Simulation of Human Organizations with Computational Human Factors Against Phishing Campaigns

Jeongkeun Shin, Richard Carley and Kathleen Carley
CASOS Center, Carnegie Mellon University, Pittsburgh, USA

jeongkes@andrew.cmu.edu
lrc@andrew.cmu.edu
kathleen.carley@cs.cmu.edu

Abstract: Traditionally, cybersecurity has focused on identifying and addressing system-level vulnerabilities that cybercriminals could exploit. As technical defenses have become more sophisticated, cybercriminals have shifted their tactics toward exploiting human users through social engineering techniques. This shift demonstrates how a single mistake by an individual within an organization can allow attackers to bypass even the most robust cybersecurity systems. Consequently, researchers in human factors and educators developing effective cybersecurity training have long sought to understand which human factors make individuals more susceptible to social engineering attacks. While the relationship between susceptibility to social engineering attacks and static human factors, such as age, gender, and personality, has been widely explored in empirical studies, research into the relationship between dynamic human factors, such as fatigue, perceived vulnerability, and job performance, and susceptibility to social engineering tactics has been limited. This limitation is due to the practical, temporal, and ethical challenges of continuously tracking such variables in real-world settings. To address this gap, we propose a simulation-based methodology to explore how dynamic human factors correlate with susceptibility to spearphishing, one of the most prevalent forms of social engineering. In this study, we replicate a real-world human organization that was previously the subject of a spearphishing empirical study. Then, we computationally model dynamic human factors such as fatigue, perceived vulnerability, and job performance by integrating regression models from various human factors studies. Next, we simulate spearphishing attacks with the goal of data exfiltration, using different combinations of dynamic human factor values to explore their relationship with susceptibility to these attacks. Our simulation study reveals that when end users within an organization exhibit higher perceived vulnerability, higher job performance, and lower fatigue, they are more likely to adhere to security policies, which in turn results in both the overall number of users tricked by a spearphishing campaign and the total amount of exfiltrated data decreasing. Based on these hypotheses derived from simulation results and statistical analysis, we recommend which organizational policies should be prioritized to effectively mitigate spearphishing risks.

Keywords: Agent-based simulation, Organization modeling, Human factors

1. Introduction

As social engineering attacks continue to rise, cyberattacks that exploit human mistakes within organizations are becoming increasingly frequent. In light of this, there is growing interest in understanding the human factors that contribute to critical errors, leading to cybersecurity threats. To accurately identify these factors, it is essential to monitor various human factors before conducting simulated phishing campaigns in the organization, and then analyze the relationship between those factors and the phishing campaign results. Many researchers have successfully identified correlations between static human factors and susceptibility to phishing attacks. However, due to various challenges, it has been difficult to establish the relationship between dynamically changing human factors and susceptibility to phishing attacks. This paper proposes a heuristic methodology for computationally modeling these dynamic human factors. We modeled phishing susceptibility, fatigue, perceived vulnerability, and job performance based on regression models from several empirical studies. Through this process, similar to assembling a collage where individual pieces of art come together to form a complete picture, the regression models from various empirical studies combined to create a more realistic human model. Using this method, we formulated several hypotheses regarding the relationship between different dynamic human factors and organizational damage from phishing. We also analyzed which specific human factors an organization should focus on improving to most effectively mitigate damage, given limited cybersecurity budgets. Previous cybersecurity simulation studies have typically considered very few human factors, and often relied on hypothetical values rather than data derived from empirical research to assess their impact on organizations. In contrast, our study distinguishes itself by leveraging regression models from a range of existing empirical studies, providing a novel approach to building realistic human models in simulations even when data collection on dynamic human factors is limited.

2. Related Works

Agent-based Modeling and Simulation (ABMS) is a modeling approach that uses a system of autonomously interacting agents, each with independent behaviors and decision-making capabilities, to understand and

simulate the dynamic characteristics and structure of complex systems effectively (Macal and North, 2009). Properly designed and validated simulation models allow for faster and more cost-effective systematic testing of many different scenarios (Carley et al., 2006). This simulation approach is extensively employed to address cybersecurity challenges, particularly for assessing potential damages from various cyber threats and evaluating the efficacy of different cybersecurity defense strategies (Kavak et al., 2021). As cybercriminals increasingly employ diverse social engineering tactics to exploit human errors, numerous efforts have been made to model and simulate these mistakes in order to analyze their impact on organizational cybersecurity. Blythe et al. modeled agents to replicate human behaviors, such as ignoring warnings, underestimating risks, and inconsistently using security tools due to factors like fatigue and stress (Blythe et al., 2011). Burns et al. modeled organizational dynamics using various social science theories and conducted sensitivity analyses to observe how each theory affected the organization's information security in response to phishing campaigns. (Burns et al., 2017). Shin et al. developed the OSIRIS framework and demonstrated how factors such as organization size, the cybersecurity expertise level, and the proportion of online communication correlate with the overall number of virus infections within a virtual organization (Shin et al., 2022a, Shin et al., 2022b). Shin et al. also simulated the impact of cybersecurity education frequency and the recency of human memory on phishing susceptibility and the overall organizational damage from phishing campaigns (Shin et al., 2023b).

