2018

Social Engineering Knowledge Measured as a Security Countermeasure

Christopher Artejus Sanders
University of South Carolina

Social Engineering Knowledge Measured as a Security Countermeasure

By

Christopher Artejus Sanders

Bachelor of Science
University of South Carolina, 2015

Submitted in Partial Fulfillment of the Requirements

For the Degree of Master of Science in

Engineering Management

College of Engineering and Computing

University of South Carolina

2018

Accepted by:

Matt Thatcher, Director of Thesis

Csilla Farkas, Reader

Amir Karami, Reader

Cheryl L. Addy, Vice Provost and Dean of the Graduate School

DEDICATION

I dedicate this work to myself. It has been a long and grueling path, but nothing worth having will come easy. My work, school, and personal life has pushed me to the edge, but it was worth it. Push forward and succeed, old king.

ABSTRACT

Social Engineering has become a significant threat to the security of business, government, and academic institutions. As vulnerabilities to social engineering attacks increase, organizations must incorporate risk mitigation strategies to their portfolios of Information Systems Security Countermeasures (ISSC). The goal is to implement mitigation strategies that balance the cost of implementation, the privacy of employees, and the resulting expected costs of social engineering attacks. In this paper we develop an analytical model that calculates the total cost of protection, including the trade-off between the cost of implementing protection strategies and the resulting expected cost of social engineering attacks. We use the model to examine the sensitivity of total costs to various model parameters, including costs of training, knowledge retention and depreciation rate, and number of employees.

This model builds on prior work from the Ponemon Institute examining the economic costs of social engineering attacks and the methods implemented to reduce the risk and mitigate the costs of such attacks. In particular, we leverage the empirical analysis presented in Ponemon Institute(2015) to develop a model that examines the economic impacts of various mitigation strategies and the resulting economic trade-offs. This works illustrates that knowledge and awareness among users is an effective method for controlling social engineering threats. The scenarios highlighted in this work illustrated how costs play a role in protection using knowledge as a countermeasure and found the most cost-effective solutions using the same model used by Ponemon(2015).

This analysis may help companies develop efficient ways to protect themselves from social engineering attacks while efficiently managing resources in the social engineering realm.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION TO SOCIAL ENIGNEERING

Overview of Social Engineering in Cyber Space

Information Technology (IT) Security is of growing importance to businesses, governments, and academics. Rapid advancements in technology have been a double-edged sword – on the one hand providing attackers more opportunities to breach security while on the other hand providing defenders tools to prevent, detect, and address security breaches. When an organization quantifies its level of IT security, they often attempt to measure the success rate of detection or prevention of security threats created by a particular technology. While this may depict the security of a system from a network perspective, it does not accurately reflect the effectiveness of the security system in the presence of social engineering. Social Engineering is the use of relationships with people to attain a goal - in this case, obtaining access to or knowledge of a protected system. Social engineering essentially bypasses technological protections (e.g., firewalls, intrusion detection systems) altogether. Technologies implemented to provide security, automated or not, will at some point require human-computer interaction (HCI). These interactions provide an opportunity for social engineers to gain important information that gives them access a system and its data. Therefore, social engineering can be specifically defined as the methods of influencing users to divulge sensitive information or performing a task that may present an unforeseen threat to the security of a system. This threat vector is one of the few in which the threat is not necessarily an insider threat, but could be linked to honest users with limited understanding of the consequences of their actions. Common examples of social engineering include spearfishing attacks, pretexting, baiting, and quid pro quo attacks. These attacks involve a social engineer preying on the trust of a user to provide information that will enable the social engineer to infiltrate a secured system. The user may not even be aware of the attack since these attacks are typically embedded in personal interactions with a seemingly non-threatening individual (such as a customer). Social engineering presents a substantial, often ignored, threat to the security of IT systems and thus must be considered when organizations build their portfolio of Information Systems Security Countermeasures (ISSC).

The vulnerability to the risk of social engineering is based on the human component and can be linked to the lack of knowledge of best practices for technology use and protection by the growing base of technology users. According to Natalie Ebner [11] older adults are more susceptible to these kinds of attacks due to declines in cognitive functions and deception sensitivity. The human component of protection is vested in the knowledge of the person using the system.

Human Interaction

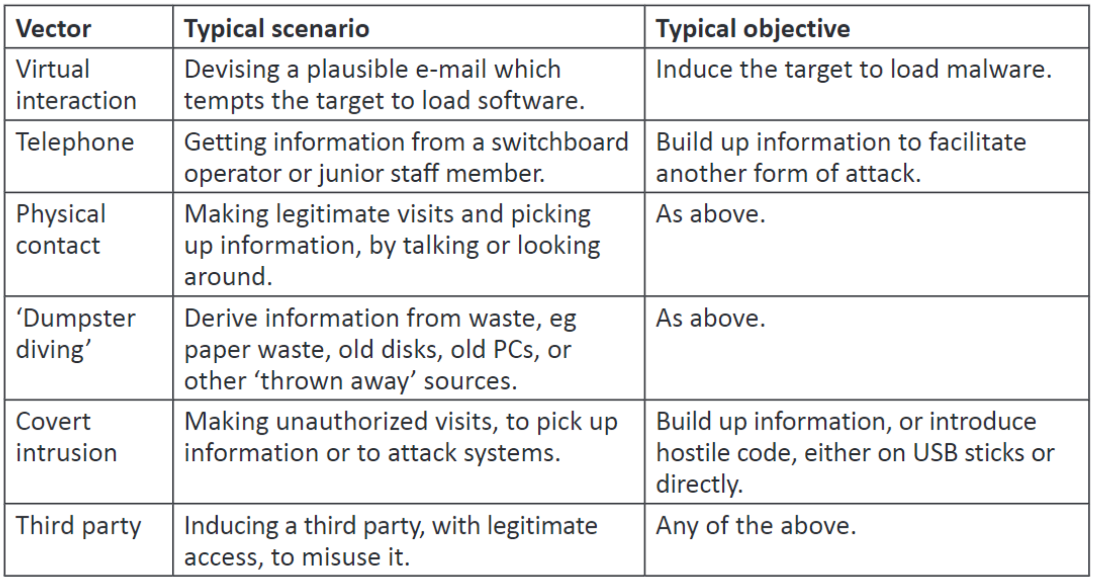
The user is one of the most important factors affecting the security of a system. In the 2017 Data Breach Investigations Report (2017 DBIR) produced by Verizon, there has been substantial growth in the use of social attacks to breach security since 2010; in fact, 43% of all security attacks in 2017 involved social engineering. Most individuals that work around security related information must obtain clearance prior to obtaining access to systems. Social engineering seeks to take advantage of the human-computer interaction by encouraging users to deliver information that may help the social engineer infiltrate a network. The human aspect of an ISSC cannot be overlooked due to the severity of the consequences. One uninformed user that falls prey to social engineering may generate substantial financial harm for a company and its stakeholders (e.g., customers, suppliers, distributors). According to the 2017 DBIR, only 20% of users falling prey to a phishing attack reported the suspicious activity as required by company policy. The 2016 Cost of Cyber Crime Study & the Risk of Business Innovation reports in their study that 70% of the companies surveyed experienced phishing and social engineering attacks on a worldwide scale. Phishing and social engineering accounted for 15% of the cyber-crime costs in the U.S. or approximately $2.6 million per company.

