OSIRIS: Organization Simulation in Response to Intrusion Strategies

Jeongkeun Shin(✉), Geoffrey B. Dobson, Kathleen M. Carley, and L. Richard Carley

Carnegie Mellon University, Pittsburgh, PA 15213, USA
jeongkes@andrew.cmu.edu, {gdobson,kathleen.carley}@cs.cmu.edu
LRC@cmu.edu

Abstract. OSIRIS, Organization Simulation In Response to Intrusion Strategies, is an agent-based simulation framework that models virtual organization composed of end user agents with complex and realistic behavior patterns. The purpose of OSIRIS is to predict and analyze the scale of cyberattack damage on the organization once targeted by cybercriminals with a consideration of organization members' properties, behavior patterns, and social relations. In this paper, we detail how we reflect real world organization environments and cyberattack scenarios to OSIRIS by illustrating our organization and cybercriminal design.

Keywords: Agent-based modeling and simulation · Human behavior modeling · Organization studies

1 Introduction

As the Internet is universally supplied and innovative information technologies emerge, the number of cybercrimes consistently increase year by year. Cybersecurity Ventures predicts that "global cybercrime costs will grow by 15% per year over the next five years, and it will reach $10.5 trillion USD annually by 2025" [13]. It is surprising that over 95% of security incidents come from "human error", and the most common human error is "Double Clicking" a malicious attachment or unsafe URL [8]. Thus, it is essential to analyze what causes end users to make human errors to reduce cybercrime incidents. However, vulnerabilities caused by human factors are often overlooked, partly because human tests are expensive and very difficult to repeat [1]. Moreover, conducting a human test in the real organization is often not welcomed by organization members. For example, when Rizzoni and his team ran a phishing simulation campaign, they sent custom phishing emails that asked employees to click the malicious link to receive a Christmas bonus. Disappointed that the bonus was not real, some employees complained about the campaign, and it was eventually terminated [14]. To analyze human errors and their impacts without conducting actual human tests, we introduce OSIRIS, an agent-based simulation framework that models a virtual organization and end user agents with realistic

R. Thomson et al. (Eds.): SBP-BRiMS 2022, LNCS 13558, pp. 134–143, 2022.
https://doi.org/10.1007/978-3-031-17114-7_13

human behavior patterns. Carley stated, "the human organization has long been used as a metaphor for the organization of computational process" [2]. Thus, if computational model of human behaviors, organization settings, and cyberattack scenarios is appropriately designed, simulations of virtual human tests against cyberattacks can not only be cost-effective, faster, and more comprehensive, but also allows systematic examination of various complicated outside-the-box scenarios [3]. The ultimate goal of OSIRIS is to provide a testbed where a client can build a custom virtual organization, and then simulate cyberattack scenarios on that organization to predict potential cyberattack damage and to test the effectiveness of various cyber-defense strategies to minimize human errors.

2 Related Works

There have been various attempts to implement models to simulate cyberattacks on virtual end users. Schultz proposed a framework that predicts and detects insider attack using end users' behaviors and symptoms including deliberate markers, meaningful errors, preparatory behaviors, correlated usage patterns, verbal behavior and personality traits [15]. Kotenko implemented multi-agent simulation of cyber-attacks and a multi-level cyber-defense system where defense agents can cooperate to counter cyber-attacks [11]. Blythe et al. developed the agent community systems to test cyber security systems by modeling human behaviors, physiology, and emotion [1]. Vernon-Bido et al. introduced a model that examines factors that make a user become an attacker by leveraging rational choice theory, routine activity theory, social learning theory, and planned behavior theory [17]. Dobson and Carley introduced Cyber-FIT framework [4], an agent-based cyber warfare simulation framework that models and simulates military cyber forces that defend cyber terrains against adversaries. Dobson et al. expanded this framework by adding more realistic adversary behaviors to explore the cyber defense teams' defensive efforts in the organization [5] and then modeled the agents' ability to perceive cyber situational awareness [6].