3. Spearphishing Campaign Model

We use the spearphishing campaign for data exfiltration designed by Shin et al. (Shin et al., 2024b), utilizing MITRE ATT&CK techniques (Strom et al., 2018). The cybercriminal agent targets intellectual property, confidential documents, and customer data stored on each end user agent's computing device. We assume that each end user agent in the virtual organization holds 10GB of such data. During the first three days of the simulation, the cybercriminal agents send a spearphishing email once per day. Once a user is tricked and executes the attached malware, the cybercriminal agent gains access to the user's computer. After establishing persistence via a scheduled task, the agent stages the targeted data in one location, compresses it, exfiltrates the data, and finally deletes the data from the user's system. Shin et al. empirically measured the time required for each phase of this process: staging 10GB of data takes 1,042 seconds (SD = 1.16 seconds), archiving the collected data takes 276 seconds (SD = 43.65 seconds), exfiltrating the archived data takes 3,952 seconds (SD = 252.74 seconds), and data destruction takes 2 seconds (SD = 0.337 seconds) (Shin et al., 2024b). We apply this empirical data to our cyberattack simulation scenario.

4. Human and Organization Model

In our study, we modeled a medium-sized software company by replicating a software company with 235 end users based on regression models from Eftimie et al.'s empirical research (Eftimie et al., 2022). They measured age, gender, and the Big Five personality traits of each user to determine the correlation between each human factor and susceptibility to spearphishing emails before and after cybersecurity training. However, since Eftimie et al. did not disclose the specific human factor data of each subject, we randomly generated the human factor values for each end user agent in our simulation model by leveraging the mean and standard deviation data from their study. Shin et al. replicated and validated this organizational model through two methods: 1) by calibrating the age distribution of randomly generated end user agents until the virtual spearphishing campaign result aligns with the overall phishing susceptibility reported in Eftimie et al.'s study (Shin et al., 2024a) and 2) by continuously regenerating the organization and simulating multiple spearphishing campaigns until the overall phishing susceptibility closely matched the empirical results before and after cybersecurity training reported in Eftimie et al.'s study (Shin et al., 2024b). While this approach allows us to model the initial phishing susceptibility of each end user agent accurately, it does not account for dynamically changing human factors such as perceived vulnerability, fatigue, or job performance, which could significantly correlate with susceptibility. Additionally, the limited range of human factors considered makes it challenging to model diverse behaviors, such as the likelihood of an end user reporting a phishing incident to a security officer or the probability that they will carefully read security alert emails about recent spearphishing attempts. To address the absence of these dynamic human factors in our model, we computationally incorporated multiple dynamic human factors by integrating regression models from various human factors empirical studies.

4.1 Computational Human Factors

In this study, 'Computational Human Factors' refers to the use of mathematical models and simulations to represent and analyze human behavioral factors, utilizing previously established empirical regression models

instead of directly collected empirical data. This approach is particularly valuable when direct data collection is impractical or costly, as it allows us to simulate a variety of human factors in different contexts. As illustrated in Figure 1, we modeled phishing susceptibility, fatigue, job performance, and perceived vulnerability, along with the impact of fatigue on phishing susceptibility and overall job performance, using various independent human factor variables from different empirical studies. When multiple regression models were available for predicting a particular human factor, we combined them into a single model to capture a wider range of independent variables, enabling greater generalization in the predictions. To minimize distortion caused by differences in variable ranges across models, we selected the variable whose range modifications had the least impact on the other variables.

