

Old Dominion University

ODU Digital Commons

Engineering Management & Systems
Engineering Theses & Dissertations

Engineering Management & Systems
Engineering

Spring 5-2023

Systemic Risk Analysis of Human Factors in Phishing

Mark Guilford

Old Dominion University, mguilfor@odu.edu

Follow this and additional works at: https://digitalcommons.odu.edu/emse_etds



Part of the [Computer Engineering Commons](#), [Risk Analysis Commons](#), and the [Systems Science Commons](#)

Recommended Citation

Guilford, Mark. "Systemic Risk Analysis of Human Factors in Phishing" (2023). Doctor of Philosophy (PhD), Dissertation, Engineering Management & Systems Engineering, Old Dominion University, DOI: 10.25777/fe48-z245
https://digitalcommons.odu.edu/emse_etds/194

This Dissertation is brought to you for free and open access by the Engineering Management & Systems Engineering at ODU Digital Commons. It has been accepted for inclusion in Engineering Management & Systems Engineering Theses & Dissertations by an authorized administrator of ODU Digital Commons. For more information, please contact digitalcommons@odu.edu.

SYSTEMIC RISK ANALYSIS OF HUMAN FACTORS IN PHISHING

by

Mark Guilford

B.S. May 2000, Old Dominion University

M.E. May 2011, Old Dominion University

A Dissertation Proposal Submitted to the Faculty of
Old Dominion University in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

ENGINEERING MANAGEMENT & SYSTEMS ENGINEERING

OLD DOMINION UNIVERSITY

May 2023

Approved by:

C. Ariel Pinto (Director)

Holly Handley (Member)

Chunsheng Xin (Member)

ABSTRACT

SYSTEMIC RISK ANALYSIS OF HUMAN FACTORS IN PHISHING

Mark Guilford
Old Dominion University, 2023
Director: Dr. C. Ariel Pinto

The scope of this study is the systemic risk of the role of humans in the risk of phishing. The relevance to engineering managers and systems engineers of the risks of phishing attacks is the theft of data which has significantly increased in the past couple of years. Phishing has become a systemic persistent threat to all internet users. Understanding the role of humans in phishing from a systemic perspective is a critical objective towards creating a strong defense against complex and manipulative phishing attacks. The systemic view of phishing concentrates on how phishing affects the entire organizational system, not just parts or individual components of a system. This study will address the systemic view of phishing which puts focus on how the entire organizational system performs and the purposeful tasks and goals to minimize phishing. This study will use a grounded theory approach to the following questions. First, how can the interaction between the human and the phishing lure be adjusted to mitigate the risk of phishing (i.e., from a systemic perspective)? Second, how can developing a systematic method help in mitigating the risk of phishing by reducing the likelihood of a successful attack? With the advanced persistent threat of phishing, this study anticipates assisting organizations in measuring how proficiently they are presently handling the risk of phishing and to suggest how the organizations can increase their proficiency and mitigate the risk of phishing.

Copyright, 2023, by Mark Guilford, All Rights Reserved

This thesis is dedicated to my wife, Lisa, my father, Abraham Guilford (2010), my parents, Mrs. Chiyoko Chu, and Dr. Joseph Chu. All who have given me hope, encouragement and comfort throughout the years. All who I love and cherish.

ACKNOWLEDGMENTS

I want to express my deepest gratitude to my awesome advisor Dr. C. Ariel Pinto. He has been patient, given me great advice, very encouraging, extremely helpful, and most of all greatly knowledgeable about my dissertation and my research. He has been a rock on my journey to becoming a PhD. I am very grateful for him having confidence and being honest with me. As my advisor, he guided me through many challenges and immensely difficult situations that I faced on my journey. I am enormously thankful for all his help.

I want to express my deepest appreciation to my committee members, Dr. Holly Handley and Dr. Chunsheng Xin for their patience, support, and knowledgeable advice. They have been very encouraging and inspiring during my journey. I want to thank Dr. Adrian Gheorghe for his words of wisdom and his enjoyable talks and advice. I want to thank the Chair of Engineering Management & Systems Engineering, Dr. Andres Sousa-Poza for his support and guidance on my journey. I want to thank all the Faculty, Staff, Students and Friends in Engineering Management & Systems Engineering for your kind words and help. A special thanks to everyone in the College of Engineering and Information Technology Services for your support and encouragement. I am grateful to the University for the Opportunity.

I want to thank my parents Mrs. Chiyoko Chu and Dr. Joseph Chu who gave me love, hope, support, and encouragement. I want to thank my brother, Abraham Jr., and my sister, Sharene for their encouragement. I want to thank all my friends and family.

Most of all, I am grateful to my lovely wife, Lisa. She is the love of my life, and she gave me the time, comfort, love, hope, drive, and encouragement to get me to the finish line.

Thank You Everyone!

TABLE OF CONTENTS

| | Page |
|--|------|
| LIST OF TABLES | viii |
| LIST OF FIGURES | ix |
| Chapter | |
| 1. INTRODUCTION | 1 |
| 1.1 OVERVIEW | 1 |
| 1.2 Key Concepts | 2 |
| 1.3 Description of the Research | 20 |
| 2. LITERATURE REVIEW | 23 |
| 2.1 INTRODUCTION | 23 |
| 2.2 Risk Management | 24 |
| 2.3 Phishing..... | 34 |
| 2.4 Phishing Models | 46 |
| 2.5 Models to Collect Socio Systems Data | 52 |
| 2.6 Conclusion | 60 |
| 3. METHODOLOGY | 61 |
| 3.1 GROUNDED THEORY | 61 |
| 4. RESEARCH ANALYSIS AND FINDINGS | 79 |
| 4.1 COLLECTING DATA | 79 |
| 4.2 Code Data..... | 79 |
| 5. THE MODEL..... | 84 |
| 6. TOOLIFICATION OF THE MODEL..... | 89 |

| Chapter | Page |
|-------------------------|------|
| 7. CONCLUSIONS..... | 96 |
| 8. FUTURE RESEARCH..... | 101 |
| REFERENCES | 102 |
| GLOSSARY | 112 |
| VITA..... | 115 |

LIST OF TABLES

| Table | Page |
|---|------|
| 1. Seven Generalizable Guiding Questions in Risk Management (Handley, 2019)..... | 11 |
| 2. Mapping of How the Steps in Human View Methodology May Provide Answers to the Seven Generalizable Guiding Questions in Risk Management (Handley, 2019)..... | 18 |
| 3. Table of Pros and Cons of 3 Different Models..... | 52 |

LIST OF FIGURES

| Figure | Page |
|--|------|
| 1. Phishing Attack Diagram | 5 |
| 2. Phishing Interaction Diagram (Handley, 2019) | 9 |
| 3. Simple Representation of the Hierarchy of Goals, Capabilities, Functions, Subsystems in architecture..... | 11 |
| 4. Goal G1 and Anti-Goal G1' Together with the Mirrored Architecture (Adapted from Pinto, eta al., 2010)..... | 12 |
| 5. Mirrored Architecture with Anti-goal G1' and Contributing Failed Capabilities, Functions, Subsystems..... | 14 |
| 6. Common Risk Matrix Highlighted with Severity and Likelihood Ratings for Failures of Timeliness (T), Accuracy (Ac), and Availability (Av) Goals (Handley, 2019) | 15 |
| 7. Two Strategies to Address Operational Risks May Contribute Toward a New Risk Event (Handley, 2019) | 17 |
| 8. Steps Common to a Risk Management Process (Garvey Book, p272) | 26 |
| 9. Threats and Vulnerabilities Affect Cybersecurity (Hoffmann, Napiórkowski, Protasowicki, and Stanik, 2019) | 28 |
| 10. Model of the Risk Management Process in an Organization (Hoffmann, Napiórkowski, Protasowicki, and Stanik, 2019) | 29 |
| 11. ISO 27001 ISMS Risk Management Process Model in Cyber Attack Management (Aluede, 2020) | 30 |
| 12. Risk Matrix for Phishing..... | 32 |
| 13. Developed Risk Matrix for Alphanumerical Classification (Aminudin, 2016)..... | 33 |

| Figure | Page |
|--|------|
| 14. Common Risk Matrix with Consequence and Likelihood Ratings (Handley, 2019) | 34 |
| 15. Total Phishing Attack Incidents (Gupta, 2016) | 36 |
| 16. Representation of Anti-Phishing Tool (Qabajeh, 2018) | 37 |
| 17. Taxonomy of Phishing Detection (Gupta, Tewari, Jain, and Arrawal, 2017) | 38 |
| 18. U.S. Cert Total Attacks (U.S. CERT, 2011)..... | 40 |
| 19. Impact of Email Fraud (U.S. CERT, 2011) | 40 |
| 20. Annualized Risk of Phishing Attacks (Brink, 2017) | 42 |
| 21. Potential Victim Phishing Susceptibility (Ting, 2016)..... | 47 |
| 22. HSM Model Phase Chart (Zhang, 2012) | 49 |
| 23. Direct Effects Chart (Bailey, 2018) | 51 |
| 24. Phishing Attack Taxonomy (Rastenis, 2020) | 53 |
| 25. Extended Phishing Attack Taxonomy (Rastenis, 2020) | 54 |
| 26. Overview of the Human Views Developed under NATO HFM-155 (Brusberg, 2011)..... | 55 |
| 27. Evolution Towards a Unified Architecture Framework (Hause, 2013)..... | 57 |
| 28. Personnel Taxonomy (UAFP, 2016)..... | 58 |
| 29. Grounded Theory Data Analysis Steps (O’Hagan and O’Connor, 2015)..... | 62 |
| 30. Flow Chart of Methodology Used for this Study | 63 |
| 31. NVivo Auto Coded Hierarchy Block Chart..... | 67 |
| 32. NVivo Auto Coded Hierarchy Circular Chart | 68 |
| 33. Auto Coded Themes and References | 69 |
| 34. Sequence of Individual Views (Handley, 2019) | 71 |
| 35. Risk Matrix in Phishing..... | 73 |

| Figure | Page |
|---|------|
| 36. Sargent’s Validation Techniques and Methods (Sargent, 2009)..... | 76 |
| 37. NVivo Document Database and Organization | 81 |
| 38. NVivo Document Relation Code..... | 82 |
| 39. NVivo Word Tree | 82 |
| 40. NVivo Article Word Search..... | 83 |
| 41. Representation of 3D Matrix Model for this Study | 85 |
| 42. IDEFO Systematic Phishing Mitigation Model..... | 87 |
| 43. Systematic Tool Operation Flow Chart | 93 |
| 44. Block Definition Diagram for the Systematic Phishing Mitigation Tool..... | 95 |

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

A popular method used by cybercriminals to steal sensitive information from online users and companies or to disrupt the operation of organizations is phishing. The number of phishing attacks has escalated in the past couple of years causing massive damage to companies and the loss of sensitive information to individuals (Iuga, 2016). It is estimated that phishing attacks have cost 500 million dollars a year in company revenues in the past 3 years (Mathews, 2017). This does not include the amount of money and sensitive data that individuals have lost due to phishing emails and pop-up web phishing scams.

Phishing's main objective is to deceive individuals who are members of a system into giving up sensitive information that can be used to exploit or extort them (Xu, 2012). Currently, there are several current models on phishing, each having its particular purposes such as Heuristic-Systematic Model (HSM), Elaboration Likelihood Model (ELM), and the interpersonal deception theory (IDT) (Xu, 2012). This study intends to create a systematic model that will help mitigate the risk of phishing. This will be accomplished by studying different models and engineering a model that will best fit the scope of this study. This study will seek to create a model that will produce a resolution from current given information.

In this study, systemic is a set or group of components that are related to or represent a select system. Systematic is a set or a group of components that work together to perform a specific task or have a specific goal in a procedural manner (Chyung, 2001). The core element in phishing is the individual human, hence the great importance of the field of the human factor. Phishing exploits the weakness, unawareness, and ignorance of humans and manipulates one into

thinking that one may have a great opportunity or a severe problem and must act immediately (Millettary, 2005). From a systemic perspective, phishing is directed at the system's human element to act in a way that will divulge sensitive information or disclose monetary information residing within the system, by extortion or deception (Frauenstein, 2016). Many existing models examine phishing with the human component. The direction of this model is not to detect phishing. This study will be evaluating the design of a model that will examine the current state of phishing and then seek to improve the current state of phishing.

1.2 KEY CONCEPTS

1.2.1. Phishing

Phishing is a technique in which cybercriminals try to deceive an individual into divulging sensitive and compromising information. This is done mostly with urgency but can also be accomplished passively using highly manipulative and deceptive persuasion. Phishing attacks typically have three components that make them effective: the lure, hook and catch (Chaudhry, 2016).

The lure is anything that attracts the attention of the individual. It is most often an email that offers a great reward if the individual acts right away and clicks on the included link or an email that states one must urgently click on the included link to change the password to an account. The lure can also be a phone call that offers economic benefits, e.g., a great deal on a vacation or a popular consumer item. It could be a phone call that says you are in danger, and you must act right away to avoid the consequences. Regular mail and text messages are also known to be used as lures.

The hook is when criminals have the individual's attention, the moment the individual thinks: What do I do? If one does what the criminals tell one to do, the individual is hooked. If one gets a phishing email and one clicks on the link with intentions of paying criminals, divulging any sensitive information to the criminals, or logging into the spoofed site using the link, the individual has been hooked. This is the reaction to the action of the lure. It is a positive reaction for scammers and cybercriminals. But a negative reaction in protecting oneself or the organization. A website, phone number, or any representation that mimics a legitimate institution to which an individual is willing to divulge sensitive or confidential information, is the hook.

The catch is the information that an individual divulges to the cybercriminal or scammer. This includes social security numbers, passwords, birth date, address, names, phone numbers, and any information that can be used to steal your identity or to infiltrate other systems. Any information collected that the phisher could make use of.

1.2.2 Human as Element of a System

In this research, the focus is on the human element of a system. The human individual comprises interrelated parts contained within a boundary serving one or more functions within an environment, then humans are both systems themselves as well as parts of larger ones. Humans are living systems (England, 2017), meaning that each human individual is different and can change without notice making the human individual system complex and unpredictable. The human – as a system on its own - has different properties and so need different methods for technical systems engineering. Humans are social animals with complex communication capabilities who gather for mutual benefit (e.g., share food, values, beliefs). Such groups

constitute social systems and become ‘Capabilities’ or Socio-Technical Systems (STS) when they include technology (England, 2017). The inherent difference of a human with other more technical elements of a system is best represented by Human Factors, which are the information related to characteristics, abilities, and limitations of humans that are applicable to a specific system design (Handley, 2010).

The Human View enables an understanding of the human role in systems/enterprise architectures. It provides a basis for decisions by stakeholders by providing a structured linkage from the engineering community to the manpower, personnel, training, and human factors communities (Handley, 2008). A Human View Diagram maps the activities that humans perform when interacting with a system.

Figure 1 is a Phishing Attack Diagram of the essential activities that humans perform while interacting with the phishing system including tasks, roles, and training. It shows the tasks of targeted humans in front of the computer as a ‘gatekeeper’ in process information and maintains communication, as well as the task of the attacker to steal sensitive information tasks. In particular, the primary tasks of the potential victim are through the computer as well as phones which point to risk mitigation strategies on these two interfaces by training on how to more accurately identify emails and phone calls that are not legitimate and possibly attempts to phish sensitive information. Many organizations are very aware that training is a major factor in reducing phishing. But even though organizations invest greatly in awareness and training there remains a risk. This study will help companies evaluate the remaining risk and seek to reduce that risk.

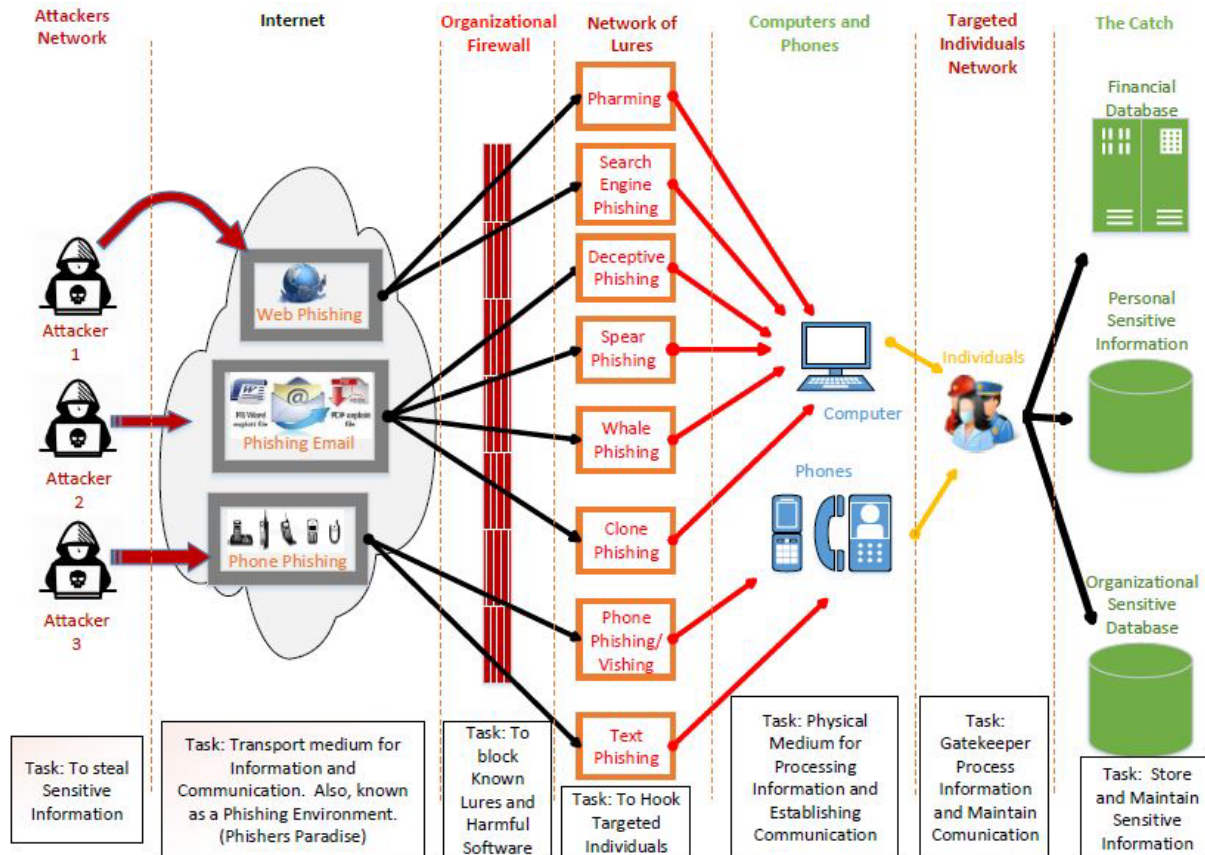


Figure 1. Phishing Attack Diagram

The definitions listed below are in the labeled zones in Figure 1. These are defined to give a better understanding of the process of an attack on an organization or individual represented by Figure 1.

Attackers Network: A system of 2 or more criminals that either work together or anonymously work in sync to disrupt systems or deceive and exploit individuals.

Internet: A globally interconnected system of computer networks that provide communication and information transport to computers, phones, and many other IoT devices to humans.

Organizational Firewall: A coordinated barrier designed to block unauthorized access or any harmful software from getting to the individuals' computers. This barrier monitors and controls any incoming or outgoing network traffic.

Network of Lures: A variety of different phishing techniques designed to attract the attention of the individual to deceive a human individual into divulging personal or organizational sensitive information.

Targeted Individual: The person that is focused upon by phishing exploits and could be the weakest link in a system. Not all people are the same and therefore they may be considered the weakest link. Humans that have many different characteristics, response, and systems of thought which can make them unpredictable and vulnerable.

Targeted Individuals Network: A system of two or more people that attackers seek to deceive or exploit to obtain sensitive and compromising information.

Organization: A coordinated body of people who work together to perform a specific purpose.

Database, Financial: The physical system in which a structured set of sensitive monetary data is stored.

Sensitive Information, Personal: The physical system in which personal data is stored or the individual which stores the data mentally in their brain.

1.2.3 Critical Types of Phishing

Phishing has many different techniques that are used to attack the human individual. Listed in this section are some of the most critical and effective types of phishing techniques. It is important to understand how these techniques are implemented and used, so the relevance of the systematic model can be understood with more clarity. The phishing types listed below are

identified in figure 1 as Network of Lures. This is to further understand the role of the types of network lures. Understanding these roles will help organizations access and understand the nature of the attacks and clarify the purpose of the attacks. This will allow organizations to modify or change the training material and/or methods.

Pharming: This is a more advanced attack on users. It is an attack on the organization's DNS Server also referred to as DNS poisoning. The DNS server converts names to IP addresses. The attacker can substitute a different IP for a name so that it would redirect users to the attackers' website. For instance, the attacker would substitute his IP for the Facebook website. When you type in the Facebook address name, the user gets redirected to the attackers' website that looks like Facebook. When the user tries to log in, the attacker records the login and password. The user tries to log in again and now is redirected to the actual Facebook website to login. But now the attacker has the user's login name and password.

Search Engine Phishing: This is when a hacker designs a website that has incredibly attractive offers that draw the user in to sign up for a deal that gets the user to give up sensitive information. This website has been registered legitimately with the search engine. These offers could be incredible prices on vacations or low-interest rates for credit cards.

Deceptive Phishing: This is the most common type of phishing where the phishers send an email impersonating a legitimate establishment in the hopes of deceiving an individual into giving up sensitive information.

Spear Phishing: This is the type of phishing that is specifically directed at a person or a group of people. Phishers will research specific people in an organization and will tailor the message specifically for that one person or that group of people to trick them into voluntarily divulging sensitive information.

Whale Phishing: This is phishing specifically directed at a CEO, President, or Owner of an organization. Phishers have become aware that most CEOs' or Owners do not attend security awareness programs and are vulnerable to phishing.

Clone Phishing: This is a method in which the attacker uses an exact clone of a legitimate email except the attacker changes the link in the email to redirect you to the phishers' site.

Phone Phishing or Vishing: This type of phishing is when an individual will typically get a phone call saying the individual's computer has a problem and it is attacking their network. Please log onto your computer and give them access to it for them to clean it. This typically comes with a cost. Or it could be a call from a bank or some financial institution asking an individual to enter their pin or account number to ensure your safety when it is the phisher trying to obtain your information.

SMS Phishing or Text Phishing: This is a method in which you get a text message in which you must respond with urgency to their message either by phone or by visiting their web page.

Figure 2 is a Phishing Interaction Diagram describing the interactions of humans with the phishing environment from the time the user clicks on a phishing email up to when the user is eventually becoming a victim, or 'hooked and caught'. Through this diagram, it becomes apparent the multiple times a human may have the opportunity to prevent being a victim. To prevent successful phishing, each block serves as a potential mitigation point. Through this interaction diagram, more pertinent details can be built into the model for more specificity. By identifying mitigation points, the model in this study will seek to clarify these points for improvement. If an organization conducts a study to discover that users are getting to the third mitigation point or worse, continuing to get phished. The organization can then modify its training materials to try to stop the individuals at the first mitigation point. This will mitigate the organization's risk of phishing.

Phishing Interaction Diagram in relation to HV - C

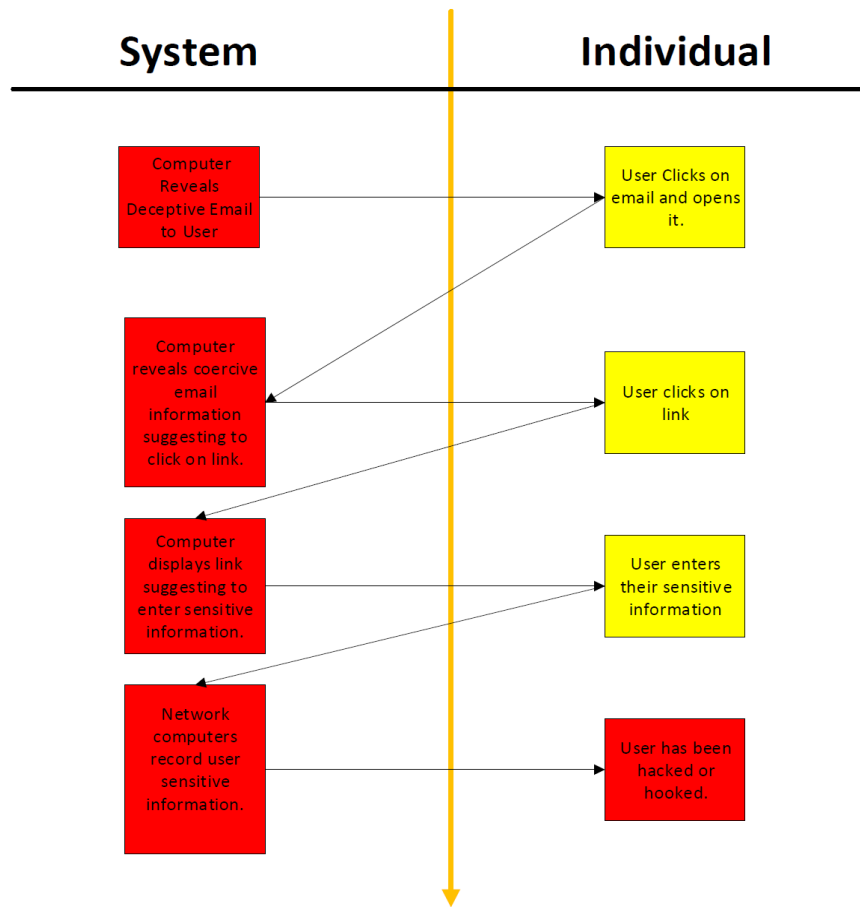


Figure 2. Phishing Interaction Diagram (Handley, 2019)

1.2.4. Operational Risk

1.2.4.1 General Descriptions of Operational Risk

When considering systems engineering, the operation may be considered as a set of processes designed to attain the objectives of the elements or the system. Risk is quite often thought of as things that go wrong. Basel II (2004) qualitatively expresses operational risk as:

“the potential undesirable consequences directly or indirectly resulting from failure of one or more elements of the system of interest.”