While users are often entrusted to avoid compromising a secured system or improperly disseminating protected information, these same users often do not understand the importance or their role in information security (Hong, 2012). For example, many users are susceptible to attackers who impersonate another employee (e.g., upper management) to generate an action or obtain some information from the victim. One popular example was the attack on Ubiquiti Networks in 2015. In this case, an email spoofing attack successfully convinced employees to transfer up to $46.7 million dollars to a third party overseas account – all without the employees taking additional steps to confirm the identity of the requester. Threats like these have leveraged the growing reliance of companies on technology – targeting users with links, on social media and in emails, that seemingly from the user the attacker is impersonating. While advances in technological security on some devices has helped to automate the detection of some of these attacks, defenses always lag behind attacks, leaving the user as the first line of detection. Regardless of the situation, the problem either begins or ends with the user.

As highlighted in Trim (2013) the human operator is susceptible to not only phishing attacks (as described above) but also other security attacks such as shoulder surfing, dumpster diving, reverse social engineering, and baiting:

- Phishing - duping an e-mail user to reveal personal or confidential information which the scammer can use illicitly.
- Shoulder Surfing – looking over someone's shoulder to capture information.
- Dumpster Diving – obtaining sensitive information, by sifting through discarded materials, that can be used to compromise a system.
- Reverse Social Engineering – setting up a scenario in which the victim would rely on the attacker to aid them in solving a problem; in this case the attacker impersonates someone who could help - e.g., an IT Help Desk representative.
- Baiting – leaving a malware infected device in a location where a targeted victim can find it.

Potential victims of a social engineering attacks must be aware of the type of attacks (see above), the sources/methods of each attack, and the consequences of attack. As shown in Figure 1.1, there are many different sources of a social engineering attack. According to Junger, "*An important advice is that users need more knowledge about how attackers operate, hence user education is necessary. In developing user education, it is important to determine priorities, teaching everything may amount to learning nothing much.*" Such education is likely an important element of an ISSC portfolio that may reduce the likelihood that a user inadvertently becomes a victim of social engineering.



Vector	Typical scenario	Typical objective
Virtual interaction	Devising a plausible e-mail which tempts the target to load software.	Induce the target to load malware.
Telephone	Getting information from a switchboard operator or junior staff member.	Build up information to facilitate another form of attack.
Physical contact	Making legitimate visits and picking up information, by talking or looking around.	As above.
'Dumpster diving'	Derive information from waste, eg paper waste, old disks, old PCs, or other 'thrown away' sources.	As above.
Covert intrusion	Making unauthorized visits, to pick up information or to attack systems.	Build up information, or introduce hostile code, either on USB sticks or directly.
Third party	Inducing a third party, with legitimate access, to misuse it.	Any of the above.

Figure 1.1 Attack Vectors (from Trim & Upton 2013) [10]

But in whom do we invest education? Simply, everyone. Every person ranging from the CEO of the company to the janitor that never touches a computer must understand how their behaviors affect an organization's vulnerability to cybersecurity attack. Every individual in a company presents some form of social engineering threat to the company. For instance, an individual without access to any system may unintentionally deliver a bad USB to a target because someone asked them to do so.

"The Cost of Phishing and Value of Employee Training" report presented by the Ponemon Institute revealed that the majority of the costs associated with a successful phishing attack performed is related to losses in employee productivity. According to the report, for an organization of approximately 9,552 users, at the expected average annual cost of phishing in 2015 was $3.77 million; productivity loss was expected to account for 48% of the loss. The report further implies implementing an annual training program that yields a 47.75% net improvement will lead to a 50% reduction in total costs or approximately $188.40 per employee/user. The rate of return is great based on their parameters, but this is not a universal rate of return nor is it representative of all learning styles.

The Social Engineering Cycle

The design and execution of a social engineering attack tends to follow a general framework. The social engineer begins by formulating an attack with a goal. The information gathering cycle follows and the attacker begins identifying information about its target until the information is actionable. The preparation then begins for the attack vector (Trim, 2013) and victim. The attacker then develops a relationship with its victim and tries to use that relationship to exploit the victim to attain the desired goal. Based on prior events, the end users should be educated to help them recognize the signs of social engineering.

Rating an ISSC

An Information Systems Security Countermeasure (ISSC) portfolio (Kumar, 2008) protects a system from threats, reduces downtime, and enables system restoration. Factors that affect the optimal ISSC portfolio include the cost and effectiveness of the countermeasure, the economic impact of a successful attack, and the probability of a threat (Kumar,2008). Kumar (2008) calculates the optimal countermeasure portfolio based on a specific objective – for example, minimizing worst-case costs versus minimizing expected costs. For an ISSC portfolio to remain effective, it must adapt with the changing methods of attacks.