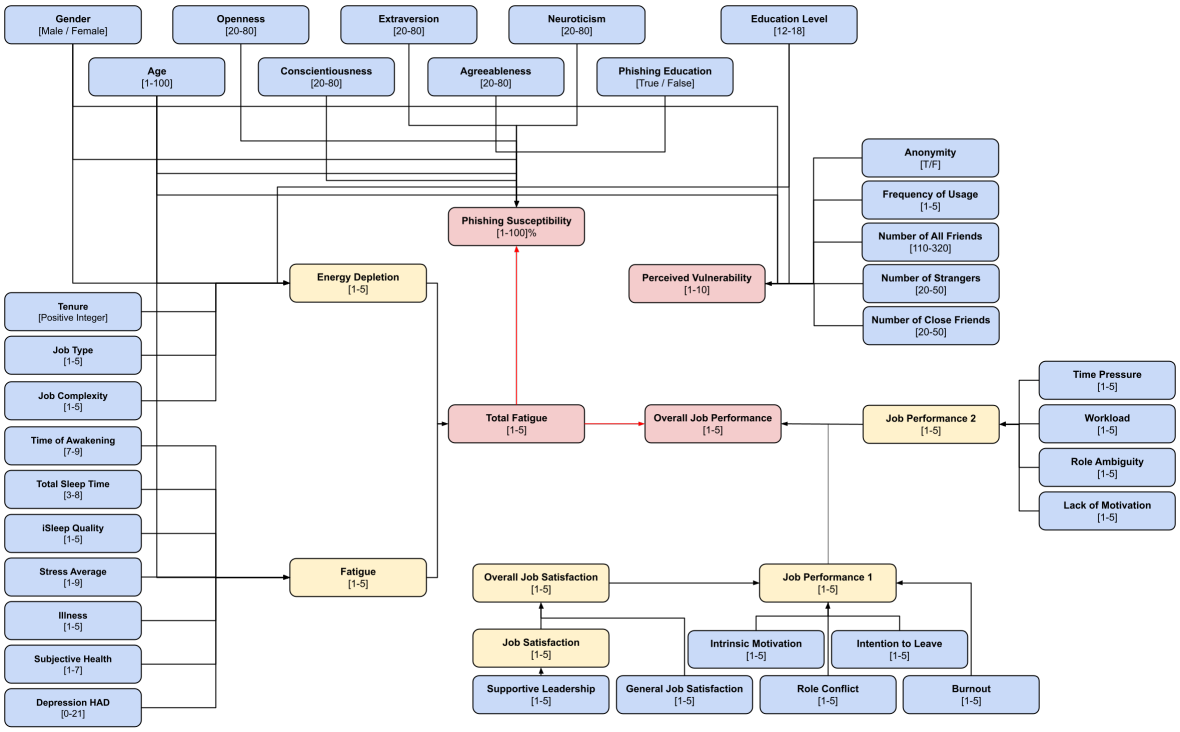

Figure 1: Comprehensive Human Factor Model of End User Agents

4.1.1 Phishing susceptibility

Eftimie et al. conducted an empirical study to predict end users' phishing susceptibility based on age, gender, and the Big Five personality traits (Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism) measured on a 20-80 scale (Eftimie et al., 2022). This study, conducted before and after cybersecurity education, led to the development of two logistic regression models. Each model predicts phishing susceptibility based on these human factors. We employed these logistic regression models to assess the initial phishing susceptibility of each end user agent.

Table 1: Equations for Phishing Susceptibility before and after cybersecurity education (Eftimie et al., 2022)

Phishing Susceptibility Before Education	$\frac{1}{1+e^{-(-7.33-0.011\times\text{Age}-0.191\times\text{Gender}-0.072\times O-0.065\times C+0.075\times E+0.1\times A+0.063\times N)}}$
Phishing Susceptibility After Education	$\frac{1}{1+e^{-(-3.87-0.092\times\text{Age}+0.696\times\text{Gender}-0.066\times O-0.072\times C+0.06\times E+0.025\times A+0.114\times N)}}$

* O: Openness, C: Conscientiousness, E: Extraversion, A: Agreeableness, N: Neuroticism

4.1.2 Perceived vulnerability

In our study, we examined the perceived vulnerability of end users to cyber threats, employing a model based on empirical findings from Alqarni et al. This research outlines a regression model designed to predict perceived vulnerability based on several independent variables: gender, anonymity, age, education level, frequency of social network service (SNS) usage, and the number of total, stranger, and close friends on SNS

platforms (Alqarni et al., 2016). Due to the absence of variable ranges in Alqarni et al.'s original study, as depicted in our Figure 1, we established our own ranges for these variables. These ranges ensure that the perceived vulnerability scores consistently fall between 1 and 10. We categorize perceived vulnerability scores from 1 to 3 as 'Low', from 4 to 7 as 'Medium', and from 8 to 10 as 'High'.

Table 2: Equation for Perceived Vulnerability (Alqarni et al., 2016)

Perceived Vulnerability
$3.896 - 0.013 \times \text{Gender} + 0.027 \times \text{Anon} + 0.046 \times \text{Age} - 0.048 \times \text{EL} - 0.034 \times \text{FoU} + 0.019 \times \text{NoAF} - 0.047 \times \text{NoS} - 0.051 \times \text{NoCF}$

* Anon: Anonymity, EL: Education Level, FoU: Frequency of Usage, NoAF: Number of All Friends, NoS: Number of Strangers, NoCF: Number of Close Friends

4.1.3 Job performance

To model the job performance, we leveraged two distinct regression models. The first model, developed by Rehman et al., predicts job performance based on variables such as current levels of burnout, intrinsic motivation, satisfaction, role conflict, and leave intention (Rehman et al., 2015). Additionally, we integrated the factor of supportive leadership by incorporating a model by Mwaisaka et al., which predicts job satisfaction based on levels of supportive leadership (Mwaisaka et al., 2019). The second model created by Basit et al. estimates job performance using variables including time pressure, workload, lack of motivation, and role ambiguity among employees (Basit and Hassan, 2017). These models collectively provide a comprehensive framework for assessing the job performance of end user agents under various conditions. After calculating job performance using the two distinct regression models, we averaged the results to provide a holistic assessment of the end user agents' job performance.

