MODELING AND SIMULATION OF THE HUMAN FIREWALL AGAINST PHISHING ATTACKS IN SMALL AND MEDIUM-SIZED BUSINESSES

Jeongkeun Shin
L. Richard Carley

Department of Electrical and Computer Engineering
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA, USA
{jeongkes,lrc}@andrew.cmu.edu

Geoffrey B. Dobson
Kathleen M. Carley

School of Computer Science
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA, USA
{gdobson,kathleen.carley}@cs.cmu.edu

ABSTRACT

Small and medium-sized businesses (SMBs) are increasingly targeted by cybercriminals due to their limited cybersecurity budgets and lack of expertise. This paper proposes an alternative solution to the advanced but expensive security plan by employing a human firewall system. The system comprises a group of end-user agents with a cybersecurity expertise agent who can detect and prevent cyberattacks. We evaluate the proposed system's effectiveness in mitigating cyber attack damage in SMBs using agent-based modeling and simulation. Our results show that if the end-user agents have above-average cybersecurity expertise and cybersecurity motivation, the proposed human firewall strategy can be a comparable or better defensive tactic than employing an advanced security plan. Our paper provides insights for SMBs on how to allocate their limited cybersecurity budgets to build a human firewall system to mitigate cyber attack damage.

Keywords: Cybersecurity, Human Firewall, Knowledge Sharing, Community Learning.

1 INTRODUCTION

Cyberattacks are a major concern for small and medium-sized businesses (SMBs) as they often lack the resources to invest in advanced security systems. (Imagine IT 2022). Many SMBs adopt basic security plans, which are often inadequate against sophisticated attacks such as phishing campaigns. Employees at SMBs with less than 100 employees receive 350% more social engineering attacks than employees at a large business (Barracuda 2022). As a result, in 2021, 47% of all SMBs experienced cyberattacks, and 60% of them could not recover from them (Zinnov 2022). In this paper, we propose an alternative strategy for SMBs with limited cybersecurity budgets: building a human firewall system, which involves leveraging the knowledge and behavior of employees to enhance the organization's security posture. This strategy does not confine the security issues to the technological problems but gives equal attention to human management and worker behavior (Whitman et al. 2005). To successfully manage this system, employees should be trained to react to threat activities and report threat incidents effectively so that security professionals can take proper action (Williams et al. 2021). We use agent-based modeling and simulation (Macal and North 2009) to investigate the effectiveness of this strategy and compare it against the use of advanced security plans. Our work contributes to the literature by highlighting the potential of human firewall systems as a viable option for SMBs with limited cybersecurity budgets to enhance their security posture.

2 RELATED WORKS

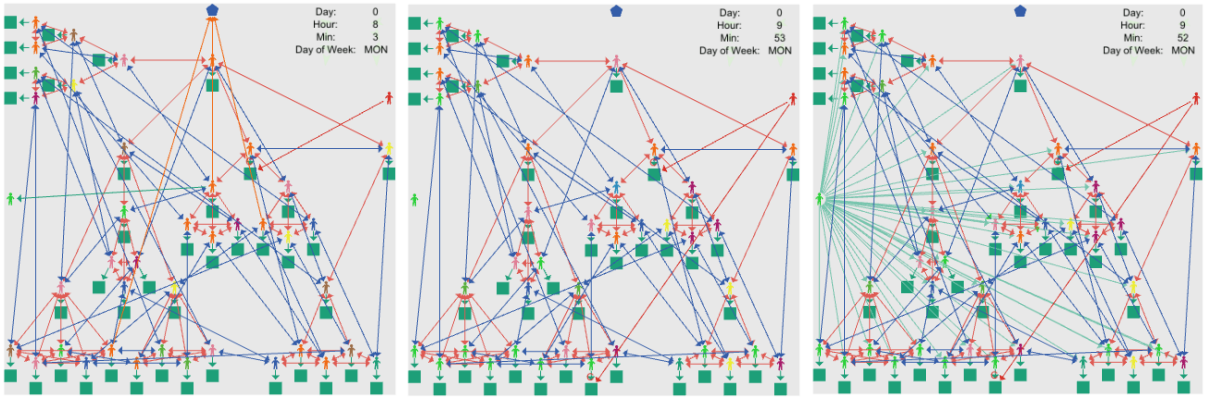
Cybercriminals initiate phishing attacks by sending emails or messages to targeted end users in the organization. These emails and messages induce targeted end users to click the malicious link or download the malware attachment. In this way, despite using security systems, cybercriminals could effortlessly bypass the defense system, gain unauthorized access, and exfiltrate sensitive information (Bhardwaj et al. 2021). Because of the advantage of bypassing sophisticated security technological systems, phishing has been one of the most popular cyberattacks. According to IBM, over 95% of security incidents starts from "human error", and the most common human error is "Double Clicking" a malicious attachment or unsafe URL (IBM. 2014). As the human problem gets equal attention in information security (Whitman et al. 2005), the importance of increasing the overall cyber situational awareness (Jajodia et al. 2009) by educating employees on cybersecurity knowledge and building the cybersecurity culture in the organization has been emphasized, and various human firewall models and strategies were introduced.