There are corresponding concepts that works as a foundation in the systemic approach to tackling operational risks, such as: accident, hazard, and of course, risk. Kaplan (1997) quantitatively described risk as:

$$R = F(S, L, X)$$

where

S – risk scenarios

L – likelihood of the scenarios

X – damage of resulting consequences

Keep in mind that the actual function $F()$ takes many forms depending on the theoretical and contextual perspective. A number of forms are simple products of the factor's likelihood L and damage X while the other ones are more complex.

1.2.4.2 Common Risk Management Steps

1.2.4.2.1

Risk management is a formal procedure used to constantly identify, analyze, and adjudicate risk events (Garvey, 2008). There are many risk management procedures used in numerous industries, disciplines, and professions. However, the seven generalizable guiding questions used in risk management are listed in Table 1 contains most of these processes.

| 7 Generalizable Guiding Questions in Risk Management |
|--|
| <ol style="list-style-type: none"> 1. What should go right? 2. What can go wrong? 3. What are the causes and consequences? 4. What is the likelihood of occurrence? 5. What can be done to detect, control, and manage them? 6. What are the alternatives? 7. What are the effects beyond this particular time? |

Table 1. Seven Generalizable Guiding Questions in Risk Management (Handley, 2019)

1.2.4.2.1.1 What should go right? (Handley, 2019)

A system is interpreted not only by the enumeration of its subsystems or elements, but more notably by assertion of its goal (or coupled, by its constraints). These intents or constraints – or things that go correctly – sets off engineering and management undertakings and are basic features of any design procedure. It may sound trivial, but the fundamental principle in this initial step is to know what can fail. Also, what should be successful. From a design point of view, one may deem a system to be a list of Goals, Capabilities, Functions, Subsystems, etc., as illustrated in Figure 3.

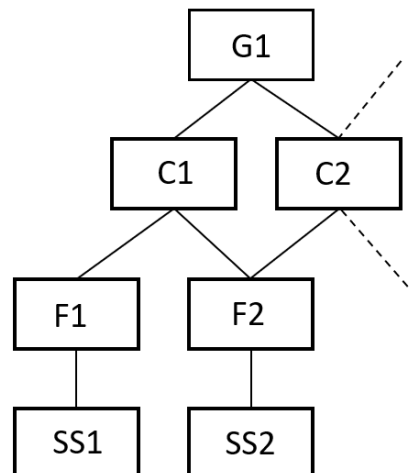


Figure 3. Simple Representation of the Hierarchy of Goals, Capabilities, Functions, Subsystems in architecture

1.2.4.2.1.2 What can go wrong? (Handley, 2019)

After the quintessential or right framework has been expressed in the form of objectives and constraints, one can now begin to identify what can go wrong. Predominately, recognizing risk events is essentially done by searching earlier on what has gone wrong in the past and understanding the procedure that occurred in events other than those coveted, i.e., those that are assumed to go right. Negative scenario identification is one frequent strategy that firstly develops different ways objectives can go wrong in a system rooted on what are known as coveted events. It is helpful to envision deviations from the norm. Using inherent language, sticking *not* to statements of objectives and constraints will frame first order - yet simplistic - risk statements. This has been previously pointed out as anti-goal by Pinto, et al (2010).

These anti-goals are shown in Figure 4.

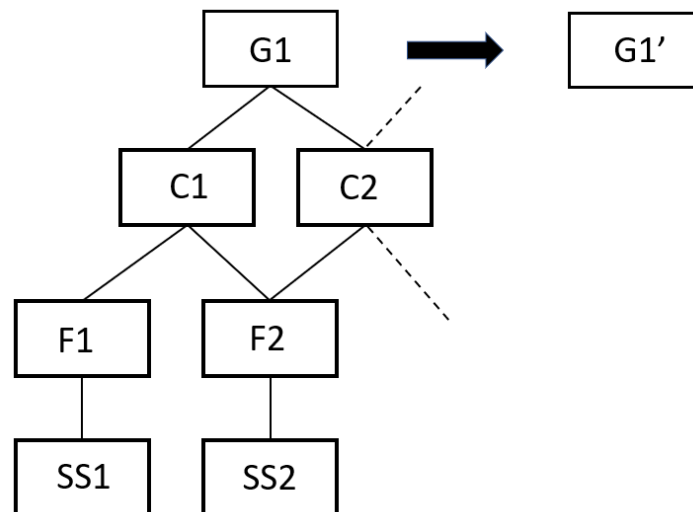


Figure 4. Goal G1 and Anti-Goal G1' Together with the Mirrored Architecture (Adapted from Pinto, et al., 2010)

1.2.4.2.1.3 What are the causes and consequences? (Handley, 2019)

Once risk events are discovered, the next stage is to detail these events for the intension of extending the comprehension and knowledge about the occurrence. This necessitates initiating

causality, distinguishing root causes and their probability, as well as designating consequences and impact. This is helpful in creating suitable and advantageous decisions or measures associated with the management of risk.

Formation of causes and consequences is established on the evidential relationship between incidents such that the event of one implies the events of the other. Nevertheless, the toughness of this causal relationship may rely on the attributes of their essential and sufficient relationships. Essential cause relationship proposes that a set of events (e.g., set B) is described to be essential to the cause of another set of events (e.g., set A) if B is a requisite circumstance for the occurrence of A, not that A occurs. Otherwise, ample cause relationship suggests that a set of events (e.g., set B) is described to be ample to cause another set of events (e.g., set A) if the occurrence of B assures the occurrence of A.

The contributing causes on the left side of the diagrams would be, singularly and completely, adequate causes for the events in the middle. Nevertheless, there are other feasible causes notwithstanding those shown in Figure 4. Hence, these causes are not essential.

1.2.4.2.1.4 What is the likelihood of occurrence? (Handley, 2019)

Succession of events that lead to a distinct risk event, being the causal chain of events, need to be defined in terms of their relevant chances of occurrence. The frequency or possibility of occurrence of a risk event relates to the quantitative or qualitative representation of how often or how soon a specific risk event may occur. This is often obtained from historical facts or data of the risk event. This can also be obtained from team-based provocation.

The concepts of necessary-and-sufficient causes placed together shape the foundation of determining causality in many fields as well as systems engineering and risk analysis. From a

risk management point of view, the utmost (yet perhaps impossible) goal is to pinpoint the necessary-and-sufficient set of cause, where an event B is essential and adequate condition for another event A if A takes place if-and-only-if B takes place. That is,

$$P(A|B) = 1 \text{ and } P(A'|B') = 1$$

Figure 5 demonstrates not only an unsuccessful scenario in the appearance of an anti-goal G1' but the additional causes as well – the unsuccessful Capabilities, Functions, and Subsystems. If C1' and C2' are compliments of C1 and C2 (i.e., unsuccessful to deliver C1 and C2, respectively), then unsuccessfulness of C1 and/or C2 assures failure of goal G1. This can be stated as:

$$P(G1'|C1' \text{ or } C2' \text{ or } (C1' \text{ and } C2')) = 1$$

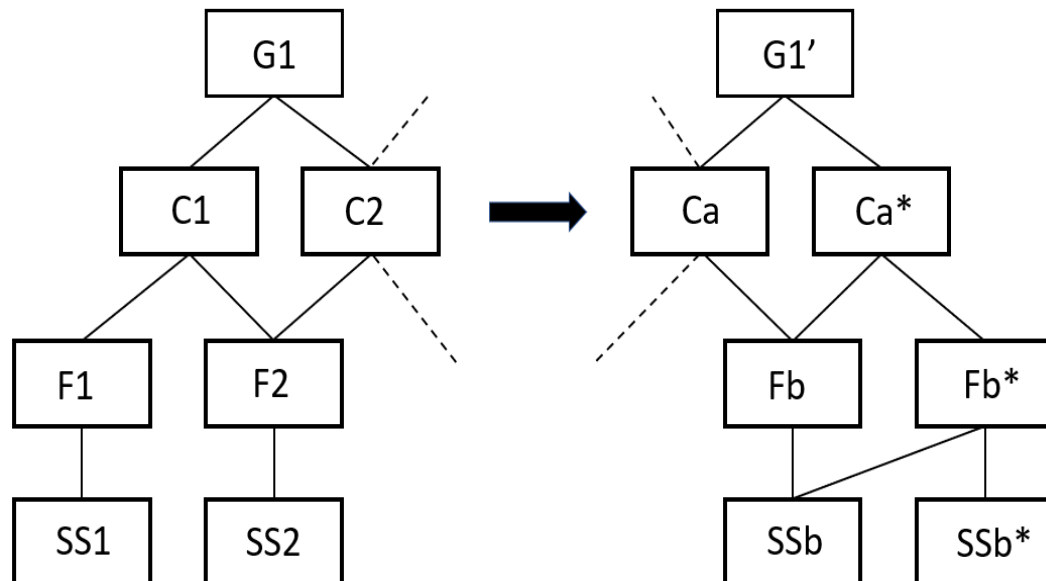


Figure 5. Mirrored Architecture with Anti-Goal G1' and Contributing Failed Capabilities, Functions, Subsystems

1.2.4.2.1.5 What can be done to detect, control, and manage them? (Handley, 2019)

Ranking and scoring is carried out to assess criticality and to decide respective importance. What could possibly be critical is contextual. Nevertheless, normal critical risks are those whose outcomes are associated to health and safety, compliance to regulatory requirements, or those that influence core mission and operational objectives. Criticality possibly could be evaluated using a risk matrix like that shown in Figure 6. This risk matrix emphasizes risk events with high intensity rankings such as those risks that fall into the catastrophic category of consequences or risks that fall into the category of likelihood of occurrence. Nevertheless, specific attention should be granted to those risks wherein consequences are catastrophic and the probability of occurring is very probable or notable. In Figure 6, these are the risk events that line up in the darker boxes. Risk events that line up in the darkest boxes are expected to be addressed right away. Risk matrix tables are beneficial for classifying and prioritizing discovered risks.

| | | Consequence | | | | |
|--------------------------|---------------------|-------------|------------|--------|-------------|--------------|
| | | Negligible | Minor | Major | Significant | Catastrophic |
| Likelihood of Occurrence | Very Likely | T | | | | |
| | Likely | | | | | High |
| | Moderately Possible | Low | Low Medium | Medium | Medium High | |
| | Unlikely | | | Av | | |
| | Very Unlikely | | | | Ac | |

Figure 6. Common Risk Matrix Highlighted with Severity and Likelihood Ratings for Failures of Timeliness (T), Accuracy (Ac), and Availability (Av) Goals (Handley, 2019).

1.2.4.2.1.6 What are the alternatives? (Handley, 2019)

Which risk treatment strategies will work well together, given the causal chain of events? Risk treatment strategies are not diametrically opposed, and gainful action plans are normally composed of the combination of strategies, yet in numerous degrees. Usually, risk treatment strategies are discovered for decreasing chances of occurrence, for decreasing consequences if they do happen, or both. Discovery and governance are the typical strategies to decrease the chances of happenings and are often deployed in prediction of a risk event, while reclamation plans tackle the mitigation of consequences after risk events have happened.

1.2.4.2.1.7 What are the effects beyond this particular time? (Handley, 2019)

From a system's point of view, it is critical to assess the effects of the risk treatment options to other components of the system. Risk treatment options may be examined in accordance with their effects to functionalities of the components of the system, the mode by which they modify interaction amidst the components, and their ability to impact future decisions. Also, this is the point where the reasonable level of risk is decided by equating the costs and benefits of each mitigated options. The idea of As Low as Reasonably Practicable, a principal approach that puts the risk to the bearable, satisfactory, and practical level is an example of a technique for this stage. Also, there is the thought of residual and emerging risks, which are embodiments of the reality that no risk events can be completely eradicated and that new ones possibly can materialize in the procedure of addressing others.

Take into consideration of the strategy 'Test device prior to each operation' to avert the aiding cause 'Device is faulty', and strategic plan 'Install alternative procedures if call is

abandoned' to mitigate the consequences of 'Call attempt abandonment'. Both strategies can certainly mitigate the entire operational risk but will produce added items on pre-operation check procedure which can ultimately result to prolonged pre-operative check processing time and prolonged training and certification process for the operators because of the additional procedure, as illustrated in Figure 7. These two prospective effects can then in turn produce reduction in the entire operational readiness. These prospective effects of the two strategies must be contemplated in the light of the conclusive decline in risk.

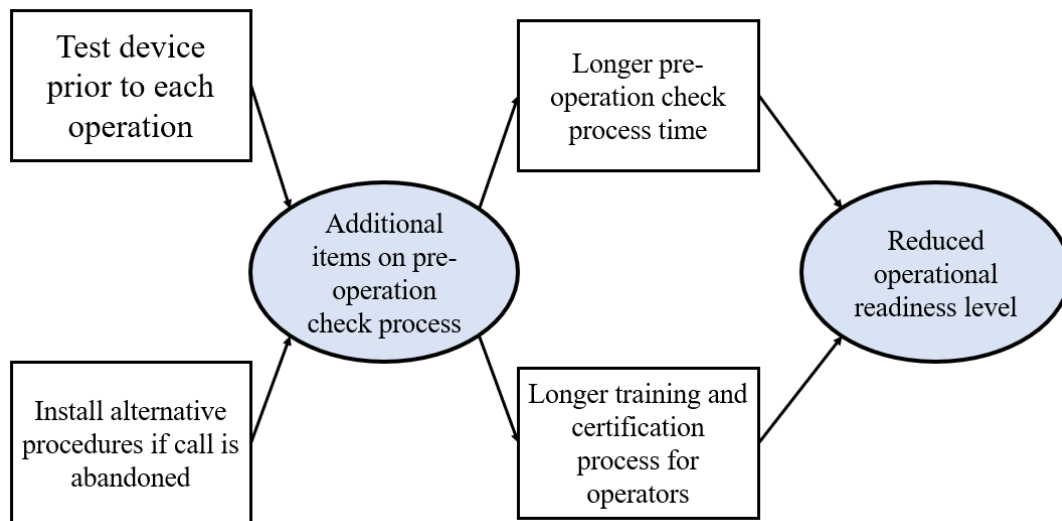


Figure 7. Two Strategies to Address Operational Risks May Contribute Toward a New Risk Event (Handley, 2019)

1.2.4.3 Operational Risk Management and Human Views

The Human Views method defines a procedure to detail the human system and capture it in a set of models to improve the architecture description by a series of verbose activities consisting of five steps: Concept, Data, Models, Analysis, and Fit for Purpose. These steps

present opportunities to answer the seven generalizable guiding questions in risk management, as shown in Table 2(Handley, 2019).

| 7 Generalizable Guiding Questions in Risk Management | Human Views Method Steps |
|--|---|
| 1. What should go right? 2. What can go wrong? | <u>Concept step</u> identifies the scope of human focused data pertinent to the area of stakeholder concern |
| 3. What are the causes and consequences? 4. What is the likelihood of occurrence? 5. What can be done to detect, control, and manage them? | <u>Data step</u> captures relevant attributes of each of the elements <u>Models step</u> illustrates the important relationships between the data elements that impact the system design |
| 6. What are the alternatives? 7. What are the effects beyond this particular time? | <u>Analysis step</u> analyzes different use cases to provide analytic data to support the decisions consistent with the context. <u>Fit for Purpose Views step</u> communicate results of analyses to support stakeholder decisions. |

Table 2. Mapping of How the Steps in Human View Methodology May Provide Answers to the Seven Generalizable Guiding Questions in Risk Management (Handley, 2019).

1.2.4.4 Example: Risks of Phishing and Human View Interaction and Task Diagrams

Humans are considered the weakest link in phishing (Boulton, 2017). Phishing's main objective is to attack the core system (the human system) to deceive individuals into giving up

sensitive information (Xu, 2012). By clicking on the link in an email or opening a document or a file that is attached to the email, the human can infect a computer and connected systems almost immediately in some cases. In other cases, the link will prompt an individual to log into a familiar site using the individual's password and ID, except the site is a fake site that captures their ID and Password. Other emails will ask the individual to call a phone number provided or click on the provided link to go to a website to enter credit card or banking information to pay for a service or product. If the individual responds to the suggested idea of the email, the individual will have divulged sensitive information to the hackers.

Hence, it is paramount in managing the risk of phishing to describe how humans interact with various aspects of phishing. Shown in Figure 2 is a Phishing Interaction Diagram describing the interactions of humans with the phishing environment from the time the user clicks on a phishing email up to when the human is eventually becoming a victim, or 'hooked'. Through this diagram, it becomes apparent the multiple times a human may have the opportunity to prevent being a victim. To prevent successful phishing, each opportunity also serves as a potential mitigation point. Through this phishing interaction diagram, more pertinent details can be built into the model for more specificity. Details such as to which mitigation point are people stopping. If individuals are stopping at the 2nd or 3rd mitigation point. We may want to know how we can train or educate individuals so they will stop at the 1st mitigation point. When an individual continues past the 1st mitigation point, the email will get even more deceptive and alluring to the individual coaxing the individual to continue a path for that individual to get hooked.

1.3 DESCRIPTION OF THE RESEARCH

The Human (or Human System) is a fragile system in relation to characteristics (curiosity, greed, compassion, and naiveté) and is considered the weakest link of a larger system and vulnerable to simple, advanced, and complex phishing attacks (Boulton, 2017). An uninformed human can be deceived even by the simplest of phishing scheme into revealing sensitive information that can cause a catastrophic failure in the technological system. Even when humans are informed, a sophisticated phishing attack such as whaling, and spear-phishing can be used to deceive an individual into revealing sensitive data causing a breach in the technological system that can lead to disastrous data and financial loss.

1.3.1. Research Goal

The goal of this study is to develop a systematic theoretical methodology to mitigate the risk of phishing.

The main objective of this study is to develop a systematic model of the role of humans in phishing. This objective is accomplished by:

- Analysis of current research in phishing
- Developing a knowledge base of phishing incidents
- Use Human View to guide and organize data in model development

1.3.2 Research Questions & Expected Results

The following questions will be addressed in this study:

1. How can the interaction between the human and the phishing lure be adjusted to mitigate the risk of phishing (i.e., from a systemic perspective)?

2. How can developing a systematic method help in mitigating risk of phishing by reducing the likelihood of a successful attack?

The Expected Results of this study are:

1. Create a knowledge base of phishing incidents.
2. Create a systematic model of phishing interactions with humans using a systemic perspective.

From these questions, this study will investigate the human factor, human view, systemic and systematic systems of phishing, which will focus on creating a knowledge base and a systematic model that will create a strong awareness of phishing tactics in the human system. By analyzing and evaluating the present state of the organization, the model will seek to decrease the risk of phishing in the organization by using a risk matrix or possibly developing a risk cube.

1.3.3 Research Methodology

1. Define the research method.
2. Identify the literature.
3. Grounded Theory Methodology is chosen.
4. Elaborate Patterns (Theory Saturation).
5. Model Development begins.
6. Interpret and report results and conclusions.

1.3.4 Significance of Research

The risk of phishing has daunted the cybersecurity community since the beginning of the internet. With over 4 billion internet users (Internet World Stats) online, phishers have an ample supply of victims to lure and hook. As the number of internet users grows, the dangers of phishing will continually be a threat to businesses, organizations, and people. This study will contribute to the body of knowledge in Risk Management and Cyber-Systems Engineering by identifying techniques used in risk management and systems engineering and applying them to the development of a theory and a systematic model that will identify the interaction of the human system with phishing techniques to effectively mitigate the threat of phishing. This model is not intended to detect phishing, rather it will help mitigate the current state of phishing of a company or organization.

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

Phishing risk has been investigated from the technology side (firewalls, anti-phishing software, browsers, etc.) for decades. However, investigating phishing risk from the socio side (human operator, organizations) can be used to further manage and reduce the risk of phishing. This literature will cover three main topics. First, Risk Management which will be used to measure the control over how likely a harmful event may happen by using the process of prioritizing, recognizing, and evaluating threats to the system. This will be characterized by the following risk formula:

$$\text{Risk} = F(\text{Consequence (Who, What), Frequency}) \quad (2.1)$$

Second, Phishing continues to grow at an alarming rate and has become the most profitable and economical technique for cybercriminals. Phishing has impacted the world market with heavy monetary losses for companies around the world. In 2018, the FBI reports losses over 12 Billion dollars and increasing. Akamae (2020) suggests that for every 99 legitimate emails, there is one phishing email (Guntrip, 2018). Addressing phishing risk through socio systems can mitigate the risk by identifying the lag between the occurrence of novel phishing threats and the response of directed organizational training. Negil (2011) agrees that there is a strong need for training and awareness. Third, phishing models which have led this study to develop a phishing matrix that would aid an organization in reducing the risk of phishing. Handley's conclusions of the NATO Human View Workshop have prompted this study to look at Three of the Eight NATO Human

Views (HV-C: Tasks, HV-D: Roles, HV-F: Training). Incorporating human views with risk management is a unique feature of this study.

2.2 RISK MANAGEMENT

Evaluating the risk of phishing is an important task. The body of knowledge in Risk Management will help many organizations understand how to approach the risk of phishing to the classification of the phishing attack. For this study, the definition of Risk Management is a process used to analyze, identify, and examine events that may occur that have undesirable impacts on a system's ability to attain its desired objectives or goals (Garvey, 2008). This describes the term 'risk' as the event that, if it occurs, has an undesirable impact on a system's ability to attain its desired objectives or goals (Garvey, 2008).

2.2.1 Risk Definition

Today's global cyberinfrastructure is threatened by many different risks. As the infrastructure continues to grow and reaches an increasing number of people, the risks exhibit more emergent properties, such as the increasing cost and impact of a successful phishing attack. The global interconnectivity of this system allows the formation of small security vulnerabilities that have not yet been discovered. This allows cybercriminals to discover and maliciously exploit these security vulnerabilities (targeting the human operators) using various phishing techniques.

In the 1980s, Kaplan (1980) suggested two quantitative formulas for risk. The first formula highlights a distinction between uncertainty and loss (or damage). This formula is:

$$\text{Risk} = \text{Uncertainty} + \text{Damage} \quad (2.2)$$

Uncertainty is the state of the ‘unknowing’, meaning, one does not know what to expect in each situation. Damage is what kind of loss has occurred. This leads Kaplan (1980) to the second formula with the distinction between risk and hazard. This formula is:

$$\text{Risk} = \text{hazard/safeguards} \quad (2.3)$$

Kaplan (1980) expresses that “risk is the possibility of loss or injury and the degree of probability of such loss”, while the hazard is the source of danger (Kaplan,1980). If a hazard is a source of danger, then a safeguard is needed to counteract hazards. Kaplan expresses that safeguards are the “idea of simple awareness”, meaning that the “awareness of risk reduces risk” (Kaplan, 1980).

Later in the 2000s, Haines (2008) characterized risk as “large-scale, complex, multiscale interconnected and interdependent systems with life cycles and uncertainty with emergent behavior” (Haines,2008). Haines (2008) expands on the idea of how large emergent complex and interdependent systems can pose a risk to the stability of the system itself. The interdependencies can either be an impediment or support to the system. When a system within the multisystem fails; what is the risk of that system causing a multisystem failure and causing the total system to fail? Haines (2008) describes this as a system vulnerable to specific threats that cause adverse losses and results in a risk to the system. But if the system recovers from this risk, this results in resilience. The speed of recovery results in a system being more resilient or less resilient. Haines (2008) states “when risk and uncertainty are addressed in a practical

decision-making framework, knowledge of risk assessment and management markedly fills a critical void that supplements and complements the theories and methodologies of systems engineering and analysis”.

More recently, Pinto, McShane, and Bozkurt (2012) described the risk in the perspective of systems of systems. They state that “to conduct efficient and effective identification, analysis and management of risk, the characteristics of both the event and the system it acts upon the need to be defined adequately” (Pinto, McShane, and Bozkurt, 2012). In this work, risk can be described as “undesirable events and consequences”.

2.2.2 Risk Management Process

Pinto (Garvey Book, 2013) states that “risk management can be characterized by the process illustrated below” (p272).