Assessing the Social Engineering Threats

Analyzing the risk of a successful social engineering attack comes down to threat recognition. Can the user recognize the threat as it is occurring? For socially engineered attacks, can knowledge be used to combat these threats? Using knowledge as a countermeasure requires the user to draw on their knowledge of what a threat is and how to respond to them should they occur. Knowledge without application does not benefit the ISSC. In order for this awareness to be recognized and utilized regularly, users need to be trained. This training, when bestowed upon users, will serve to empower the users to leverage their newfound knowledge in practice. The training provided to the users should be recurring to improve their ability to recognize the threats as recognized in Knowledge and Practice in Business and Organizations[14]. This will provide users a chance to continually build upon their knowledge or at a minimum keep up with changes in the social engineering attacks the user may experience.

The goal is to build individual knowledge and awareness on the subject in order to understand what the users of a system know about threats and quantify/identify weaknesses in their knowledge.

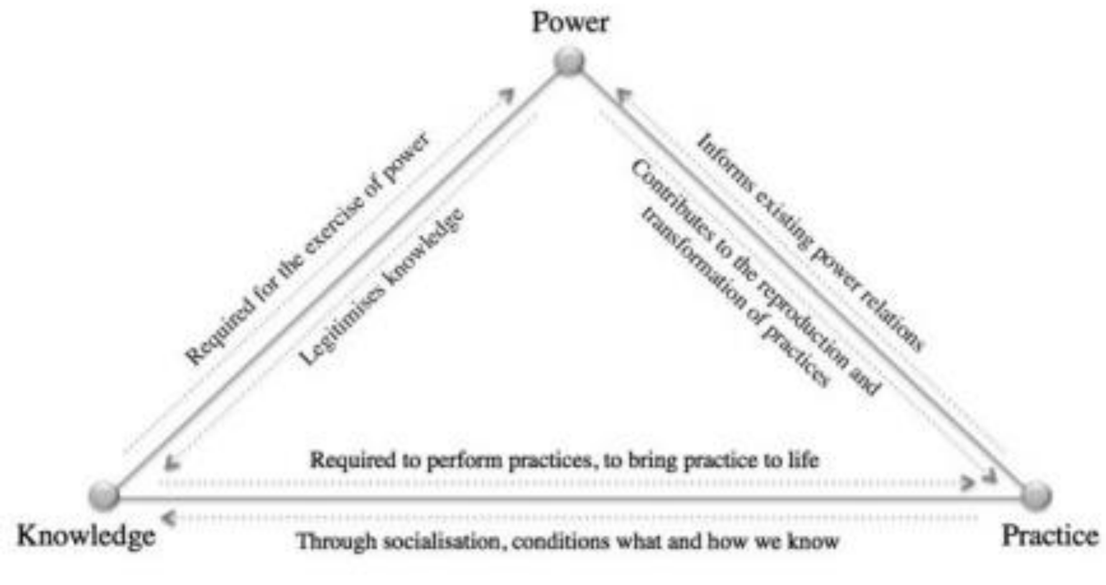
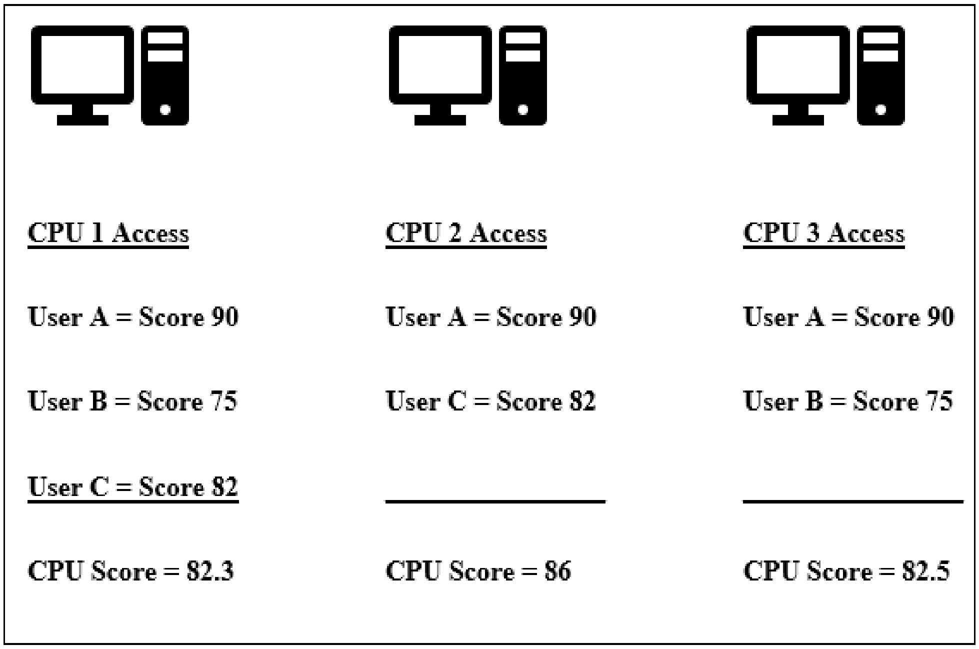

Power
Required for the exercise of power
Legitimises knowledge
Informs existing power relations
Contributes to the reproduction and transformation of practices
Required to perform practices, to bring practice to life
Knowledge
Through socialisation, conditions what and how we know
Practice

Figure 1.2: The triangular relationship between power, knowledge, and practice [14]

The concept of an observed score for each user can then be developed to represent more accurately what a user has learned while taking into account items such as overestimating or undervaluing the points assigned to a problem. The observed score can then be used as a basic baseline of the user’s understanding of social engineering. Further evaluation can then be used to identify what the user base may see as a more significant risk to the system using a scoring scale. The scoring scale would consider user responses to questions to understand their level of understanding about certain subjects. Once the administrator is able to identify a pattern, she can then use the emails or reminders to fill the knowledge gaps identified by the graded approaches. This is extremely important to a network of systems where user A may have access to several systems whereas user B may have access to only one of the systems to which user A has access.