Rajivan and Cooke used human-in-the-loop experiments and agent-based modeling to demonstrate that improvements to teamwork and team interactions can augment the security situational awareness and overall cybersecurity defense performance in the organization (Rajivan and Cooke 2017). Dobson and Carley used the Cyber-FIT framework (Dobson and Carley 2017) to measure the cyber situational awareness in various military environments (Dobson and Carley 2018). El Hajal et al. created a human firewall with an AI-based conversational bot to enhance security by raising users' cyber awareness (El Hajal, Daou, and Ducq 2021). The chatbot automatically evaluates a user's security weakness and proposes proper security training. Elharmeel suggests building the human firewall by employing an individual to defend human-based cyberattacks targeting employees within the organization using awareness sessions and information traversal inspection (Elharmeel 2009). Jensen et al. used the knowledge management approach where an individual combats phishing attacks collectively with other organization members using the message board system where all employees report suspicious emails and the result of phishing confirmation are shared (Jensen, Durcikova, and Wright 2017).

To build a robust human firewall, motivating the employees in the organization to contribute to building the human firewall is essential. As the model of Jensen et al. (Jensen, Durcikova, and Wright 2017), if a human firewall is built with a knowledge sharing approach, three factors control the employees' willingness to share knowledge in the organization: Extrinsic rewards, an employee's desire to maintain relationships with others, and the employee's self-worth that considers his knowledge sharing provides value to the organization (Bock et al. 2005). Vance et al. used the Protection Motivation Theory (PMT) (Rogers 1975) model to demonstrate that making employees recognize the risk of security threats and ensuring employees that complying with security policies is also their responsibility are crucial to motivate employees to follow the security policies (Vance, Siponen, and Pahnila 2012). Burns et al. designed agent-based models based on the Protection Motivation Theory (Rogers 1975) and General Deterrence Theory (Blumstein, Cohen, and Nagin 1978) to test how the level of punishment or security education motivates agents to improve organizational information security (Burns et al. 2017).

3 MODEL DESIGN

In this section, we describe our model design, which encompasses a virtual organization, a real-world phishing campaign, a security system, and a human firewall system. To create the model, we utilized Repast Simphony (North et al. 2013), a Java-based agent-based modeling tool. Each simulation step in Repast Simphony represents a 'tick', which we equate to one minute. We also track time and days of the week during simulation, with each session running for 129,600 ticks, equivalent to 90 days. Our model includes two simulation options: "Normal Mode" and "Human Firewall Mode". The key differences between the two



(a) (b) (c)

Figure 1: Virtual Organization Built with OSIRIS Framework. (a) End user agents look up a human firewall for more accurate phishing classification. (b) Cybercriminal agent exploits end user agents' computing devices. (c) A security professional agent makes notifications to end user agents about new phishing attempts.

are the behavioral patterns of the end user agents when receiving emails and the cyber defense strategies employed by the security professional agent.

3.1 Small and Medium-sized Business (SMB)

We reimplemented the OSIRIS (Shin et al. 2022) framework using Repast Simphony (North et al. 2013) and utilized it to build a customized virtual SMB composed of 40 end user agents. Within the SMB, we deployed seven different types of end user agents, each with unique work behavior patterns. These agents included 5 engineering managers, 15 software engineers, 9 general office workers, 5 human resource workers, and 6 data scientists. The end user agents in our virtual organization possess the following characteristics:

- Within the virtual organization, end user agents form a social network based on both formal and informal relationships. Formal relationships (Red links in Figure 1) are established when two agents must communicate in the course of their work, while informal relationships (Blue links in Figure 1) are based on personal connections, such as friendships. Each end user agent is arbitrarily assigned three informal relationships.
- All end user agents work from 8 AM to 5 PM during weekdays.
- All end user agents have one computing device (Square Objects in Figure 1).
- Email is the only communication tool used in the organization, and end user agents communicate with others connected by either formal or informal relationships, receiving around 100 emails daily from both inside and outside the organization. Emails may contain links, attachments, or both.
- Each end user agent is assigned a **Cybersecurity Expertise Level** from 1 to 5, with a higher level indicating greater cybersecurity training and experience. End user agents with higher levels are better at identifying malicious phishing emails and less likely to misclassify a normal email as phishing.
- Each end user agent has a **Cybersecurity Motivation Level** ranging from 1 to 5, which is only used in the human firewall simulation mode. We assume that a higher level of motivation results from higher rewards for reporting new phishing attempts or stronger penalties for being tricked by phishing emails. End user agents with higher motivation levels are more likely to use the human firewall system when identifying phishing emails and more active in reporting suspicious emails to the security professional agent.

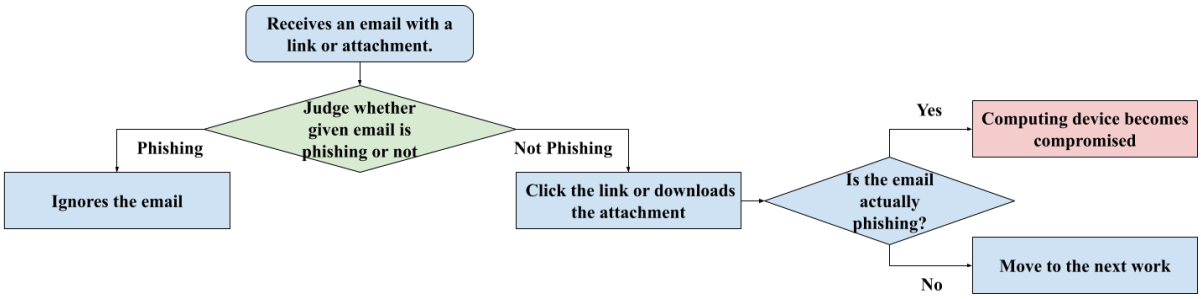


Figure 2: The flowchart of the end user agent's behavior pattern in the normal mode.

