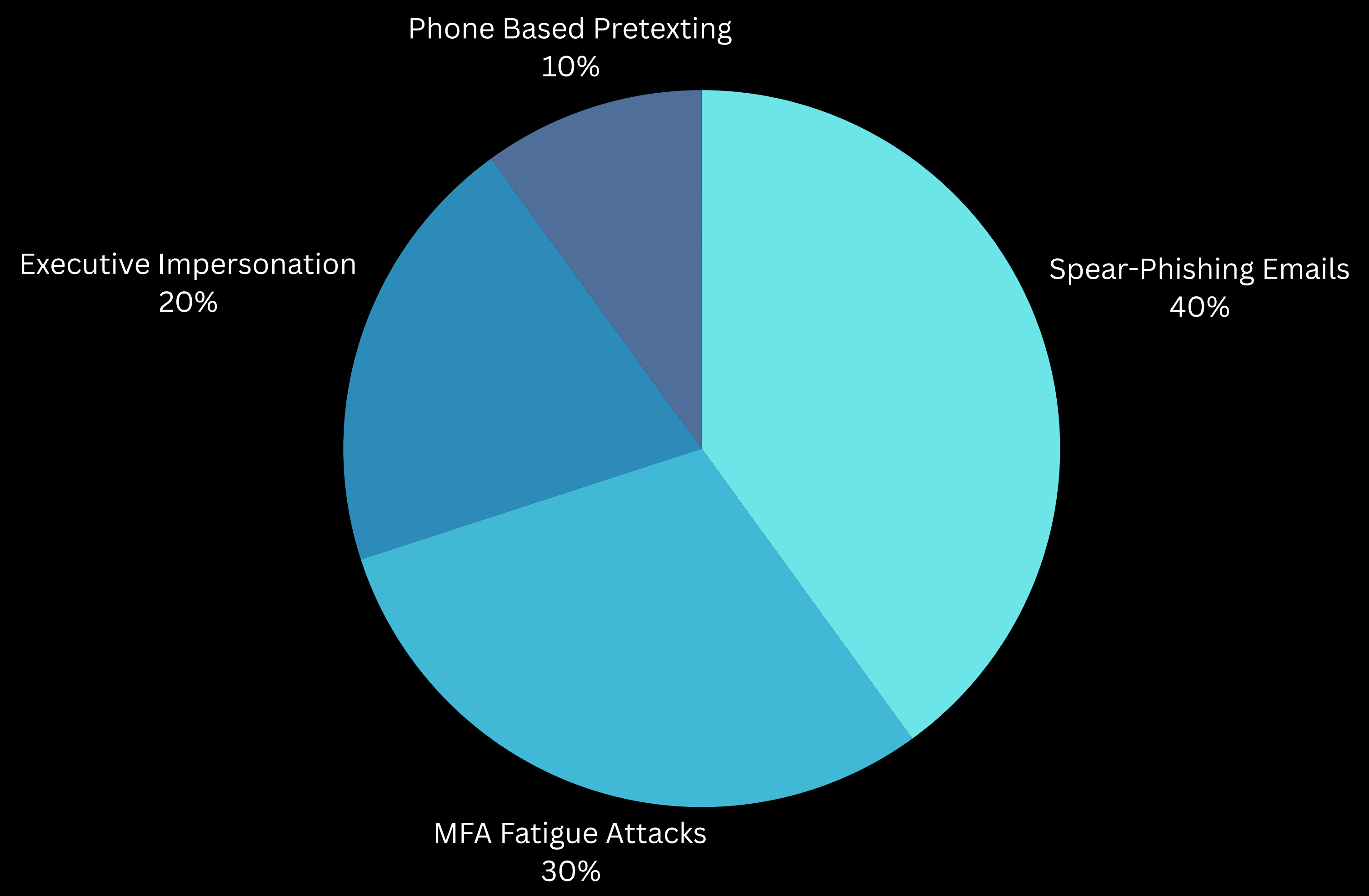
- Traditional GRC (Baseline)
- Awareness Training GRC (Current Best Practice)
- Human-Integrated GRC (Proposed Framework)