Unlike previous works, OSIRIS builds an *organizational-behavior-centric* simulation framework, which implements human agents' entire daily routine and social relationships in the organization. We modeled end user's commonly observed behaviors and software usage patterns in the organization in addition to abilities to respond to the cyberattacks. OSIRIS will provide a testbed to observe how changing one or several human factors will impact the overall cyberattack damage to the entire organization.

3 OSIRIS Simulation Framework

In this section, we introduce our simulation framework, OSIRIS, in detail. OSIRIS is implemented with NetLogo [19]. Its simulation time is counted in ticks. We assume that one tick corresponds to one minute in the real world. While a simulation is running, we keep track of ticks and translate it to real world time. Figure 1 displays OSIRIS in NetLogo [19] user interface.

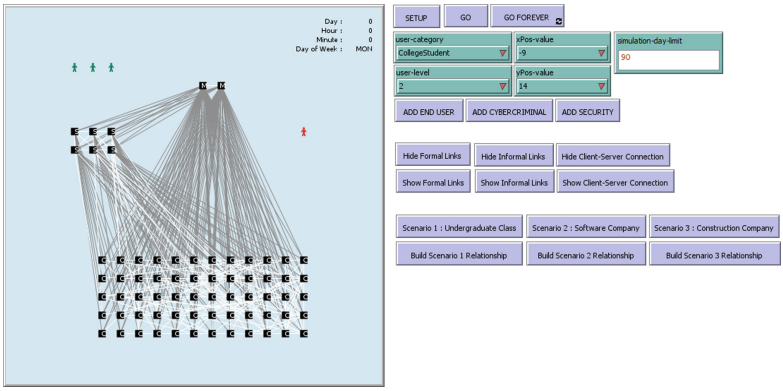


Fig. 1. OSIRIS in NetLogo environment.

3.1 End User Agent

End user agents represent people working at the organization. Similar to humans in the real world, end user agents arrive at the organization early morning or in the afternoon, work 6 to 10 hours, and then leave work. In OSIRIS, an end user class can be defined by distributing daily work time to 13 different behavior categories. While the simulation is running, each end user agent's daily behavior pattern is determined by its own predefined time allocation. We predefined 7 different end user classes that are commonly observed in various organizations. How each end user class spends time at organization is summarized at Table 1.

Table 1. How each end user class spends their time in the organization.

	Email	Messenger	Social Network	Software Development	Business Communication	Data Cleaning
College Student	15%	9%	9%	0%	0%	3%
Software Engineer	15%	3%	4%	48%	5%	10%
Engineering Manager	13%	2%	1%	34%	10%	5%
Human Resource Team	12%	4%	4%	0%	10%	0%
General Office Worker	34%	4%	3%	0%	16%	10%
Blue Collar Worker	5%	5%	5%	0%	0%	0%
Data Scientist	15%	4%	3%	0%	5%	28%

	Data Analysis	Human Resource	General Administration	Social Media	Study	Meeting	Work Outside
College Student	0%	0%	0%	14%	45%	5%	0%
Software Engineer	0%	0%	0%	5%	0%	10%	0%
Engineering Manager	0%	0%	10%	5%	0%	20%	0%
Human Resource Team	0%	36%	8%	4%	0%	22%	0%
General Office Worker	0%	0%	19%	4%	0%	10%	0%
Blue Collar Worker	0%	0%	0%	0%	0%	0%	85%
Data Scientist	30%	0%	0%	5%	0%	10%	0%