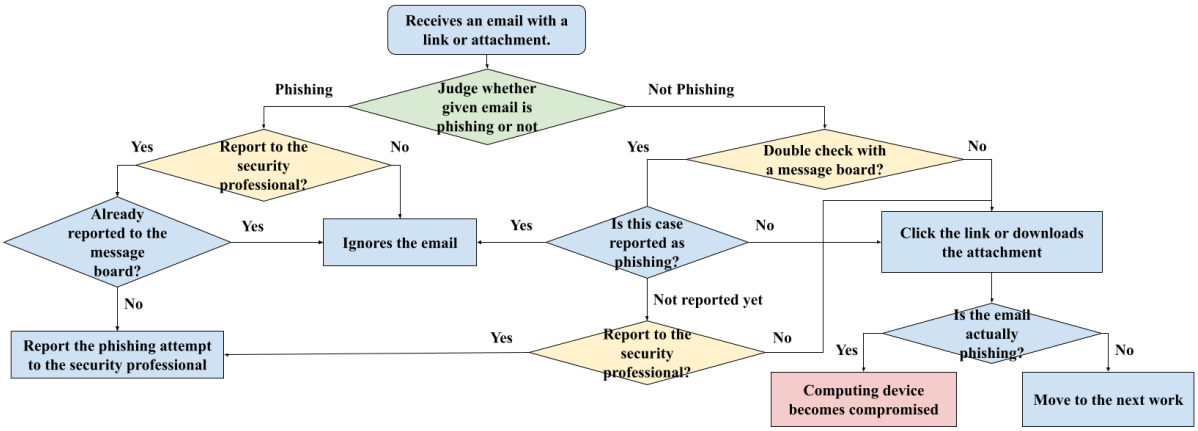


Figure 3: The flowchart of the end user agent's behavior pattern in the human firewall mode.

3.1.1 Behavior Pattern of the End User Agent

The behavior patterns of the end user agent when receiving a new email with a link or attachment are depicted in Figure 2 and Figure 3 for the normal mode and human firewall mode, respectively. In the green diamond state, the end user agent evaluates whether the email is a phishing attempt or not. The accuracy of this judgment increases with the end user agent's cybersecurity expertise level. Figure 3 shows three yellow diamond states (Report to the security professional? & Double check with a message board?) that represent decision-making processes regarding whether to contribute to the human firewall. The probability of the output being 'Yes' increases with a higher cybersecurity motivation level.

3.2 Phishing Campaign

During the simulation, we will conduct a phishing attack campaign, which is a common social engineering attack used by cybercriminals to target small and medium-sized businesses (Barracuda 2022). To carry out this campaign, we will use the Cyber-FIT framework (Dobson and Carley 2017), which imitates realistic adversarial behaviors by following the attacking steps in the cyber-kill chain (Dobson, Rege, and Carley 2018). We will deploy Cyber-FIT's attacking force as a cybercriminal agent in the virtual organization (Red-colored Human Object in Figure 1) and have it conduct the phishing attack based on the MITRE ATT&CK framework (Strom et al. 2018) instead of the cyber-kill chain as the MITRE ATT&CK framework provides more detailed steps of a cyberattack. The MITRE ATT&CK framework provides information on how each real-world cybercriminal group's cyberattack campaign is composed of various step-by-step