Table 3: Equation for Job Satisfaction (Mwaisaka et al., 2019), Job Performance 1 (Rehman et al., 2015), Job Performance 2 (Basit and Hassan, 2017), and Overall Job Performance.

Job Satisfaction	$0.094 + 0.716 \times \text{Supportive Leadership}$
Job Performance 1	$0.140 - 0.043 \times \text{BO} + 0.256 \times \text{IM} + 0.649 \times (\text{JS} + \text{GJS})/2 + 0.086 \times \text{RC} - 0.030 \times \text{LI}$
Job Performance 2	$5.5649 - 0.296 \times \text{TP} - 0.167 \times \text{WL} + 0.034 \times \text{LoM} - 0.307 \times \text{RA}$
Overall Job Performance	$(\text{Job Performance 1} + \text{Job Performance 2})/2$

* BO: Burnout, IM: Intrinsic Motivation, JS: Job Satisfaction, GJS: General Job Satisfaction, RC: Role Conflict, LI: Leave Intention, TP: Time Pressure, WL: Workload, LoM: Lack of Motivation, RA: Role Ambiguity

4.1.4 Fatigue

Fatigue is modeled in our study by integrating findings from two distinct empirical studies: one predicting energy depletion and the other predicting fatigue. The first study predicts energy depletion based on factors such as age, gender, education level, tenure, job type, and job complexity (Tian et al., 2022). The second study estimates fatigue based on variables including time of awakening, total sleep hours, sleep quality, average stress levels, illness, subjective health ratings, age, and depression (Åkerstedt et al., 2014). After calculating both energy depletion and fatigue scores individually, we average these values to provide a more generalized representation of fatigue levels in 1 to 5 scale.

Table 4: Equation for Energy Depletion (Tian et al., 2022), Fatigue (Åkerstedt et al., 2014), and Total Fatigue

Energy Depletion	$1.93 + 0.00 \times \text{Age} + 0.02 \times \text{Gender} + 0.14 \times \text{Education} + 0.00 \times \text{Tenure} - 0.12 \times \text{JT} + 0.43 \times \text{JC}$
Fatigue	$2.23 - 0.008 \times \text{ToA} - 0.012 \times \text{TST} - 0.096 \times \text{iSQ} + 0.035 \times \text{SA} + 0.070 \times \text{Illness} - 0.221 \times \text{SRH} - 0.011 \times \text{Age} + 0.050 \times \text{DH}$
Total Fatigue	$(\text{Energy Depletion} + \text{Fatigue})/2$

* JT: Job Type, JC: Job Complexity, ToA: Time of Awakening, TST: Total Sleep Time, iSQ: iSleep Quality,

SA: Stress Average, SRH: Subjective Health Rating, DH: Depression HAD

4.1.5 Impact of Fatigue on Phishing Susceptibility and Job Performance

Fatigue significantly affects phishing susceptibility and the overall job performance of end user agents. First, increased levels of fatigue correlate with diminished job performance. Hassan and Morsy demonstrated a relationship between fatigue and job performance in their regression model (Hassan and Morsy, 2023). Specifically, a 1-point increase in the fatigue score, which ranges from 0 to 10, corresponds to a decrease of 2.442 units in job performance, which is measured on a scale of 0 to 72. When adjusting this scale to the 1-5 scale that we use, each unit increase in fatigue results in a 0.34 unit decrease in job performance. This adjusted relationship was applied to determine the final job performance for each end user agent.

Table 5: Equation for Final Job Performance and Final Phishing Susceptibility.

Final Job Performance	$\text{Overall Job Performance} - 0.34 \times \text{Total Fatigue}$
Final Phishing Susceptibility	$\text{Random}[0, 100] < ((\text{Final Job Performance} - 1)/4 \times 100)\,?\,\text{PSBE} : \text{PSAE}$

* PSBE: Phishing Susceptibility Before Education, PSAE: Phishing Susceptibility After Education (Table 2)

Given the limited empirical studies directly investigating the link between phishing susceptibility and fatigue, we developed a method to estimate its impact. Drawing from Shin et al.'s list of potential human vulnerabilities, we focused on two specific vulnerabilities related to downloading and executing files from suspicious emails: EV1204.002-H1 and EV1204.002-H3 (Shin et al., 2023c). EV1204.002-H1 suggests that even when an end user agent recalls and follows the security policies learned during cybersecurity training, they may still be deceived by sophisticated social engineering tactics. EV1204.002-H3 indicates that the end user agent falls victim to a social engineering attack due to neglecting or forgetting the principles taught during cybersecurity training. In our simulation model, each end user agent's vulnerability is assessed every tick (second). For each tick, based on the agent's current final job performance, it is determined whether their phishing susceptibility prior to or after cybersecurity education is applied (Table 5). If phishing susceptibility before education is applied and a randomly generated number is lower than its threshold, EV1204.002-H3 is triggered. If phishing susceptibility after education is applied and a randomly generated number is lower than its threshold, EV1204.002-H1 is triggered. If the end user agent encounters a phishing email while either EV1204.002-H1 or EV1204.002-H3 is active, they become susceptible to the phishing attack, potentially leading to the compromise of their computing device.