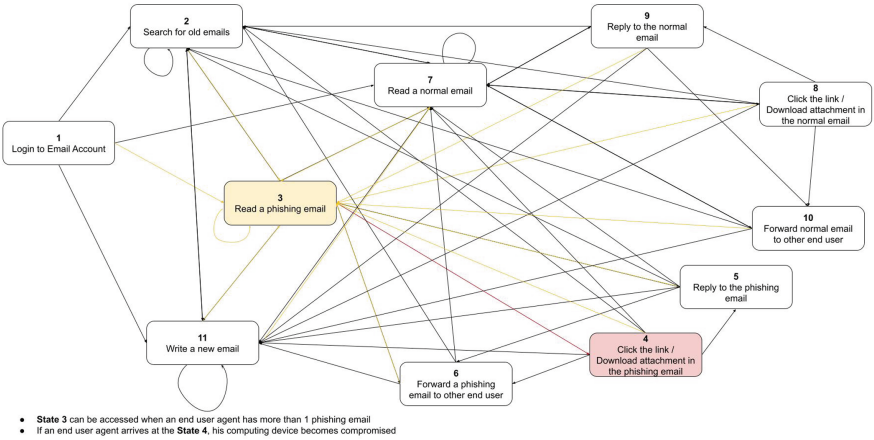


Fig. 2. Behavior flow diagram of the 'Email' behavior category.

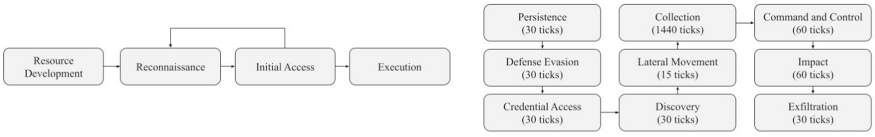
While the simulation is running, deployed end user agents' remaining time in 13 behavior categories is monitored every tick, and behavior change is made when necessary. Each behavior category is composed of a set of specific behaviors. For example, Fig. 2 illustrates the shape of the 'Email' behavior category, which is composed of 11 specific behaviors. Each specific behavior has a list of next specific behavior candidates, and an end user agent selects the next specific behavior every tick. In total, we defined 92 specific behaviors in 13 behavior categories, and 3 specific behaviors are causal factors of "human errors": 1) Read a phishing email, 2) Read a phishing message from the messenger, 3) Read a phishing message from the business communication software. These behaviors can only be accessed when an end user agent has more than 1 phishing email or message. According to the recent survey [7], 2.94% of employees eventually click on a link in the malicious email. However, this value should vary from person to person depending on an individual's level of cybersecurity knowledge. We defined the property 'Cybersecurity Expertise Level', where level 1 represents cybersecurity novice and level 5 represents cybersecurity expert. Each level has a different probability value to eventually click the phishing link or download the malware: Level 1 = 11.76%, Level 2 = 5.88%, Level 3 = 2.94%, Level 4 = 1.47%, and Level 5 = 0.735%. This property is assigned to the end user agent when it is deployed. When an end user agent's current specific behavior is one of three causal factors of human error, its computing device can become compromised with a probability corresponding to its cybersecurity expertise level.

In the real world, people build a human network at organizations. Similarly, end user agents in OSIRIS are intertwined with each other formally or informally. Formal relationships are formulated among end user agents who work together to achieve a certain goal while informal relationships are structured based on friendships or personal relationships. The survey [7] states that there is a 0.78% probability that an end user eventually forwards a phishing email to another

end user. Reflecting this in OSIRIS, when an end user agent reads a phishing content, it is forwarded to one or more formal and informal relationships with 0.78% probability. Moreover, while a cybercriminal agent is exploiting an end user's computing device, it can deliver phishing contents to the end user's formal and informal relationships using the end user's personal account (Lateral Movement). Reflecting the fact that phishing contents delivered by a credible person seems more persuasive, the probability to be deceived by phishing contents forwarded by formal or informal relationships is a double of the probability value corresponding to the recipient's cybersecurity expertise level.

3.2 Cybercriminal Agent

In OSIRIS, one cybercriminal agent can be deployed. It conducts a phishing attack on end user agents in the organization based on MITRE ATT&CK [16], the collection of adversary tactics and techniques based on real-world observations, which covers almost all types of cyberattacks. Among all tactics and techniques, Korea Internet & Security Agency (KISA) sorts out ones involved in a phishing attack [9,10]. The cybercriminal agent uses these selected cyberattack tactics and techniques in its phishing attack scenario. Broadly, the attack scenario is divided into two phases. If no compromised computing device exists in the organization, a cybercriminal agent is at the Attack Phase 1, attempting phishing through several delivery methods. As soon as one computing device becomes compromised, the cybercriminal moves on to the Attack Phase 2, exploiting compromised computing devices.



