Open Access License Notice

Higher Education Social Engineering Attack Scenario, Awareness & Training Model

Thai H. Nguyen
School of Computer Science and Engineering
Jack Welch College of Business & Technology
Sacred Heart University
Fairfield, CT, USA
nguyent62509@mail.sacredheart.edu

Sajal Bhatia
School of Computer Science and Engineering
Jack Welch College of Business & Technology
Sacred Heart University
Fairfield, CT, USA
bhatias@sacredheart.edu

***Abstract*—In today's information security ecosystem, hackers and threat actors are increasingly using social engineering tactics to circumvent advanced technical security technologies. While every year there are vast leaps in technical security systems, one critical dynamic, the human psychology still needs a dire upgrade to their operating system. The human dynamic and our innate psychological processing algorithms need a new approach to mitigate social engineering attacks. Higher education institutions are prime target for social engineering engagement missions as they house a large diverse population of faculties, students, alumni, and employees in their ecosystem. This diversity paired with increasing inclusion of international individuals only expands the existing dynamic vulnerable landscape, thereby requiring innovative methods to secure it. In this paper, the authors utilize an existing framework to develop nine specialized and publicly available social engineering attack scenarios geared toward a higher education environment. The paper also proposes preliminary models for social engineering awareness and training to combat such attacks. The effectiveness of the proposed models will be assessed by comparing pre- and post- awareness surveys as part of the future work.**

Keywords—Information Security, Social Engineering, Social Engineering Attack Scenario, Social Engineering Awareness Model, Social Engineering Training Model, Social Engineering Ethics

I. INTRODUCTION

In the 21st century, information technology (IT) is ingrained into the fabric of nearly every society in the world. There isn't an industry that IT is not utilized from Financial, Government, Healthcare, Education, Industrial, Hospitality, Entertainment, Transportation, Retail, Telecommunication, and more. Technology that we all use today is also the very same technology that is used against us to cause harm to ourselves and society, either physically, mentally, and/or financially. Information security (IS) is continually becoming an essential in-demand and on-demand service for all of society's industries. It is critical that society's industries protect data at-rest, in-transit, and in-use from internal and external threats. The need for more IS has created a steadfast emergent of hardware and software technologies to combat a multitude of technical vulnerabilities and threats [17, 18, 23, 26 – 28]. It has made it harder for hackers and threat actors (the authors will refer to them as "attackers") to circumvent the technical security technologies but has not made it impossible.

Attackers are turning to social engineering (SE) tactics to circumvent the technical securities emplaced. SE is the deliberate act of manipulating an individual or group of individuals into giving access to confidential and unauthorized information voluntarily [1 – 14, 17, 21 – 23]. Research showed that an ontological definition of SE by Mouton et al. provided a more concrete definition of SE stating, "the science of using social interaction as a means to persuade an individual or an organization to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity" [2]. The techniques that attackers will use in a SE attack (SEA) are identified by Mitnick as, "research, developing rapport and trust, exploiting trust, and utilize information" [4].

The authors surveyed ethical concerns pertaining to SE penetration testing and research [9, 10, 11]. SE penetration testing and research are crucial in assessing and evaluating the weaknesses in an industry such as higher education (HE). Experimentation and live executions of SEA can yield significant results, but conducting such excursions raise ethical concerns. To gather unfettered and unbiased results from the experiments, deception is a critical factor in testing and research missions [9, 10, 11]. Attackers are not restrained by the ethical constraints that penetration testers and researchers are held to. The authors propose that crafting specialized SEA scenarios based on real-world SE events can come close to those that attackers will utilize in their profession and satisfy ethical concerns.

To assess the current state of SE awareness training policies in HE institutions, the authors examined several publicly available HE institutions information via a search engine index. The findings showed that all provided information security awareness training to their students, faculty, and employees. The authors could not assess the actual content of the training material as they were only

authorized to their appropriate institutions[1-6]. From the surface level information assembled, one institution provided about two 5 min general IS awareness videos[7] and another provided only a broad generalized IS awareness text-based information[8]. Although HE institutions are providing IS awareness training, the propriety nature and generalization of IS awareness is holding back the good it can provide to the educational community.