Table 6: Human Vulnerabilities relevant to executing suspicious files attached to email (Shin et al., 2023c).

EV1204.002-H1	User succumbs to social engineering tactics, leading them to open malicious files, such as .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl, facilitating adversary-initiated code execution
EV1204.002-H3	User overlooks or dismisses user training, diminishing user's awareness of common phishing and spearphishing techniques and reducing their ability to raise suspicion for potentially malicious event

4.2 End User Agent Behavior Model

As depicted in Figure 2, we extend the human behavior model interacting with suspicious emails developed by Shin et al. (2023a). Their model includes two primary limitations. First, it incorporates a message board system that records outcomes of phishing inspections. This system allows end user agents to consult recorded data to classify phishing emails. However, such a defensive strategy is not commonly implemented in contemporary organizational settings. Second, the model relies on abstract variables such as cybersecurity expertise and motivation to influence decision-making processes. They also applied different values to these factors without grounding them in any empirical human factors data.

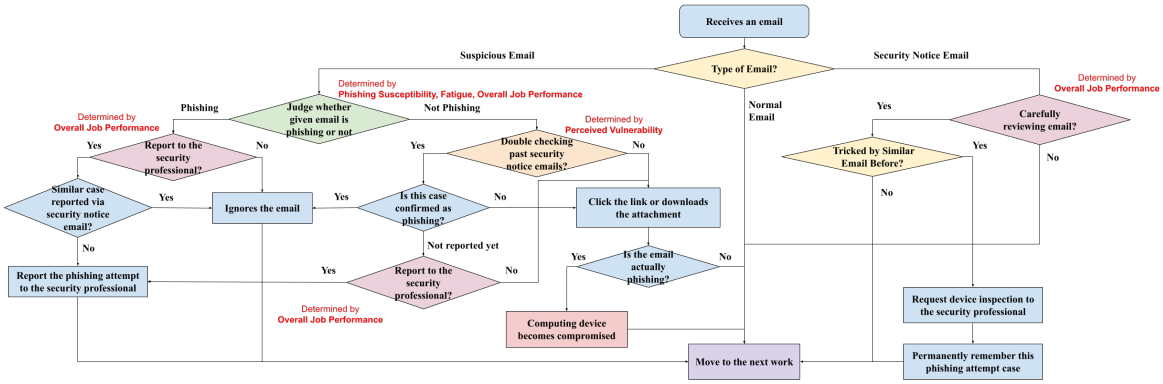

Figure 2: Decision-Making Process of End User Agents in Response to Emails

To enhance realism in the behavior model, we replaced the message board system with a series of steps that model decision-making processes using specific, measurable human factors. Initially, when an end user agent encounters a security notice email, it must decide whether to read it carefully. This decision is influenced by the agent's overall job performance score. If it opts to read the email and recognizes that it previously fell victim to a similar phishing attack, resulting in malware installation, it will report this to a security professional agent. Upon receiving a suspicious email, the end user agent must assess whether the email is a phishing attempt, guided by its phishing susceptibility score. If deemed a phishing email, the agent then decides whether to report this to a security professional. Part of this decision involves checking if a similar case has already been reported or announced within the organization through a security notice email. If it has not been reported, the agent will report the suspicious email. If the agent concludes the email is not a phishing attempt, it must decide whether to verify this against past security notice emails, influenced by its perceived vulnerability score. After reviewing previous notices, if the case is confirmed as a phishing attempt, the agent will disregard the email. If it is unreported, the agent must decide whether to report it, determined again by its job performance score. If the agent chooses not to recheck past emails or report the suspicious email, it may proceed to download and interact with the attachment within the email. If the email is indeed a phishing attempt, the agent's computing device will become compromised, granting the cybercriminal agent access.

5. Cyber Defense and IT Security Behavior Model

In this simulation model, we deployed two distinct types of IT security agents. The first agent is tasked with examining suspicious phishing emails. Based on Bykowski's findings, we assume it takes an average of 27 minutes to manually triage one phishing email (Bykowski, 2022). If an email is confirmed as a phishing attempt, this agent sends a warning email to all organization members, providing detailed information about the phishing threat. The second IT security agent handles inspection requests for computing devices from organization members. During the inspection, if a device is found to be compromised, the agent remedies the issue and severs any suspicious connections to the device.

6. Virtual Experiments

In this section, we detail the virtual experiments conducted using the simulation models described in previous sections. These experiments aim to investigate the impact of various human factors on the overall damage resulting from a spearphishing campaign. Through the simulation, the organizational damage is quantified by the total number of end user agents deceived and the total volume of data exfiltrated. We manipulate the human factor variables illustrated in Figure 1 to assign perceived vulnerability levels as low, medium, or high. The overall job performance of all end user agents is set within the ranges of [2-3], [3-4], or [4-5], and fatigue levels are adjusted to fall within the [2-3], [3-4], and [4-5] ranges. This results in a total of 27 distinct experimental conditions. For each condition, we will conduct 30 simulations, culminating in 810 simulations overall to robustly assess the effects of these variables on spearphishing campaign outcomes.