(a) Attack Phase 1 (b) Attack Phase 2

Fig. 3. Cybercriminal agent's phishing attack scenario.

Figure 3(a) illustrates Attack Phase 1. During this phase, the cybercriminal agent builds an infrastructure, prepares a malware software, collects end users' personal information, and attempts phishing through various delivery methods until an end user agent's computing device becomes compromised. According to the Verizon's Data Breach Investigation Report [18], 96% of phishing attacks are delivered using email. Reflecting this, our cybercriminal agent's phishing attacks are delivered through 96% email, 2% messenger, and 2% business communication software.

As described in Fig. 3(b), during Attack Phase 2, a cybercriminal agent sequentially leverages nine different MITRE ATT&CK [16] tactics to exploit

an end user's compromised computing device. Each tactic is composed of a set of attack techniques, and the cybercriminal agent randomly chooses one technique every tick to damage computing devices. Each technique produces one of five adverse effects on compromised computing devices for a tick: None, Slowdown, Data Loss, Data Modification, and Data Leakage. In total, a cybercriminal agent uses 46 attack techniques, and we assign the most relevant adverse effect to every attack technique. An end user agent with a compromised computing device suffers from one of five adverse effects every tick until the security agent fixes the computing device, or the cybercriminal agent finishes exploitation.

3.3 Security Agent

In OSIRIS, security agents monitor end user agents' computing devices and repair them if a virus is found. In every 15 ticks, each security agent randomly selects one computing device and inspects whether it is virus-infected or not. The probability to successfully detect and repair the compromised computing device during the inspection should be assigned before starting the simulation (1–100%). As soon as the security agent successfully detects and fixes the virus, the cybercriminal agent immediately loses the access to that computing device. If the last compromised computing device becomes fixed, the cybercriminal agent has no computing device to exploit. Then, it is immediately transferred to Attack Phase 1, and should deliver phishing contents to end user agents again until another computing device in the organization becomes compromised.

4 Virtual Experiment

We conducted virtual experiments to observe how three factors, 1) organization size, 2) cybersecurity expertise level, and 3) proportion of communication, impact on the scale of the cyberattack damage once the organization is targeted by cybercriminals.

The simulation setting for this experiment is summarized in Table 2. We deployed one cybercriminal agent and three security agents. Each end user agent is asked to randomly build 1 or 2 bidirectional formal relationships and informal relationships with other end user agents in the organization. Considering the Krebs' experiment result that antivirus software successfully detects computer viruses with average 24.47% and median 19% [12], we set the security agent's inspection success rate as 20%. Then, we built 80 different simulation settings with 4 different values of organization size, 5 different values of cybersecurity expertise level, and 4 different values of end user agent's proportion of communication. The communication includes three behavior categories: Email, Messenger, and Business Communication. To conduct these experiments, we declared four different types of end user agents that respectively spend 10%, 20%, 40% and 80% of their daily work time on the communication. The remaining time is equally distributed to 10 remaining behavior categories. For each case, we run 10 simulations (800 simulations in total). Each simulation is played

Table 2. Simulation summary

Number of cybercriminal agents	1
Number of security agents	3
Number of formal relationship of each end user agent	1 or 2
Number of informal relationship of each end user agent	1 or 2
Inspection success rate	20%
Organization Size	10, 20, 40, or 80
Cybersecurity Expertise Level	1, 2, 3, 4, or 5
Proportion of Communication	10%, 20%, 40%, or 80%
Simulation period	90 days (129,600 ticks)
Number of simulations for each case	10

for 129,600 ticks, which corresponds to 90 days in OSIRIS. After running simulations of each case, we record the average cyberattack damage of 10 simulations, which are summarized in Table 3 and Table 4.