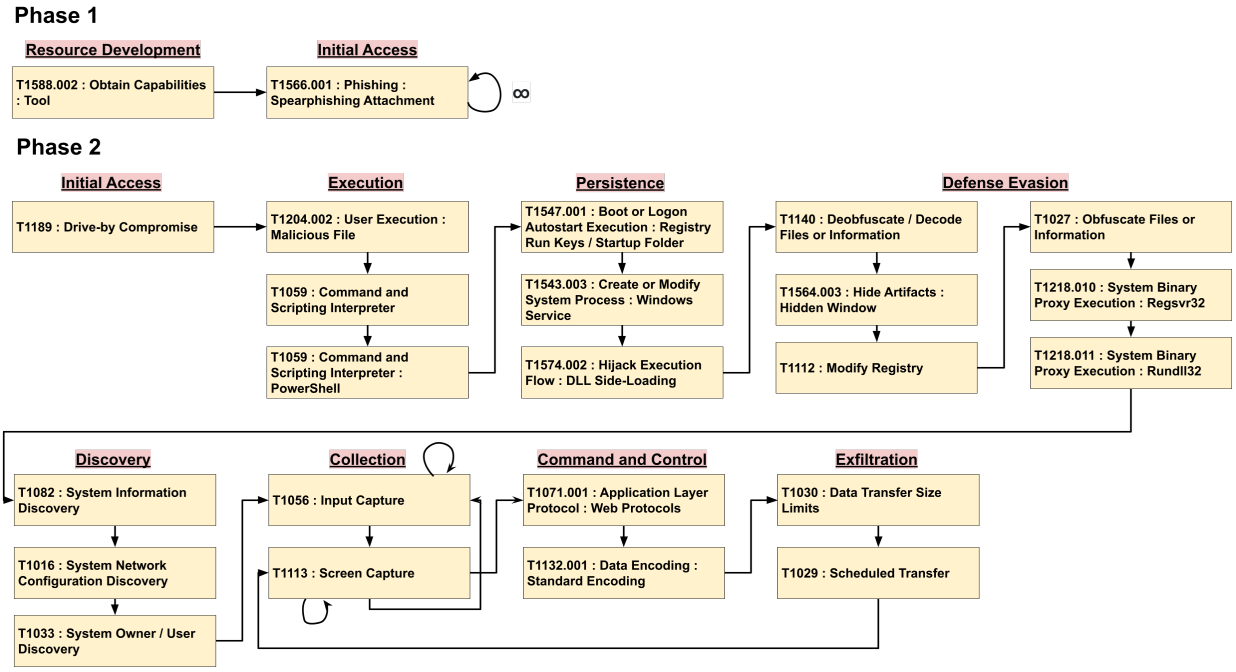


Figure 4: The cybercriminal agent's MITRE ATT&CK based phishing attack scenario.

tactics and techniques, including the malware software used. Our cybercriminal agent will imitate the attack patterns of **APT 19**, a cybercriminal group that conducts phishing attacks on various industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services (MITRE 2021). This group uses two different malware, Cobalt Strike and Empire, and its phishing campaign comprises 9 tactics and 24 techniques (MITRE 2021). Since it is unclear what attack techniques are used to collect information from computing devices, we added two attack techniques, Input Capture (T1056) and Screen Capture (T1113), in the Collection tactic (TA0009), which can be performed using Cobalt Strike. Therefore, the cybercriminal agent's phishing campaign in our model is composed of 10 MITRE ATT&CK tactics and 26 techniques.

The phishing campaign, as illustrated in the flowchart in Figure 4, is divided into two phases: Phase 1 and Phase 2. In Phase 1, when the simulation starts, the cybercriminal prepares the required malware for phishing attacks (Resource Development) and periodically sends a spearphishing email to end user agents until one end user agent becomes tricked and its computing device becomes compromised (Initial Access). Before running the simulation, the user can determine the number of types of phishing emails. In this tactic, the cybercriminal agent randomly selects one type of phishing email and delivers it. As soon as one end user agent's computing device becomes compromised in the virtual SMB, the cybercriminal agent moves on to Phase 2. After remotely accessing the computing device, it executes the malicious files (Execution), changes the system setting to maintain access (Persistence), applies methods to avoid detection (Defense Evasion), gathers system information (Discovery), collects data by input or screen captures (Collection), sets up command and control communication (Command and Control), and exfiltrates the collected data (Exfiltration). In the 'Collection' tactic, the cybercriminal agent collects one piece of information every minute. After finishing the first cycle of Phase 2, the cybercriminal has a period of inactivity on this computing device. After the inactivity period ends, if the computing device is still compromised (not inspected and fixed by a security professional agent yet), the cybercriminal agent periodically collects additional data and exfiltrates it. Details of tactics and techniques can be found on the MITRE ATT&CK website (MITRE 2021).

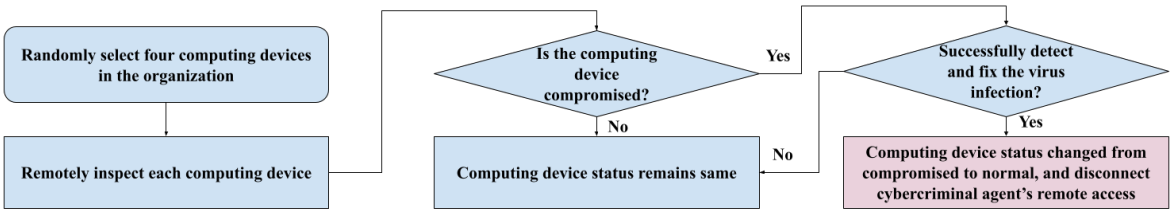


Figure 5: The flowchart of the security professional agent's behavior pattern in the normal mode.

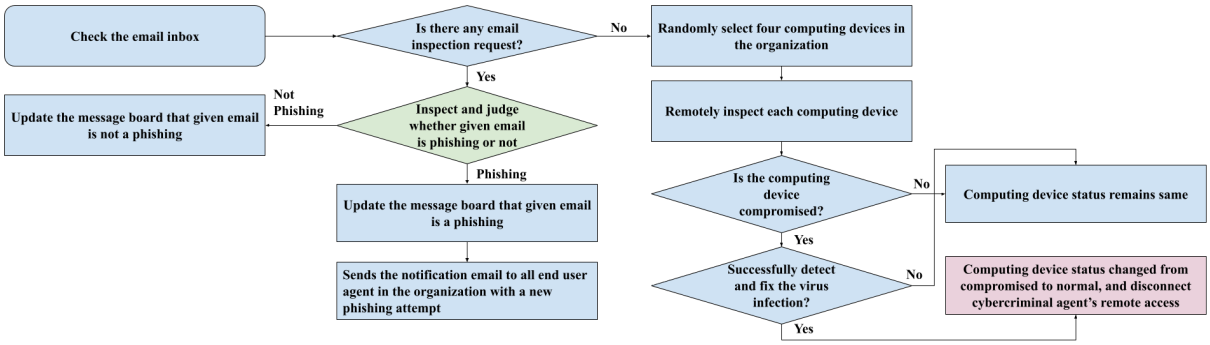


Figure 6: The flowchart of the security professional agent's behavior pattern in the human firewall mode.