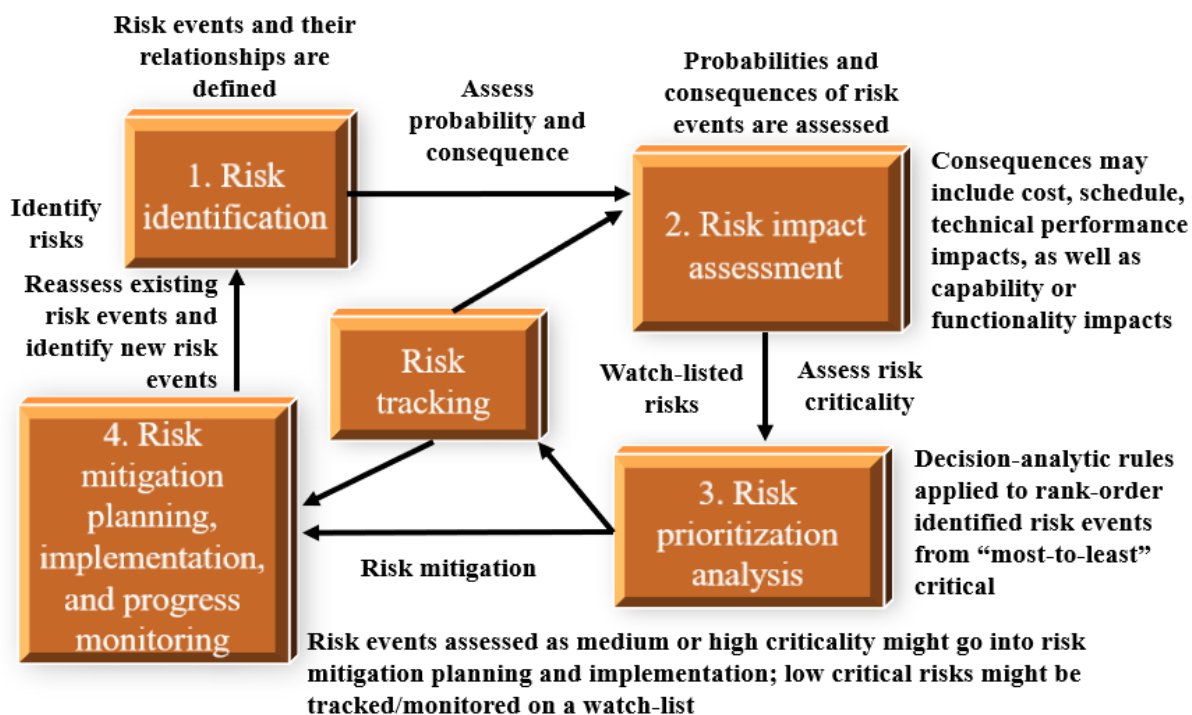


Figure 8. Steps Common to a Risk Management Process (Garvey Book, p272)

Figure 8. represents the Advanced Risk Analysis in Engineering Enterprise Systems. Step 1 is risk identification. Risk identification is the most important beginning step in the risk management procedure. Its role is to identify risk in its early stages and to steadily do so without interruption. Step 2 is a risk impact assessment. This step assesses the impact (consequence) of every risk occurrence that could affect the system project. This involves the “impact cost, schedule, and technical performance objectives” of the occurrence (Garvey Book, p272). This could also involve political or economic consequences. The probability of each risk occurrence is also taken into consideration. Step 3 is a risk prioritization analysis. This step ranks the discovered risk occurrences from the most volatile to the least volatile. “A major purpose for prioritizing (or ranking) risks is to form a basis for allocating critical resources. These resources include the assignment of additional personnel or funding (if necessary) to focus on resolving risks deemed most critical to the engineering system project.” (Garvey Book, p11). Step 4 is risk mitigation planning and progress monitoring. This step develops the plan to mitigate, “manage, eliminate or reduce risk to an acceptable level” (Garvey Book, p272). While the four steps are being processed, the system is always being monitored by the risk tracking section in the middle of the diagram.

For this study, the risk of phishing will be examined as a function of consequence and frequency of phishing which is both known to be affected by an organization in which the target human operator belongs (e.g., governmental/private, industry, size, etc.) and the organizational role of the targeted human (e.g., CEO, staff, contractor, etc.).

Hence, the risk of phishing can be represented by an updated version of equation 2.1:

$$\text{Risk of Phishing} = F(\text{Consequence (Organization, Organizational role), Frequency (Organization, Organizational role)}) \quad (2.4)$$

This formula will be used to assess the risk on a scale that can predict the risk to a company or individual.

In 2019, Hoffmann, Napiórkowski, Protasowicki, and Stanik describes the risk management process as ‘ongoing’. The cyber risk management process will “take the form of an ordered sequence of subsequent events, activities, decisions that result in the organization's cybersecurity” (Hoffmann, Napiórkowski, Protasowicki, and Stanik, 2019). Identifying cyber risks is the main component in avoiding surprise attacks. “The overall relationship between the various categories of cyber actors, threats, vulnerabilities, and their impact on information and data, with further consequences is shown in Figure 9. (Hoffmann, Napiórkowski, Protasowicki, and Stanik, 2019)”. Below (Figure 9) is a catalog of threats and vulnerabilities that affect cybersecurity in the risk management process.

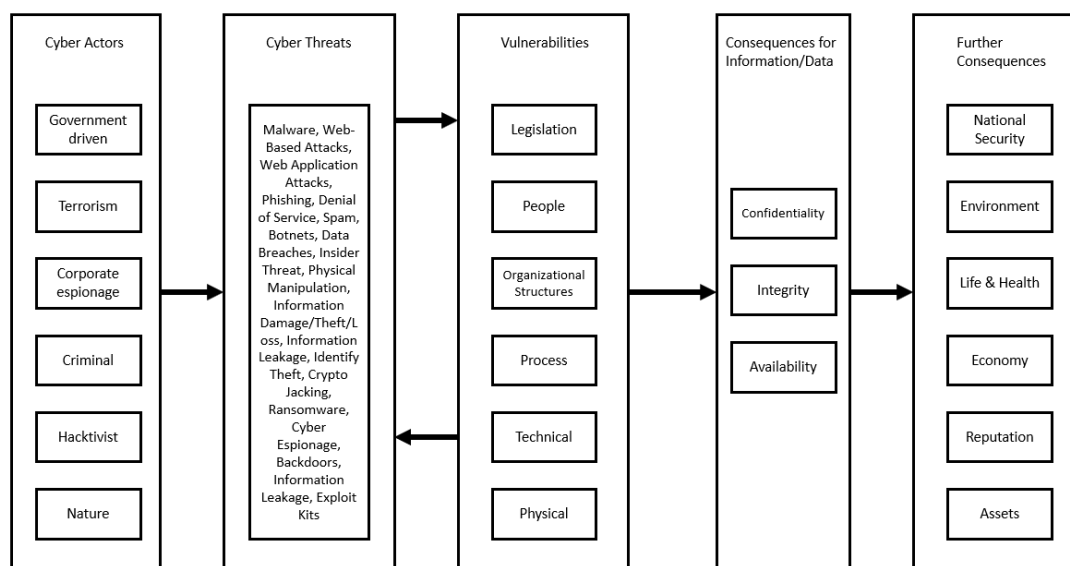


Figure 9. Threats and Vulnerabilities Affect Cybersecurity (Hoffmann, Napiórkowski, Protasowicki, and Stanik, 2019)

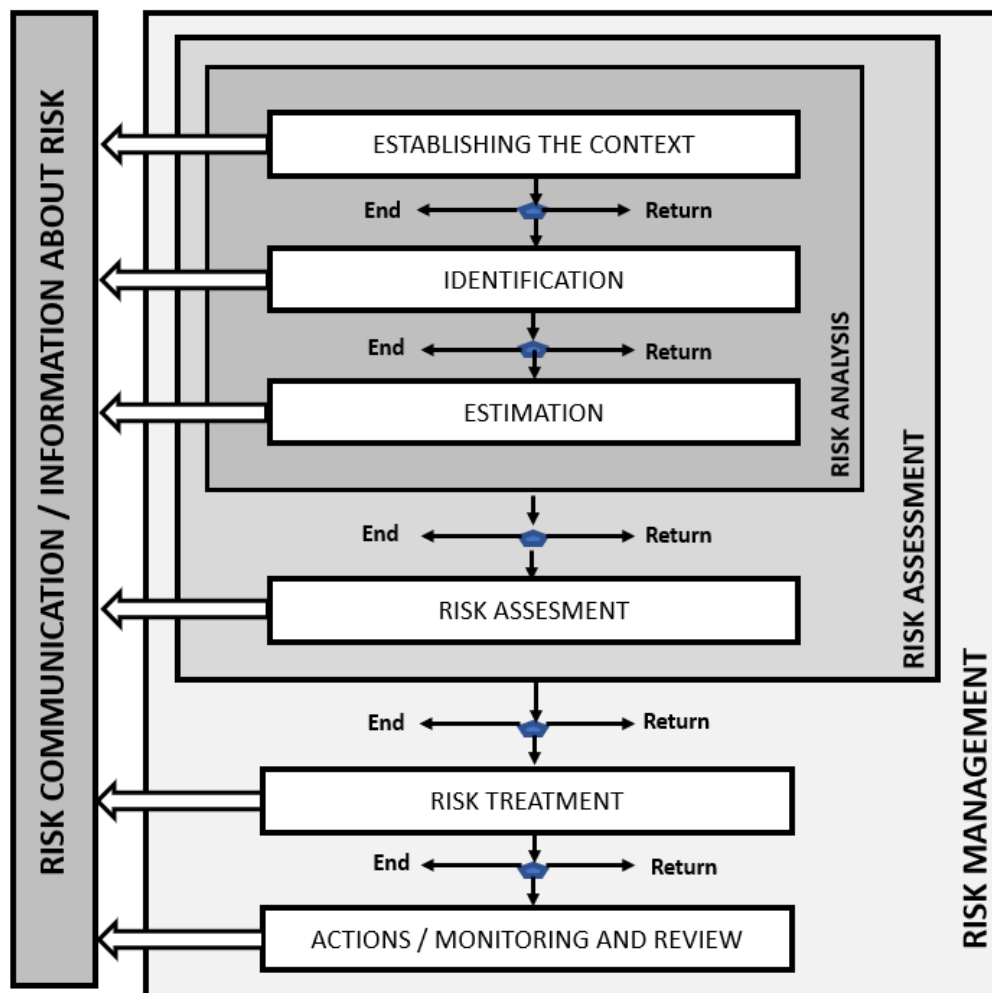


Figure 10. Model of the Risk Management Process in an Organization

(Hoffmann, Napiórkowski, Protasowicki, and Stanik, 2019)

Hoffmann states “the iterative approach to the cyber risk assessment process may be in the form of increasing the level of details of each iteration or stopping the process - after each stage, there are decision points (continue, end, return)” (Hoffmann, Napiórkowski, Protasowicki, and Stanik, 2019). This method is shown in Figure 10. Hoffman continues to say that risk assessment and risk analysis is the ‘fundamental’ stages of the “risk management system in an organization” (Hoffmann, Napiórkowski, Protasowicki, and Stanik, 2019). Once the risk has gone through the stages of analyzation and assessment, “the management of the organization”

should be able to take steps needed to mitigate the risk (Hoffmann, Napiórkowski, Protasowicki, and Stanik, 2019).

Internet Security Management System (ISMS) model is another risk management process used in cyber-attack strategy known as the PLAN DO CHECK ACT model.

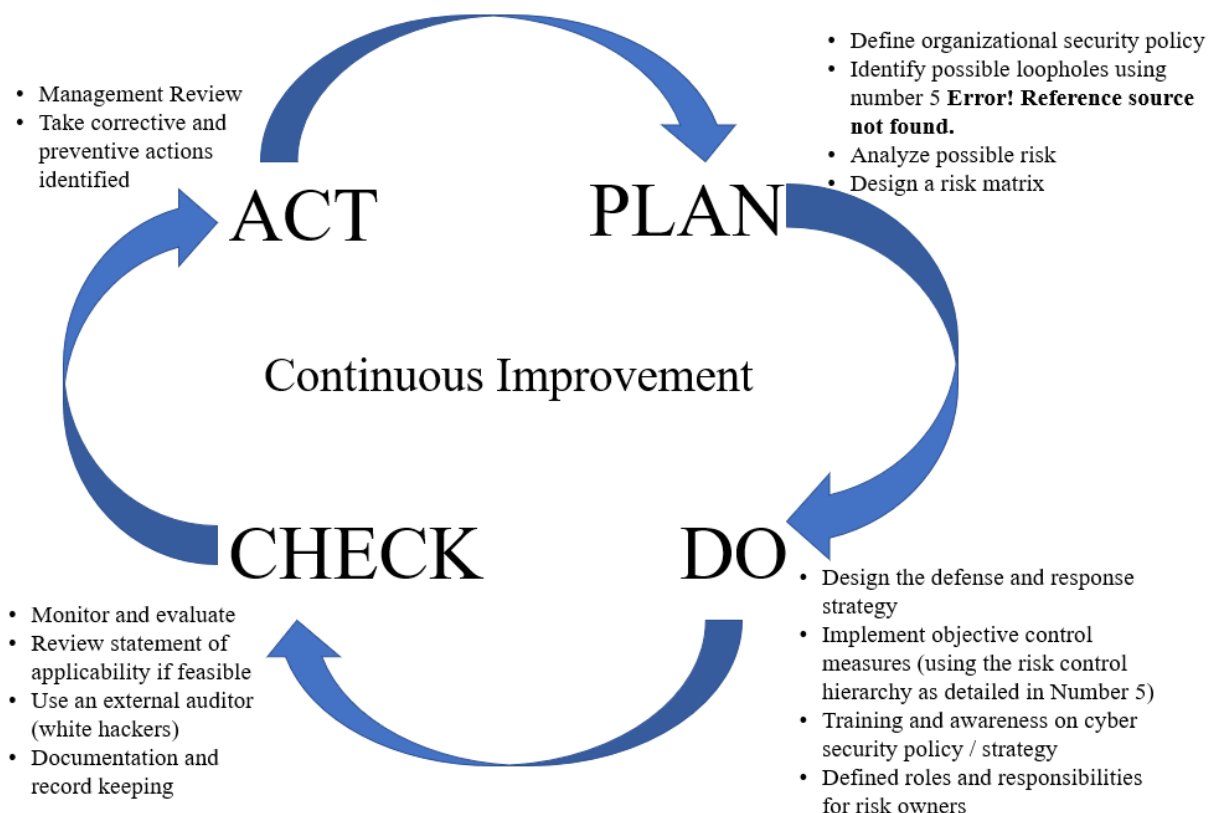


Figure 11. ISO 27001 ISMS Risk Management Process Model in Cyber Attack Management (Aluede, 2020)

This is a continuous improvement model that starts with Plan (identify and analyze possible risk), continues to Do (design and implement defense strategy), continues to Check (monitor, evaluate, and review defense posture), and continues to Act (take corrective and preventative actions). This model continues to do each of the actions until they reach the most

improved model (Aluede, 2020). This model seeks to continuously improve the process of mitigating phishing.

2.2.3 Risk Matrix

A Risk Matrix is a tool that is used by risk professionals to create a visual risk assessment of the impact of potential risk on a project which will permit an organization to develop an effective risk mitigation procedure. The risk matrix normally has three different regions of risk: low, medium, and high. The regions can be expanded, depending on the categories that the risk professional wants to evaluate. Green normally represents low, yellow normally represents medium, and red normally represents high. The risk matrix is commonly used for risk assessment or risk analysis. Its objective is to quickly identify the level of risk involved in a project.

Normally the risk matrix is used by multiplying the likelihood and the consequence to obtain a visual categorizing of risk as shown below in Figure 12.

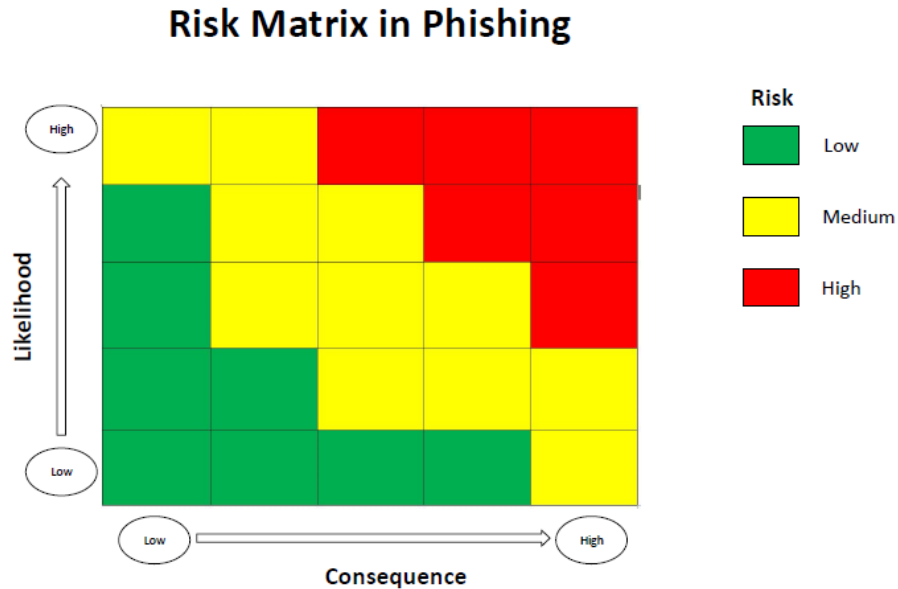


Figure 12. Risk Matrix for Phishing

Xiaosong states that “a Risk Matrix is a tool used in the risk analysis process. A Risk Matrix model can be used to capture identified risks, estimate their probability of occurrence and impact, and rank the risks based on this information” (Xiaosong, 2009). Xiaosong continues to explain, that risk levels in the risk matrix uses consequence and likelihood on a two-dimensional axis. By combining consequence and likelihood, a level of risk can be estimated (Xiaosong, 2009).

On the other hand, Aminudin (2016) states that a “risk matrix is a tabular illustration of the probability and severity of hazardous events. The basis of this approach is to rank the events according to their significance and screen out insignificant events by mapping its probability and severity in risk matrix form”. The Aminudin distinction is represented below in Figure 13.

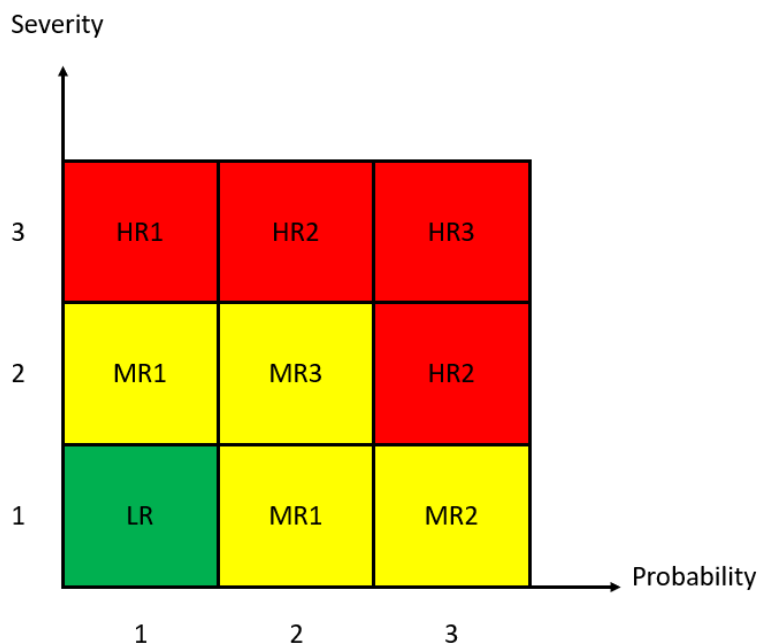


Figure 13. Developed Risk Matrix for Alphanumerical Classification (Aminudin, 2016)

Aminudin designed this risk matrix to determine the risk at a certain point of operation. The Alpha Numeric Characters in the risk matrix represent the risk of voltage collapse in a circuit in the Aminudin study. The advantages to a risk matrix are as follows: risk levels are easily understood, it can be created quickly with provided data, it aids in quicker decision making, can stimulate discussions about risk, it allows for a quick ranking of risk, and it allows individuals to focus quickly on certain categories.

The disadvantages to a risk matrix are as follows: data provided could be incorrect causing an improper classification of risk, basing decision making on a risk matrix alone may cause improper decisions to be made, can cause subjective (feelings involved or personal opinions are used) analysis, and it can cause an inconsistent value for the level of risk. More recently, Pinto and Guilford (2019) showed how risk matrix can be used to rank and score failure scenarios in a communication system with multiple criteria, i.e. Timeless (T), Accuracy

(Ac), and Availability (Av), as shown below. This was then used as a basis for evaluating and ranking various strategies to mitigate risks, and eventually formed the risk management plan.

| | | Consequence | | | | |
|--------------------------|---------------------|-------------|------------|--------|-------------|--------------|
| | | Negligible | Minor | Major | Significant | Catastrophic |
| Likelihood of Occurrence | Very Likely | T | | | | |
| | Likely | | | | | High |
| | Moderately Possible | Low | Low Medium | Medium | Medium High | |
| | Unlikely | | | Av | | |
| | Very Unlikely | | | | Ac | |

Figure 14. Common Risk Matrix with Consequence and Likelihood Ratings (Handley, 2019)

2.3 PHISHING

Most cyber-attacks start by using a phishing attack to gain access to sensitive data from an individual or organization. After exploiting the individual, cybercriminals gain entry to the individuals or organizations system, thus gaining access to the organization's sensitive data.

A few recent examples of these types of phishing attacks are as follows.

On January 29, 2020, Eastern Virginia Medical School (EVMS) discovered that personal data of their employees had been compromised by an email request from an illegitimate account not associated with EVMS. When discovered, EVMS immediately began an investigation.

On February 3, 2020, EVMS notified its employees via email that their name, address, date of birth, Social Security number, salary, and bank account may have been compromised. They

suggested that employees immediately take steps to protect themselves. EVMS recommended the following:

“Contact one of the three major credit-reporting agencies (Equifax, TransUnion or Experian) to place a fraud alert on your credit file. The agency you notify will contact the other two agencies.

Request a copy of your credit report from

<https://www.annualcreditreport.com/Index.action>

Complete and submit IRS Form 14039, Identify Theft Affidavit, found at <https://www.irs.gov/pub/irs-pdf/fl4039.pdf>. It alerts the IRS that you have reason to believe your personal information may have been compromised and /or used fraudulently. Alternatively, you may call the IRS toll-free at 1.800.829.1040. Monitor your bank account transactions carefully” (EVMS, 2020).

EVMS also offered free credit monitoring to the employee for 12 months.

This phishing event has cost the employee’s time and aggravation by following the steps given by EVMS and by knowing that they must continuously monitor their banks, credit, and pay information as well as their tax returns. EVMS suffered an unknown monetary impact for providing credit monitoring to its employees as well as investigative funds for the phishing attack to discover how it took place. Also, EVMS may suffer a negative impact on their reputation and trustworthiness.

On February 27, 2020, Valinsky from CNN Business reported that Barbara Corcoran (Shark Tank Judge) lost \$388,700 to an email phishing scam. The phisher portrayed her assistant and sent a bill to her bookkeeper for a renovation payment. Corcoran said, “there was no reason to be suspicious about the email because she invests in real estate all the time.” They discovered there was something wrong was when they noticed the email was not her assistants’ email. They had wired the money to someone in China. That someone, who is the phisher, has since disappeared and supposedly there was no way to get her money back. Fortunately, the

German-based bank who made the transfer, froze the transfer before it was deposited in the Chinese Bank. Barbara Corcoran was able to recover the money (Valinsky, 2020).

According to Akamae (2020), phishing has staggering effectiveness. 1 out of 99 emails is usually a phishing email; 62% of the emails are effective and get their victims to click on the link, and 1.5 million phishing web sites are popping up every month.

TechRepublic (Whitney, 2019) reports that Kaspersky has seen phishing attacks increase by 21%. Going on to say, “Greece was hit by the greatest number of phishing attacks at 26.2%, followed by Venezuela, Brazil, Australia, and Portugal. In terms of industries and organizations, banks received the greatest percentage of phishing emails at 30.7%, followed by payment systems at 20.1%, global Internet portals at 18%, and social networks at 9%” (Whitney, 2019).

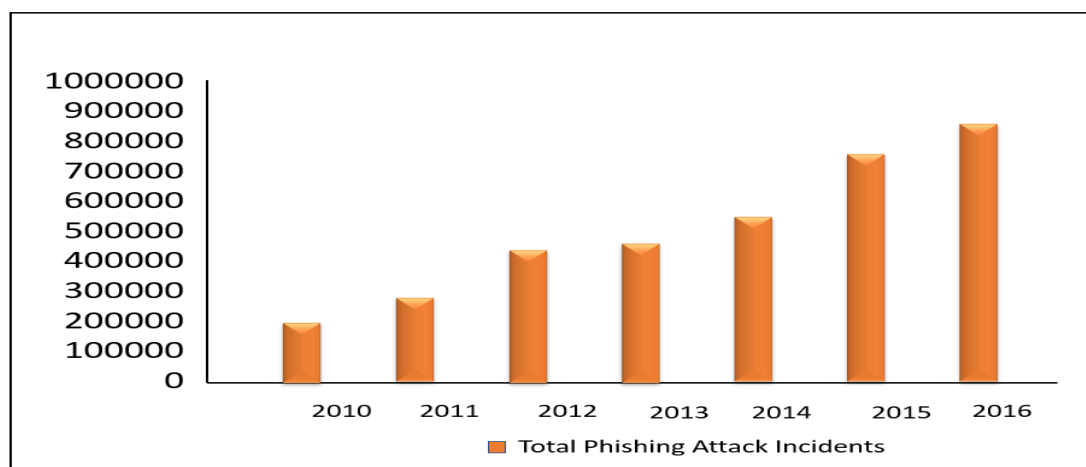


Figure 15. Total Phishing Attack Incidents (Gupta, 2016)

Phishing attacks continue to grow, and no decrease is predicted in years to come. Figure 15, above, demonstrates that phishing has become an Advanced Persistent Threat (APT) that has increased every year with no sign of decreasing.