Simulation results in Table 3 illustrate that the number of overall virus infection in the organization tends to increase as the organization size increases, end user agents' cybersecurity expertise level decreases, and the proportion of communication increases. Table 4 illustrates that the magnitude of 4 different cyberattack damage increases as organization size increases, end user agents' cybersecurity expertise level decreases, and the proportion of communication increases. One noticeable thing is the 'Data Loss' adverse effect. It tends to be close to 0 when the organization size is small, but rapidly increases as the organization size increases. Data Loss damage occurs during 'Impact' MITRE ATT&CK [16] tactic, which is located at the latter part of Attack Phase 2. This implies that when the organization size is small, three security agents succeed to detect and fix the virus before the cybercriminal agent reaches the endpoint, but cannot manage to do so as the organization size gets bigger.

5 Discussion and Future Works

Although not represented in this paper in detail, the OSIRIS can be used to test the effectiveness of cybersecurity strategies to mitigate cyberattack damage. For example, one common strategy to keep end users cautious is to intermittently pop up the warning message at the end user agent's computing device. If an end user agent's cybersecurity expertise level becomes maximum for a while after an end user agent sees the warning message, running two different simulations, one with the strategy and the other without it, will show how much this strategy is effective to mitigate the overall damage from phishing attacks.

There are still limitations in the OSIRIS. Currently, end user agents cannot directly report and ask for inspection to security agents when they recognize

Table 3. Projected number of virus infections and standard deviation.

		Proportion of communication							
Organization size	CyberSecurity Expertise Level	10%		20%		40%		80%	
		Infections	SD	Infections	SD	Infections	SD	Infections	SD
10	1	5.7	2.263	12.1	3.573	24.9	5.971	38.9	10.34
	2	2.8	1.989	4.6	1.955	12.5	3.689	17.3	6.129
	3	1.4	1.075	4.5	2.068	5.6	2.366	9.1	2.424
	4	1.4	0.966	1.8	1.135	2.8	2.201	4.3	2.002
	5	1.2	0.919	1.3	1.059	1.4	1.265	2.5	1.08
20	1	9	3.266	21.8	3.853	49.3	8.166	81.3	10.199
	2	5.1	1.969	10.6	2.797	21.1	5.087	33.4	8.488
	3	1.6	1.173	5.4	2.459	10.5	4.836	17.4	4.526
	4	1.3	0.949	3.8	1.135	5.3	2.908	6.1	2.807
	5	0.7	0.823	1.5	1.08	3.1	1.912	3	1.563
40	1	21.1	4.28	47.6	13.689	101.7	16.687	246.6	22.897
	2	10.9	3.573	20.4	3.718	37.3	7.675	74.1	10.796
	3	4.3	1.494	11.1	3.035	17.6	3.748	30.2	5.77
	4	2.6	2.17	4.5	1.841	8.4	2.319	15.5	4.743
	5	0.9	0.876	2.3	1.567	4.3	2.359	7.2	2.573
80	1	37.4	6.398	106.4	20.14	333.7	35.393	680.1	41.72
	2	16.6	5.103	33.9	6.082	81.5	10.32	243	25.373
	3	7.2	3.765	15.2	5.959	33.2	8.162	63.6	9.046
	4	4.1	2.331	8.2	3.824	13.8	4.872	25.5	7.322
	5	2.4	1.897	4.5	2.121	9.8	4.211	12.6	3.239

Table 4. Projected overall cyberattack damage in the organization.