Due to these limitations, in this paper the authors proposes utilizing an open source approach in developing and providing specialized SEA scenarios based on Mouton et al. proposed, Social Engineering Attack Framework, which expands on Mitnick's "Social Engineering Cycle" [3, 4]. The proposed scenarios are based on real-world SE events, which will replicate actual prior SEAs and be able to satisfy ethical concerns. SEA scenarios will focus specifically on the threat landscape of HE institutions. By incorporating specialized SEA scenarios into SE Awareness and Training, technical and non-technical individuals will be able to spot SEAs [6, 7, 17, 19 – 25]. This will provide individuals within institutions a superior security awareness and be more vigilant against such types of SEAs [3].

The rest of the paper is organized as follows: Section II provides an overview of the impact of SE on HE institutions, and the ethical constraints of conducting SE experimentation by penetration testers and researchers. Section III provides a detailed overview of the Social Engineering Attack Framework used in the paper for developing attack scenarios. Section IV details the authors' contribution to mitigating higher education social engineering attacks with specialized crafted SEA scenarios. Section V outlines the authors' proposed SE awareness and training model to be implemented by HE institution's in their ecosystem. Finally, Section VI concludes and summarizes the research and outlines future directions for research in this area.

II. Background and Related Work

Social engineering (SE) is on the rise and higher education (HE) institutions are faced with an increasing vulnerable landscape [27 - 32]. Every year there are massive migrations of local, national, and international high school graduates, transfer students, faculty and employees hire. All interfacing with HE institution systems, adding hundreds to thousands of dynamic vulnerabilities to their information technology and information security (IT/IS) ecosystem [19 – 26]. These individuals need to adapt to the IT/IS systems to be able to conduct their duties as students, professors, and employees.

HE institutions are a prime target for attackers because of the stockpiles of valuable information (VI) they collect and store [26]. As well as the openness and transparency of institutional public information provides enormous amounts of open source intelligence (OSINT) information. Information is a critical necessity involved in running a HE institution, which offer attackers a one-stop-shop for VI. Firstly, types of VI include the following: Personal Identifiable Information (Students, Parents, Faculty, and Employees), Protected Health Information, Free Application for Federal Student Aid, Financial Information, Employment Information, Institutional Endowment Donors, Intellectual Property, Academic Research, 3rd Party Vendor Information, and Payment Card Information. Secondly, OSINT information include the following: Full Name (First, Last, Middle), Job Title & Role, Social Media Accounts, Individual & Institutional News Feed, Old Version of Websites, Institutional Directory (Department, Phone, & Email), Google Map & Satellite Imagery, and Photo Repository (Flickr, Google Image, etc.). The multiple public-facing information that attackers can compile in their research to formulate a refined engagement mission against an individual or group of individuals at a HE institution [17, 21].

Individuals at every level in HE institutions are mandated at one point to provide multiple data points when entering the institution's ecosystem. Attackers will not need to initiate SE engagement missions into individual industries. Attackers merely need to conduct a single SE engagement mission on an unprepared HE institution and gain access to a treasure trove of VI. VI can be utilized in a follow up SEA into other industries. Armed with enough time, motivation and unchained ethical constraints, attackers will achieve their goals of infiltrating HE/IT infrastructure. HE institutions around the world have a lot to lose in the aftermath of a security breach. Types of negative impacts on HE institutions include the following: Financial Losses, Loss of Trust, Legal Action, Negative Publicity, Reputation Damage, Decline in Retention Rate, Decline in Admission Rate, and Loss of Research Grants [26, 27].

For professional penetration testers and researchers conducting live social engineering attack (SEA) experimentations for the improvement of society, to attain accurate and unfettered results from their experimentations, penetration testers and researchers must engage in a high level of deception and manipulation [9, 10, 11]. By executing tactics that malicious social engineers will utilize in their own engagement missions against real-world targets, they are able to enlighten the organization(s) of the weaknesses in their environment. The individual or group of individuals conducting SEA experimentations must also abide by ethical guidelines to satisfy their respective ethical oversight committee such as their institutional review board [11].

1 https://is.richmond.edu/infosec/securityawareness/training/index.html

2 https:// cybersecurity.yale.edu/mss/yale-mss-12.1

3 https://www.technology.pitt.edu/security/information-security- awareness-training

4 https://it.arizona.edu/seecurity

5 https://cuit.columbia.edu/ciso/security-training

6 https://its.gse.harvard.edu/services/information-security/awareness-training

7 https://informationsecurity.princeton.edu/training

8 https://its.ucsc.edu/security/training/index.html

According to Mouton et al. penetration testers and researchers must adhere to the 3 major normative ethics principles of virtue ethics, utilitarianism, and deontology, to be viewed as ethical [9]. If there are any deviation from the 3 principles, then the individual or group of individuals are unethical in their actions. In the following, the authors emphasize the distinctions between ethical and unethical in each principle [9].