2.3.1 Current Phishing Research

New technology has removed some of the burdens of detecting phishing schemes from humans. These new technologies (anti-phishing tools, firewalls) examine the pattern of each email and if the email resembles known phishing emails, it will deny the human access to the email. Other current technologies will allow humans to access the email but will warn the human that the email may be a phishing email, leaving the decision up to the human to open the email. Figure 16 describes this process.

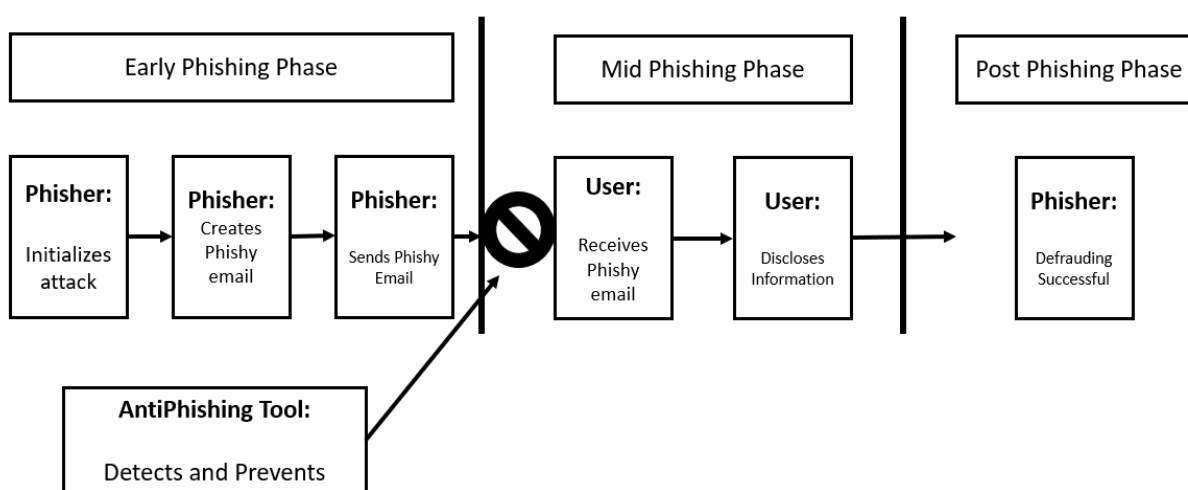


Figure 16. Representation of Anti-Phishing Tool (Qabajeh, 2018)

In the past, governments have been slow in recognizing phishing, but currently, they are using more aggressive techniques such as computer anti-phishing techniques to combat phishing. Anti-spam software tools and anti-phishing software has been used to either block suspicious emails or by moving the suspicious and spam emails to a junk email folder (Qabajeh, 2018). In current technology, Higbee suggests a partnership between man and machine to fight the threat of phishing attacks (Higbee, 2017). While machines will respond to coordinated and

programmed inputs; human response still depends on their level of knowledge. Humans may or may not respond to a phishing email. Higbee states that “hackers have mastered the art of social engineering. They know how to bypass our normal caution and get us to act impulsively” (Higbee, 2017). Due to the diverse knowledge of humans, employees can be both the strongest and weakest links in your organizations (Higbee, 2017). The Proposal of Man and Machine defense system has been well received in the cyber system community and Higbee insists that “Man + Machine = Defense in depth” (Higbee, 2017).

As current technology expands its defense against phishing attacks, Gupta, Tewari, Jain, and Arrawal (2017) have expanded their methods of defense against phishing attacks which is an example of a human and machine partnership advocated by Higbee (2017).

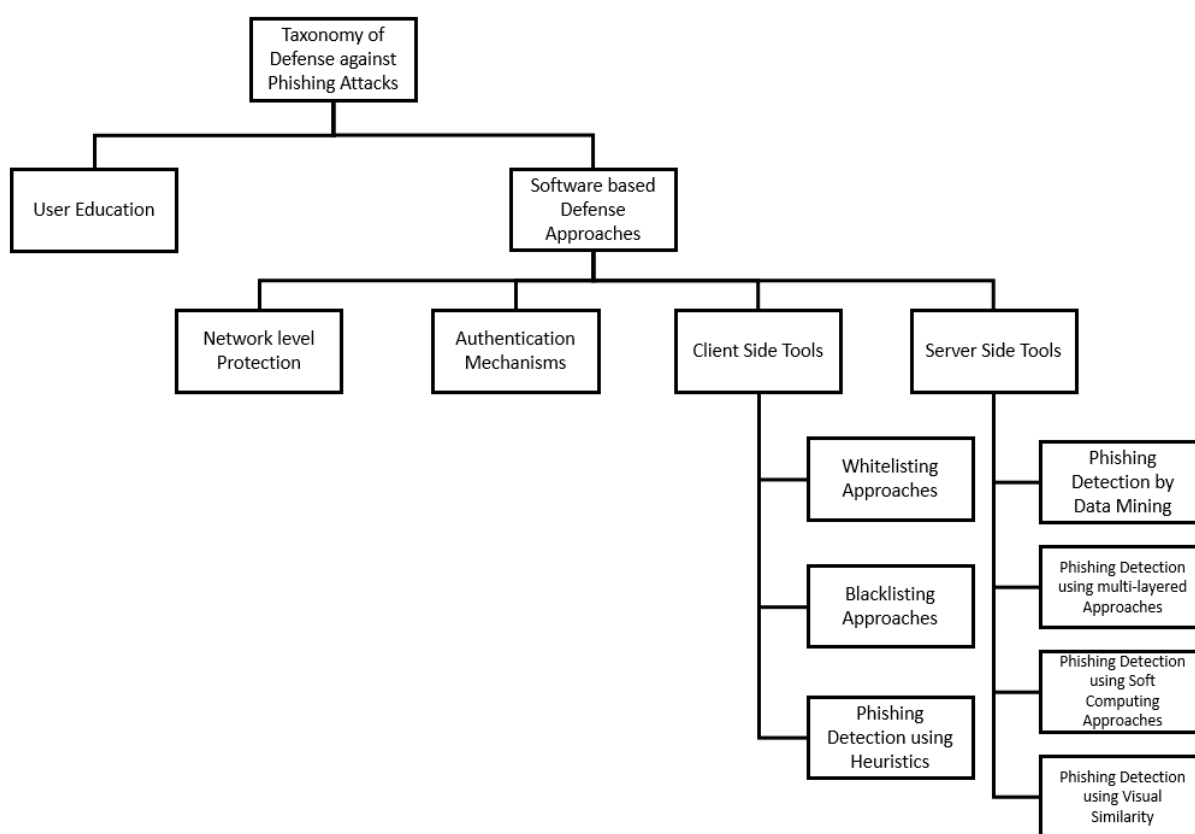


Figure 17. Taxonomy of Phishing Detection (Gupta, Tewari, Jain, and Arrawal, 2017)

Figure 17 is a taxonomy of the modern-day defenses against phishing. The block called User Education represents the human aspect. In Figure 10, the block called Software-based Defense Approaches represents the machine aspect. In retrospect, current technologies are adapting the partnership of man and machine to battle phishing attacks.

2.3.2 Impact of Phishing

Phishing attacks can cause a severe impact on organizations and individuals. The impact on an organization can be the loss of money, loss of time, and loss of reputation. Many organizations have lost customers due to their loss of reputation. Individuals are impacted by identity theft, credit card theft, and the time it takes to continuously monitor their banks, credit, and pay information as well as the possibility of their tax returns.

Phishing is a continuous Advanced Persistent Threat (APT) that continues to grow every year. Due to the ease of deployment, the lack of criminal prosecution, and the tremendous amount of monetary gain for the criminals; phishing has become one of the best sources of profit for the cybercriminal.

In 2011, total attacks reported by US-CERT (United States Computer Emergency Readiness Team); shows phishing had become the dominant form of attack, as shown in Figure 18.

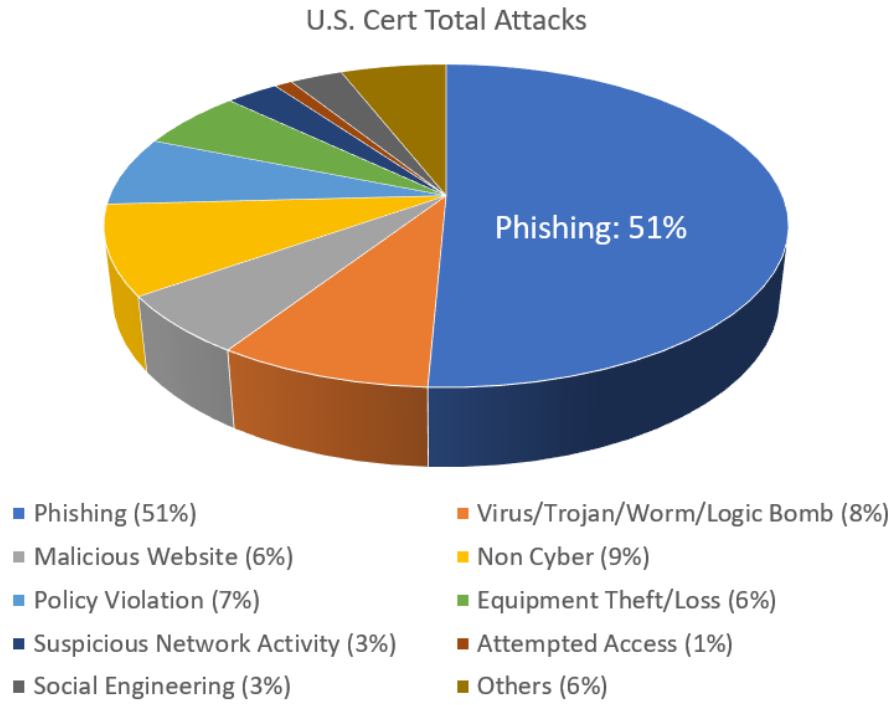


Figure 18. U.S. Cert Total Attacks (U.S. CERT, 2011)

The FBI (Guntrip, 2018) reports a monetary impact loss of \$12.5 Billion in the Global Financial market due to email and email account compromise.

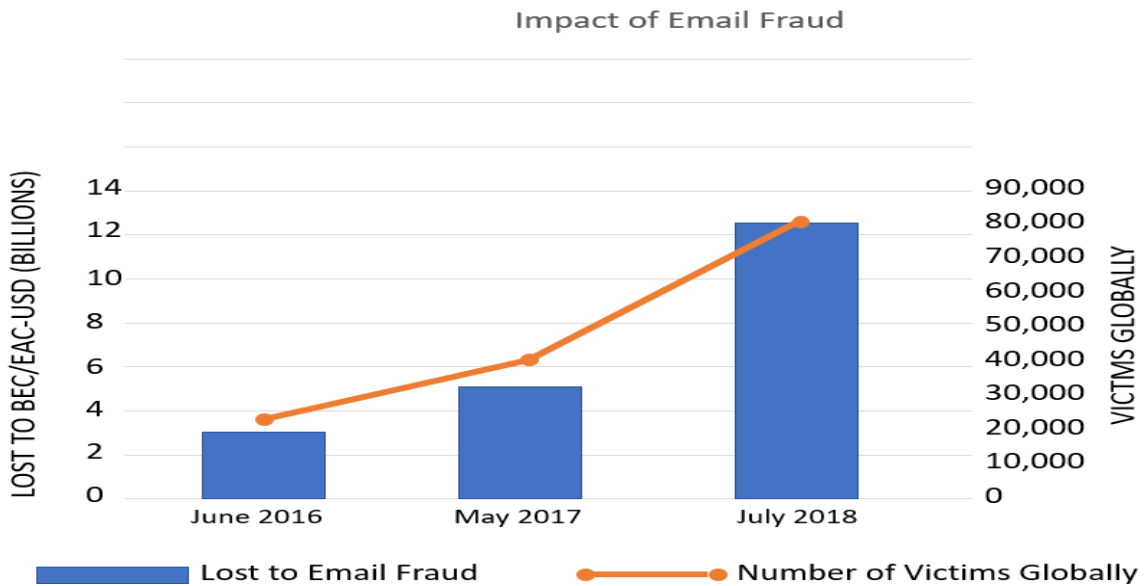


Figure 19. Impact of Email Fraud (Guntrip, 2018)

The FBI considers the phishing email as the “Top Attack Vector” for business email compromise and email account compromise. They believe it is the most effective path for criminals to take rather than hacking a system.

2.3.3 Risk of Phishing

Vishwanath (2016) proposes that training is effective if done in a manner that will identify different training methods for different people. If training is conducted properly, it would be an ideal tool in mitigating phishing (Vishwanath, 2016). In this article, Vishwanath (2016) proposes three changes to improve risk protocols in the fight against phishing.

1. Developing a Cyber Risk Index (CRI).
2. Using CRI to define who gets trained, how, and the types of training.
3. Using CRI to create a behavior-based admin authorization system.

These three approaches together would build a system that is resilient enough to address phishing security risks. The creation of a CRI is much like the development of a constructed scale in the risk matrix described earlier.

Brink (2017) discusses how organizations trust their security people to make the best-informed business solutions about risk. In this article, Brink suggests that presenting business leaders with technical information such as what, who, why, and where of phishing, as well as technical charts and graphs does not describe the risk. He states that risk is defined by how likely it is to happen and what the business impact would be. Figure 13 below describes how “the annualized risk of phishing attacks is significant particularly when senior business leaders are provided with a proper understanding of the “Long Tail” of phishing risk.” (Brink, 2017)

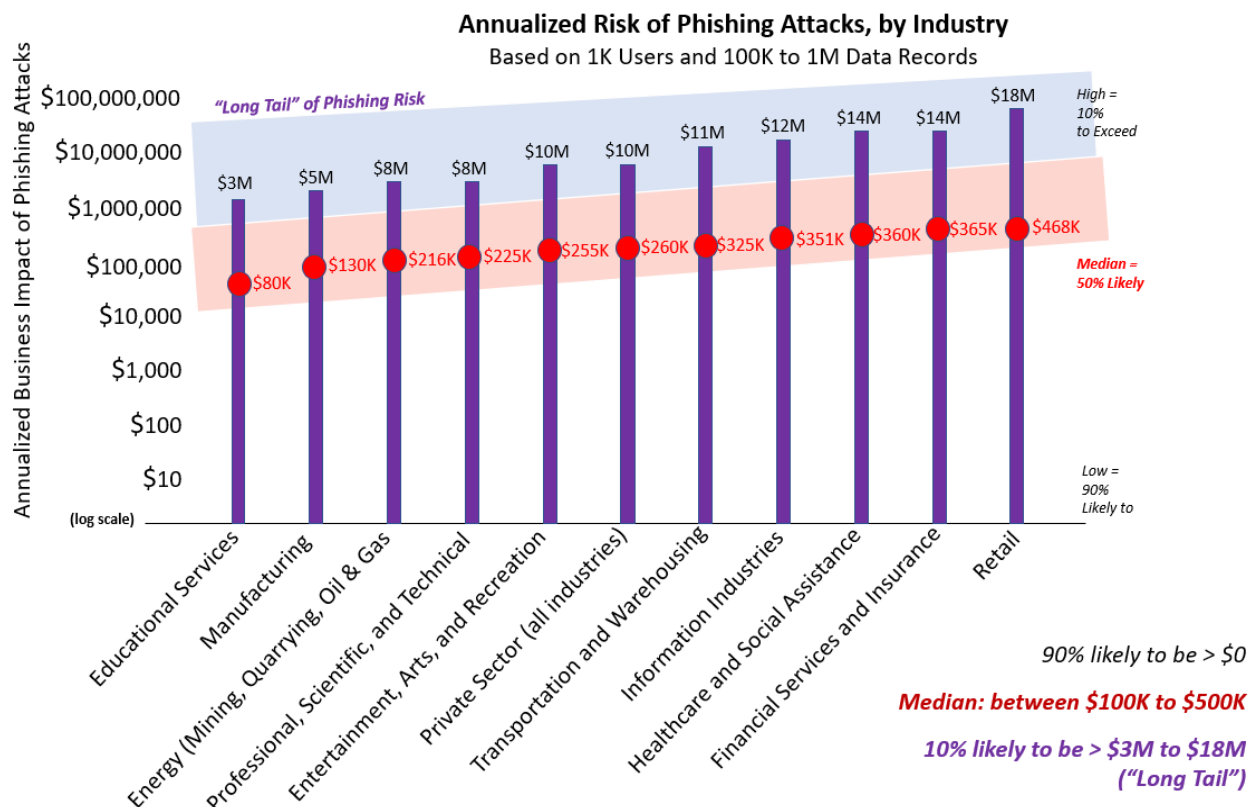


Figure 20. Annualized Risk of Phishing Attacks (Brink, 2017)

Brink (2017) also discusses how Aberdeen's view of security awareness and training constantly plays an important role in cost-effectiveness and the reduction of risk of successful phishing attacks. By expressing how likely and how much impact a phishing attack will have on an organization, he believes that business leaders will understand the quantitative risk estimates.

2.3.4 Economics of Phishing

Evaluating the cost of phishing due to the nature of the risk can be difficult. Many organizations do not understand the risk or choose to ignore the risk of phishing. Due to the impact and the nature of the phishing attack, it can be difficult to access the cost involved if a breach were to happen. If the phishing incident is identified immediately, the cost can be minimal. If the phishing incident is not identified immediately, the cost could be enormous,

especially if the incident caused the theft or loss of data. The main goal of cybercriminals (phishers) is to use phishing to gain access to data that will allow criminals to gain wealth. Through deception, phishers can gain maximum wealth with very little cost. This ability has increased the number of phishing attacks on many organizations and companies.

Phishing is very lucrative to cybercriminals and has become a large profitable business. With a small investment, hackers can profit hugely. The first six months of 2008 saw a 47 percent increase in the number of phishing attacks (Websense Security Labs, 2008) – a frightening statistic when because \$3.2 billion was lost to phishing in 2007 (Litan, 2007) up to \$500 million from 2006 (Keizer, 2007). Phishing is very profitable for criminals with higher rewards and fewer penalties. Phishing has become one of the biggest money makers economically. Many people are willing to pay to get their information back rather than losing their information.

Evaluating the cost of phishing due to the nature of the risk can be difficult. Many organizations do not understand the risk or choose to ignore the risk of phishing. Due to the impact and the nature of the phishing attack, it can be difficult to access the cost involved if a breach were to happen. If the phishing incident is identified immediately, the cost can be minimal. If the phishing incident were not identified immediately, the cost could be enormous, especially if the incident caused the theft or loss of data. This ability has increased the number of phishing attacks on many organizations and companies.

2.3.5 Addressing Phishing Risk through Technology

Cranor (2020) is of the opinion that even with all the technologies (filters for email, browser capability of flagging phishing, anti-phishing software) that are being developed to

combat phishing; people still succumb to phishing emails. As technologies get more sophisticated, so do the phishers. Phishers are constantly modifying and evolving their phishing tactics to stay in front of developing technologies. New technologies, such as phishing games has influenced users; but technologies alone cannot stop users from being phished.

Milletary (2005) discusses what, how, and why phishing has become a significant criminal activity on the internet. Phishing attacks have increased causing a “negative impact on the economy through financial losses” (Milletary, 2005). Phishing deceives individuals into revealing sensitive information that could potentially cause financial stress to the company or the individual. Phishers normally do this by tailoring the message to appear authentic and to motivate the user with some urgency to act. “Phishers today have a large tackle box of tools available to them. These tools serve a variety of functions, including email delivery, Phishing site hosting, specialized malware, Bots/Botnets, Phishing Kits, Technical Deceit, Session Hijacking, Abuse of Domain Name Service (DNS) and Specialized Malware” (Milletary, 2005). Milletary offers recommendations on fighting phishing with awareness, vigilance, and foresight. The trend in phishing has increased and is becoming more sophisticated. While the article focuses on the technical view of phishing, it also confirms that training would greatly improve human’s awareness.

Ting (2016) expresses that the major factors that influenced the targeted human to become a phishing victim based on the Heuristic Systematic Model of phishing are Argument Quality, Source credibility, Genre conformity, Need for cognition, Time pressure, Pre-texting, Less damage, Knowledge, and Trust. Technology has led to an increase in phishing. Due to the rapid increase in technology and the ease of connecting to the internet, leaves unsuspecting

people open to cybercriminals that can defraud individuals with clever and official looking scams (Ting,2016).

2.3.6 Addressing Phishing Risk through Socio Systems

The socio system of risk can be identified as a function of consequence and frequency. The consequence is represented as Human or Organization loss and/or cost. Frequency is represented as the number of times the user has clicked on the email. This formula can be represented as:

$$\text{Risk} = F(\text{Consequence } (Human, Organization), \text{Frequency}) \quad (2.5)$$

In the Socio-Technical field, Negi (2011) discusses the impact of information technology systems on people and the way they learn. Technologies have progressed so quickly that some teachers are uncomfortable with the rapid advancement of the new technology. “Teaching is geared towards the transfer of particular and therefore limited knowledge and skills. This approach has a long-standing tradition” (Negi, 2011). This new technology (intellectual computer systems) has also changed the way society learns. Negi discussed how technology has many societal ways of learning and suggests how the human skillset is lagging. By identifying the lag in the way people are learning, Negi agrees that there is a need for training and awareness.

Iuga states that phishing is a scalable act of deception (Iuga, 2016, pg. 1). This article discusses phishing attacks, human factors, and user studies. In this article, several participants were instructed to go to several different web pages to decide whether they were phishing pages

or not. 214 of the participants (56%) answered incorrectly. Two important points were made in this article. “Firstly, experienced users do not necessarily trust correct security indicators or notifications, and secondly, phishing attacks which rely on malicious pop-ups may be harder for users to detect” (Iuga, 2016). This article further confirms the fact that individuals still have a very difficult time identifying non-phishing and phishing sites. This conveys that more training could help users. Additionally, many of the participants did not observe the warning signs about phishing pages. As a result, this article confirms that there are still many individuals that are not security conscience either because of a lack of training or a lack of awareness.

2.4 PHISHING MODELS

Researchers have used phishing models such as the Interpersonal Deception Theory, Elaboration Likelihood Model, and Theory of Deception plus other relatable factors to estimate’s potential victims' phishing susceptibility (Ting, 2016). Figure 16 displays four cues at the top that could draw a person’s attention (Email Source, Grammar and Spelling, Urgency Cues, and Title/Subject Line). To the left are variables (Involvement, Email Load, Knowledge, and Computer Self Efficacy) that affect the influence of the person. The lines represent the level of involvement of different factors, while the box on the bottom (Elaboration) represents the elaboration or lengthiness of the phishing message. All these conditions lead to the box on the left, the likelihood of responding to phishing (Vishwanath, 2011), or the potential victims' phishing susceptibility (Ting, 2016).

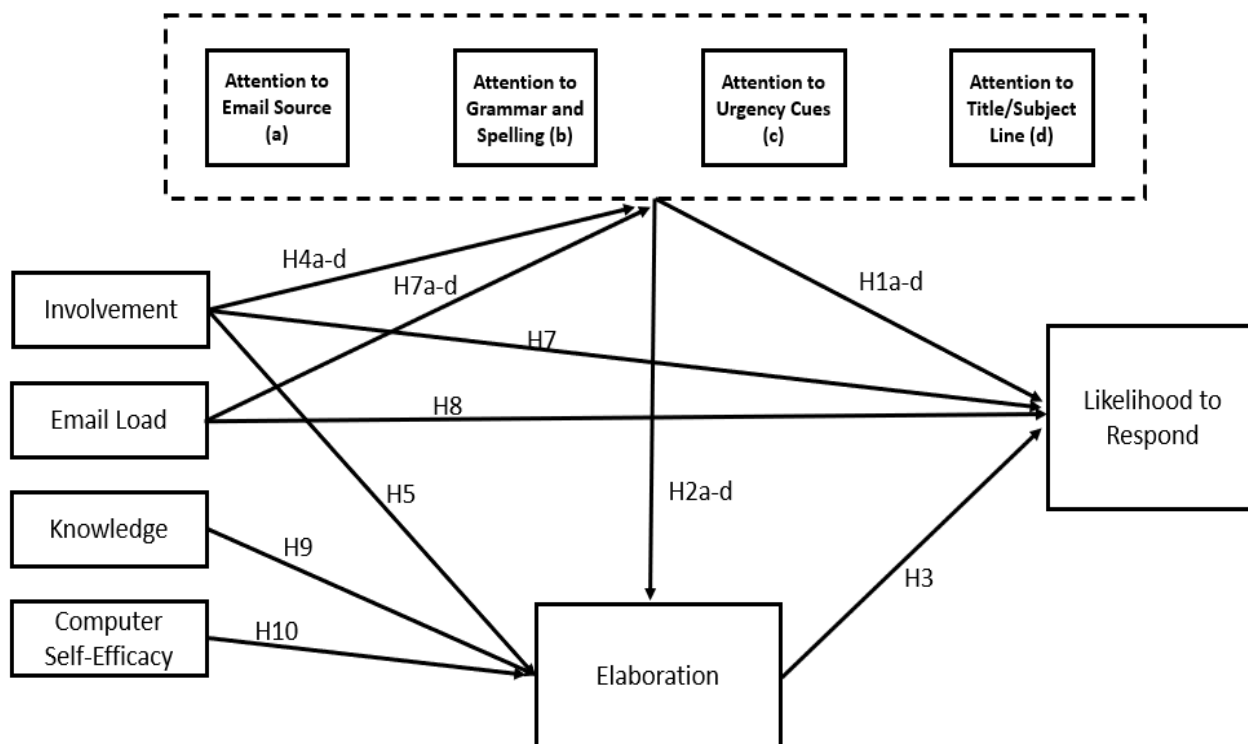


Figure 21. Potential Victim Phishing Susceptibility (Ting, 2016)

Ting concludes that the cues, variables, and levels listed above play a major role in turning an individual into a victim of phishing. These roles are a good starting focal point. However, there are some flaws in their study. First, they only interviewed 15 people of the 250 that took the survey. Therefore, the representation of the number of people interviewed to the number being represented could easily skew the results. Second, they only targeted 250 people as far as the sample size to take the survey. Third, their findings were not deployed to either the public or the company to record its impact and to test its “usefulness due to time constraints” which were the major limitations in the survey (Ting, 2016). This article is a good example of how training and awareness could affect the outcome of human response. It also represents a

good starting point of a model that can define the reference points of training. This study also examines how training and awareness will affect the outcome of the reaction to phishing.