Organization size	Proportion of communication	Expertise level	Data modification	Slow down	Data leakage	Data loss	Proportion of communication	Expertise level	Data modification	Slow down	Data leakage	Data loss
10	10%	1	61.3	193.6	900.9	0	20%	1	126.4	408.5	2571.9	6
		2	26.6	94.9	429.9	0		2	45.7	154.9	828.2	0
		3	13.7	44.9	167.4	0		3	42.6	153	770.7	0
		4	16.5	54.1	321.7	0		4	17.6	60.7	289.3	0
		5	12.2	43.1	251.7	0		5	12.8	40.7	186.6	0
	40%	1	257.6	844.2	4456	0	80%	1	393	1293.3	6605.6	0
		2	120.6	424.3	2193.9	0		2	174.5	573.9	2941.8	0
		3	55.4	186.6	919.7	0		3	99.8	320	2072.8	0
		4	30.2	99.8	581.9	0		4	43.3	139.6	632.8	0
		5	16.7	50.8	309.3	0		5	23.9	83.3	371.3	0
20	10%	1	105.7	318.3	3542.3	18	20%	1	252.4	791.7	8485.7	30
		2	59.3	178.9	1684.9	1.3		2	133	378.1	4546.1	24
		3	28.8	60.2	749.3	0		3	63.2	187.2	2191.8	10.9
		4	12.6	46.5	272.7	0		4	52.1	137.3	2140.2	12
		5	8.7	25.7	249.8	0		5	20.7	53.9	731.1	6
	40%	1	587.9	1726.4	20663.7	114.8	80%	1	966.7	2776.9	35186.4	225.3
		2	247.1	740.9	8296.8	20.8		2	387.1	1149.4	13364.5	47.7
		3	136	362.9	4199	40.4		3	204.9	593.7	6096	32.3
		4	64	188.6	2282.9	18		4	80.8	215.4	2771.5	18
		5	33.6	105.8	1227.9	0		5	32.2	104.1	1078.4	0
40	10%	1	324.5	743.8	14437.9	221.7	20%	1	767.1	1664.9	33740	538.9
		2	167.2	388	7878.8	108		2	337.6	734.3	15780.8	258.6
		3	69.8	151.9	3145.9	47.3		3	188.2	409.3	8307.1	134.2
		4	36.9	94.4	1781.5	18		4	76.8	167.9	3937.8	58.9
		5	15.5	33.7	763.6	12		5	34.9	82.4	1671.7	18
	40%	1	1601.2	3569.8	72001.9	1110.1	80%	1	3660	8350.7	169237.2	2481.2
		2	583.3	1336.8	24692	384.7		2	1162.2	2587.2	52278.3	809.6
		3	283.6	631.8	13044.1	199.1		3	482.3	1093.5	22451	315.7
		4	154.7	308.4	7388.9	149.1		4	260.4	549.2	12478.4	215.3
		5	73.7	152.9	3599	63.8		5	109.1	263.4	5003.6	54
80	10%	1	848.9	1361.4	38490.8	1026.3	20%	1	2315	3795.4	99661.8	2682.1
		2	385.9	604.6	17778.9	468		2	759.8	1240.5	35672.5	892.7
		3	156.3	263.4	7317.7	177.2		3	334.4	558.4	16089	367.6
		4	102.1	153.1	4605.1	133.4		4	192.4	299.6	8315.1	237.5
		5	50.6	90.9	2328.9	48		5	105.3	171.2	4938.4	126
	40%	1	6994.6	11340.4	323031.2	8210.2	80%	1	13271.5	21533.6	611702.1	15602.6
		2	1739.8	2908.4	79772.3	1988.9		2	5054.9	8382.3	235521.8	5811
		3	754.5	1229.9	34730	875		3	1399.5	2306.6	64276.9	1641.4
		4	326.9	515.7	15014.2	392.3		4	575.5	932	26184.3	657
		5	232.4	360.7	10197.6	281		5	295.2	458.3	13987.9	366

abnormal symptoms in its computing device. They cannot learn from the mistakes in the past. Also, only one type of cyberattack, phishing, can be simulated. Lastly, the end user agent's emotional states such as hunger, fatigue, or the motivation, which influence its performance level, are not fully implemented.

In the future, as we implement these functionalities, OSIRIS can be used in more diverse analysis such as calculating the optimal number of security agents in the organization to minimize the damage, observing organization's vulnerabilities from various types of cyberattacks, and analyzing the impact of end users' emotional states against cyberattacks.