A. Virtue Ethics

The actions of an individual in the context of virtue ethics is considered to be ethical or "virtuous" if the individual is adhering to a defined moral code or code of ethics[9]. If the actions taken by the individual deviates from the moral code or code of ethics, then they are considered unethical. For penetration testers and researchers, Mouton et al. focuses on the Code of Ethics described by the IEEE & ACM as the guiding principles [9].

B. Utilitarianism

Utilitarianism, also known as consequentialism, considers an individual to be ethical if the individual's actions benefits society[10]. Otherwise, if the individual's actions do not benefit society it is considered unethical. Penetration testers and researchers conducting SEA are considered ethical if it provides beneficial outcomes to the greatest number of people. It disregards the consequences it has on the victim in which the SEA was directed toward [9].

C. Deontology

Deontological ethics defines what individual(s) should and should not do by the moral standards of society[11]. If such actions by the individual deviates into morally forbidden norms of society then it is considered unethical. According to Mouton et al., SEA needs to strictly adhere to the deontological rules of the world from the very beginning, regardless of the consequences [9].

There is no substitute to genuine live SEA, but conducting these experimentations require thorough and precise navigation to be within ethical standards. Malicious attackers are uninhibited by such ethical limitations. The authors recognize the limitations that penetration testers and researchers face in conducting meaningful SEA experimentations. To bridge the unethical advantages of malicious attackers, the authors proposes using Mouton et al. proposed social engineering attack framework (SEAF) [3]. Penetration testers and researchers can step into the mindset of a malicious social engineers and plan full spectrum SEA engagements targeted at their specific environment. SEAF will allow penetration testers and researchers to create a multitude of ethical and unethical SEA scenarios. An additional benefit for penetration testers and researchers in utilizing SEAF is the ability to provide detailed execution procedures of their experiment to their respective ethical oversight committee for review.

III. Social Engineering Attack Framework

Mouton et al. proposed social engineering attack framework (SEAF) expanded upon their ontological SEA model defines 7 components [2] and 6 core phases [3]. SEAF provides a comprehensive outline of the processes that attackers utilize in conducting their social engineering attack (SEA). The authors recognize the thoroughness of SEAF, and it is the basis to the authors' specialized crafted higher education (HE) social engineering (SE) scenarios. The authors outlines the 7 components then 6 core-phases of SEAF. In the following, the 7 components of SEAF:

1. ***Communication***: Direct (includes Bidirectional & Unidirectional) & Indirect
2. ***Social Engineer***: Individual or Group of Individuals
3. ***Target***: Individual or Organization
4. ***Medium***: Method of Initiating Communication (Social Engineer to Target)
5. ***Goal***: Financial Gain, Unauthorized Access, or Service Disruption
6. ***Compliance Principles***: Reasons why a Target complies with the Social Engineer's Request
7. ***Technique***: Method(s) a Social Engineer utilizes in achieving their Goal

The authors recognized that the medium component can be broken down into 2 types of defined methods, human-based and technology-based [8, 17]. Workman and Aldawood et al. defined human-based and technology-based medium allows individuals and organizations to better recognize and categorize the medium in which social engineers are utilizing in their attack. In the following, the 6 core-phases of SEAF:

1. ***Attack Formulation***: Goal Identification & Target Identification
2. ***Information Gathering***: Identify Potential Sources, Gather Information from Sources & Assess Gathered Information
3. ***Preparation***: Combination and Analysis of Gathered Information & Development of an Attack Vector
4. ***Develop Relationship***: Establishment of Communication & Rapport Building
5. ***Exploit Relationship***: Priming the Target & Elicitation

9 https://plato.stanford.edu/entries/ethics-virtue/

10 https://plato.stanford.edu/entries/consequentialism/

11 https://plato.stanford.edu/entries/ethics-deontological/

6. ***Debrief***: Maintenance, Transition & Goal Satisfaction

Refined advancements Mouton et al. implemented to their ontological SEA model in creating their SEAF provides an important step forward for penetration testers and researchers [2]. For penetration testers, it provides the individual or team of individuals a preliminary tool to utilize in formulating their authorized SEA mission. For researchers, the comprehensiveness of every phase and associated steps of the SEAF provides accurate repeatable results which can be utilized in verifying and comparing to other models, processes and frameworks within SE [3].