Elaboration Likelihood Model (ELM) is a dual processing model that concentrates on an individual's ability to detect the context of a given circumstance. ELM is a model that looks at how people react when being persuaded. By observing the reactions of individuals when being persuaded, it defines a central path to gaining the confidence of an individual. Petty states "the Elaboration Likelihood Model (ELM) was developed to explain past inconsistencies in attitudes research. Whereas past models tended to emphasize one effect of a given variable and one process by which that effect occurred, the ELM organized multiple persuasion processes into two routes to attitude change. The central route involves change that occurs when people are relatively thoughtful in their consideration of the issue-relevant information presented. In contrast, the peripheral route to persuasion involves processes requiring relatively little thought about issue-relevant information. Instead, attitudes are changed by simple association processes (for example, classical conditioning) or the use of various mental shortcuts and heuristics" (Petty, 2009, pg. 4). In its evaluation, this model has found that the longer the message of an email, the more confidence it gains in the individual.

Heuristic-Systematic Model (HSM) is another dual processing model that engages two important theoretical causes. First, heuristic processing is "more advanced compared to Elaboration Likelihood Model (ELM)" (Xu, 2012). Second, theoretical extensions such as additive effect ("a phenomenon in which heuristic processing may exert influence during message validity assessment over and above the influence of systematic processing") and sufficiency threshold [the "desired judgmental confidence" that people wish to reach when

making decisions under a given circumstance (Eagly & Chaiken, 1993, p330)] made HSM applicable to a wider range of validity-seeking contexts than the Elaboration Likelihood Model (ELM) (Xu, 2012). This model resonates the two dynamics that will most likely cause a person to fall victim to a phishing email. The time constraint given and the authenticity of the email. Most people trust an email coming from a friend or someone they know. This trust causes one to fall victim to phishing when one is subjected to the pressure of time to react when coming from a somewhat credible source. Figure 22 depicts the dual-processing phase (that is suggested by this model) when a human is deciding the credibility of a website that is unknown to them.

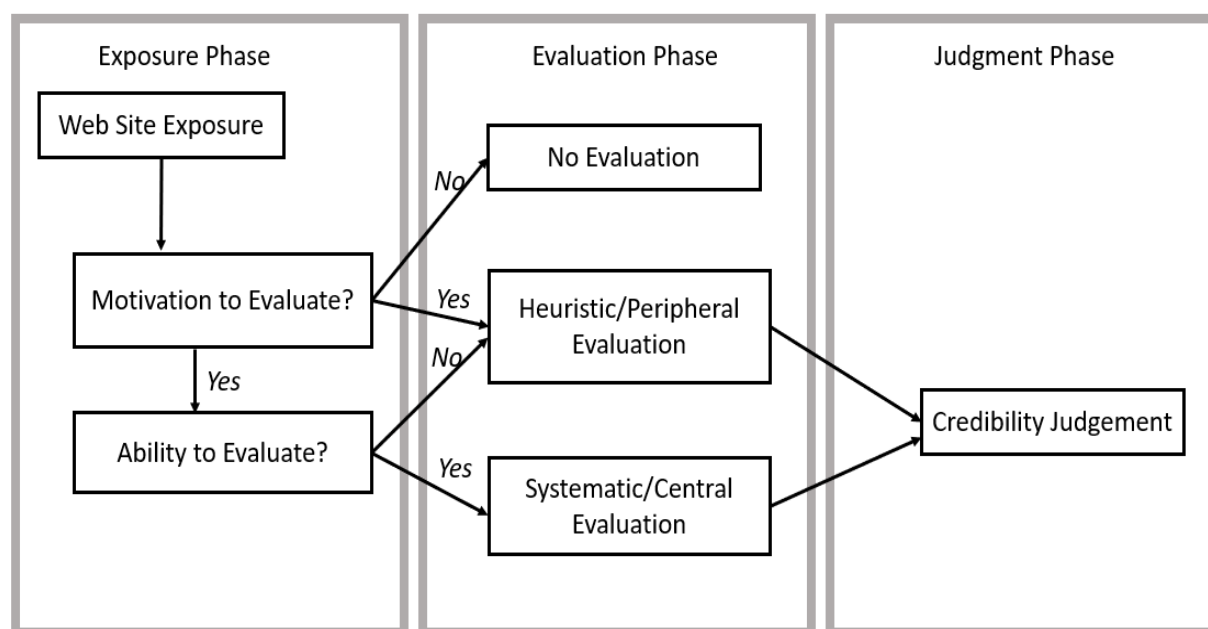


Figure 22. HSM Model Phase Chart (Zhang, 2012)

Interpersonal Deception Theory (IDT) is a theory that describes how verbal and non-verbal cues can identify a deceptive methods or process. Buller expresses that the “Interpersonal

deception theory (IDT) arose out of just this concern that deception be examined within the nexus of interpersonal encounters. It was formulated to contextualize an explanation of deceptive communication in what we know about conversation. This approach stands in contrast to more psychological explanations for deceptive communication. It also draws attention to the dynamic nature of deception displays and to the mutual influence between sender and receiver that occurs in all conversations” (Buller, 2006, pg. 2). Buller goes on to state that the “Interpersonal deception theory (IDT) represents a merger of interpersonal communication and deception principles designed to better account for deception in interactive contexts. At the same time, it has the potential to enlighten theories related to (a) credibility and truthful communication and (b) interpersonal communication (Buller, 2006). In phishing, this may help individuals determine what is and what a phishing email is not.

The Big-Five Model defines five traits that are a predictor for human behavior with high validity, openness, conscientiousness, extraversion, agreeableness, and neuroticism. In this model, the five traits are considered the most important traits of an individual. “Openness is the desire to seek out new experiences without anxiety and an appreciation of different ideas and beliefs. Conscientiousness focuses on self-discipline, dutiful action, and respect for standards and procedures. Extraversion is the tendency to seek out the company of others and reflects the energy and positive emotions in one’s personality. Agreeableness is a measure of the quality of the relationships a person has with others. Neuroticism is the tendency to feel that reality is a problem and to experience readily unpleasant emotions” (Bailey, 2018). These Five traits can lead to phishing susceptibility as shown in Figure 23.

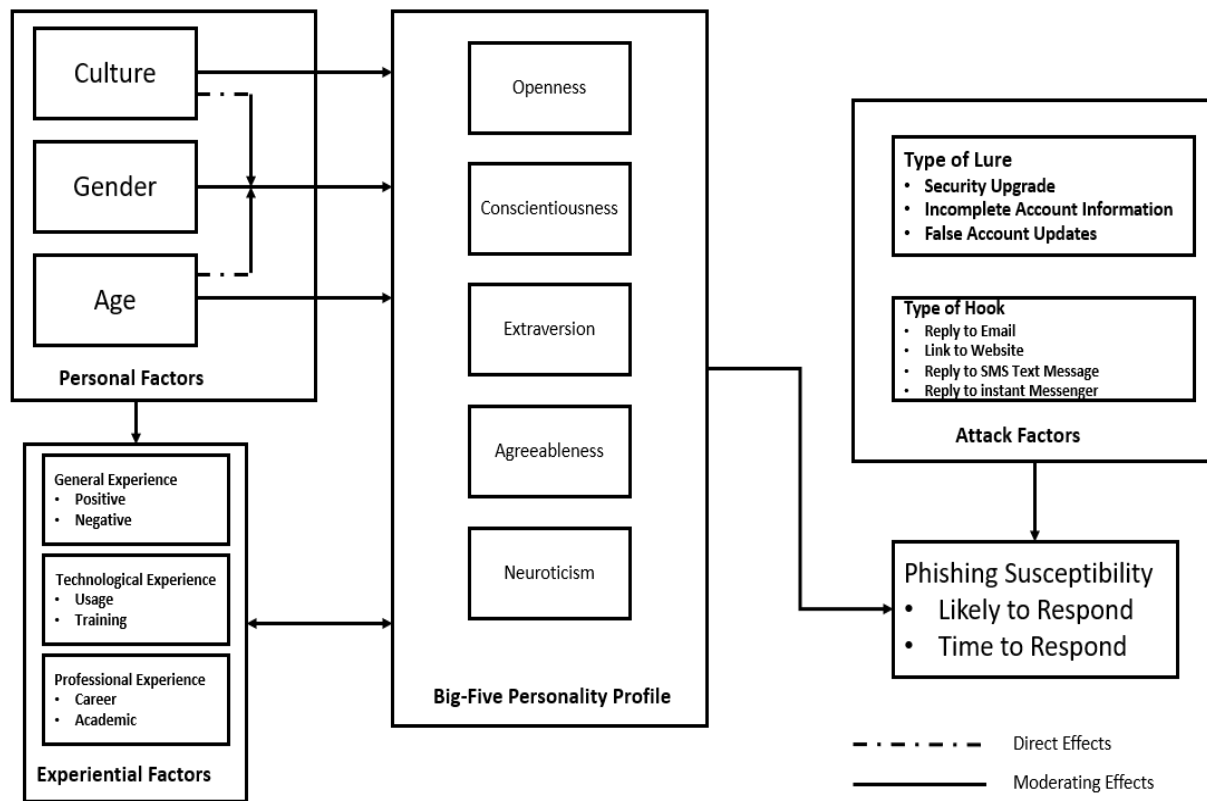


Figure 23. Direct Effects Chart (Bailey, 2018)

The Big-Five model has been successful in predicting different aspects of human behavior but has been unclear in determining an individual's vulnerability to different types of phishing attacks. It will take more research for the Big-Five model to determine the individual's vulnerability.

Table 3 identifies the Pros and Cons of the Models described in this section.

Table 3. Table of Pros and Cons of 3 Different Models

| Model | Pro's | Con's |
|---|--|--|
| Heuristic-Systematic Model (HSM) | Dual-Process Info Processing (Systematic / Heuristic) Organizes Human Factor 4 Step Process Heuristic Cues | Systematic Process Lack of Availability and/or Awareness of heuristic cues |
| Elaboration Likelihood Model (ELM) | Dual-Process Info Processing (Systematic / Heuristic) Theoretical Tool Issue-Relevant Thinking Heuristic Cues | Central Route / Peripheral Route Systematic Process |
| Interpersonal Deception Theory (IDT) | Verbal Cues detected Non-Verbal Cues detected | Limits study to non-interactive attacks. Focuses on intentional deceptions. |
| The Big-Five personality traits | Predicts different aspects of Human Behavior. | Predicting individual's susceptibility to different phishing attacks is unclear. |

2.5 MODELS TO COLLECT SOCIO SYSTEMS DATA

As part of the Socio System, the human is a function of the roles, tasks, and training. This means, this study will examine how roles, tasks, and training will impact the human target. The human has a role in an organization defined by the job description. The task is what the individual would do or perform in the job description. The training is how much or how often the individual is trained in avoiding phishing attacks.

This being represented as:

$$\text{Human} = F(\text{roles, task, training}) \quad (2.6)$$

Jacobsson (2007) examines the importance of the psychological aspect of phishing and reveals how the consumer psychology of phishing can affect the way people react to phishing.

The article explains how too much security can backfire on the security of the system, but it does note that the education of the user is just a start. Phishing is becoming more complex and phishers are getting smarter. Jacobsson looks for indicators of people that may be vulnerable to attacks. Jacobsson approaches phishing from a psychological view and does not go into developing a system model that will help mitigate phishing.

Rastenis (2020) states that “A phishing attack is a social engineering attack aimed at fraudulently acquiring private and confidential information from intended targets”. Rastenis concentrates on the phishing attack taxonomy mainly focusing on email attacks, shown in Figure 24.

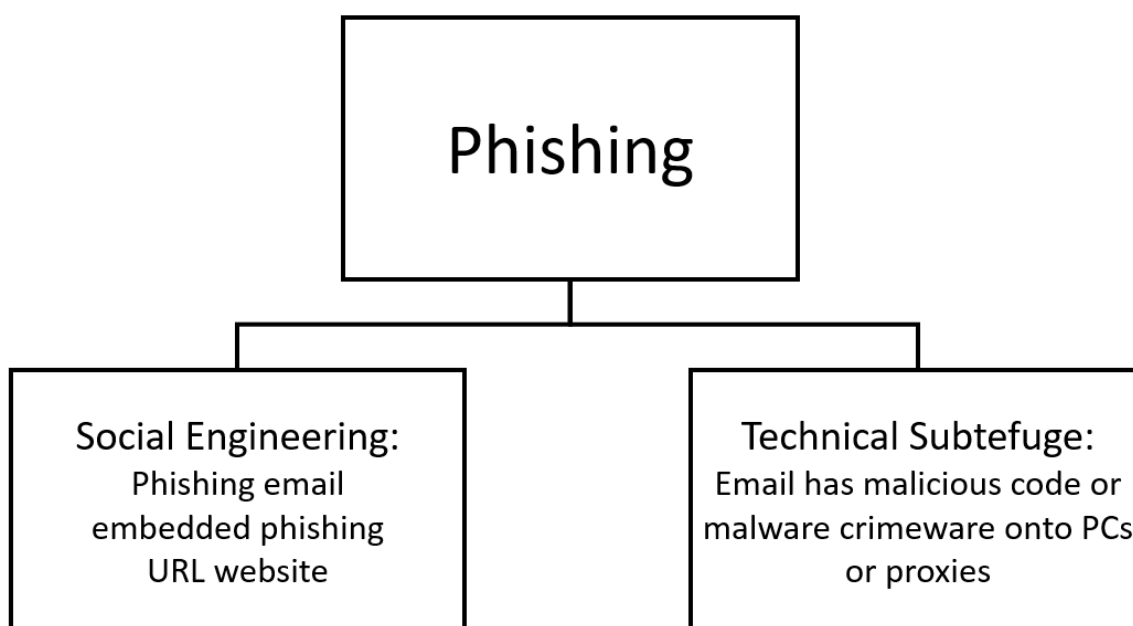


Figure 24. Phishing Attack Taxonomy (Rastenis, 2020)

Rastenis (2020) defines six phases of an email-based social engineering attack. Phase one is selecting the email address. Phase two is content creation for email. Phase three is sending emails to recipients. Phase four is waiting for the response from the email recipients. Phase five

is the phishing attack results and data gathering. Phase six is the “usage of gathering results and data” (Rastenis, 2020). This method is shown in Figure 25.

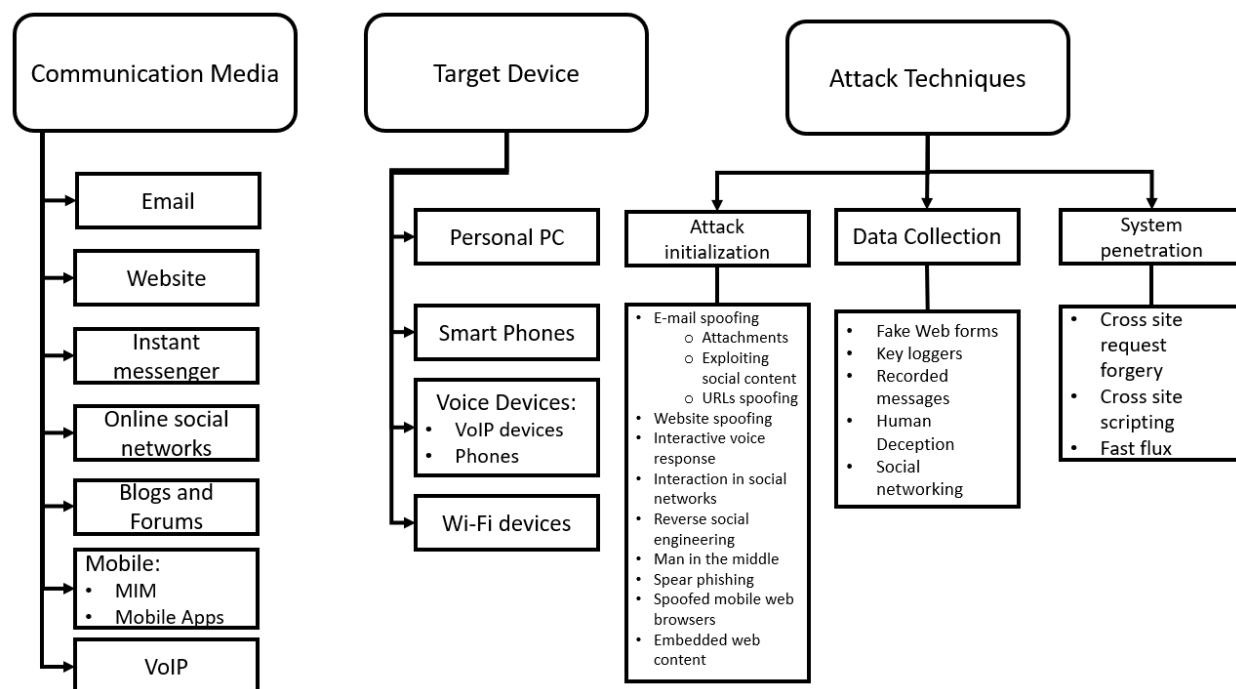


Figure 25. Extended Phishing Attack Taxonomy (Rastenis, 2020)

Rastenis (2020) states there are two main categories of “email address selection strategies.” The first category is “the usage of existing email addresses” (Rastenis, 2020) and the second is “the generation of email addresses” (Rastenis, 2020). This article explains thoroughly how phishers use email-based phishing attacks on unsuspected victims.

2.5.1 Human View

The Human Views are visual descriptions of the data that represents the human context of a system. Brusberg (2011) goes into depth about the Human View (HV). Brusberg describes the Human View elements and relationships in the context of enterprise architectures. This handbook describes the HVs in the context of the Ministry of Defense Architectural Framework

(MODAF) and the importance of the human component in the improvement of the performance of the overall system (MODAF).

Figure 26 describes the HV element and relationships.

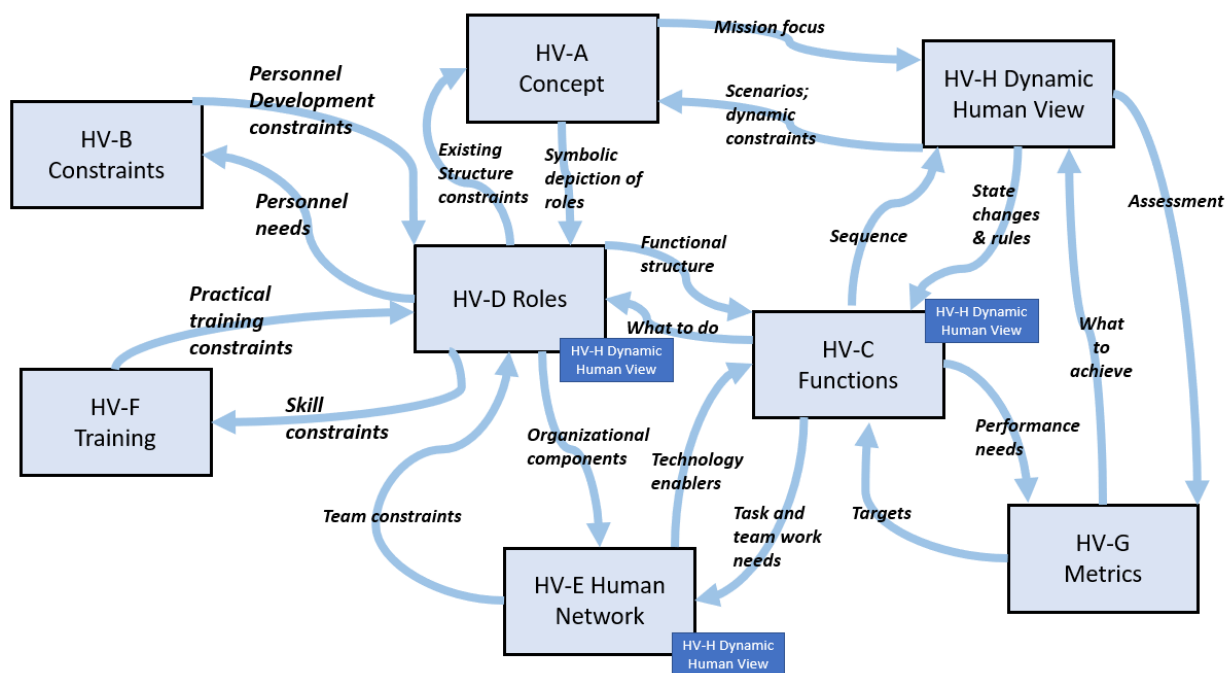


Figure 26. Overview of the Human Views Developed under NATO HFM-155 (Brusberg, 2011)

This handbook describes in detail the many different elements involved in the human view concept according to NATO human views. It outlines the differences between the MODAF HVs and NATO HVs. The descriptions and guidelines of the NATO Human Views (HV-C, HV-D, HV-F) described in this handbook will be reviewed to aid in the development of a systematic phishing model.

Handley (2010) describes the conclusions of the NATO Human View Workshop.

Handley focuses on in-depth descriptions of the eight NATO Human View Architecture. These

Eight NATO Human View products describe how humans interact with each other and how they interact with the system.

“Human Views organize human-centered information into distinct models which provide a working inventory of human system data. The set of Human Views is referred to as the Human Viewpoint: the term Human Views, and Human Viewpoint are used interchangeably. The Human Views capture human-centric data and organize the information into a framework to model the impacts of human performance from tasks, personnel, and system resources. The human Viewpoint provides a set of models that captures information on human capabilities, constraints, tasks, roles, networks, training, and metrics” (Handley, 2019, pg 10-11).

The following human views will be evaluated to discover if they can be used to contribute to developing a model in this study:

“HV-C: Tasks - descriptions of the human specific activities in the system.

HV-D: Roles - descriptions of the roles that have been defined for the humans interacting with other elements of the system.

HV-F: Training - a detailed accounting of how training requirements, strategy, and implementation will impact the human.” (Handley, 2010).

This paper not only described human views, but it also describes how humans interact with a technology-supported network. More importantly, this paper references training in the HV-F human view role. It describes how training requirements, strategy, and implementation can greatly affect the human and their role in a system. The lack of training has been a proven point in the fight against phishing. The value of this HV-F would be to propose a way that an organization could use it to gather data for the risk matrix model in their organization.

In September of 2012, a multi-national meeting at NATO headquarters in Brussels was convened to discuss the idea to establish a Unified Architecture Framework (UAF). “Each organization presented their view of the project requirements, the current issues, potential solutions, and a projected timetable to work towards an agreement” (Hause, 2013).

The developmental timeline for the UAF is represented below.

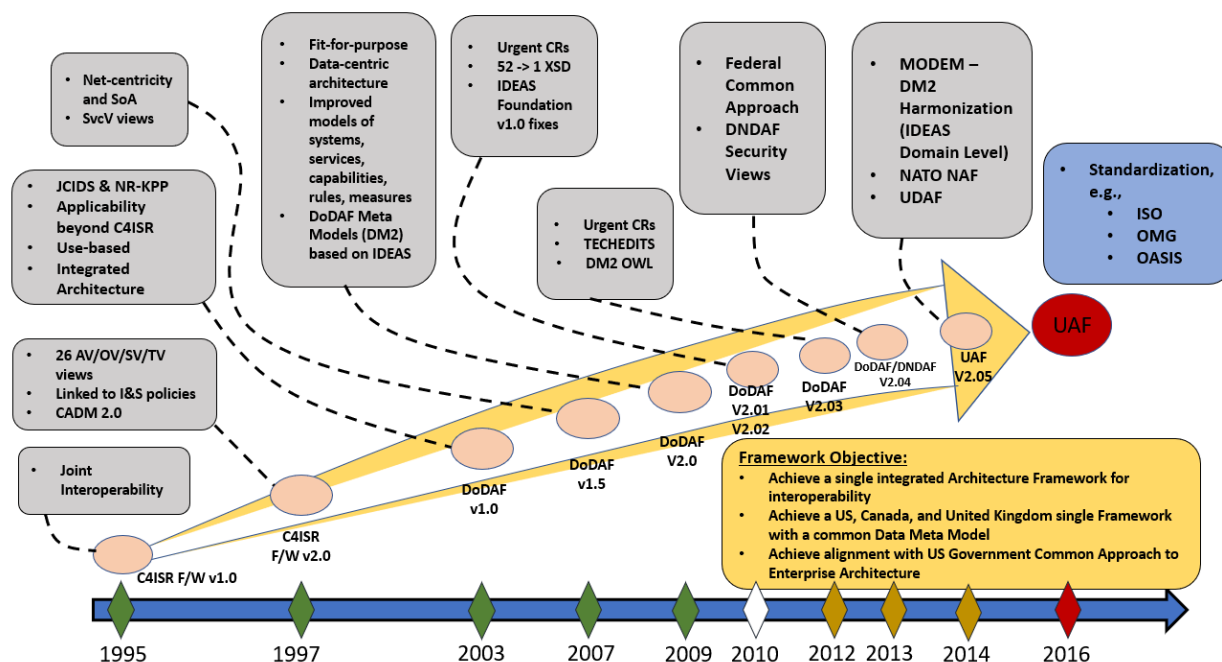


Figure 27. Evolution Towards a Unified Architecture Framework (Hause, 2013)

The UAF was designed to improve understanding, reduce costs, and provide a true interchange of data by providing a common framework (Hause, 2013). Weisman describes the UAF as an extensive update to the NATO, MODAF, and DODAF Architecture Frameworks (Weisman, 2019). UAF enables complex architectures to be developed and implemented by providing necessary viewpoints (Weisman, 2019).