Table 6: Summary of Virtual Experiments

Type	Name	Implication
Independent Variables	Perceived Vulnerability	Low [1-3], Medium [4-7], High [8-10]
	Overall Job Performance	[2-3], [3-4], [4-5]
	Fatigue Level	[2-3], [3-4], [4-5]
Dependent Variables	Number of Tricked Users	Total number of tricked end user agents
	Total Data Exfiltrated	Total data exfiltrated in Gigabyte (GB)
Control	Virtual Organization	Virtual medium-sized company with 235 end user agents. Each end user agent is assigned with one personal computer device agent. Each device agent contains 10 Gigabyte (GB) crucial data.
	Spearphishing Campaign	Three spearphishing campaigns with 20 different types of spearphishing emails that target the virtual organization to exfiltrate data from each end user agent's PC.
	Cyber Defense Strategy	Security Alert Email & Computing Device Inspection
	Number of Simulations Per Case	30

6.1 Simulation Results

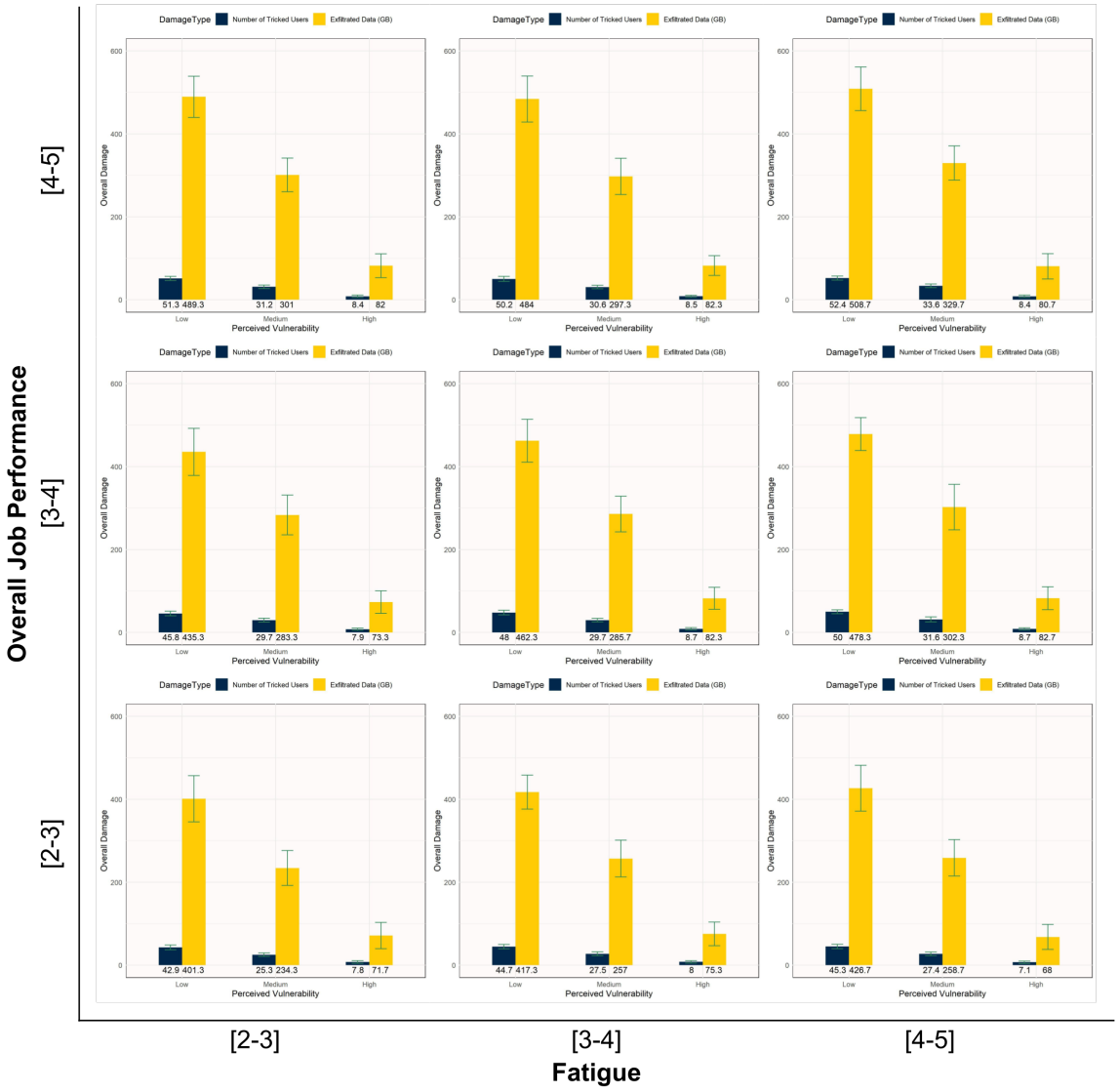

Figure 3: Simulation Results

Figure 3 illustrates the overall damage experienced by a virtual organization after a simulated spearphishing campaign, based on the organization's average levels of fatigue, overall job performance, and perceived vulnerability. In general, simulation results shows that as perceived vulnerability increases, and both fatigue and overall job performance decrease, the overall damage to the organization, measured by the number of tricked users and total exfiltrated data in gigabytes (GB), tends to decrease.