IV. Proposed Social Engineering Attack Scenarios in Higher Education

Utilizing Mouton et al. proposed Social Engineering Attack Framework [3], the authors developed 9 total higher education social engineering attack scenarios. Attack scenarios are separated into 3 Bidirectional Attacks, 3 Unidirectional Attacks, and 3 Indirect Attacks. Below the authors provides an example of a Bidirectional Attack.

A. Higher Education Information Technology Technician Attack

Description of Attack Scenario: A social engineer (SE) impersonates an institution's information technology technician. The SE convinces a faculty member that he/she needs to gain access to their office data ports to conduct a network communication test. From there the SE install a man-in-the-middle device between the network port and the faculty's computerized terminal.

Components:

1. ***Communication***: Bidirectional Communication
2. ***Social Engineer***: Individual
3. ***Target: Primary***: Higher Education Institution, Secondary: Faculty
4. ***Medium***: Face-to-Face (Human-Based)
5. ***Goal***: Gaining Unauthorized Access
6. ***Compliance Principles***: Consistency Principle
7. ***Technique***: Pretexting

Phases:

1. ***Attack Formulation***

- **Goal Identification**: The goal is to gain unauthorized access to the higher education institution's computerized terminal.
- **Target Identification**: "Primary target" of the attack is the higher education institution. To engage their primary target, the SE will initiate attacks on any faculty member within the institution. The "secondary target" have the ability to grant the SE access to the institution's computerized terminal.

2. ***Information Gathering***

- **Identify Potential Sources**: Potential intelligence sources include but not limited to higher education's internet facing website, social media accounts, and physical reconnaissance. Social media intelligence sources can encompass any faculty member, ranging from national, international, undergraduate professor, and graduate professor, that are associated with the institution. As well as information on everyone in the institution's information technology department. Physical reconnaissance intelligence gathering include roaming reconnaissance of information technology department locations.
- **Gather Information from Sources**: Assemble intelligence from the above sources.
- **Assess Gathered Information**: Compiled intelligence into a cohesive insight of the attack vector. Type of faculty members that have access to computerized terminal(s). Type of IT Technicians that work for the institution's IT Department. Type(s) of clothing and uniform specific IT Technicians wear. Compile a detailed mapping of faculty members' location. Detailed mapping of the IT Department's main and sub locations. Compile a timeline of when faculty members are located that have access to computerized terminal(s). A timeline of when IT technicians are located in specific locations in the institution's footprint.

3. ***Preparation***

- **Combination and Analysis of Gathered Information**: Determine the best time slot when faculty members and IT technicians are actively located in the same location. The SE will ensure to wear the prescribed uniform of the institution's IT technician.
- **Development of an Attack Vector**: Develop an engagement plan that detail the specific time and location of the attack. Details include the types of IT technician uniform, location of faculty member, and precise conversation script used in the attack.

4. ***Develop Relationship***

- **Establishment of Communication**: SE will engage in conversation with the faculty

member. Informing the faculty member that the IT Department has to check the data communication of their data port. This is to ensure the faculty member doesn't have any unplanned network interruptions.

- **Rapport Building**: SE will engage in friendly conversation and build a relationship with the faculty member at the institution to gain their trust.

5. ***Exploit Relationship***

- **Priming the Target**: SE is required to inform the faculty member that the work needs to be done so the faculty member can stay productive. This primes the target to allowing and assisting the attacker in resolving possible network issues.
- **Elicitation**: SE offers to assist the faculty member in any future IT issues that he/she might have. Provides the faculty member with a fake IT helpdesk phone number.

6. ***Debrief***

- **Maintenance**: After the SE has install the MITM device and conducted the network check. The attacker informs faculty member that their network communication is OK and will not be interrupted.
- **Transition**: Attacker was able to successfully gain access to the unauthorized computerized terminal and then proceeds to the "Goal Satisfaction" step.
- **Goal Satisfaction**: SE successfully completed the initial goal of gaining unauthorized access to a computerized terminal.

All the specialized higher education social engineering attack scenarios are publicly available on open source GitLab repository [33].