Part of those viewpoints is the Personnel viewpoint. The personnel viewpoint includes stakeholders such as Human Resources, Solution Providers, and PMs with concerns identified as

organizational resource types (UAFP, 2016). Below is the representation of the Taxonomy of Personnel. The UAF provides the opportunity to extend the Human Views using the Personnel views to the common framework.

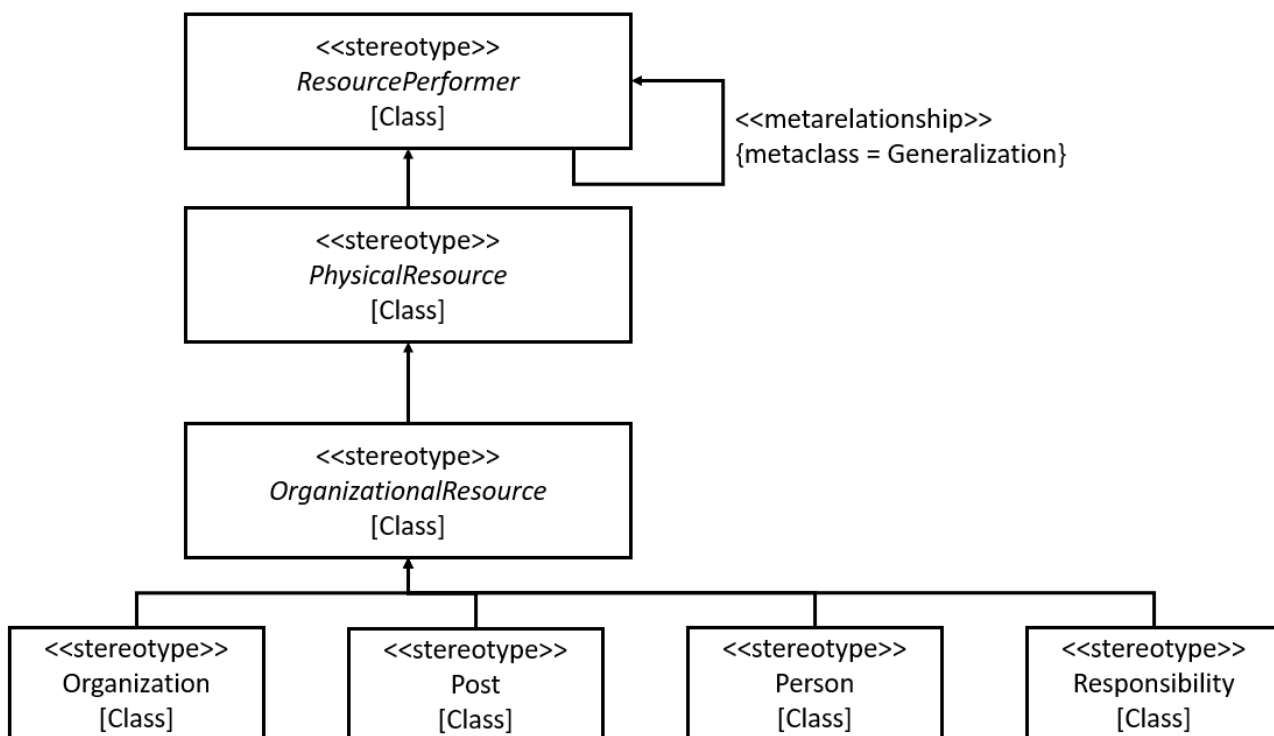


Figure 28. Personnel Taxonomy (UAFP, 2016)

2.5.2 Organizations and Phishing

On January 28, 2020, the Health Insurance Portability and Accountability Act known as HIPAA posted that the 2020 State of the Phish report from Proofpoint (Cybersecurity Firm) reports that “65% of U.S. organizations (55% globally) had to deal with at least one phishing attack in 2019” (HIPAA, 2020).

An organization has many definitions. Glass states that “an organization can be looked upon as a hierarchical network of positions each carrying specific role expectations and a

formally or informally defined level of status” (Glass, 1991). Gibson considers “an organization is a coordinated unit consisting of at least two people who function to achieve a common goal or set of goals” (Gibson, 2009). Gibson also defines an organization as “entities that enable society to pursue accomplishments that can’t be achieved by individuals acting alone” (Gibson, 2009). The Business Dictionary defines a common definition of an organization as “a social unit of people that is structured and managed to meet a need or to pursue a collective of goals. All organizations have a management structure that determines relationships between the different activities and the members, and subdivides and assigns roles, responsibilities, and authority to carry out different tasks.”

Pinto (Garvey Book, 2012 p18) states the “behavior of a system” is just one of the definitions of an organization. In this study, we will look at an organization as a function of type and policies. Hence the formula:

$$\text{Organization} = F(\text{type, policies}) \quad (2.7)$$

Type is the category of the organization. Policies are the plan or strategy that the organization will implement to keep them safe from phishing. The policies depend heavily on the type of organization. If the organization is a university that has a very high bandwidth on their network infrastructure, then the policy may be very detailed due to the intricacies of the University. Given that researchers prefer less restriction in the policies so that they can perform their work; cybercriminals are attracted to the high bandwidth infrastructure and mount multiple attacks on the network hoping to gain entry making policies more intricate and more detailed.

Smaller organizations that have a smaller or non-existent bandwidth may be absent of policies or have less restrictive policies.

2.6 CONCLUSION

In review, phishing attacks have been increasing each year. Phishing has become a very lucrative business for cybercriminals because of the low investment and high profitability. In this study, Risk Management will be used to categorize and analyze phishing attacks to create a model that can be used to mitigate phishing. Human Viewpoint will be used to categorize and organize data from phishing events. There are many different technological phishing deterrents, such as anti-phishing software, anti-spam software, and firewalls. But the technology aspect alone will not effectively prevent phishing. The present body of knowledge expresses that the risk of phishing has been investigated rigorously from the technology side, such as firewalls, anti-phishing software, etc. However, the gap in knowledge is that this risk can be further managed and reduced by focusing on understanding the risks of phishing from the socio side, both the human operator and the employing organization (e.g., human view). After reviewing different models, this study will propose a risk matrix that will be used to allow organizations to scientifically assess how vulnerable an organization or individual is to phishing attacks.

CHAPTER 3

METHODOLOGY

Grounded Theory (GT) and inductive reasoning are an iterative process of collecting and identifying journals and articles, incidents and web posted interviews on phishing. This study analyzed the journals, articles, incidents, and web posted interviews using NVivo Software until it reached theory saturation (meaning there are no more visible patterns emerging from the iterations). A knowledge base of phishing was created as a result. The theory that emerged from this process was used to create a model (phishing matrix).

3.1 GROUNDED THEORY

The Grounded Theory Method (GTM) encourages researchers to “develop their own theories rather than merely fine-tuning existing ones. GTM is based around heuristics and guidelines rather than rules and prescriptions” (Charmaz, 2007, pg.18). Grounded theory is obtained from data and then depicted by characteristic examples of data (Glaser & Strauss, 1967). The purpose of GTM is to generate an abstract concept and define the relationships between them (Charmaz,2007). Charmaz and Belgrave (2015, pg. 1) define GT as “a general methodology with systematic guidelines for gathering and analyzing data to generate middle-range theory. The name “grounded theory” mirrors its fundamental premise that researchers can and should develop theory from rigorous analyses of empirical data. The analytic process consists of coding data; developing, checking, and integrating theoretical categories; and writing analytic narratives throughout the inquiry.” Glaser and Strauss (1967), “first proposed that researchers should engage in simultaneous data collection and analysis. From the beginning of the research process, the researcher codes the data, compares data and codes, and identifies

analytic leads and tentative categories to develop through further data collection. A grounded theory of a studied topic starts with concrete data and ends with rendering them in an explanatory theory” (Charmaz and Belgrave, 2015).

Figure 29 is an example of a Grounded Theory analysis process used by O’Hagan and O’Connor.

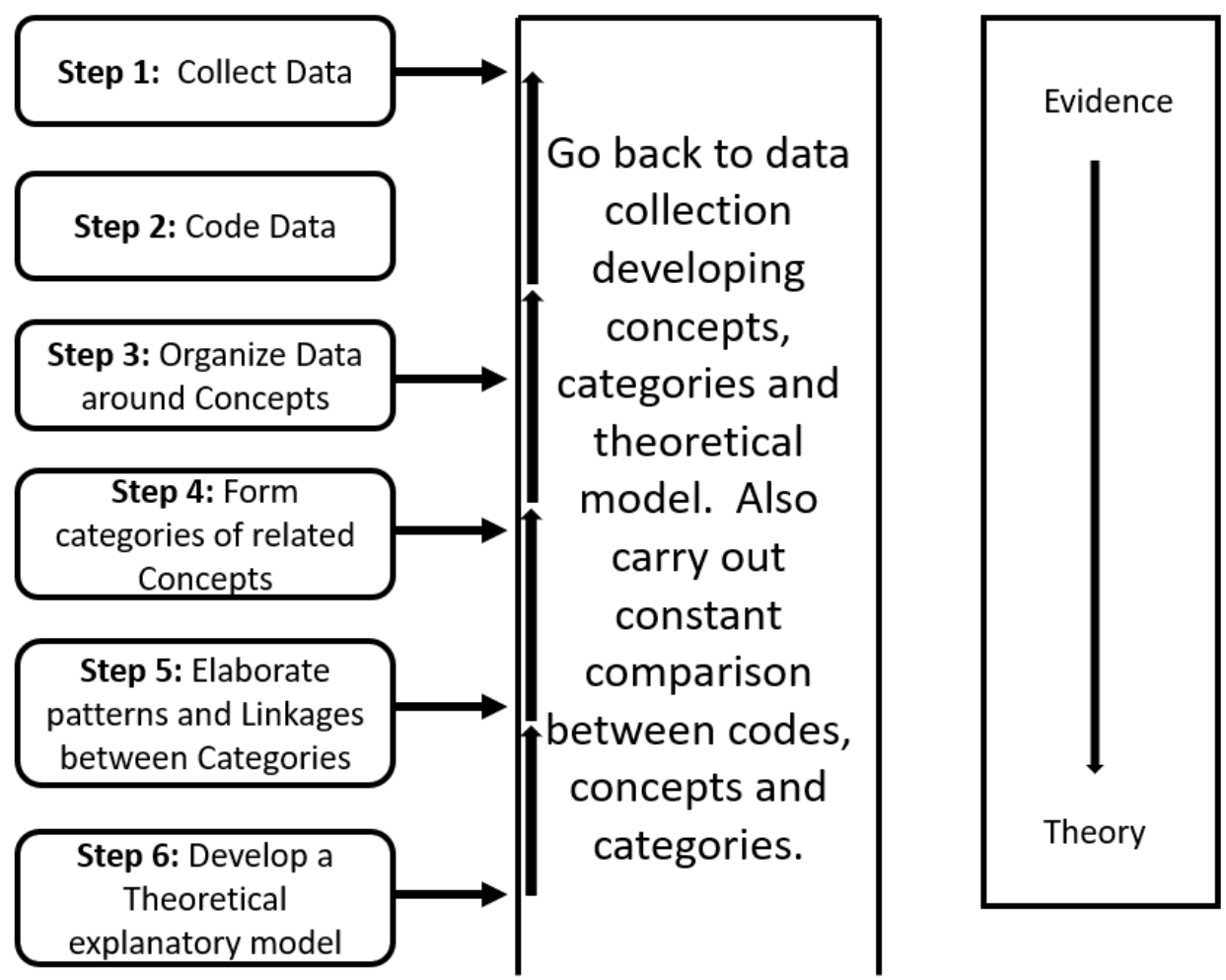


Figure 29. Grounded Theory Data Analysis Steps (O’Hagan and O’Connor, 2015)

Figure 30 is the Grounded Theory Process that was used in this study.

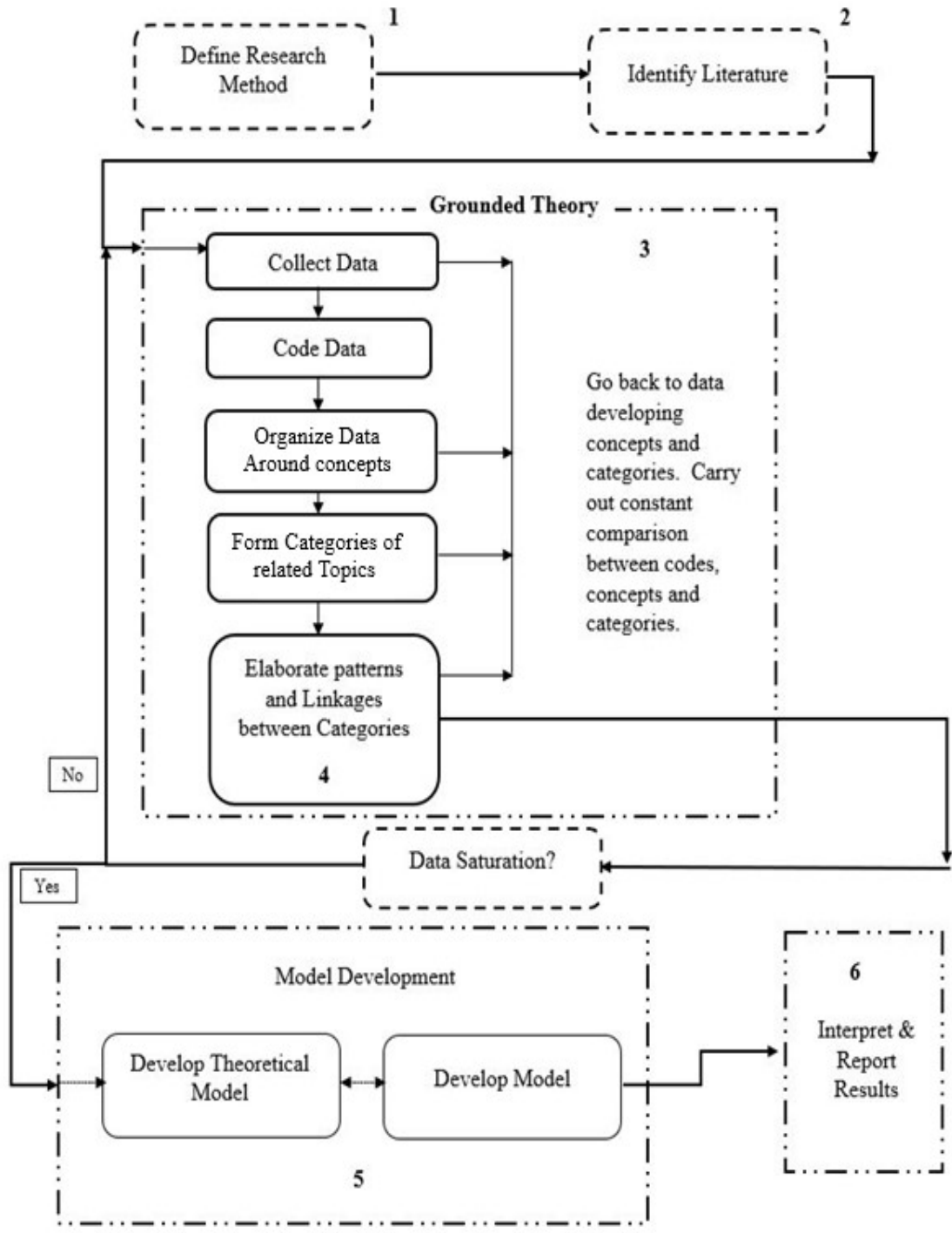


Figure 30. Flow Chart of Methodology Used for this Study

3.1.1 Steps for Methodology

3.1.1.1 Define Research Method

This step identifies the Research Method. In this study, Grounded Theory was the method used.

3.1.1.2 Identify Literature

This step identified the literature that was reviewed for this study. This study identified articles of Human View, Human Factors, Risk Management, Risk, and Human related to Phishing.

3.1.1.3 Grounded Theory Methodology

3.1.1.3.1 Collect Data:

The data for the basis of GTM was collected through two sources:

- Journals, articles, and written documentation relevant to this study using IEEE Xplore, Google Scholar, ODU Library Monarch One Search, and Association for Computing Machinery (ACM) Digital Library, and ScienceDirect Journals and Books.
- Phishing incidents collected from journals and websites.

3.1.1.3.2 Code Data

3.1.1.3.2.1 Open Coding

Glaser's (1978) coding approach is to code everything "characterized by the data open" (LaRossa, 2005). Strauss and Corbin (1990) coding approach rely on the "data analysis that focuses on the conceptualization and categorization of phenomena through an intensive analysis of the data. First, the data are broken up into smaller parts that are deeply analyzed. This analysis aims to grasp the core idea of each part and to develop a code to describe it." The goal is "to develop a wealth of codes with which to describe the data. To reach this goal, sensitizing questions are posed regarding the data when they are being analyzed" (Kaiser,2016).

3.1.1.3.2.2 Axial Coding

Strauss and Corbin (1990) believe this coding process "is needed to investigate the relationships between concepts and categories that have been developed in the open coding process to develop the relations between the categories, they suggest examining the data and the codes based on a coding paradigm that focuses on and relates causal conditions, context, intervening conditions, action/interaction strategies, and consequences" (Kaiser,2016).

3.1.1.3.2.3 Selective Coding

This is the process of choosing one category to be the main category and then associating the rest of the categories to that main category. The idea is to develop a single-story line which everything else follows (Borgatti, 2020).

3.1.1.3.2.4 Theoretical Coding

Glaser's (1978) coding approach is the procedure of making one category the main category and combining all the other categories into that one category. Essentially creating one perspective idea (Borgatti, 2020).

3.1.1.3.2.5 NVivo Coding

NVivo software was used in many ways. NVivo was used to code and organize the data around concepts. By using a keyword search, word mapping, line search, and paragraph search looking through 100 to 200 articles looking for certain keywords like Training, Human View, Human Factors, Risk, Phishing, Human, Risk Management, and other words identified by this research to code and find cross-sections in data. Secondly, it will look for words associated with consequences and the likelihood to populate and evaluate the equations with data.

3.1.1.3.2.5.1 Organize Data

- Data was organized around concepts.
- Categories was formed from related concepts.
- Patterns and linkages were identified between the categories.

3.1.1.3.2.5.2 The Output of the NVivo Software Produces a Table of Themes, References, Patterns of Categories and Concepts.

NVivo Auto Coding allows visual identification of significant content in each Journal. It can create 2 types of hierarchy charts. The hierarchy chart can be used to identify the theme of each article. By looking at each chart, a major content word can be identified as being part of the

major theme or the minor theme. This Chart shows the major content discovered by auto coding. The major word is located at the top of each block. The size of the block demonstrates the frequency of that word in the article. The words that appear inside the blocks are sub-content words that have been auto coded as seen in Figure 31.



Figure 31. NVivo Auto Coded Hierarchy Block Chart

NVivo Auto Coded Hierarchy Circular Chart shows the main auto coded major content words in the article and the visual size of the content word as seen in Figure 32.

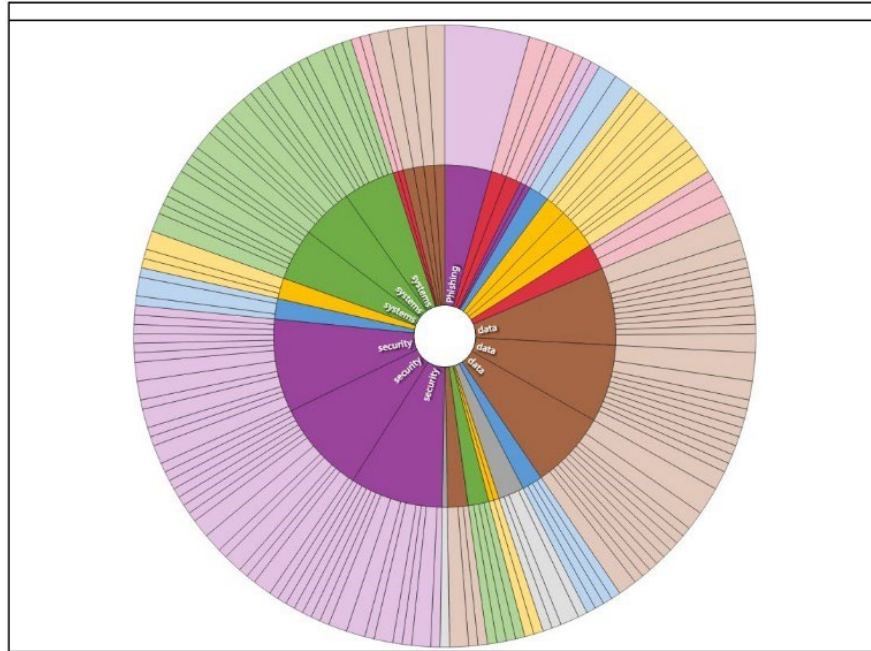


Figure 32. NVivo Auto Coded Hierarchy Circular Chart

Discovering the Major Content of an article determined the classification of the article. Examining the classification of the article determined if the article was related to the study and if it should be examined further. NVivo can identify themes and causes given the correct criteria. By Auto Coding themes, major and minor themes can be determined. This led to defining the root cause and identifying solutions that lead to hypothetical results as well as identifying the number of references. NVivo identified the reference as seen in Figure 33.

The screenshot displays a software interface for analyzing literature. The main window is titled 'Autocoded Themes from Literature' and features a search bar and a table of themes. The 'training' theme is selected, showing 9 files and 69 references. A detailed view on the right shows six references with their respective coverage percentages and content.

| Name | Files | References |
|-----------------------------------|-------|------------|
| training | 9 | 69 |
| annual cyber security training | 1 | 1 |
| anti-phishing training approach | 1 | 1 |
| anti-phishing training experime | 1 | 1 |
| anti-phishing training methods | 1 | 1 |
| comic strip training interventio | 1 | 1 |
| compared classroom training | 1 | 1 |
| contextual training | 1 | 1 |
| current antiphishing training lit | 1 | 1 |
| different training conditions | 2 | 2 |
| digital training | 1 | 1 |
| disaster preparedness training | 1 | 1 |
| effective antiphishing training | 1 | 1 |
| effective anti-phishing training | 1 | 1 |
| effective online training | 1 | 1 |
| embedded training intervention | 1 | 1 |
| embedded training materials | 2 | 2 |
| followed classroom training | 1 | 1 |
| formal classroom training | 1 | 1 |
| game-based training | 1 | 1 |
| immediate training | 2 | 2 |
| ineffective training | 1 | 1 |
| management training | 1 | 1 |
| mandatory training | 1 | 1 |
| phishing training material | 1 | 1 |
| presented training | 1 | 1 |
| proper training | 1 | 1 |
| received training | 2 | 2 |
| security awareness training | 1 | 1 |
| similarity threshold training | 1 | 1 |
| trained children | 1 | 1 |
| trained users | 4 | 4 |
| training activity | 1 | 1 |

References for the 'training' theme:

- Reference 1 - 2.12% Coverage: <Files\\Literature\\Peoples Role in Cyber Security> - \$ 1 reference coded [2.12% Coverage]
- Reference 1 - 2.12% Coverage: Lack of understanding and awareness of implications of security compromises · A relaxed culture where system reliability is not taken seriously · Lack of training for admin staff so they can understand functions and risk implications · Lack of management training to be aware of value of security and cost of being exposed to risks to their businesses · Shortage of suitability trained and skilled technical staff who manage the operations of the system · An environment where teamwork is not encouraged · Cultural differences in multicultural environments where culture clashes may also result in teams not working together towards shared outcomes.
- Reference 1 - 0.20% Coverage: <Files\\Literature\\Phishing - Educating the Internet users> - \$ 11 references coded [2.73% Coverage]
- Reference 1 - 0.20% Coverage: Various techniques deployed in security awareness training to curb the phishing attacks with no avail.
- Reference 2 - 0.24% Coverage: In this conceptual paper we propose a mandatory training or education programs for home users by using email screen shots.
- Reference 3 - 0.29% Coverage: According [15], all users can be trained to detect suspicious looking emails although sometimes it takes considerable time in the training process.
- Reference 4 - 0.26% Coverage: Education still plays an important role in educating the user but it is only effective if the users really read the training material.
- Reference 5 - 0.66% Coverage: This would be our rationale to make it mandatory (or force) forall users to read the training content and it will be the responsibility of the financial institutions to constantly change the content of the training materials by publishing latest information and design the training materials so that it is fun and attractive for the users.
- Reference 6 - 0.26% Coverage: The survey respondentssuggest that testing is important to ensure that users understand the training material after a training session.