According to RiskIQ, the average cost of a breach is $7.2 per minute (RiskIQ 2022). Therefore, we consider each piece of data collected every minute to be worth $7.2. The total damage after the phishing campaign simulation is calculated by **($7.2 x the total number of successfully exfiltrated data)**.

3.3 Security System & Human Firewall System

In the virtual organization, we use the defensive troops of Cyber-FIT (Dobson and Carley 2017) as security professional agents (Yellow-green human object in Figure 1) to safeguard the organization's assets against cybercriminals and minimize cyberattack damage by utilizing the provided security resources. Security professional agents possess the following characteristics:

- Security Professional Agents have the highest **level of cybersecurity expertise**, 5. According to the original OSIRIS paper (Shin et al. 2022), an end user agent with the highest cybersecurity expertise level of 5 has 99.265% accuracy in identifying phishing emails.
- The organization can either have a **Basic Security Plan** or an **Advanced Security Plan**. With the **Basic Security Plan**, there is a 20% chance of successfully detecting and fixing the compromised computing device, while the **Advanced Security Plan** raises the success probability to 50%. These probabilities are based on the assumption that the advanced security plan has more advanced detection and mitigation capabilities.
- The behavior pattern of the security professional agent in 'Normal Mode' is shown in the flowchart in Figure 5. Every 30 minutes, the security professional agent randomly selects four computing devices to inspect. If a virus is identified and removed from the compromised computing device, the cybercriminal agent loses its connection and can no longer exploit it. If the security professional agent fixes the last compromised computing device in the organization, the cybercriminal agent is forced to revert to Phase 1, distributing phishing emails again until it tricks another end user agent, and their computing device gets compromised.

3.3.1 Human Firewall System

In this paper, we utilize Jensen et al.'s knowledge management approach (Jensen, Durcikova, and Wright 2017) to build a human firewall system. At the start of the simulation in the 'Human Firewall Mode', the online message board (Pentagon Object in Figure 1) is activated. As described in Section 3.1.1, end user agents report suspicious emails to the security professional agent, which then reviews and determines if the reported email is a phishing attempt. Each review takes between 10 to 20 minutes. If the email is confirmed to be phishing, the message board is updated with the email information and phishing confirmation, and a warning email containing the phishing email information is sent to all end user agents in the organization. End user agents with higher cybersecurity motivation levels are more likely to read the warning email more carefully and become more resistant to the same type of phishing email. Therefore, if the same type of phishing email is received by an end user agent again, they can automatically identify it as phishing and ignore it. As depicted in Figure 6, in the 'Human Firewall Mode', the security professional agent prioritizes the development of a robust human firewall by reviewing reported emails. If there are no email inspection requests remaining, it proceeds to inspect computing devices following the same process as in the 'Normal Mode'.

4 VIRTUAL EXPERIMENT

In this section, we conduct two virtual experiments to answer the following research questions: 1) Can the human firewall system effectively mitigate the magnitude of damage caused by cyberattacks? 2) If so, can we conclude that using a basic security plan with the human firewall system can replace the advanced security plan?

Experiment 1: We simulate our model in the 'Normal Mode' with variations in the security plan and the cybersecurity expertise level to examine the effectiveness of different security plans and cybersecurity expertise levels in mitigating damage. Specifically, we investigate how using the Advanced Security Plan is more effective than using the Basic Security Plan and how keeping the end user agents' cybersecurity expertise level high helps mitigate the damage. Since there are 5 different values for the cybersecurity expertise level and 2 different values for the security plan, there are 10 cells, and we run 30 simulations for each cell. Table 1 summarizes the simulations for this experiment.

Experiment 2: We simulate our model in the 'Human Firewall Mode' to investigate how the cybersecurity expertise level and cybersecurity motivation level influence the magnitude of the cyberattack damage when the human firewall system is used. In this experiment, the security plan is fixed with a 'Basic Security Plan', and we vary the cybersecurity expertise level and cybersecurity motivation level. Since there are 5 different values for both the cybersecurity expertise level and cybersecurity motivation level, there are 25 cells, and we run 30 simulations for each cell. Table 2 summarizes the simulations for this experiment.

4.1 Experiment Results

The results of the two experiments are presented in Figure 7 and Figure 8. Figure 7 shows that if all other parameters are fixed, the overall damage decreases as the cybersecurity expertise level increases. Moreover, the SMB with the advanced security plan suffers 47% to 60% less damage than the SMB with the basic security plan when all other conditions are the same.