V. Proposed Social Engineering Awareness and Training Models

Current technical information security (IS) commodities have provided organizations across major industries greater capabilities in securing their information technology (IT) infrastructure. While every year there are incremental advances in IS products, they still fail to secure the human operators [26]. It is due to the expansion of technical IS solutions have pressed attackers into conducting social engineering (SE) engagements against an individual(s) of an organization [12 – 14, 20, 21, 25, 26]. The authors theorize that it is due to the lack of awareness and knowledge of SE tactics which is the main factor in increased social engineering attacks (SEA). Technical and non-technical individuals do not need to understand the weaknesses in an IT system. They need to be aware of the tactics used by attackers to circumvent the technical security systems [19 – 21, 23, 24, 26]. If a person sees something suspicious, they can report and stop the incident from escalating to compromised IT systems.

Individuals are an essential component to the IS landscape. Not only are individuals a part of the IS problem, but they are an integral part of the IS solution [12, 26]. Organizations across the industries have implemented security awareness and training solutions to enhance their organizational human security. An example is The Department of Homeland Security's (DHS): National Cybersecurity Awareness Month[12] (NCSAM). NCSAM does a great job in providing annual guidance and awareness to industries and the general public for the month of October.

The authors propose developing a High Education (HE) Awareness and Training Model similar to Mohammed et al. and Jansson et al. [13, 14] but improves upon their limitations. By incorporating specialized crafted social engineering attack (SEA) scenarios into awareness and training programs. It will greatly increase the level of preparedness in student, faculty, and employees when challenged with a SEA. In the following sections are the Higher Education Awareness and Training Models.

A. Higher Education Awareness Lifecycle Model

HE awareness model is tailored to 3 human domains (HD) in HE institutions. HD encompasses: (1) Students, (2) Faculty, and (3) Employees. Segmenting awareness education allows for effective absorption of the information [13]. Each HD combined together interface with varying ITs and hold varying levels of access privileges. Tailored awareness education provides each HD clarification to their defined responsibilities in their realm of influence. Method of distributing awareness materials will take the form of physical and electronic mediums. Figures 1 below detail the types of mediums:

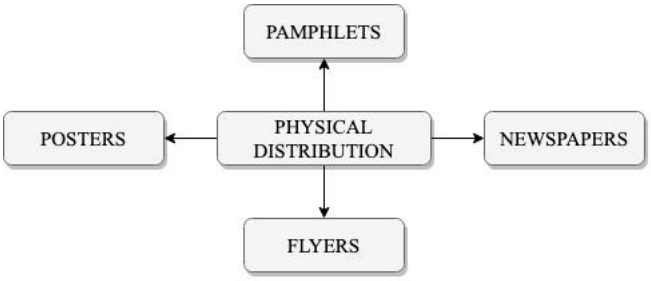

Figure 1a: Physical Distribution Medium

12 https://www.cisa.gov/national-cyber-security-awareness-month

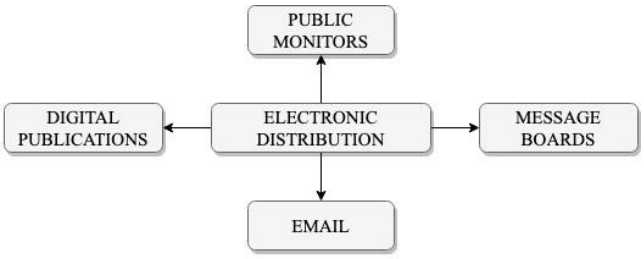

Figure 1b: Electrionic Distribution Medium

Fig. 1. Awareness Training Distribution Mediums

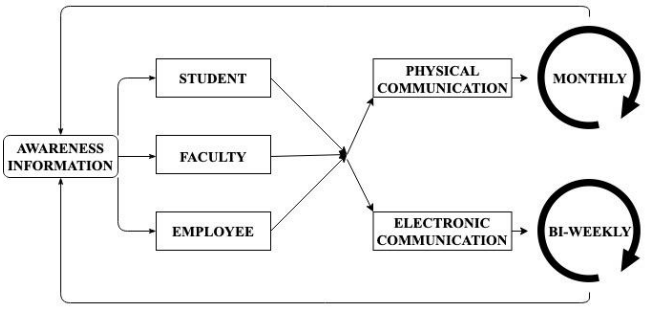

Fig. 2. Higher Education Awareness Lifecycle Model

The authors propose a continuous rotating lifecycle approach to HE awareness education. This approach can also be classified as passive learning. Awareness information is distributed but does not mandate the HD to engage with it. The proposed lifecycle tailors specialized awareness information for each HD, utilizing each communication medium, and refreshes monthly and bi-weekly. Figure 2 below details the HE Awareness Lifecycle Model:

B. Higher Education Training Lifecycle Model

Similar to the proposed HE Awareness Lifecycle Model, HE Training Lifecycle Model proposes an active learning approach. The proposed model will mandate incoming or transfer, undergraduate or graduate students, new faculty, and employees to physically participate in an IS on-boarding program with an institutional directed IS professional. The on-boarding program will provide guidance and orient individuals to the higher education's specific IT ecosystem and IS policies. Throughout the individual's duration in the institution, electronic refresher training is required. Refresher training will be conducted in a tri-annual cycle. The proposed tri-annual timeline commences January, May, and September. Training will also include review of on-boarding concepts and up-to-date SE attacks. Figure 3 details the Higher Education Training Lifecycle Model.

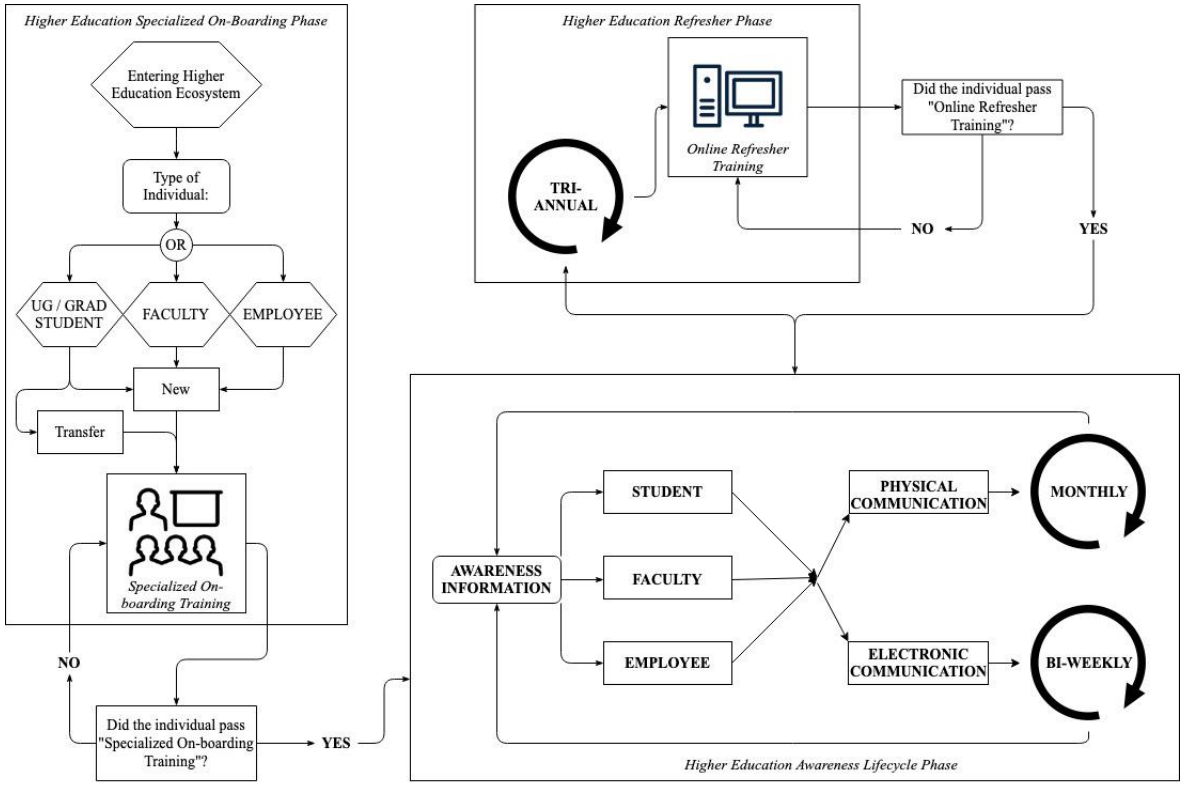

Fig. 3. Higher Education Training Lifecycle Model

VI. Discussion and Future Work

The paper proposes 9 specialized social engineering attack (SEA) scenarios focusing on the higher education (HE) landscape. These attack scenarios provide a detailed mission plan for SEAs on higher education institutions. The social engineering attack framework (SEAF) allows penetration testers and researchers to step through each phase an attacker will take in conducting a SEA. This grants penetration testers, researchers, and ethical oversight committees another tool in fulfilling their professional obligations. For penetration testers and researchers, it allows them to engage in both ethical and unethical SEA planning and research. For ethical oversight committees it allows the committee body to review the work of penetration testers and researchers so that they are within ethical standards.