CPU 1 Access	CPU 2 Access	CPU 3 Access
User A = Score 90	User A = Score 90	User A = Score 90
User B = Score 75	User C = Score 82	User B = Score 75
User C = Score 82		
CPU Score = 82.3	CPU Score = 86	CPU Score = 82.5

Figure 1.3 Example of Social Engineering Scheme

Training in Cyber Security

Training is an important aspect of many jobs to ensure that employees learn and maintain up-to-date knowledge related to their roles and jobs at their company. With the growth in technology integration across multiple industries, training in cyber security or best security practices in general has become equally as important to companies regardless of industry (2017 DBIR). Training helps individuals better prepare themselves for responding to cyber disasters or identify potential threats prior to the realization of any damage. The learning from training can take many forms based on the National Training Laboratories, Learning Pyramid (Strauss, 2013):

1. Lecture – Lectures commonly involve an education talk to a group of listeners. The knowledge retention rate is averaged to be 5%.

2. Reading – Reading comes in many forms such as email, newsletters, reports, etc. Reading information averages a 10% knowledge retention.
3. Audio/Visual – Videos and other forms of multimedia fills this niche and provide an average knowledge retention rate of 20%.
4. Demonstration – A demonstrator/instructor is demonstrating an experiment or process to the viewer. The average knowledge retention rate is 30%.
5. Discussion Group – This involves the students gathering and discussing the subject at large while providing an average retention rate of 50%.
6. Practice by Doing – The student performs the desired actions to get the desired outcome. The average knowledge retention rate of practice is 75%.
7. Teach Others/Immediate Use – Making the student the instructor can yield an average 90% knowledge retention rate for the student teaching.

Based on the Learning Pyramid, we see the many modes of teaching and their "expected" retention rates. Using these expected retention rates, we can deduce the associated improvement rate and potential costs and time commitment of each.

The Associated Costs of Training

When considering the economic implications of training users, we must consider the cost of a successful attack, the costs to train each user, and the rate of return that one will receive. The underlying variable that directly impacts all costs is time lost to low or no productivity for each user. The time needed to prepare, disseminate, and evaluate social engineering training is an important resource that organizations need to manage to maximize the rate of return. There is a need for balance between the cost of training the users and total cost of the attacks mitigated and with that balance an organization can defend itself without exceeding an optimal rate of return. Another important factor when considering the cost of training is the knowledge depreciation of users or the organization over time. The knowledge depreciation can be caused by numerous factors such as user turnover or natural depreciation among the users. If the knowledge depreciation rate is high, then more time/money needs to be invested in ensuring the knowledge retention rate can support the depreciation.

The Economic Cost Model

The total rate of return for training investment is a function of the cost of the attacks being mitigated in the year divided by the total cost of providing training. The cost of attacks, as calculated by Ponemon(2015), involved calculating the cost to contain malware, the cost of malware not contained, productivity lost due to phishing, the cost to contain credential compromises, and the costs of credential compromises not contained. The cost of attacks mitigated can be calculated by finding the product of the net improvement in knowledge and the initial annual costs of attacks (Ponemon 2015). Net improvement is calculated by the total improvement provided by the training multiplied by the knowledge depreciation rate. The cost of training is equal to the time invested into creating and disseminating the training and the cost of training materials/ knowledge retention. Time, in this model, will include the time lost in productivity and the time lost in implementation. These parameters can be manipulated year to year to model the changes in an organization; the rate of return from year to year can shift depending upon the cost of social engineering attacks, the knowledge depreciation rate, and the cost of training. The models discussed within look to provide further insight into how these parameters affect the effectiveness and the associated cost of using training to deter social engineering.

The Modeling Problem

Understanding the how to maximize the value of training for users is necessary for managers to make a determination in how to approach training (2015 Ponemon Institute). As seen in the previous section, there are several parameters that can play a role in determining the effectiveness of various training methods. This evaluation must be conducted periodically due to changes in attack methods and changes in costs. The cases examined further in the next chapter of this paper will explore how each of these parameters can impact the rate of return for organizations.

Table 1.1 Parameters Explained

Parameters/Equations/Variables	Description
t	Time invested in training
$c(t)$	Cost of training as a function of time and is the product of time invested in training and knowledge retention costs.
k_r	Average knowledge retention rates of the users
ω	Rate of return on training investment as determined be the cost of attacks being mitigated by training divided by the cost of training users.
α	The cost of attacks being mitigated which is calculated by the net knowledge improvement percentage multiplied by the costs of the total costs of all attacks had they been successful.
β	The cost effectiveness of a learning method.
ε	The net improvement provided by training which is a function of the average knowledge retention rates and the average knowledge depreciation rate of the users.
k_d	Knowledge depreciation rates of the users.

CHAPTER 2

MODELING KNOWLEDGE AS A COUNTERMEASURE

We model how knowledge and costs play a role in the selection of training methods to prevent and mitigate social engineering attacks. The model will take the aforementioned variables and demonstrate their relationships in practical application. The model will have one hundred users that require training. Case 1 will examine the correlation between cost of training parameters, time and knowledge retention, versus the cost effectiveness as the cost of training increases. Case 1 also looks at the expected net improvement as the knowledge depreciation rate among users increases. This case takes Table 2.1 and 2.2 to demonstrate the tradeoffs between the amount of money one can invest into training and the average knowledge depreciation rate of the users. Case 2 will examine the expected average rate of return and the cost effectiveness when given the different learning retention rates as presented by the Learning Pyramid (Strauss, 2013) and with assigned costs to each learning method. Case 2 seeks to find the practical cost effectiveness and rate of return of the learning methods to identify the most optimal method to utilize in a real world application by applying the same methods used by the Ponemon Institute (2015) to evaluate the utility in training users against social engineering attacks.