# IMPLEMENTATION

THREE SECURITY MODELS COMPARED



| Component | Traditional GRC | Awareness Training GRC | Human-Integrated GRC |
|---|---|---|---|
| Technical Controls | ✓ Firewall, AV, Patches | ✓ Same | ✓ Same |
| Security Training | Initial orientation only | ✓ Quarterly training | ✓ Continuous |
| Phishing Simulations | ✗ None | Monthly (reporting only) | ✓ Weekly (adaptive) |
| MFA Testing | ✗ None | ✗ None | ✓ Fatigue monitoring |
| Impersonation Exercises | ✗ None | ✗ None | ✓ Detection testing |
| OS-Level Monitoring | ✗ None | ✗ None | ✓ Behavioral analytics |
| Risk Scoring | ✗ None | ✗ None | ✓ ML-driven |
| Access Controls | Static | Static | ✓ Dynamic (risk-based) |



Spear-Phishing Emails: 400 attempts (40%)

- Credential harvesting, malware delivery

MFA Fatigue Attacks: 300 attempts (30%)

- Repeated approval request bombing

Executive Impersonation: 200 attempts (20%)

- CEO fraud, urgent wire transfers

Phone-Based Pretexting: 100 attempts (10%)

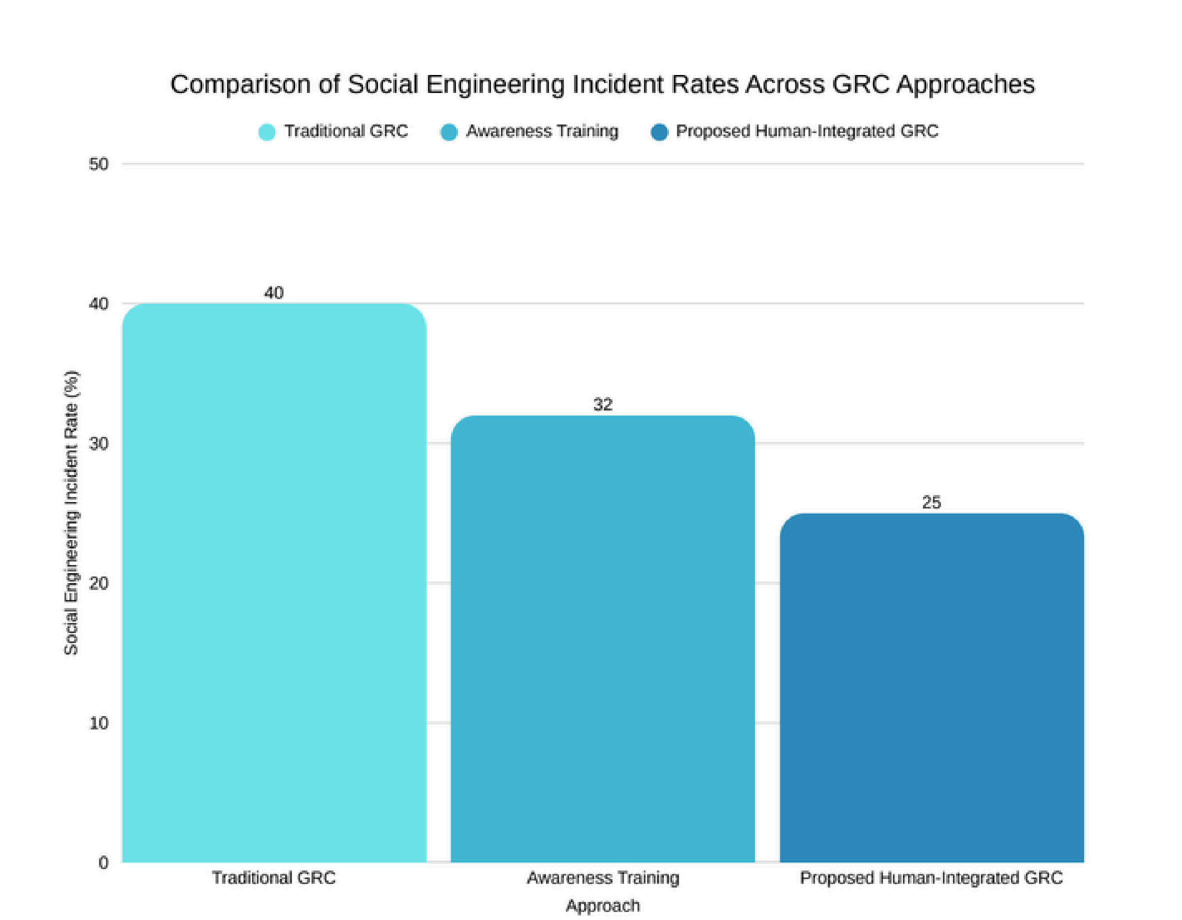
- Help desk manipulation, password resets