The authors theorize the proposed HE social engineering awareness and training models will assist in securing the human dynamic. Through policies of continuous social engineering awareness and training, across every level of the human dynamic, HE institutions will be able to actively and passively educate an individual the moment they enter the institution's technology ecosystem until they leave. This affords HE institutions a comprehensive information security defensive formation alongside their physical security, hardware and software security technologies.

The authors realize the necessity for quantifiable data on the effectiveness of proposed HE social engineering awareness and training. With the foundation of the specialized higher education social engineering attack scenarios created, the authors propose a 3-phase methodology in gathering the data set and conduct efficiency analysis of proposed awareness/training models. In the authors' future work, the first phase is collecting a baseline awareness of social engineering concepts and techniques by conducting a pre-awareness survey [15, 16, 23, 24]. In the second phase, implement the proposed higher education awareness lifecycle to initiate passive learning on existing individuals in the ecosystem. In parallel implement the higher education training lifecycle to initiate active learning on new individuals entering the ecosystem. In the third phase, conduct a post-awareness survey [15, 16, 23, 24] to gather quantifiable data on the effectiveness of the proposed awareness and training lifecycle model.

References

[1] T. Thornburgh. Social Engineering: The "Dark Art", in Proceedings of the 1st Annual Conference on Information Security Curriculum Development, InfoSecCD Conference October 8, 2004, Kennesaw, GA, USA, 2005.

[2] F. Mouton, L. Leene, M. M. Malan and H. S. Venter. Towards an Ontological Model Defining the Social Engineering Domain, in: K.K. Kimppa et al. (Eds.): HCC11 2014, IFIP AICT 431, 2014, pp.266 – 279.

[3] F. Mouton, L. Leene, M.M. Malan and H.S. Venter. Social Engineering Attack Example, Templates and Scenarios, Computer & Security, Volume 59, 2016, pp.186-209. ISSN 0167-209. https://doi.org/10.1016/j.cose.2016.03.004.

[4] K. D. Mitnick, W. L. Simon. THE ART OF DECEPTION: Controlling the Human Element of Security, Wiley Publishing, Indianapolis, 2002.

[5] T. R. Peltier. Social Engineering: Concepts and Solutions, Information Systems Security; Nov 2006; 15, 5; ABI/INFORM Collection pg. 13.

[6] S. D. Applegate, Major. Social Engineering: Hacking the Wetware!, in Information Security Journal: A Global Perspective, 18:40-46, 2009, Taylor & Francis Group, LLC. ISSN: 1939-3555 print / 1939 – 3547 online. DOI: 10.1080/19393550802623214.

[7] R. Heartfield, G. Loukas and D. Gan. You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks, in IEEE Access, vol. 4, pp. 6910 – 6928, 2016.

[8] M. Workman, Ph.D. Gaining Access with Social Engineering: An Empirical Study of the Threat, Information Systems Security, 16:6, 315 – 331, 2007. DOI: 10.1080/10658980701788165

[9] F. Mouton, M.M. Malan, K.K. Kimppa and H.S. Venter. Necessity for Ethics in Social Engineering Research, Computer & Security, Volume 55, 2015, pp.114 – 127. https://doi.org/10.1016/j.cose.2015.09.001

[10] J. Pierce, A. Jones, and M. Warren. Penetration Testing Professional Ethics: a conceptual model and taxonomy, in Australasian Journal of Information Systems, 13(2). 2006. https://doi.org/10.3127/ajis.v13i2.52

[11] D.B. Resnik and P.R. Finn. Ethics and Phishing Experiments, Science & Engineering Ethics, 2018, 24:1241 – 1252. https://doi.org?10.1007/s11948-017-9952-9

[12] G. Rotvold. How to Create a Security Culture in Your Organization: A recent study reveals the importance of assessment, incident response procedures, and social engineering testing in improving security awareness programs, Information Management Journal, vol. 42, no. 6, Nov-Dec, 2008, ABI/INFORM Collection, pp 32+.

[13] S. Mohammed and E. Apeh. A model for social engineering awareness program for schools, 2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA), Chengdu, 2016, pp. 392 – 397.