Assumptions

When working with people there are a lot of variables that can deviate at random and drastically such as memory loss, illness, or personality that cannot be accounted for by simulation. However, in this model we assumei each individual user is healthy, rational, and able to use solid judgement with proper knowledge. None of the users have malicious intent or seek to compromise the components. The users are adequetely trained to perform their job role on the component(s) they are allowed to access.

The next assumption is that each of the learning/ training methods are going to take roughly an hour to participate in for the user. This eliminates the ambiguity of how much time will be lost in productivity from user to user or the organization as a whole. This also means that we are assuming that the time to learn something for each user keeps each user within the allotted average from the Learning Pyramid. The users will receive the same benefits from the training.

The final assumption is the Learning Pyramid's accuracy and legitimacy in organizational learning. The learning pyramid has been challenged in its accurate approximation of the knowledge retention of users and their wide use of the methods. In this model, the methods are aligned with the way that learning method would be closely approached by an organization.

Case 1: Globally Evaluating the Model

Given the average knowledge retention rates based on the learning pyramid, linear trends are expected as shown in Tables 2.1 and 2.2. For Table 2.2, we illustrate the cost of attack as the 3.8 million annual average found in the 2015 Ponemon Institue Report.

From the trends, it is evident that ,in all cases, the higher knowledge retention rates, primarily the practice by doing and discussion group methods, will prove the most rewarding. Since knowledge depreciation is treated as a global variable among users, the knowledge retention rates can be the driver for maximizing net improvement. The issue with accepting these results is the real world practicality. In the application of these results, it is important to acknowledge the different learning methods will not all cost the same at any given time e.g. to implement the reading method may be as cheap and simple as sending an email while practice by doing may require an outside firm to train the employees which could cost significantly more; reading cost effectiveness is greater at $500 than practice by doing cost effectiveness at $10,000.

Case 2: Applying Knowledge Retention Costs

Acknowledging the real world issue, the models used in this case analysis will be approximations based on sources. The demonstration and the teaching others methods have been left out of the model due to either inconclusive approximations of costs or due to the productivity time lost would be too great to a fairly approximate. Utilizing the costs of training, Table 2.4 and 2.5 show how cost effectiveness can tell a different story when given the parameters of costs of training. The cost effectiveness of reading is far superioir than all other methods due to the ease of electronic publication and/or electronic messaging. The cost effectiveness of reading could have been lower in some other forms e.g. providing physical communications to each user. Although reading is the most cost effective method, it still yields the second lowest rate of return. The other drawbacks of the reading method is guaranteeing the users will read/receive the electronic communication. The secondmost cost effective method is the practice by doing method which provides the highest rate of return through knowledge depreciation.