6.2 Statistical Analysis and Discussion

Table 7: Regression Table1 - Correlation between Average Job Performance, Fatigue, and Perceived Vulnerability and the Number of Tricked Users

	B	*SD B*	β	*t*	*p*
(Constant)	65.556	1.003		65.389	<0.0001
Average Job Performance	-2.292	0.214	-0.002	-10.693	<0.0001
Average Fatigue	0.608	0.158	0.001	3.841	0.0001
Average Perceived Vulnerability	-5.584	0.057	-0.020	-98.608	<0.0001

Table 8: Regression Table2 - Correlation between Average Job Performance, Fatigue, and Perceived Vulnerability and the Total Exfiltrated Data (GB).

	B	*SD B*	β	*t*	*p*
(Constant)	637.415	9.826		64.870	<0.0001
Average Job Performance	-26.530	2.101	-0.003	-12.629	<0.0001
Average Fatigue	7.129	1.551	0.001	4.596	<0.0001
Average Perceived Vulnerability	-53.245	0.555	-0.020	-95.935	<0.0001

As shown in Table 7 and Table 8, we conducted a statistical analysis to examine the correlation between an organization's average job performance, fatigue, and perceived vulnerability and the number of tricked users and the total exfiltrated data (GB). The results of the analysis indicate that average job performance and perceived vulnerability are negatively correlated with organizational damage from a spearphishing campaign, while fatigue is positively correlated with organizational damage. Based on these simulation results and statistical analysis, we developed three hypotheses:

> ***Hypothesis 1****: As an organization's job performance increases, the number of tricked users and the total data exfiltrated during a spearphishing campaign decrease.*
>
> ***Hypothesis 2****: As an organization's perceived vulnerability increases, the number of tricked users and the total data exfiltrated during a spearphishing campaign decrease.*
>
> ***Hypothesis 3****: As an organization's fatigue increases, the number of tricked users and the total data exfiltrated during a spearphishing campaign increase.*

An analysis of the standardized beta values illustrated in Table 7 and Table 8 shows that in both tables, the absolute beta value for average perceived vulnerability is the largest, followed by job performance, and then fatigue. This indicates that perceived vulnerability has the greatest impact on overall organizational damage from spearphishing campaign, with job performance being the second most influential factor and fatigue the least. Therefore, based on these simulation results, to effectively improve the organization's social cybersecurity (Carley, 2020) against phishing campaigns, organizations should prioritize improving employees' perceived vulnerability. Specifically, they should educate employees to not rely solely on intuition when encountering suspicious emails but to refer back to previously issued security alert emails and actively communicate with internal cybersecurity experts. Next, organizations should focus on researching how to improve overall job performance by enhancing employee satisfaction and motivation and fostering a positive organizational culture. Finally, if budget permits, organizations should explore ways to support employees in reducing fatigue, potentially through organizational-level support and policy initiatives. For organizations with limited cybersecurity budgets, it's crucial to consider these priorities when developing policies to maximize the impact of cybersecurity efforts against phishing attacks.

7. Conclusion and Future Works

In this paper, we computationally modeled and simulated three dynamically changing human factors: perceived vulnerability, fatigue, and job performance, to accurately capture how these factors correlate with overall organizational damage during a spearphishing campaign targeting end users for data exfiltration. Our simulation results demonstrate that perceived vulnerability and job performance have a negative correlation with damage, while fatigue has a positive correlation. According to the statistical analysis of the simulation results, to effectively mitigate damage from spearphishing campaigns, organizations should prioritize improving perceived vulnerability, followed by focusing on enhancing overall job performance, and lastly, identifying ways to reduce fatigue. In future work, we plan to model more diverse human vulnerabilities, such as end users' tendency to postpone crucial operating system updates or their susceptibility to granting access to suspicious users. By incorporating relevant computational human factors, we aim to accurately model and evaluate the potential damage associated with these human vulnerabilities. Furthermore, we will assess how different defensive solutions impact various human factors and, consequently, correlate with an organization's overall resilience and robustness to cyberattacks.

Acknowledgements

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was supported in part by the Minerva Research Initiative under Grant #N00014-21-1-4012 and by the Center for Computational Analysis of Social and Organizational Systems (CASOS) at Carnegie Mellon University. The views and conclusions are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Office of Naval Research or the US Government.