[14] K. Jansson & R. von Solms. Phishing for phishing awareness, Behavior & Information Technology, 32:6, 584-593, 2013. DOI: 10.1080/0144929X.2011.632650

[15] R.M. Groves, F.J. Fowler Jr, M.P. Couper, J.M. Lepkowski, E. Singer and R. Tourangeau. Survey Methodology. John Wiley & Sons, 2011, pp.149 – 253.

[16] T.L. Jones, M.A. Baxter, V. Khanduja. A Quick Guide to Survey Research. The Annals of The Royal College of Surgeons of England. 2013, pp.5 – 7.

[17] H. Aldawood and G. Skinner. An Advanced Taxonomy for Social Engineering Attacks. International Journal of Computer Applications. 177. 975-8887. 10.5120/ijca2020919744. Jan 2020.

[18] J. Jang-Jaccard and S. Nepal. A Survey of Emerging Threats in Cybersecurity. Journal of Computer and System Science, Volume 80, Issue 5, 2014, pp. 973 – 993, ISSN 0022-0000, https://doi.org/10.1016/j.jcss.2014.02.005

[19] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas and G. Giannakopoulos. The Human Factor of Information Security: Unintentional Damage Perspective. Procedia – Social and Behavioral Sciences, 147, 2014, pp. 424 – 428, DOI: 10.1016/j.sbspro.2014.07.133

[20] M. D. Richardson, P. A. Lemoine, W. E. Stephens, and R. E. Waller. Planning for Cyber Security in Schools: The Human Factor. Studies in Systems, Decision and Control, Educational Planning 2020, Vol. 27, No. 2, 2020, pp. 23 – 39, ISSN 2198-4190, https://doi.org/10.1007/978-3-030-43999-6

[21] W. Fan, K. Lwakatare and R. Rong. Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations. I. J. Computer Network and Information Security, 2017, 1, pp. 1 – 11, DOI: 10.5815/ijcnis.2017.01.01

[22] I. Ghafir, V. Prenosil, A. Alhejailan and M. Hammoudeh. Social Engineering Attack Strategies and Defense Approaches. 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, IEEE, 2016, pp. 145 – 149, DOI: 10.1109/FiCloud.2016.28

[23] H. Aldawood, T. Alashoor and G. Skinner. Does Awareness of Social Engineering Make Employees More Secure? International Journal of Computer Applications (0975 – 8887), Vol. 177, No. 38, Feb 2020.

[24] H. Aldawood and G. Skinner. Evaluating Contemporary Digital Awareness Programs for Future Application within the Cyber Security Social Engineering Domain. International Journal of Computer Applications (0975 – 8887), Vol. 177, No. 31, Jan 2020.

[25] H. Aldawood and G. Skinner. Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools and Solutions. IEEE Access, DOI: 10.1109/ACCESS.2020.2983280

[26] I. Corradini. Building a Cybersecurity Culture in Organizations, Chapter 3: Redefining the Approach to Cybersecurity. Studies in Systems, Decision, and Control 284, pp. 49 – 62, https://doi.org/10.1007/978-3-030-43999-6_3

[27] National Cyber Security Centre. The cyber threat to Universities. https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities, Sep 2019, (Accessed 02/21/2020).

[28] PurpleSec LLC. The Ultimate List of Cyber Security Statistics For 2019. https://purplesec.us/resources/cyber-security-statistics/#Education, (Accessed 07/09/2020).

[29] BlackFog, Inc. The State of Ransomware in 2020. https://www.blackfog.com/the-state-of-ransomware-in-2020/, (Accessed 07/09/2020).

[30] B. Freed. Michigan State hit by ransomware threatening leak of student and financial data. https://edscoop.com/michigan-state-hit-by-ransomware-threatening-leak-of-student-and-financial-data/, EDSCOOP, May 2020, (Accessed 07/09/2020).

[31] C. Osborne. University of California SF pays ransomware hackers $1.14 million to salvage research: The malware infected crucial research stored in the UCSF medical school's network. https://www.zdnet.com/article/university-of-california-sf-pays-ransomware-hackers-1-14-million-to-salvage-research/#ftag=CAD-03-10abf5f, Jun 2020, (Accessed 07/09/2020).

[32] P. Waldie, C. Freeze. https://www.theglobeandmail.com/canada/article-four-canadian-military-schools-affected-by-cyberattack/, Jul 2020, (Accessed 07/09/2020)

[33] T. Nguyen. https://gitlab.com/chuck_x_chuck/social-engineering-attack-scenarios/, (Accessed 03/14/2020).