Table 2.1 Net Improvement as Knowledge Depreciation Increases

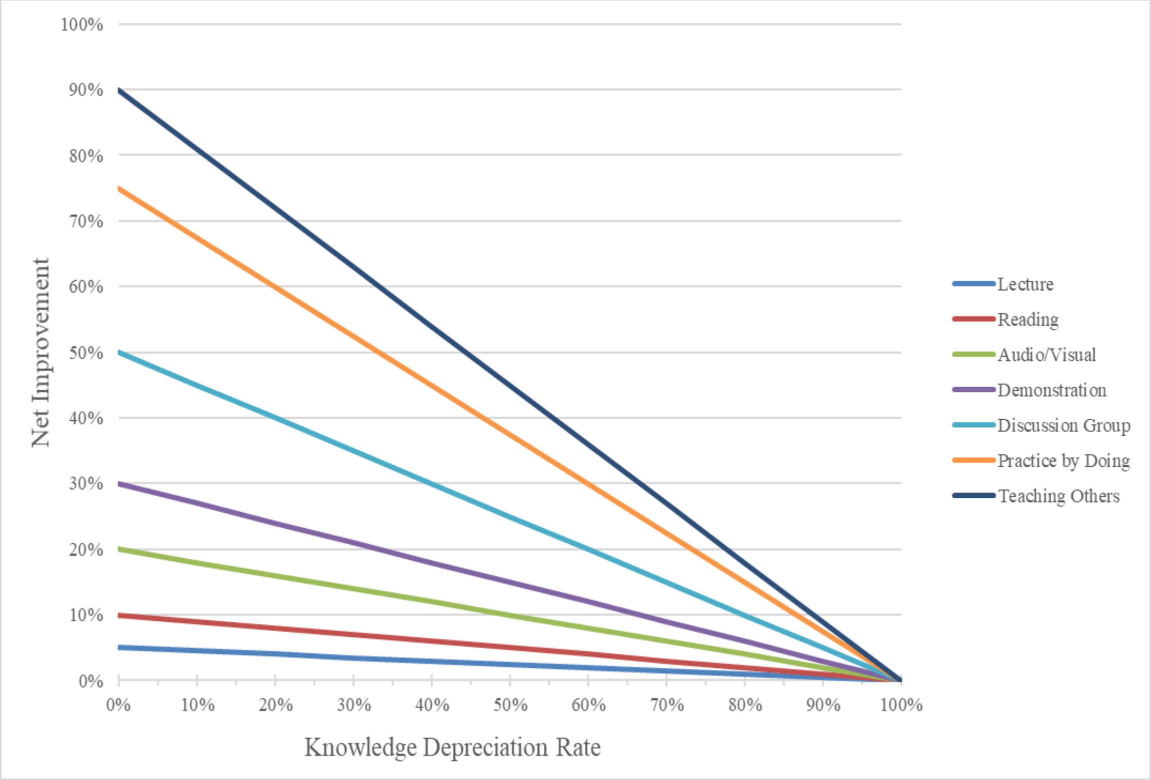


Table 2. 2 Cost Effectiveness as the Cost of Training Increases

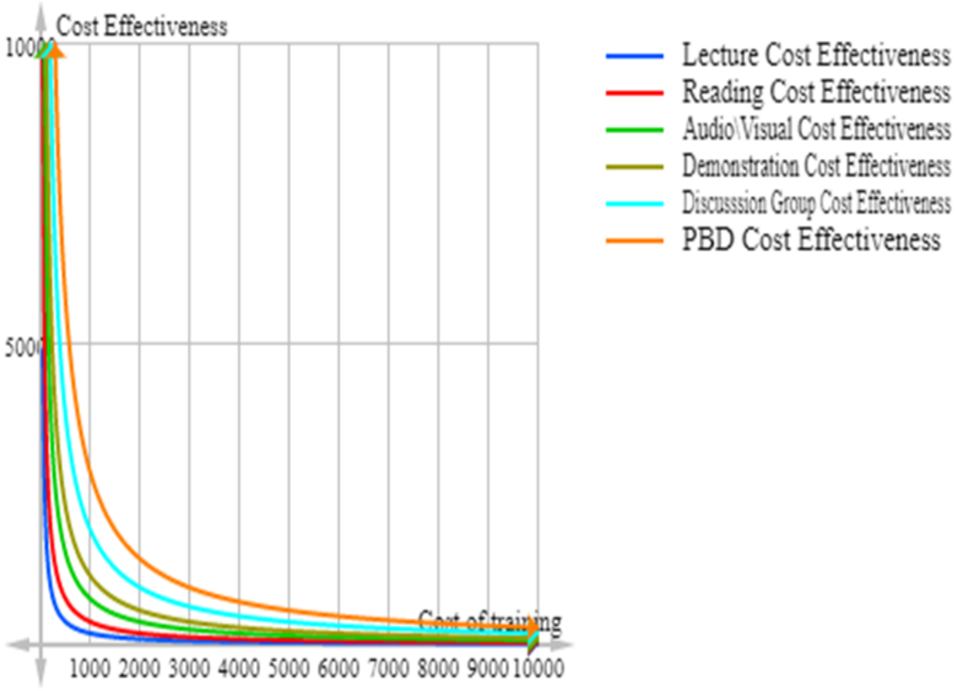
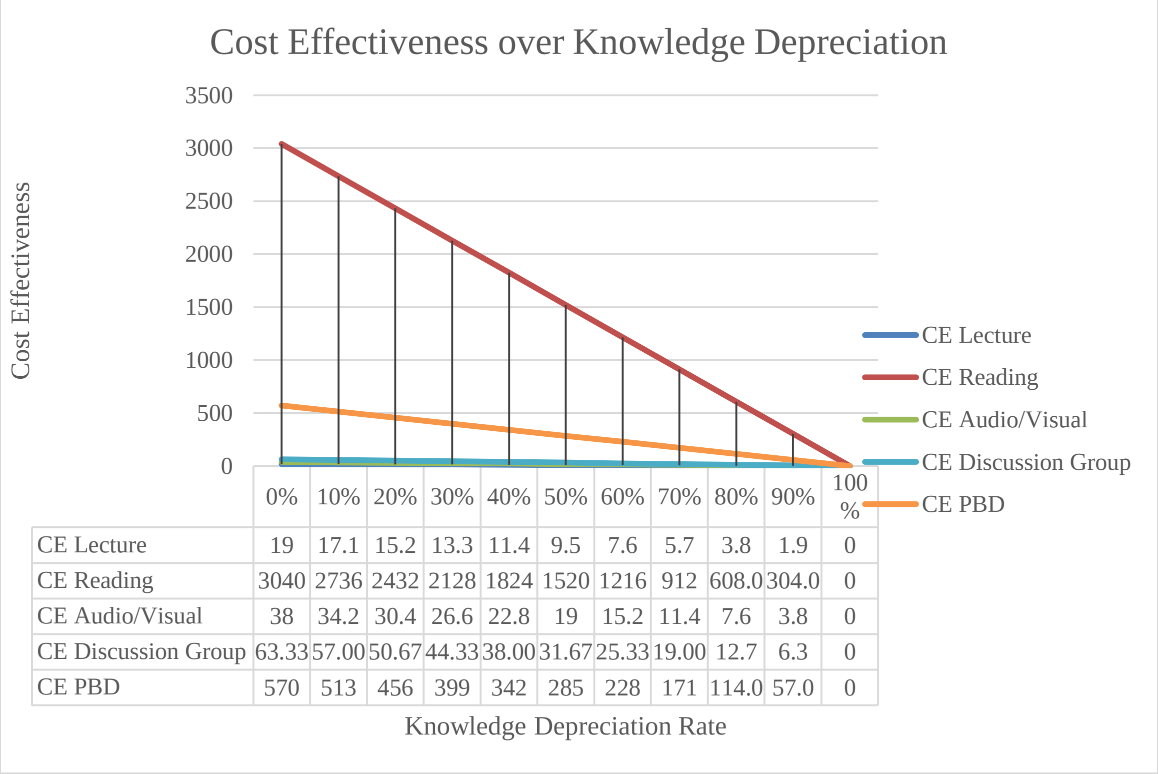


Table 2.3 Sample Cost of Training Used

Learning Method	Cost of Training	Description
Lecture	$10,000 [24]	Having a social engineering professional speak to the users.
Reading	$125 [27]	Creating an email newsletter to send to the users.
Audio/Visual	$20,000 [25]	Creating a professional video discussing the social engineering threats.
Discussion Group	$30,000 [26]	Holding several focus groups led by a trained facilitator.
Practice by Doing (PBD)	$5.00 per user/ $5000 [19]	Utilizing an outside company like Wombat Security to train users.