# SOCIAL ENGINEERING ATTACK DISTRIBUTION

## TARGET AREAS:

Authentication portals
Privileged access workflows
Internal communication channels

# FINDINGS - PART 1: MAIN RESULTS



## SOCIAL ENGINEERING INCIDENT RATES

37.5% reduction from baseline
21.9% improvement over awareness training
Hypothesis confirmed: Exceeded 25% target
Statistical significance: $p < 0.001$

# FINDINGS - PART 2: MAIN RESULTS

| Attack Type | Traditional GRC | Awareness Training | Training Human-Integrated | Improvement |
|---|---|---|---|---|
| **MFA Fatigue** | **50% success** | **38% success** | **22% success** | **45% reduction** |
| Exec Impersonation | 45% success | 35% success | 20% success | 42% reduction |
| Spear-Phishing | 38% success | 30% success | 27% success | 28% reduction |
| Phone Pretexting | 35% success | 28% success | 25% success | 26% reduction |

***

## CONTINUOUS BEHAVIORAL MONITORING MOST EFFECTIVE AGAINST SOPHISTICATED ATTACKS EXPLOITING ORGANIZATIONAL DYNAMICS

***

Machine Learning Performance:

- 82% accuracy predicting future victims
- High-risk users (top 25%) = 61% of incidents

# NEXT STEPS

## FUTURE RESEARCH DIRECTIONS

Real-World Validation

- Longitudinal studies in production environments
- Partner with enterprise organizations
- Measure long-term behavioral adaptation

Extended Behavioral Modeling

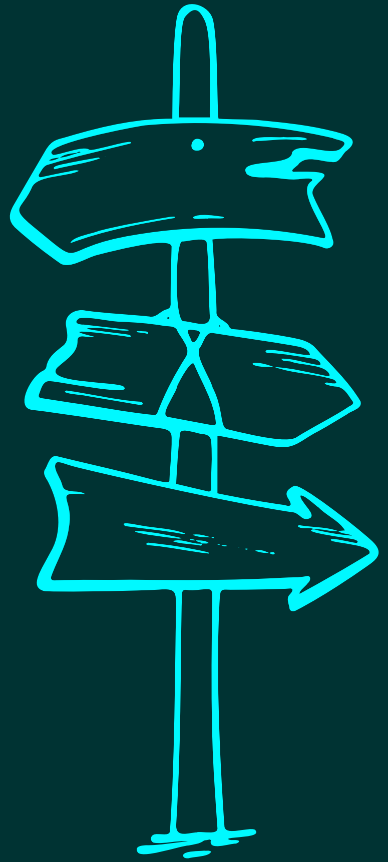
- Insider threat prediction
- Privilege abuse detection
- Supply chain security contexts

Ethical Framework Development

- Privacy-preserving monitoring techniques
- Employee consent and transparency
- Legal compliance (GDPR, CCPA)

Technical Integration

- Security orchestration platform integration
- GRC framework standardization
- API development for existing tools (NIST, ISO)



# CONCLUSION

## !! THANK YOU !!

Treating human behavior as a continuously measurable vulnerability component significantly improves enterprise security posture beyond current compliance-driven approaches.

Human behavior IS measurable

Not just a training problem
Quantifiable risk component

Integration achieves results

37.5% incident reduction
Outperforms compliance + training

GRC frameworks must evolve

Technical controls ≠ complete security
Behavioral metrics = missing piece

Adrian Necaj
an4837@nyu.edu