6 Conclusion

In this paper, we introduced OSIRIS, and illustrated how three factors, organization size, cybersecurity expertise level, and proportion of communication affect the scale of overall cyberattack damage on the organization. OSIRIS will provide a testbed that clients can replicate real world organizations, and conduct various cyberattack simulations to observe and analyze potential cyberattack damage started from human errors without conducting actual human tests. It is cost effective, easy to repeat, and allows various outside-the-box experiments without any constraints. In the future, for more realistic simulation, we will improve the model with various human factors, social interactions, and various types of cyberattacks.

Acknowledgement. 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

1. Blythe, J., et al.: Testing cyber security with simulated humans. In: Twenty-Third IAAI Conference (2011)
2. Carley, K.M.: Organizational adaptation. Annal. Oper. Res. **75**, 25–47 (1997)
3. Carley, K.M., et al.: BioWar: scalable agent-based model of bioattacks. IEEE Trans. Syst. Man Cybern.-Part A: Syst. Hum. **36**(2), 252–265 (2006)
4. Dobson, Geoffrey B.., Carley, Kathleen M..: Cyber-FIT: an agent-based modelling approach to simulating cyber warfare. In: Lee, Dongwon, Lin, Yu.-Ru., Osgood, Nathaniel, Thomson, Robert (eds.) SBP-BRiMS 2017. LNCS, vol. 10354, pp. 139–148. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-60240-0_18
5. Dobson, G.B., Rege, A., Carley, K.M.: Informing active cyber defence with realistic adversarial behaviour. J. Inf. Warfare **17**(2), 16–31 (2018)
6. Dobson, Geoffrey B.., Carley, Kathleen M..: A computational model of cyber situational awareness. In: Thomson, Robert, Dancy, Christopher, Hyder, Ayaz, Bisgin, Halil (eds.) SBP-BRiMS 2018. LNCS, vol. 10899, pp. 395–400. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-93372-6_43

7. Flouton, M.: Threat Spotlight: Post-Delivery Email Threats. Journey Notes, 21 October 2021. https://blog.barracuda.com/2021/06/02/threat-spotlight-post-delivery-email-threats/. threat-spotlight-post-delivery-email-threats
8. IBM: IBM security services 2014 cyber security intelligence index (2014)
9. Korea Internet & Security Agency (KISA): TTP #2 Analysis of the Bookcodes RAT C2 framework starting with spear phishing (2020). https://www.boho.or.kr/krcert/publicationList.do
10. Korea Internet & Security Agency (KISA): TTP #4 Phishing Target Reconnaissance and Attack Resource Analysis (2021). https://www.boho.or.kr/krcert/publicationList.do
11. Kotenko, I.: Multi-agent modelling and simulation of cyber-attacks and cyberdefense for homeland security. In: 2007 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. IEEE (2007)
12. Krebs, B.: A Closer Look: Email-Based Malware Attacks. Krebs Secur., 21 June 2012. krebsonsecurity.com/2012/06/a-closer-look-recent-email-based-malware-attacks/
13. Morgan, S.: Cybercrime to Cost the World $10.5 Trillion Annually by 2025. Cybercrime Mag., 27 April 2021. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
14. Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., Coventry, L.: Phishing simulation exercise in a large hospital: a case study. Digital Health **8**, 20552076221081716 (2022)
15. Schultz, E.E.: A framework for understanding and predicting insider attacks. Comput. Secur. **21**(6), 526–531 (2002)
16. Strom, B.E., Applebaum, A., Miller, DP., Nickels, K.C., Pennington, A.G., Thomas, C.B.: Mitre att&ck: Design and philosophy. Technical report (2018)
17. Vernon-Bido, D., Padilla, J.J., Diallo, S.Y., Kavak, H., Gore, R.J.: Towards modeling factors that enable an attacker. In: SummerSim, p. 46 (2016)
18. Widup, S., Hylender, D., Bassett, G., Langlois, P., Pinto, A.: Verizon data breach investigations report (2020)
19. Wilensky, U.: NetLogo (1999). http://ccl.northwestern.edu/netlogo/. Center for Connected Learning and Computer-Based Modeling, Northwestern University, Evanston, IL