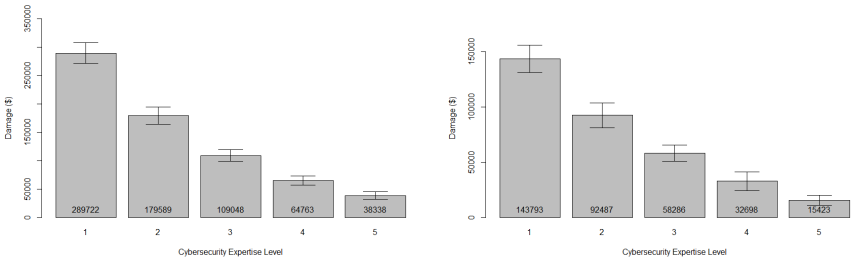
Figure 8 illustrates the result of the second experiment. The findings reveal that a higher cybersecurity motivation level guarantees less overall cyberattack damage if the cybersecurity expertise level is above the average (3, 4, 5). However, if the cybersecurity expertise level is below average (1, 2), adoption of the human firewall system may result in significantly worse overall cyberattack damage in some cases,

Table 1: Simulation Summary in Normal Mode.

Type	Name	Implication
Input	Virtual Organization	Virtual small and medium-sized business organizations composed of 40 employees with their work time patterns and daily behavior patterns
	Phishing Campaign	MITRE ATT&CK based APT 19 group's phishing campaign
	Security System	One security professional agent
	Simulation Mode	Normal (End user email-responsive behavior pattern in Figure 2 & Security professional agent behavior pattern in Figure 5)
Output	Total damage	The magnitude of phishing & data exfiltration damage in the whole organization ($)
Parameter	Security Plan	The type of security software plan the organization is using: **Basic Security Plan** (20%) or **Advanced Security Plan** (50%)
	Expertise Level	The probability that end user agent can accurately judge whether each given email is normal or phishing: **1** (88.24%), **2** (94.12%), **3** (97.06%), **4** (98.53%), **5** (99.265%)
	Phishing Email Types	200
	Number of Simulations	30

Table 2: Simulation Summary in Human Firewall Mode.

Type	Name	Implication
Input	Virtual Organization	Virtual small and medium-sized business organizations composed of 40 employees with their work time patterns and daily behavior patterns
	Phishing Campaign	MITRE ATT&CK based APT 19 group's phishing campaign
	Security System	One security professional agent & Message board system
	Simulation Mode	Human Firewall Mode (End user email-responsive behavior pattern in Figure 3 & Security professional agent behavior pattern in Figure 6)
Output	Total damage	The magnitude of phishing & data exfiltration damage in the whole organization ($)
Parameter	Security Plan	The type of security software plan the organization is using: **Basic Security Plan** (20%)
	Expertise Level	The probability that end user agent can accurately judge whether each given email is normal or phishing: **1** (88.24%), **2** (94.12%), **3** (97.06%), **4** (98.53%), **5** (99.265%)
	Motivation Level	The probability that end user agents will use the human firewall system when judging whether a given email is phishing, and their willingness to contribute to the human firewall: **1** (10%), **2** (30%), **3** (50%), **4** (70%), **5** (90%)
	Phishing Email Types	200
	Number of Simulations	30



(a) Basic Security Plan (b) Advanced Security Plan

Figure 7: Result of the first experiment.

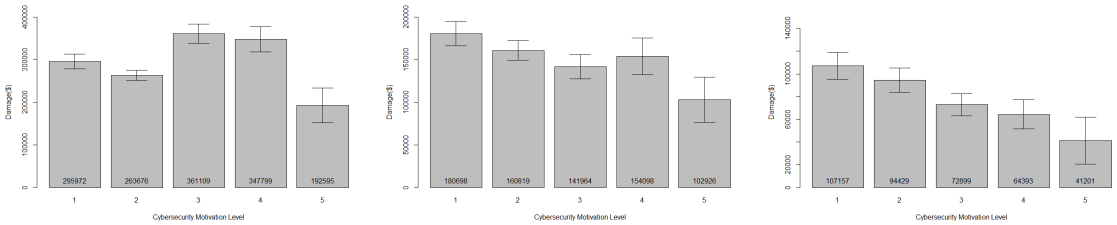
such as (Expertise Level = 1, Motivation Level = 3) and (Expertise Level = 1, Motivation Level = 4). Similarly, improving the cybersecurity motivation level may increase the overall cyberattack damage in cases such as (Expertise Level = 1, Motivation Level = 3) and (Expertise Level = 2, Motivation Level = 4). This occurs because there is only one security professional agent, and as the cybersecurity motivation level increases, more email inspection requests will arrive, reducing the time the security professional agent has to inspect and fix compromised computing devices. This, in turn, decreases the benefits of computing device inspection, and if the benefits from the human firewall system do not outweigh the decreasing benefits from the computing device inspection, the overall cyberattack damage inevitably increases.

If the end user agents have below-average cybersecurity expertise levels, the process of building a robust human firewall is slow because end user agents may request to inspect many normal emails (False Positives), wasting the security professional agent's time that could be used to inspect and fix compromised computing devices. However, if the cybersecurity motivation level is above average (3, 4, 5), the number of inspection requests of false positives decreases, and the human firewall is built at a faster pace. Thus, if the end user agents' cybersecurity expertise level is above average and their cybersecurity motivation level is high, the performance is comparable to or sometimes better than using the advanced security plan alone. In such cases, improving the cybersecurity motivation level guarantees higher defense performance.