Figure 33. Auto Coded Themes and References

After examining the articles, a distinct theme developed. It became apparent that training is essential in preventing phishing attacks. Lack of training for individuals has resulted in devastating and serious exploits that have caused the loss of sensitive data. From this analysis and examination of the initial articles, an initial theory has been developed. The Cluster analysis of the articles helped in determining the strongest articles in developing a theory and a

theoretical model. This was used in determining which articles have a high frequency of training.

During the development of the dissertation, the use of NVivo can determine the categories from the data that is found in the articles and journals. Answering the questions using theoretical sampling of the articles and data collection from the articles did help to determine major categories. Using Human View contributed to the organization and arrangement of the categories. For example: from this proof of concept, training has emerged as a specific concept among the sampled articles in the study of the risk of phishing. Initial training became a focal point in this study, the Human View was used in the following manner:

- To identify various roles of (friendly) humans in phishing.
- To identify information and business process associated with these roles.
- To organize different training methods under Data.
- Formalize these methods in the Training View.

Data was coded by NVivo, and a constant comparison method was used to decipher different or like concepts and categories involving the final theory. Coding in this study was performed when parts of the text are identified and labeled with a category name that fits its description. A constant comparison analysis was used to develop the main category from sampled articles explored by the NVivo coding process and emerging patterns in the data was highlighted. Data was constantly compared to facilitate the identification of new categories towards the final theory, which was alerted that the ‘final theory’ was attained. From the final theory, a theoretical model emerged from the selective coding that was used to explain the structure of the theory and how the core process was used to help mitigate Phishing.

3.1.1.3.2.6 Human View

This study used the Human View to organize data that may identify the interaction of humans with phishing lures. As the study progressed, it identified key traits, identifiable security cultures, and functionality that lead to the organization of data that helped in building a theory that could mitigate the risk of phishing. This study used the Sequence of Individual Views in the DoDAF Human View Architecting Process to assist in architecting a systematic model that could aid in reducing the risk of phishing.

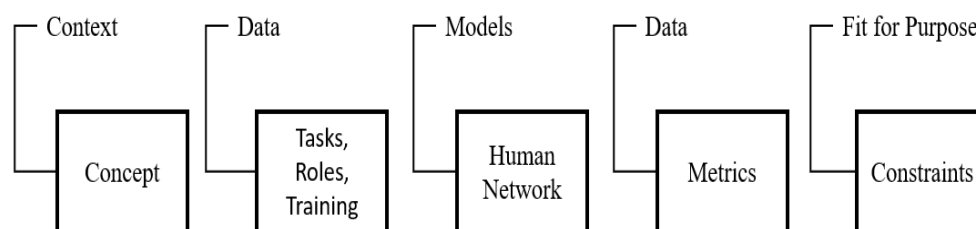


Figure 34. Sequence of Individual Views (Handley, 2019)

The views in Figure 34 would be described as the following when paired with humans and phishing:

1. The Context View described the interaction of humans with the phishing environment and the phishing components.
2. The Task View captured the essential activities that humans perform while interacting with the phishing system. This includes tasks, roles, and training.
3. The Human Network captured the interaction between the human and the phishing events focusing on how humans are coerced into exchanging or sharing sensitive information with phishers.

4. The Metric View captured how the phishing awareness standards learned by humans during training has impacted their performance when confronted with a phishing event.
5. The Constraints View captured the limitations of humans when trying to understand concepts in awareness training. (Handley,2019)

3.1.1.3.3 Organize Data Around Concepts

This is the process of evaluating all collected data and connecting the data to a particular concept that has emerged.

3.1.1.3.4 Form Categories of Related Topics

This is the process of categorizing data and relating them to core topics that emerged during coding.

3.1.1.4 Elaborate Patterns / Data Saturation (Theory Saturation)

This continued constant comparison until no changes are discovered or saturation is apparent.

Data Saturation is the point in Grounded Theory where the analysis of many different articles has reached point where the continuous analysis yielded no new concepts in category or theory. "This phase of qualitative data analysis in which the researcher has continued sampling and analyzing data until no new data appear and all concepts of the theory are well-developed....and their linkages to other concepts are clearly described, and thus data collection could cease" (Aldiabat, 2018).

3.1.1.5 Model Development

3.1.1.5.1 Develop a Theoretical Model.

Using the data gathered, a framework was constructed to initiate the design of the model.

3.1.1.5.2 Develop the Model

The goal is a model of phishing from the patterns identified in the data. This model was a matrix represented by a cube that focused on socio risks and allowed an organization to systematically identify phishing risk in the organization and define areas needed in improvement in either training or awareness. Human View, risk, phishing, and risk management were possible categories that was considered to design the risk matrix. This study will replace the likelihood with frequency.

Figure 35 is a sample of the risk matrix design.

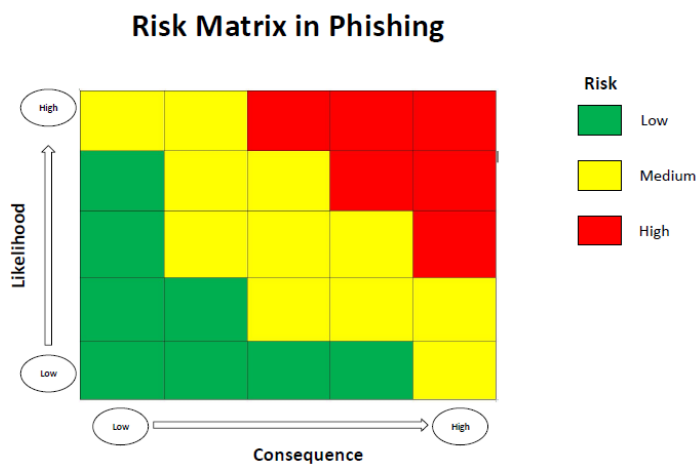


Figure 35. Risk Matrix in Phishing

The requirements in this phishing model are to obtain data points from NVivo that will change the phishing model. By obtaining data points from various keyword searches, this study has discovered if the model changes. If the model remained the same or if this study cannot produce data points for the model, then this model would have failed.

3.1.1.6 Interpret and report results and conclusions.

The documentation of the study and all the research completed and any accomplishments.

3.1.2 Generalizability of Research

The generalizability of research is the ability to take the reported results of this study and apply it to other studies or cases (Polit & Beck, 2010). According to Yusof (2011) “the word ‘generalizability’ is defined as the degree to which the findings can be generalized from the study sample to the entire population.” This study developed a conceptual generalizability that will translate to many other systems and effectively strengthen them to a point that will minimize the effect of phishing.

3.1.3 Validity of Research

Validity is the degree to which a test determines the expected results. But Creswell & Miller (2000) suggest that the validity is affected by the researcher’s perception of validity in the study and his/her choice of paradigm assumption. As a result, many researchers have developed their concepts of validity and have often generated or adopted what they consider to be more appropriate terms, such as, quality, rigor, and trustworthiness (Davies & Dodd, 2002; Lincoln & Guba, 1985; Mishler, 2000; Seale, 1999; Stenbacka, 2001)” (Golafshani, 2003).

Golafshani goes on to state in his study that “If the validity or trustworthiness can be maximized or tested then more “credible and defensible result” (Johnson, 1997) may lead to generalizability which is one of the concepts suggested by Stenbacka as the structure for both doing and documenting high-quality qualitative research. Therefore, the quality of research is related to the generalizability of the result and thereby to the testing and increasing the validity or trustworthiness of the research” (Golafshani, 2003).

While Thompson states in his study that “Messick defines validity as an integrated evaluative judgment of the degree to which empirical evidence and theoretical rationales support the adequacy and appropriateness of inferences and actions based on test scores or other modes of measurement. This definition suggests that the concept of validity contains several important characteristics to review or propositions to test and that validity can be described in several ways” (Thompson, 2013).

While Golafshani states that “in contrast, Maxwell observes that the degree to which an account is believed to be generalizable is a factor that clearly distinguishes quantitative and qualitative research approaches. Although the ability to generalize findings to wider groups and circumstances is one of the most common tests of validity for quantitative research, but Patton states generalizability as one of the criteria for quality case studies depending on the case selected and studied. In this sense, the validity in quantitative research is very specific to the test to which it is applied – where triangulation methods are used in qualitative research. Triangulation is typically a strategy (test) for improving the validity and reliability of research or evaluation of findings” (Golafshani, 2003).

Denny Borsboom, Gideon J. Mellenbergh, and Jaap van Heerden state: “the concept of validity thus expresses nothing less but also nothing more than that an attribute, designated by a

theoretical term like *intelligence*, exists and that measurement of this attribute can be performed with a given test because the test scores are causally affected by variation in the attribute. This conception does the job we want validity to do, and it does it in a simple and effective way” (Borsboom, 2004).

Sargent highlights the following validation techniques and methods in Figure 36.

| Sargent's Validation Techniques and Methods | |
|---|--|
| Validation Techniques/Method | Definition |
| Animation | The model's operational behavior is displayed graphically as the model moves through time. |
| Comparison to Other Models | Various results (e.g., outputs) of the simulation model being validated are compared to results of other (valid) models. |
| Degenerate Tests | The degeneracy of the model's behavior is tested by appropriate selection of values of the input and internal parameters. |
| Event Validity | The "events" of occurrences of the simulation model are compared to those of the real system to determine if they are similar. |
| Extreme Condition Tests | The model structure and outputs should be plausible for any extreme and unlikely combination of levels of factors in the system. |
| Face Validity | Individuals knowledgeable about the system are asked whether the model and/or its behavior are reasonable. |
| Historical Data Validation | If historical data exist (e.g., data collected on a system specifically for building and testing a model), part of the data is used to build the model and the remaining data are used to determine (test) whether the model behaves as the system does. |
| Historical Methods | The three historical methods of validation are rationalism, empiricism, and positive economics. Rationalism assumes that everyone knows whether the clearly stated underlying assumptions of a model are true. Logic deductions are used from these assumptions to develop the correct (valid) model. Empiricism requires every assumption and outcome to be empirically validated. Positive economics requires only that the model be able to predict the future and is not concerned with a model's assumptions or structure (causal relationships or mechanisms). |
| Internal Validity | Several replications (runs) of a stochastic model are made to determine the amount of (internal) stochastic variability in the model. A large amount of variability (lack of consistency) may cause the model's results to be questionable and if typical of the problem entity, may question the appropriateness of the policy or system being investigated. |
| Multistage Validation | Naylor and Finger (1967) proposed combining the three historical methods of rationalism, empiricism, and positive economics into a multistage process of validation. This validation method consists of (1) developing the model's assumptions on theory, observations, and general knowledge, (2) validating the model's assumptions where possible by empirically testing them, and (3) comparing (testing) the input-output relationships of the model to the real system. |
| Operational Graphics | Values of various performance measures, e.g., the number in queue and percentage of servers busy, are shown graphically as the model runs through time; i.e., the dynamical behaviors of performance indicators are visually displayed as the simulation model runs through time to ensure they behave correctly. |
| Parameter Variability - Sensitivity Analysis | This technique consists of changing the values of the input and internal parameters of a model to determine the effect upon the model's behavior or output. The same relationships should occur in the model as in the real system. This technique can be used qualitatively—directions only of outputs—and quantitatively—both directions and (precise) magnitudes of outputs. Those parameters that are sensitive, i.e., cause significant changes in the model's behavior or output, should be made sufficiently accurate prior to using the model. (This may require iterations in model development). |
| Predictive Validation | The model is used to predict (forecast) the system's behavior, and then comparisons are made between the system's behavior and the model's forecast to determine if they are the same. The system data may come from an operational system or be obtained by conducting experiments on the system, e.g., field tests. |
| Structured Walkthroughs | Primary techniques used to determine that the model has been programmed correctly. An examination of the code to make sure there are no language errors. |
| Traces | The behaviors of different types of specific entities in the model are traced (followed) through the model to determine if the model's logic is correct and if the necessary accuracy is obtained. |
| Turing Tests | Individuals who are knowledgeable about the operations of the system being modeled are asked if they can discriminate between system and model outputs. (Schruben (1980) contains statistical tests for Turing tests). |

Figure 36. Sargent's Validation Techniques and Methods (Sargent, 2009)

This study would use Face Validity. According to Sargent (2009), face validity is when “individuals knowledgeable about the system are asked whether the model and/or its behavior are reasonable. For example, is the logic in the conceptual model correct, and are the model’s input-output relationships reasonable.”

3.1.4 Reliability of Research

Reliability is how relentlessly a study can be repeated to yield the same results (Golafshani, 2003). While reliability is concerned with the repeatability of scientific findings, it can also be described as consistency, dependability, and confirmability (Elliott, 2004). Kirk and Miller (1986) recognized three types of reliability: (1) the degree to which a measurement, given repeatedly, remains the same (2) the stability of a measurement over time; and (3) the similarity of measurements within a given time period (pp. 41-42).

Heale & Twycross (2015) states that “reliability relates to the consistency of a measure. A participant completing an instrument meant to measure motivation should have approximately the same responses each time the test is complete. Although it is not possible to give an exact calculation of reliability, an estimate of reliability can be achieved (p. 3).”

McCrae (2011) reminds us that “it would be a mistake to say that reliability is one of the fundamentals of personality assessment because reliability is not one thing. Internal consistency, which reflects the coherence (or redundancy) of the components of a scale, is conceptually independent of retest reliability, which reflects the extent to which similar scores are obtained when the scale is administered on different occasions separated by a relatively brief interval” (p. 1). Reliability would reflect the consistency (repeatability that yields uniform scientific results) of this study.

3.2 CONCLUSION

This chapter has provided an overview of this study's research methodology. It has provided the methods, techniques of coding, type of software, and organizational and categorical approaches that was used in this study. Grounded theory was the primary method used in the third step of this study. The first step was the collection of data from various sources. The second step was the identification of literature. The third step is the implementation of Grounded Theory Coding. The fourth step is the elaboration of patterns. During the third and fourth steps, NVivo software was used when needed. The fifth step is the Model Development including Validation. The sixth and final step is to interpret and report the results. The expected outcome of this research would be a new model of a phishing scenario. This study started by building a framework that coincided with a model that included risk management using human views which would become part of the framework resulting in a risk cube.

CHAPTER 4

RESEARCH ANALYSIS AND FINDINGS

4.1 COLLECTING DATA

I reviewed over 250 written information collected from Journals, articles, and written documents related to phishing and other topics related to this study. IEEE Xplore, Google Scholar, ODU Library Monarch One Search, Association for Computing Machinery (ACM) Digital Library, and Science Direct Journals and Books were used in this study to collect data. Documented web interviews were used from the journals collected in this study.

4.2 CODE DATA

4.2.1 Opening Code

Data was collected from Journals, articles, and written documents that was obtained in this study. During this phase, over 250 documents were processed and reviewed. Documents were categorized and broken down into smaller pieces for conceptualization. The goal here was to analyze the documents and to categorize the file they represent.

4.2.2 Axial Coding

As data was coded, and categories were created. Training and awareness began to appear as categories during this process. The more the articles were reviewed, Training and awareness had become more visible to the systemic process in phishing.

4.2.3 Selective Coding

As more documents were being reviewed, Selective Coding process revealed categories that began to build a story line. Once this story line had begun to appear more evident, one main category could be developed.

4.2.4 Theoretical Coding

During this process, the documents were reviewed to begin the process of combining the categories into one category eventually leading to one perspective idea. In this study, this process led to two main categories that are training and awareness that led to one main idea.

4.2.5 NVivo Coding

NVivo Software was used to do keyword searches, word mapping, line searches, and paragraph searches looking through over 180 documents for the keywords of Training, Awareness, Human View, Human Factor, Risk, Human, and Risk Management to code and cross-sections in data. NVivo helped to organize data around concepts, helped reaffirm categories, and established patterns and links between the training and awareness categories while still incorporating human and risk. NVivo created a database of all the documents and organized them.

The screenshot displays the NVivo 12 Plus software interface. On the left, a 'Quick Access' pane shows a hierarchical tree structure with categories like 'Files', 'Data', and 'Codes'. The main window is divided into two panes. The left pane, titled 'Articles 257', contains a table listing various articles with columns for 'Name', 'Codes', and 'Referen'. The right pane shows a preview of an article titled 'An Overview on Phishing- its types and Countermeasures' published in the 'International Journal of Engineering Research & Technology (IJERT)'. The article includes author information for Antonette R. Mantode and Sandeep S. Parve, an abstract, keywords, and an introduction section. A diagram titled 'A. Core Process of phishing' is also visible, showing a flow from 'Phishing email' to 'Victim' to 'System'.

| Name | Codes | Referen |
|---|-------|---------|
| 2016-05-cybersecurity-weakest-link-humans | 0 | 0 |
| 2017 PhishLabs Phishing and Threat Intelligence Report | 0 | 0 |
| 2020_BigDataAnalyticsandComputingforDigitalForensicInvestigations_chapter81 | 0 | 0 |
| A Comparative Usability Study of Two-Factor Authentication | 0 | 0 |
| A Comprehensive Study of Phishing Attacks | 0 | 0 |
| A Description Logic Ontology for Email Phishing | 0 | 0 |
| A Framework for Detecting Phishing Websites using GA based Feature Selection and ARTMAP based | 0 | 0 |
| A Graph-Theoretic Approach for the Detection of Phishing Webpages | 0 | 0 |
| A multi-level influence model of COVID-19 themed cybercrime | 0 | 0 |
| A New Zero Day | 0 | 0 |
| A Novel Approach for Phishing Websites Detection using Decision Tree | 0 | 0 |
| A Personality Based Model for Determining Susceptibility to Phishing Attacks | 0 | 0 |
| A predictive model for phishing detection | 0 | 0 |
| A predictive model for phishing detection | 0 | 0 |
| A study of agent system model for response to spear-phishing | 0 | 0 |
| A systematic frame work of schedule risk management for power grid engineering projects, sustainabl | 0 | 0 |
| A Toolkit for Security Awareness Trainings Against Targeted Phishing | 0 | 0 |
| A_Study_on_Phishing_Preventions_and_Anti | 0 | 0 |
| A_STUDY_ON_SOCIAL_ENGINEERING_ATTACKS-PHISHINGATTACK (1) | 0 | 0 |
| Accenture-2017-CostofCyberCrimeStudy | 0 | 0 |
| AFrameworktoMitigatePhishingThreats-E.D.frauenstein | 0 | 0 |
| An Analysis of Phishing Blacklists - Google Safe Browsing, OpenPhish, and PhishTank | 0 | 0 |
| AN ASSESSMENT OF USER RESPONSE TO PHISHING ATTACKS | 0 | 0 |
| An examination of the effect of recent phishing encounters on phishing susceptibility | 0 | 0 |
| An_approach_for_profiling_phishing_activ | 0 | 0 |
| An_Enterprise_Anti_phishing_Framework | 0 | 0 |
| An_Invigation_Into_Students_Responses | 0 | 0 |

Figure 37. NVivo Document Database and Organization

NVivo Auto Coding allowed visual identification of significant content in journals, articles, and written documentation. It was used to create hierarchy charts that were used to identify themes in different articles and journals. It was used to create charts that identified major and minor themes. It discovered the major content of articles which led to the clarity of the article. The clarity of the article led to how impactful the article was to the study and whether it needed less or further examining. When given a criterion, NVivo identified major and minor themes in the articles which led to the identification of root causes. This allowed the study to identify solutions that lead to hypothetical results. NVivo has connected many different articles to the Training category.

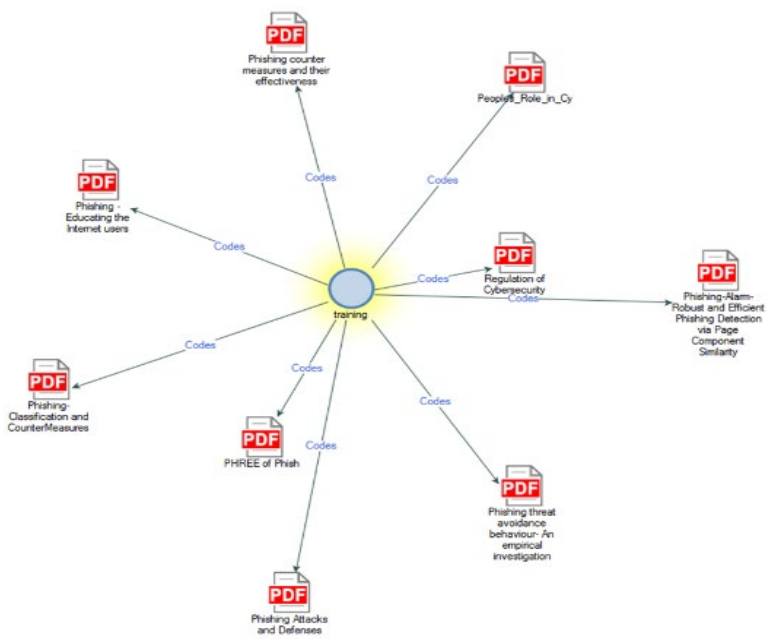


Figure 38. NVivo Document Relation Code

NVivo has developed word trees associated with the Training category. This helps to identify different areas of training. This also identified articles that are related by the same category.

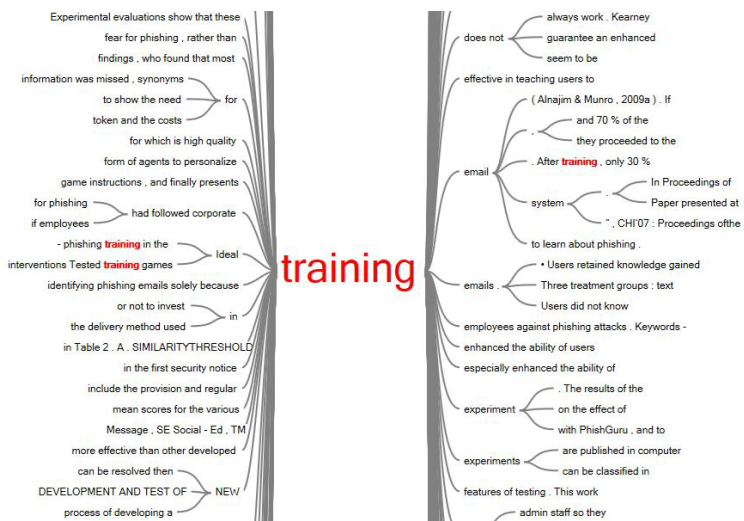
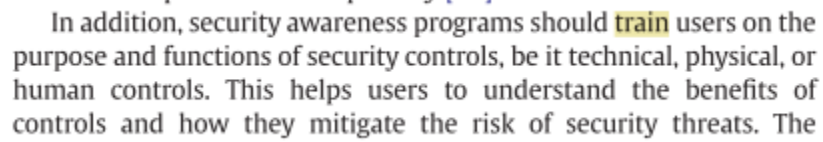


Figure 39. NVivo Word Tree

After reviewing the coding, the chosen articles, journals, and written documentation, a theme for this study was chosen. Training and awareness of phishing plays a vital role in mitigating phishing attacks. Below is a word search defined in an article.



In addition, security awareness programs should **train** users on the purpose and functions of security controls, be it technical, physical, or human controls. This helps users to understand the benefits of controls and how they mitigate the risk of security threats. The

Figure 40. NVivo Article Word Search

NVivo does not make a clear and concise determination of training and awareness as a focal point when using some of the NVivo processes. But NVivo does find focal points of training and awareness in the many other processes in NVivo such as different word and sentence searches, word trees, and word clouds that can be conducted. As the study further researched, NVivo identified training and awareness to play a vital role in the mitigation of phishing attacks.

CHAPTER 5

THE MODEL

In the pursuit for developing the model, more and more articles were reviewed until the saturation point was evident. The model would take the form of a phishing risk matrix due to the abundance of data collected. With the distinction of two categories (awareness and training) and the collection of phishing data points collected as results, a 3D Risk Matrix has been selected to represent the model.

The X axis would be named the Awareness axis which would represent three vectors of awareness. The first vector would be Voluntary Awareness (A1). The second vector would be Restrictive Awareness (A2). The third vector would be Mandatory Awareness (A3). These vectors would be numerical values representing data points for the awareness solution plot. The Y axis would be named the Training axis which would represent 3 vectors of training. The first vector would be Voluntary Training (T1). The second vector would be Restrictive Training (T2). The third vector would be Mandatory Training (T3). These vectors would be numerical values representing data points for the training solution plot.

The Z axis would be named the Consequence axis which represents the number of successful phishing attacks. This would be numerical collected data over cycle (chosen time period) that would be entered into the model to measure the effects of the Awareness Axis (X) and Training Axis(Y) over the period of time that data is collected.