Table 2.4 Cost Effectiveness over Knowledge Depreciation



	0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100 %
CE Lecture	19	17.1	15.2	13.3	11.4	9.5	7.6	5.7	3.8	1.9	0
CE Reading	3040	2736	2432	2128	1824	1520	1216	912	608.0	304.0	0
CE Audio/Visual	38	34.2	30.4	26.6	22.8	19	15.2	11.4	7.6	3.8	0
CE Discussion Group	63.33	57.00	50.67	44.33	38.00	31.67	25.33	19.00	12.7	6.3	0
CE PBD	570	513	456	399	342	285	228	171	114.0	57.0	0

Table 2.5 Rate of Return over Knowledge Depreciation

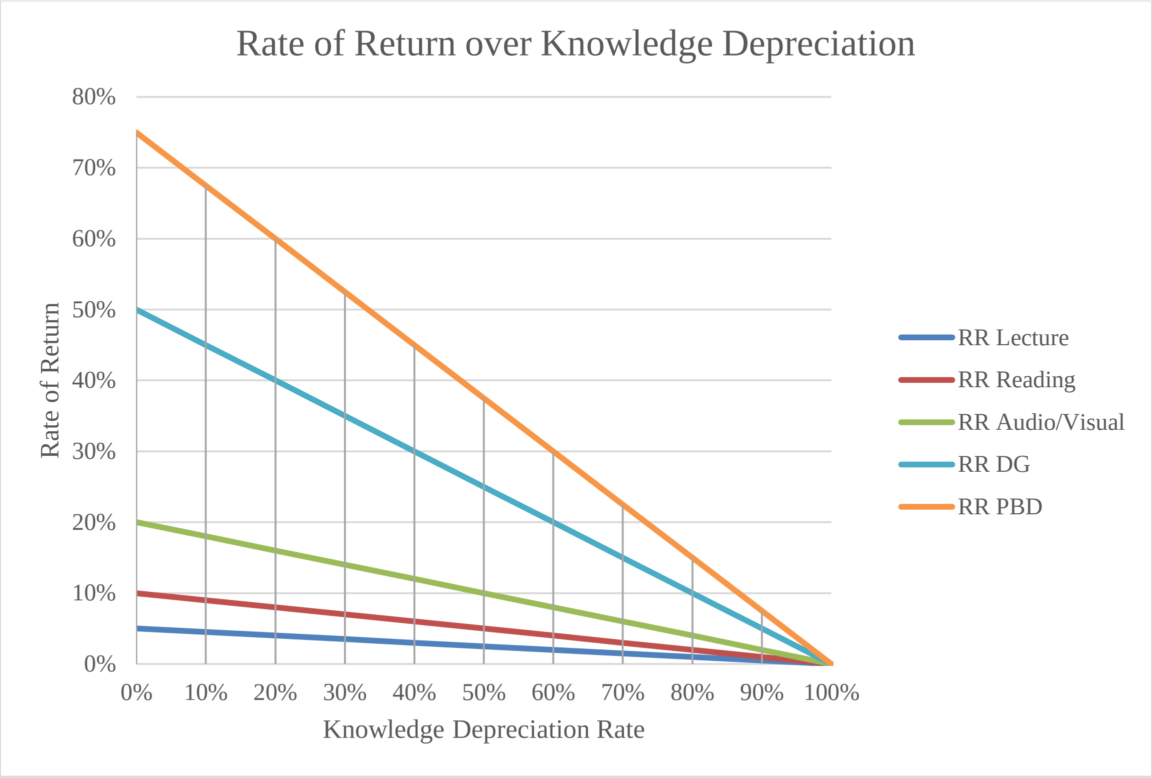


Table 2.6 Table Equations

Table number	Equation	Description
2.1	$\varepsilon = k_r * k_d$	Identify the organization's expected net improvement knowing the average knowledge depreciation levels.
2.2	$\beta = (3800000 * k_r)/c(t)$	Given the annual cost of social engineering attacks and the average knowledge retention rate, one can determine the cost effectiveness of a training method as the cost of training increases.
2.4	$\beta = (3800000 * \varepsilon)/c(t)$	Application of the costs of training in Table 2.3.
2.5	$\omega = \varepsilon$	Since the cost of an attack does not impact the rate of return, rate of return equals net improvement.

CHAPTER 3
CONCLUSION OF RESULTS

Conclusion

The use of user knowledge as a countermeasure is an important part of every ISSC that needs to be approached carefully to maximize the deterrence of social engineering attacks. Using the models provided, an organization can decide how to approach user training in a practical real-world application. The models demonstrate that based on the knowledge retention rates provided there is a linear relationship between the cost of training and the expected improvement regardless of the knowledge depreciation rate of the users, yet the knowledge depreciation rate directly affects the cost effectiveness of the training provided.

For future research, there are several aspects of the application of the models that can be expanded on. The first thing to expand on is the learning methods and their accuracy; determining the exact methods that are encompassed in the methods or if the learning retentions can be further expanded upon for newer learning methods. The second thing to consider is the impacts of the communication channels utilized for providing the knowledge e.g. physical/in-person delivery versus electronic or remote training. The third item to further investigate is how year to year rate of returns may shift due to knowledge retention, a potential knowledge cap in the users, or a higher turnover rate of users. Finally, maximizing the rate of return by mixing the training methods based on the likelihood of a user being targeted for a specific attack. It is important to gauge an individual’s “need to know” basis for training to limit unnecessary training costs; role based training may produce better cost effectiveness overall.

REFERENCES

1. Francois Mouton, Louise Leenen, H.S. Venter, Social engineering attack examples, templates and scenarios, Computers & Security, Volume 59, 2016, Pages 186-209, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2016.03.004. (http://www.sciencedirect.com/science/article/pii/S0167404816300268) Keywords: Bidirectional communication; Indirect communication; Mitnick's attack cycle; Social engineering; Social engineering attack detection model; Social engineering attack examples; Social engineering attack framework; Social engineering attack scenario; Social engineering attack templates; Unidirectional communication
2. Matthew Edwards, Robert Larson, Benjamin Green, Awais Rashid, Alistair Baron, Panning for gold: Automatically analysing online social engineering attack surfaces, Computers & Security, 2016, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2016.12.013. (http://www.sciencedirect.com/science/article/pii/S0167404816301845) Keywords: Social engineering; Vulnerability analysis; Open source intelligence; Social networks; Competitive intelligence
3. Stephan M. Gasser, Margarethe Rammerstorfer, Karl Weinmayer, Markowitz revisited: Social portfolio engineering, European Journal of Operational Research, Volume 258, Issue 3, 2017, Pages 1181-1190, ISSN 0377-2217, http://dx.doi.org/10.1016/j.ejor.2016.10.043.