References

Åkerstedt, T., Axelsson, J., Lekander, M., Orsini, N., & Kecklund, G. (2014). Do sleep, stress, and illness explain daily variations in fatigue? A prospective study. *Journal of psychosomatic research*, *76*(4), 280-285.

Alqarni, Z., Algarni, A., & Xu, Y. (2016, June). Toward predicting susceptibility to phishing victimization on Facebook. In *2016 IEEE International Conference on Services Computing (SCC)* (pp. 419-426). IEEE.

Basit, A., & Hassan, Z. (2017). Impact of job stress on employee performance. *International Journal of Accounting and Business Management*, *5*(2), 13-33.

Blythe, J., Botello, A., Sutton, J., Mazzocco, D., Lin, J., Spraragen, M., & Zyda, M. (2011, August). Testing cyber security with simulated humans. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 25, No. 2, pp. 1622-1627).

Burns, A. J., Posey, C., Courtney, J. F., Roberts, T. L., & Nanayakkara, P. (2017). Organizational information security as a complex adaptive system: insights from three agent-based models. *Information Systems Frontiers*, *19*, 509-524.

Bykowski, K. (2022, September 26). *Don't take the bait: Automated phishing investigation and response*. AI-enhanced Security Automation. https://swimlane.com/blog/soar-automated-phishing-investigation-and-response/

Carley, K.M., Fridsma, D.B., Casman, E., Yahja, A., Altman, N., Li-Chiou Chen, Kaminsky, B. and Nave, D. (2006). BioWar: scalable agent-based model of bioattacks. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 36(2), pp.252–265

Carley, K. M. (2020). Social cybersecurity: an emerging science. *Computational and mathematical organization theory*, *26*(4), 365-381.

Eftimie, S., Moinescu, R., & Răcuciu, C. (2022). Spear-phishing susceptibility stemming from personality traits. *IEEE Access*, *10*, 73548-73561.

Kamal Hassan, S. M., & Morsy, S. M. (2023). Effect of Work Conditions and Fatigue on Job performance of Staff Nurse's at Al Eman General Hospital. *Assiut Scientific Nursing Journal*, *11*(34), 317-327.

Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: state of the art and future directions. *Journal of Cybersecurity*, *7*(1), tyab005.

Macal, C. M., & North, M. J. (2009, December). Agent-based modeling and simulation. In *Proceedings of the 2009 winter simulation conference (WSC)* (pp. 86-98). IEEE.

Mwaisaka, D. M., Ouma, C., & K'Aol, G. (2019). Influence of supportive leadership style on employee job satisfaction in commercial banks in Kenya. *Journal of Human Resource and Leadership*, *4*(1), 44-66.

Rehman, W. U., Janjua, S. Y., & Naeem, H. (2015). Impact of burnout on employees' performance: an analysis of banking industry. *World Review of Entrepreneurship, Management and Sustainable Development*, *11*(1), 88-105.

Shin, J., Dobson, G. B., Carley, K. M., & Carley, L. R. (2022, September). OSIRIS: organization simulation in response to intrusion strategies. In *International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation* (pp. 134-143). Cham: Springer International Publishing.

Shin, J., Dobson, G. B., Carley, K. M., & Carley, L. R. (2022). Leveraging OSIRIS to simulate real-world ransomware attacks on organization. In *2022 Winter Simulation Conference (WSC) Poster Session*.

Shin, J., Carley, L. R., Dobson, G. B., & Carley, K. M. (2023, May). Modeling and simulation of the human firewall against phishing attacks in small and medium-sized businesses. In *2023 Annual Modeling and Simulation Conference (ANNSIM)* (pp. 369-380). IEEE.

Shin, J., Carley, K. M., & Carley, L. R. (2023, September). Integrating Human Factors into Agent-Based Simulation for Dynamic Phishing Susceptibility. In *International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation* (pp. 169-178). Cham: Springer Nature Switzerland.

Shin, J., Dobson, G. B., Carley, L. R., & Carley, K. M. (2023) Revelation of System and Human Vulnerabilities Across MITRE ATT&CK Techniques with Insights from ChatGPT.

Shin, J., Carley, L. R., & Carley, K. M. (2024, May). Simulation-Based Study on False Alarms in Intrusion Detection Systems for Organizations Facing Dual Phishing and Dos Attacks. In *2024 Annual Modeling and Simulation Conference (ANNSIM)* (pp. 1-13). IEEE.

Shin, J., Dobson, G. B., Carley, L. R., & Carley, K. M. (2024). *Design, Modeling and Simulation of Cybercriminal Personality-based Cyberattack Campaigns.* In *2024 Winter Simulation Conference (WSC).* Forthcoming.

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). MITRE ATT&CK: Design and philosophy. In *Technical report*. The MITRE Corporation.

Tian, Q., Bai, J., & Wu, T. (2022). Should we be" challenging" employees? A study of job complexity and job crafting. *International Journal of Hospitality Management*, *102*, 103165.