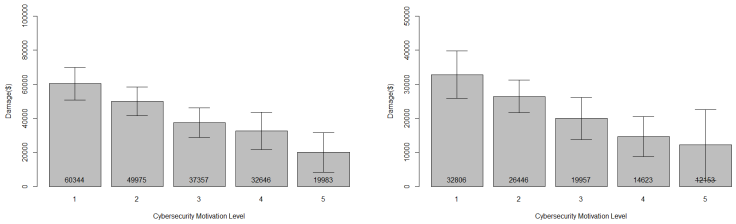
5 CONCLUSION AND DISCUSSION

The average cost of data breaches for SMBs were $105K in 2021 (Kaspersky 2021). It is close to the overall damage of our simulation result with normal mode, cybersecurity expertise level 3, and basic security plan ($109,048). This validates that our model reflects the magnitude of the cyberattack damage in the real world SMBs. If there are two security professional agents (one takes charge of the human firewall, and the other takes charge of the computing device inspection), the simulation will always give better results as either the cybersecurity expertise level or cybersecurity motivation level increases because there will not be a case that the security agent becomes careless with the computing device inspection while prioritizing building a human firewall. However, hiring additional security experts can be too expensive for small and medium-sized businesses. Actually, on average, SMBs spend only $13K to hire new security staff for their business, which proves that SMBs are reluctant to spend their budget on hiring another security staff (Kaspersky 2021). Reflecting on this real-world factor, we fixed the number of security professional agents as one.

In conclusion, we have proposed an alternative approach to cybersecurity in SMBs with limited budgets. Our approach leverages the human firewall concept, which is a system that promotes a culture of security awareness and enables end users to act as the initial barrier against cyber attacks. We developed an agent-based model to simulate the activities of end-users and the security infrastructure and evaluated the effectiveness of our approach in mitigating damages caused by a realistic phishing campaign. Our simula-



(a) Expertise Level = 1 (b) Expertise Level = 2 (c) Expertise Level = 3



(d) Expertise Level = 4 (e) Expertise Level = 5

Figure 8: Result of the second experiment.

tion results show that, in the scenario where end-users have above-average cybersecurity expertise and high motivation levels, the human firewall strategy is comparable to or outperforms an advanced security plan in terms of reducing the damage caused by cyberattacks. This finding suggests that small and medium-sized businesses with limited budgets can benefit from implementing a human firewall system, especially when the end-users are well-trained and motivated to follow security protocols.

ACKNOWLEDGMENTS

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

Barracuda 2022, Mar. "Spear phishing: Top threats and trends". Technical report, Barracuda.

Bhardwaj, A., F. Al-Turjman, V. Sapra, M. Kumar, and T. Stephan. 2021. "Privacy-aware detection framework to mitigate new-age phishing attacks". *Computers & Electrical Engineering* vol. 96, pp. 107546.

Blumstein, A., J. Cohen, and D. Nagin. 1978. *Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates*. National Academy of Sciences Washington, DC.

Bock, G.-W., R. W. Zmud, Y.-G. Kim, and J.-N. Lee. 2005. "Behavioral intention formation in knowledge sharing: Examining the roles of extrinsic motivators, social-psychological forces, and organizational climate". *MIS quarterly*, pp. 87–111.

Burns, A., C. Posey, J. F. Courtney, T. L. Roberts, and P. Nanayakkara. 2017. "Organizational information security as a complex adaptive system: insights from three agent-based models". *Information Systems Frontiers* vol. 19 (3), pp. 509–524.

Dobson, G., A. Rege, and K. Carley. 2018. "Informing active cyber defence with realistic adversarial behaviour". *Journal of Information Warfare* vol. 17 (2), pp. 16–31.

Dobson, G. B., and K. M. Carley. 2017. "Cyber-FIT: an agent-based modelling approach to simulating cyber warfare". In *International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation*, pp. 139–148. Springer.

Dobson, G. B., and K. M. Carley. 2018. "A computational model of cyber situational awareness". In *International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation*, pp. 395–400. Springer.

El Hajal, G., R. A. Z. Daou, and Y. Ducq. 2021. "Human Firewall: Cyber Awareness using WhatApp AI Chatbot". In *2021 IEEE 3rd International Multidisciplinary Conference on Engineering Technology (IMCET)*, pp. 66–70. IEEE.

Elharmeel, Muhammad 2009. "Human Being Firewall". https://sansorg.egnyte.com/dl/mu7iMSdXIw. Accessed, Jan. 28, 2023.

IBM. 2014. "IBM security services 2014 cyber security intelligence index".

Imagine IT 2022, Oct. "Cost of cyber security for small to midsized businesses". https://imagineiti.com/how-much-does-cybersecurity-cost-for-small-to-mid-sized-businesses/. Accessed Jan. 28, 2023.

Jajodia, S., P. Liu, V. Swarup, and C. Wang. 2009. *Cyber situational awareness*. Springer.

Jensen, M., A. Durcikova, and R. Wright. 2017. "Combating phishing attacks: A knowledge management approach". In *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Kaspersky 2021. "IT security economics 2021: executive summary". Technical report, Kaspersky.