(http://www.sciencedirect.com/science/article/pii/S0377221716308773)

Keywords: Finance; Socially responsible investments; Portfolio optimization; International financial markets

4. Waldo Rocha Flores, Mathias Ekstedt, Shaping intention to resist social engineering through transformational leadership, information security culture and awareness, Computers & Security, Volume 59, 2016, Pages 26-44, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2016.01.004.
   (http://www.sciencedirect.com/science/article/pii/S0167404816000067)
   Keywords: Transformational leadership; Information security culture; Information security awareness; Theory of planned behavior; Social engineering; Mixed methods research
5. Hossein Siadati, Toan Nguyen, Payas Gupta, Markus Jakobsson, Nasir Memon, Mind your SMSes: Mitigating social engineering in second factor authentication, Computers & Security, Volume 65, 2017, Pages 14-28, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2016.09.009.
   (http://www.sciencedirect.com/science/article/pii/S016740481630116X)
   Keywords: Phishing; 2-factor authentication; 2-step verification; SMS; Verification code forwarding attack; Human factors; Warning
6. Francois Mouton, Mercia M. Malan, Kai K. Kimppa, H.S. Venter, Necessity for ethics in social engineering research, Computers & Security, Volume 55, 2015, Pages 114-127, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2015.09.001.
   (http://www.sciencedirect.com/science/article/pii/S0167404815001224)
   Keywords: Consequentialism; Deontology; Ethical concerns; Ethics; Penetration

testing; Public communication; Social engineering; Social engineering research; Utilitarianism; Virtue ethics

7. Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl, Advanced social engineering attacks, Journal of Information Security and Applications, Volume 22, 2015, Pages 113-122, ISSN 2214-2126, http://dx.doi.org/10.1016/j.jisa.2014.09.005. (http://www.sciencedirect.com/science/article/pii/S2214212614001343) Keywords: Security; Privacy; Social engineering; Attack scenarios; Knowledge worker; Bring your own device
8. M. Junger, L. Montoya, F.-J. Overink, Priming and warnings are not effective to prevent social engineering attacks, Computers in Human Behavior, Volume 66, 2017, Pages 75-87, ISSN 0747-5632, http://dx.doi.org/10.1016/j.chb.2016.09.012. (http://www.sciencedirect.com/science/article/pii/S0747563216306392) Keywords: Priming; Warning; prevention; Social engineering; Phishing; Disclosure of personal information
9. Kumar, Ram L., Sungjune Park, and Chandrasekar Subramaniam. "Understanding the Value of Countermeasure Portfolios in Information Systems Security." Journal of Management Information Systems 25.2 (2008): 241-80. Web. 14 July 2017.
10. Trim, Peter R. J., and David Upton. Cyber security culture: counteracting cyber threats through organizational learning and training. Routledge, 2013.
11. Silman, Jon. Plugged in: cybersecurity in the modern age. University of Florida, 2016.

12. Lasky, Mary. “The value of tabletop exercises and one-Page planning documents.” *Journal of Business Continuity & Emergency Planning*, vol. 4, no. 2, 2010, pp. 132–141.

13. Russ-Eft, Darlene F. and Hallie S. Preskill. *Evaluation in Organizations : A Systematic Approach to Enhancing Learning, Performance, and Change*. vol. 2nd ed, Basic Books, 2009. EBSCO*host*, login.pallas2.tcl.sc.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=286538&site=ehost-live.

14. Knowledge and Practice in Business and Organisations, edited by Kevin Orr, et al., Taylor and Francis, 2016. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/southcarolina/detail.action?docID=4456342

15. Marzano, Robert J. and Development Association for Supervision and Curriculum. *Classroom Assessment & Grading That Work*. Assoc. for Supervision and Curriculum Development, 2006. EBSCO*host*, login.pallas2.tcl.sc.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=179528&site=ehost-live.

16. Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, 55(1), 74-81. http://dx.doi.org/10.1145/2063176.2063197.

17. *2017 Data Breach Investigations*. 10th ed., Verizon, 2017, pp. 1–72, *2017 Data Breach Investigations*.

18. Grubler, Arnulf, et al. “Sources and Consequences of Knowledge Depreciation.” *Energy Technology Innovation*, 2012, pp. 133–145., doi:10.1017/cbo9781139150880.014.

19. *The Cost of Phishing & Value of Employee Training*. Ponemon Institute, 2015, *The Cost of Phishing & Value of Employee Training*.

20. *2017 Cost of Data Breach Study*. Ponemon Institute, 2017, *2017 Cost of Data Breach Study*.

21. *2016 Cost of Cyber Crime Study & the Risk of Business Innovation*. Ponemon Institute, 2016, *2016 Cost of Cyber Crime Study & the Risk of Business Innovation*.

22. *2015 Cost of Data Breach Study: United States*. Ponemon Institute, 2015, *2015 Cost of Data Breach Study: United States*.

23. Strauss, Valerie. "Why the 'learning pyramid' is wrong." *The Washington Post*, WP Company, 6 Mar. 2013, www.washingtonpost.com/news/answer-sheet/wp/2013/03/06/why-the-learning-pyramid-is-wrong/?utm_term=.29163cb28495.

24. "How Much Do Speakers Really Cost?" Event Resources, 28 June 2016, eventresources.com/much-speakers-really-cost/.

25. 2017, Lee Frederiksen Ph.D. | December 4. "What Is the Cost of Video Production for the Web?" Hinge Marketing, 4 Dec. 2017, hingemarketing.com/blog/story/what-is-the-cost-of-video-production-for-the-web.

26. "Focus Group Research Costs Explained." Athena Brand Wisdom, 31 May 2016, www.athenabrand.com/blog/focus-group-research-costs-overview/.

27. "Our pricing." Email Monks, emailmonks.com/email-template-design-code-prices.html.