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

MITRE 2021. "APT19, Codoso, C0d0so0, Codoso Team, Sunshop Group, Group G0073 | MITRE ATT&CK®". https://attack.mitre.org/groups/G0073/. Accessed Jan. 28, 2023.

North, M. J., N. T. Collier, J. Ozik, E. R. Tatara, C. M. Macal, M. Bragen, and P. Sydelko. 2013. "Complex adaptive systems modeling with Repast Simphony". *Complex adaptive systems modeling* vol. 1 (1), pp. 1–26.

Rajivan, P., and N. Cooke. 2017. "Impact of team collaboration on cybersecurity situational awareness". In *Theory and Models for Cyber Situation Awareness*, pp. 203–226. Springer.

RiskIQ 2022. "Evil Internet Minute 2021". https://safe.riskiq.com/rs/455-NHF-420/images/Evil-Internet-Minute-RiskIQ-Infographic-2021.pdf. Accessed Jan. 10, 2023.

Rogers, R. W. 1975. "A protection motivation theory of fear appeals and attitude change1". *The journal of psychology* vol. 91 (1), pp. 93–114.

Shin, J., G. B. Dobson, K. M. Carley, and L. R. Carley. 2022. "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. Springer.

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

Vance, A., M. Siponen, and S. Pahnila. 2012. "Motivating IS security compliance: Insights from habit and protection motivation theory". *Information & Management* vol. 49 (3-4), pp. 190–198.

Whitman, M. E., P. Fendler, J. Caylor, and D. Baker. 2005. "Rebuilding the human firewall". In *Proceedings of the 2nd annual conference on Information security curriculum development*, pp. 104–106.

Williams, J., J. King, B. Smith, S. Pouriyeh, H. Shahriar, and L. Li. 2021. "Phishing Prevention Using Defense in Depth". In *Advances in Security, Networks, and Internet of Things*, pp. 101–116. Springer.

Zinnov 2022, Dec. "Why SMB cybersecurity is a non-negotiable Today". https://zinnov.com/macro-trends/why-smb-cybersecurity-is-a-non-negotiable-today-blog/. Accessed Jan. 28, 2023.

AUTHOR BIOGRAPHIES

JEONGKEUN SHIN is a Ph.D. student in the Department of Electrical and Computer Engineering at Carnegie Mellon University. He is a member of the Center for Computational Analysis of Social and Organization Systems (CASOS). His research includes modeling and simulation of human and organizational behaviors relevant to cybersecurity. He holds a bachelor's degree in computer science from the University of Michigan and a master's degree in electrical and computer engineering from Carnegie Mellon University. His email address is jeongkes@andrew.cmu.edu.

GEOFFREY B. DOBSON is a research engineer at Carnegie Mellon University's Software Engineering Institute, where he investigates emerging trends in cyber warfare modeling and simulation. He earned his Ph.D. in Societal Computing from Carnegie Mellon University. He has over twenty years of professional experience in engineering and technology in a variety of roles supporting projects in medical devices, missile testing, data centers, and simulation. Dr. Dobson has been serving in the United States Air Force for 17 years, on both active duty and reserve. He's currently stationed at the Air Force Research Laboratory at Wright-Patterson, AFB, OH, where he oversees and advises on cyber modeling and simulation projects. His email address is gdobson@cs.cmu.edu.

L. RICHARD CARLEY received an S.B. in 1976, an M.S. in 1978, and a Ph.D. in 1984, all from the Massachusetts Institute of Technology. He joined the Electrical and Computer Engineering Department at Carnegie Mellon University (CMU) in Pittsburgh, Pennsylvania in 1984, and in March 2001, he became the STMicroelectronics Professor of Engineering at CMU. Dr. Carley's research interests include analog and RF integrated circuit design in deeply scaled CMOS technologies, and novel micro-electromechanical and nano-electro-mechanical device design and fabrication. For the past several years, Dr. Carley has studied the design of efficient RF Power Amplifiers in advanced BiCMOS technologies. Dr. Carley has been granted 27 patents, authored or co-authored over 250 technical papers, and authored or co-authored over 20 books and/or book chapters. He has won numerous awards including Best Technical Paper Awards at both the 1987 and the 2002 Design Automation Conference (DAC), a Most Influential Paper award from DAC, and a Best Panel Session award at ISSCC in 1993. In 1997, Dr. Carley co-founded the analog electronic design automation startup, Neolinear, which was acquired by Cadence in 2004. His email address is lrc@andrew.cmu.edu.

KATHLEEN M. CARLEY (H.D. University of Zurich, Ph.D. Harvard, S.B. MIT) is a Professor of Societal Computing, Software and Societal Systems Department (S3D), Carnegie Mellon University; Director of the Center for Computational Analysis of Social and Organizational Systems (CASOS), Director of the Center for Informed Democracy and Social Cybersecurity (IDeaS), and CEO of Netanomics. Her research blends computer science and social science to address complex real world issues such as social cybersecurity, disinformation, disease contagion, disaster response, and terrorism from a high dimensional network analytic, machine learning, and natural language processing perspective. She and her groups have developed network and simulation tools, such as ORA, that can assess network and social media data. Her email address is kathleen.carley@cs.cmu.edu.