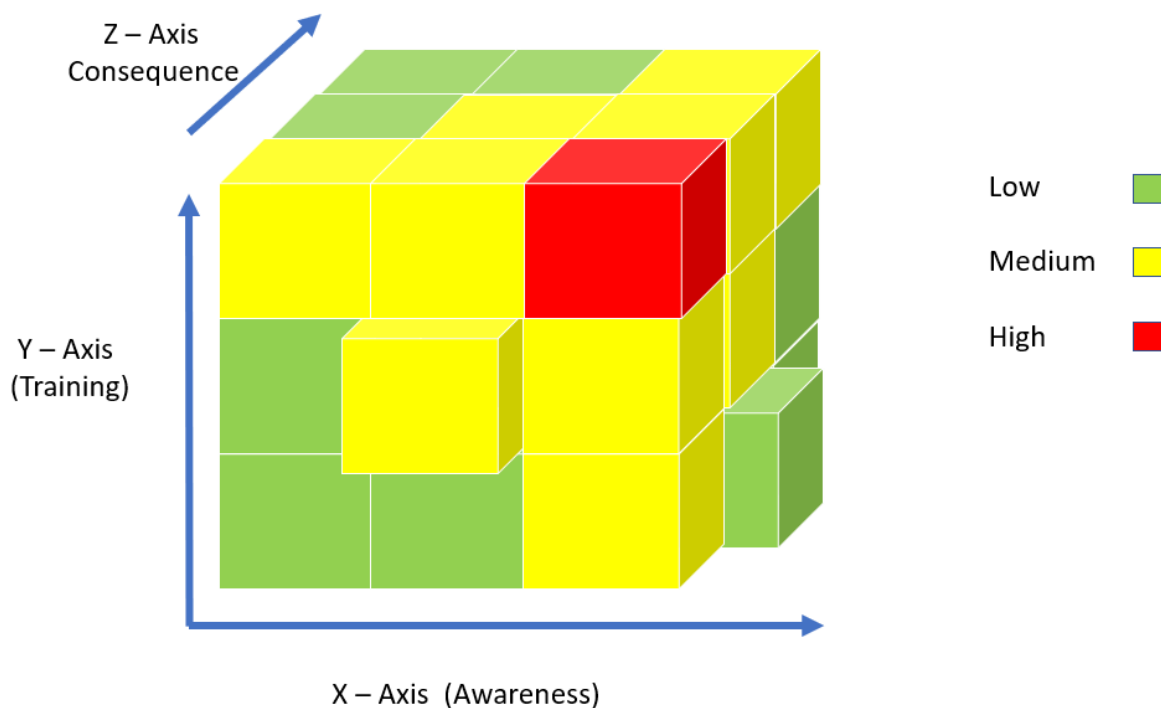


Figure 41. Representation of 3D Matrix Model for this Study

This model would be embedded in the security system of the organization and gather data. The data gathered would be data relating to the positive and negative effects of different selected awareness techniques and training techniques implemented by an organization. This data can be successfully measured in a systematic risk cube. The level of consequence in this model is determined by the number of successful attacks that are recorded by the organization. This will be measured with the mitigation solutions that were in place during a given time cycle. In this study, Training and Awareness is solution driven. They are represented by numerical points that can be plotted on a graph to create a risk comparison of the two solutions. This will become a deciding factor in choosing a more favorable phishing mitigation solution.

In the model, the range of numerical values can be from 1 to 10. 1 being the lowest risk and 10 being the highest risk. If a company gets 1 to 100 hundred attacks during a specified time (1 month). Then 1 would be associated to 10 attacks. 2 would be associated to 20 attacks..., 10 would be associated to 100 attacks. During the time a solution is implemented (1 month), these values would be recorded for each day during the month determining a data point for the axis (x, y, z) that the solution was configured for. Data point being 1 if they had 10 or under 10 attacks that day. Data point being 2, if they 11 to 20 attacks that day... Data point being 10 if they had 91 to 100 attacks. One axis coordinates the total attacks, the other axis coordinates attacks during the time one solution is running and the third axis coordinated the time the second solution is running. If the company wanted to configure tool to directly use the number of attacks for each axis, they could. It would be up to the company to decide the range and risk depending on their size and how many solutions they want to test. To one company, 4 attacks would be low to them if they experience an average of 86 attacks a day. To another company just 1 attack may be too high. The appropriate value would be chosen by the company using the model.

The model would be customized by the organization. By knowing the number of attacks during a specified time period (1 hour, 12 hours, 24 hours, 1 week, 2 weeks, 3 weeks, 1 month, 2 months, 3 months, up to a 1 year), data points can be chosen. Type of solution (voluntary awareness, restrictive awareness, mandatory awareness, voluntary training, restrictive training, mandatory training) would determine one axis. The data point of each solution would be the amount of phishing attacks that happen during the given time constraint. These would be the parameters that would be entered into the interface. The risk level would be another chosen parameter. So, the parameters would be amount of time, solution, and risk level the company

chooses. To implement this model, you will first need to develop the model using a software. The representation below will allow you to create the model.

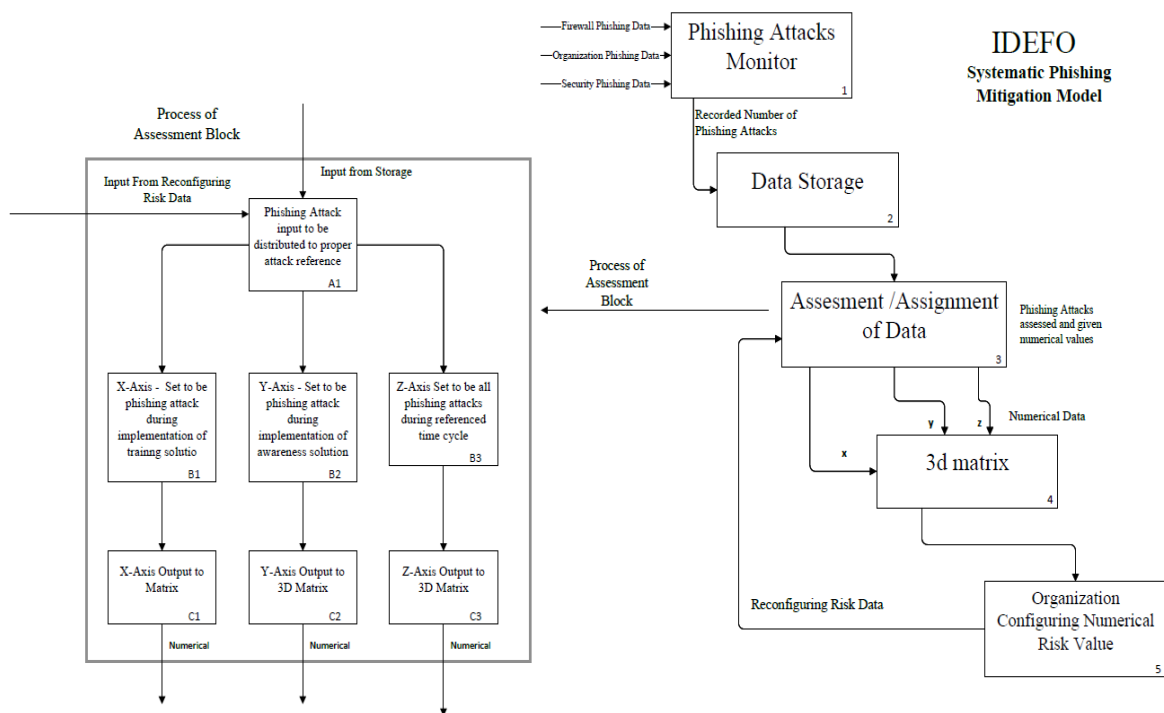


Figure 42. IDEFO Systematic Phishing Mitigation Model

To enhance the ability of the model, a systematic tool can be produced. The systematic tool (a tool that is incorporated into the security system as part of the system) would be a software interface between the model and the security personnel that would pull information from the model and enhance the process for security personnel to measure different mitigation techniques and allow the security personnel to make a more beneficial decision on which awareness programs or training programs that the organization would use to mitigate the effect of phishing on the organization. This tool will be able to help organizations discover the

effectiveness of one technique compared to the effectiveness of another technique. In addition, this tool could systematically lower the cost of mitigation methods being used depending on which methods that are suggested by the tool.

CHAPTER 6

TOOLIFICATION OF THE MODEL

The systematic tool would monitor what works better for the organization by analyzing the data provided by the model, whether it is training or awareness. Organizations may have several training and awareness programs. Organization may not always know which mitigation techniques work better than the others. This tool would help organizations decide which mitigation technique has given better results. The tool is a systematic software program that would collect data from the embedded systematic model. The tool would run over a given time. During this time, the tool would gather information on phishing events. It will measure the degree of successful and unsuccessful attacks during the time given when using a selected mitigation technique. It will keep records of attacks during a specified time and reserve them in a database. When another technique is selected, it will repeat the method during the time that technique has been selected. It will compare the different techniques selected to measure the differences in the number of successful phishing attacks and rate each technique. For example, in a university, the tool would be given one semester to analyze an awareness mitigation solution. During that semester it would collect information on successful and unsuccessful phishing attacks in the University and store the information in its own or provided database to the tool. After four semesters, it will gather information on several awareness and training mitigation solutions. Such information would be the amount of successful phishing attacks during the implementation of each phishing mitigation solution. Other information would be the cost of providing the phishing mitigation solution. After the fourth semester, the tool would be used to compare the information it collected and report the differences in the mitigation solutions and the Security Engineer would be able to select the most favorable mitigation solution to use

Steps on using the tool:

1. Install the systematic tool.

The systematic tool would be software that the Security Engineers would install into their system, and it would be used to interface with present monitoring technologies in the organizations systems. Such technology could be CrowdStrike, Microsoft Endpoint Security, etc. This software tool would gather information from the present technology in the organization. This information would include attacks on the system both successful and unsuccessful. The tool would then measure differences in successful phishing attacks and compare them to specific times that awareness solutions and/or training solutions were implemented.

2. Configure the Tool

Security Engineers would start the tool using graphical user interface and make proper configurations to the tool. Configuration would consist of selecting the appropriate cycle to run the tool. The suggested cycle would be no less than a month and suggested maximum would be six months but no greater than a year. One month is chosen to be the minimum because when changing mitigation solutions in an organization it will take some time at first to propagate into the organization and then to get proper results. The maximum for a mitigation solution is year because phishing attacks are constantly changing, a year would leave the mitigation solution to be questionable if it were not updated. The cycle time would still be the organization's decision on the minimum or maximum to gather data from the chosen data systems and would monitor and record the amount of successful and unsuccessful attacks within the organization. A

mitigation solution would be selected to use during the time the tool is gathering data on phishing attacks.

Second, the Security Engineer would use the graphical interface to set mitigation techniques such as: the awareness solution being used, the training solution being used, and what cycle the software would collect data using those set solutions. This model is not reliant on measuring just the difference between training solutions and awareness solutions. It will be able to measure the differences between two training solutions or two awareness solutions. Thirdly, the Security Engineer would set the different possibilities and decide and initiate the type of data collection the tool would perform.

3. Gather Data

The Security Engineer would initiate the starting of the tool and allow tool to record phishing events, successful and unsuccessful. The tool would begin collecting data on phishing attacks on the organization and will record it per the time of a particular awareness solution or training solution has been implemented. The engineer would choose type of data storage and how long to store the data in this step.

4. Choose the mitigation techniques to query.

After several given cycles, the tool would be queried to measure changes in the selected cycles. The tool would be used to compare differences in the cycles of different selected mitigation techniques. Gather information the tool to reported on. Compare changes to measure the most favorable differences.

After a selected cycle, the Security Engineer will bring up the graphical interface of the tool and will select and review the performance calculations of the different cycles the tool has collected. The Security Engineer would let the tool analyze the data for

differences and discrepancies. The Engineer would examine the tools performance reference of various training and awareness solutions to discover which solutions the tool suggests as more beneficial and favorable taking into consideration of cost and effects.

5. Decide on the favorable mitigation technique.

The Security Engineer will review all the data provided by the tool. This data will include when each mitigation awareness and/or training solution was implemented. During the times that the solution was implemented, the tool will examine the amount of successful attacks on the organization and the cost of the solutions that were deployed during the time of successful phishing attacks. By measuring and calculating the cost and the amount of attacks during the time each mitigation solution was implemented, the tool would provide the most favorable and beneficial solution to the organization.

Below is a Flow Chart representing the steps in the use of the Systematic Tool.

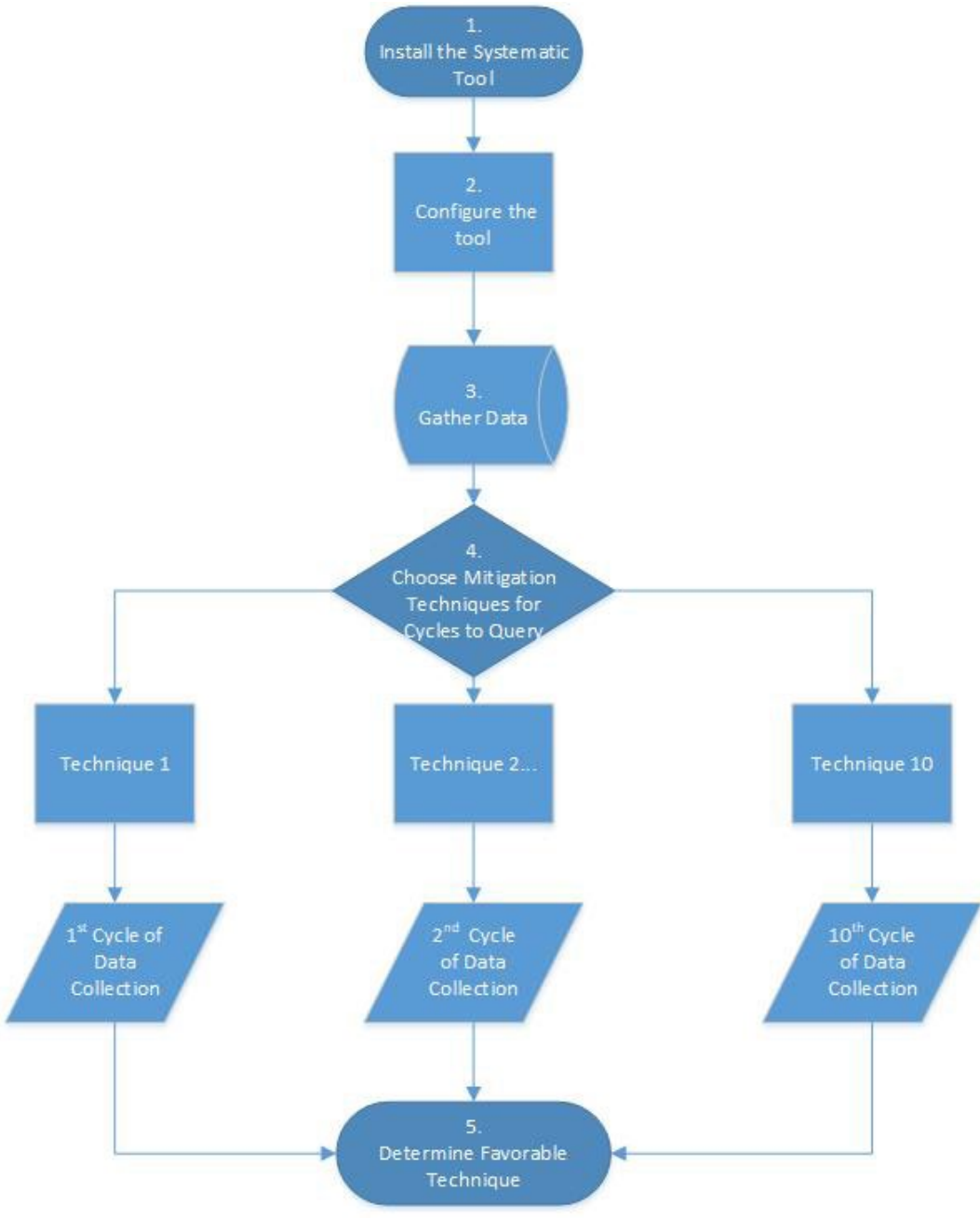


Figure 43. Systematic Tool Operation Flow Chart

When using this model, many different organizations have different levels of risk that they would define as low, medium, or high. For example, if a company has experienced 24 phishing attacks in a year. They could designate 24 attacks as the maximum level for high, 16

attacks as maximum level for medium and 8 attacks as the maximum level for low. It is left to the organizations to define what their levels of risk are and to set the model or tool accordingly and effectively. The blocks are dependent on the organization's choice of which is low, medium, or high. They are not fixed; they can change according to color and designation that is set when the organization decides how they want to measure the risk. Also, rather than levels of risk, organizations could choose a number representing the risk factor rather than the level of risk. If the company wanted a yes/no value, they could choose to use that in the configuration, but it would not be recommended due to the use of numerical values in this model. For this model presently, the value ranges are the number of attacks that happen during the cycle configured for awareness and the cycle configured for training. The consequences value is the number of phishing attacks on the organization during the configured cycle of time. Presently, the cycles range from one month at minimum to 1 year at maximum.

The output of the tool would be a report on the number of attacks that occurred during the time a solution was implemented. It would list the number of attacks, when the attacks happened, what solution was implemented during the attacks, what time period was set, the risk involved (according to the setting of the company) for the solution that was set to be monitored.

Below is the Block Definition Diagram for the Systematic Phishing Mitigation Tool.

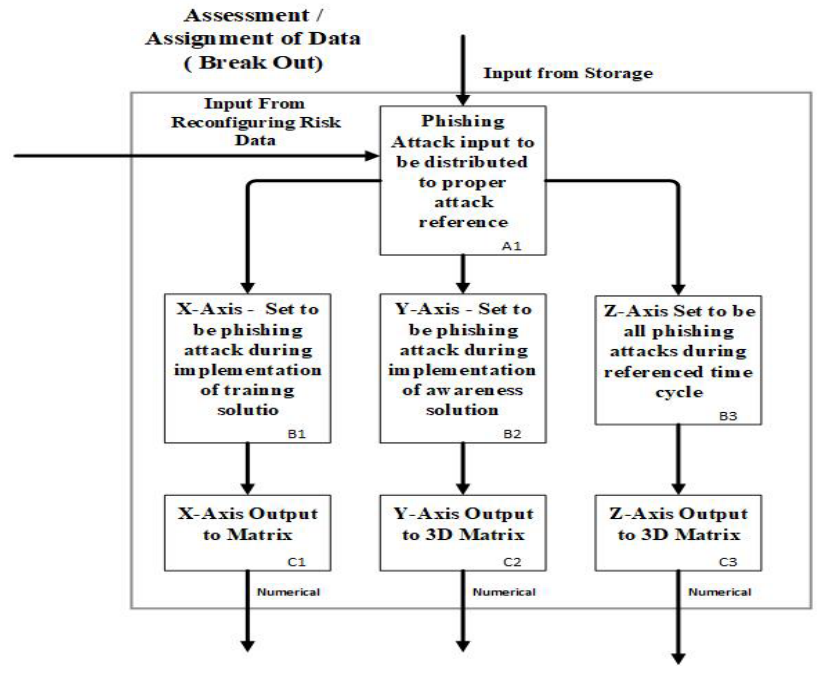
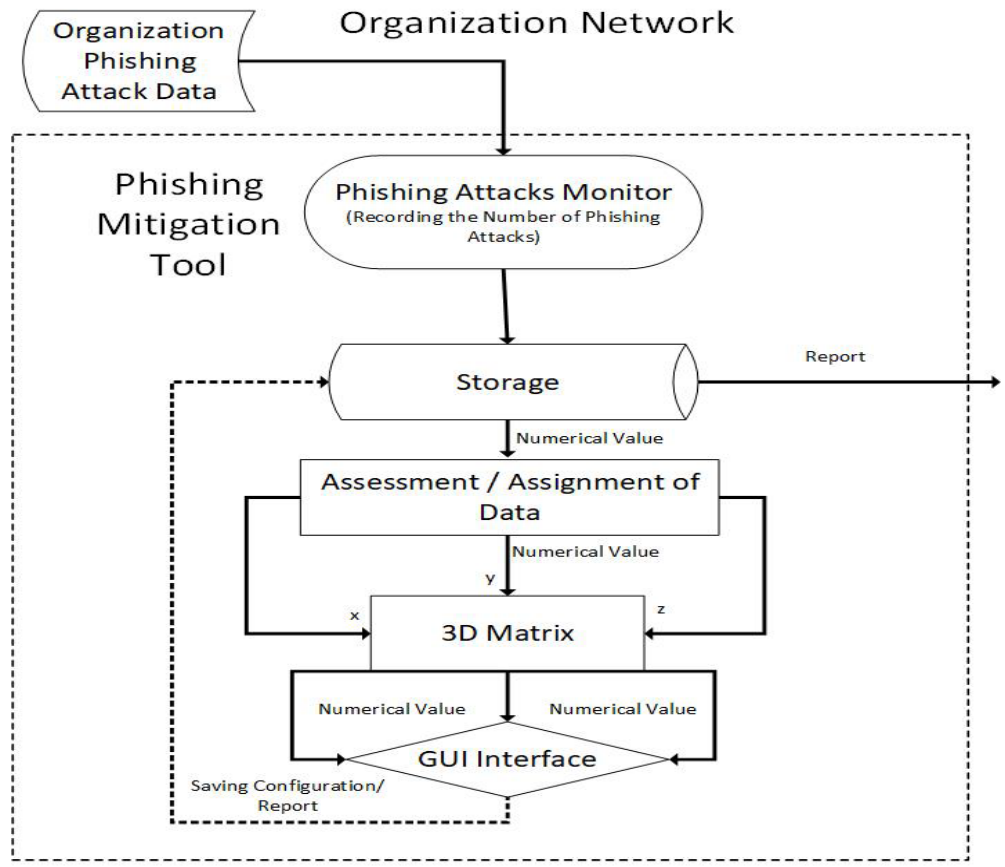


Figure 44. Block Definition Diagram for the Systematic Phishing Mitigation Tool

CHAPTER 7

CONCLUSIONS

Software and Hardware Anti-Phishing solutions are commonplace in most companies today. The threat of getting phished and allowing phishers to obtain sensitive data is constant. Phishers are getting more resilient and more savvy with different attacks targeting humans. Software and hardware components have evolved to take the human component out of the equation. But with more zero-day phishing events and insider attacks, the human component has become the last line of defense when a phishing event has penetrated the software and hardware barriers.

Section 1 in this study has identified phishing and the three components; the lure, hook and catch. This study explored Humans as a living system. Expressed how the Human View enabled the understanding of the human roles in systems architectures. Developed the phishing attack diagram and explained the components of the diagram to increase the body of knowledge of phishing attacks. Different types of phishing were revealed and defined to gain a better understanding of the increasing dangers phishing. A Phishing Interaction Diagram was introduced to understand step by step how the individual is manipulated during a phishing encounter. Seven generalizable guiding questions in risk management was reviewed as well as a common risk matrix highlighted with severity and likelihood ratings. Operational Risk Management and Human Views were expressed and defined. Objectives of this research, goals, questions, and methodology were disclosed for this study.

Two questions were predicated:

1. How the interaction between the human and the phishing lure be adjusted to mitigate the risk of phishing (i.e., from systemic perspective)?

2. How can developing a systematic method help in mitigating risk of phishing by reducing the likelihood of a successful attack?

First, this study has identified methods to reinforcing the human component. The two categorical methods can be used systematically to effectively mitigate phishing in a company. The methods can improve the human's ability to detect phishing through training or by improving the human's awareness of phishing. Incorporating training into the overall company system will allow the Human Component to become a systematic anti-phishing component. Many articles referenced in this study has supported training as a strong component to making a company systemically resistant to phishing attacks. If training is not an option for an organization, then awareness is the other option. Making awareness a systemic option will allow organization to react systematically to phishing attacks that penetrate the software and hardware barrier. If organizations incorporate training or awareness or both into their security systems, this will allow the systematic response of the human component learned during training and/or awareness implementations to systematically respond to evade phishing threats.

Second, after reviewing many different articles on phishing and phishing attacks, there is powerful need for a systematic system with the ability to resist constant phishing attacks. This study has discovered how exhausting phishing attacks are on an organization and its security. Many organizations have developed a hardware and/or software component to manage the constant threat of phishing. Hardware and software components are not enough to take on the constant and relentless threat of phishing. There has always been the threat of one or more phishing campaigns that have been able to penetrate the software or hardware barrier. The human component developed by training and awareness programs become the last barrier developed to systematically combat constant phishing attacks. By creating the human component barrier using

training and awareness programs, will allow the organization to effectively mitigate phishing in the organizational system.

Goals of this study was the following:

1. Create a knowledge base of phishing incidents.
2. Create a systematic model of phishing interactions with humans using a systemic perspective.

One, through extensive research, this study has gathered over 250 phishing articles. The phishing articles were gathered from IEEE Xplore, Google Scholar, ODU Library Monarch One Search, and Association for Computing Machinery (ACM) Digital Library, FBI Website, and ScienceDirect Journals and Books. These articles represent a knowledge base of phishing incidents has been gathered in a NVivo database.

Two, by following the methodology of this study a model has been created to help produce a future systematic tool that is a phishing risk cube that could be implemented to help organizations decide how to use training and awareness to mitigate phishing risk.

Chapter 2, the Literature Review, has expressed that phishing attacks have been constantly increasing. Phishing has become a very lucrative for cybercriminals because of the low investment and high profitability. Risk Management and Human Viewpoint methodology were used to develop and organize data from phishing events. There are many different technological phishing deterrents, such as anti-phishing software, anti-spam software, and firewalls. But the technology aspect alone will not effectively prevent phishing. The present body of knowledge expresses that the risk of phishing has been investigated rigorously from the technology side, such as firewalls, anti-phishing software, etc. However, the gap in knowledge is that this risk can be further managed and reduced by focusing on understanding the risks of

phishing from the socio side, both the human operator and the employing organization (e.g., human view). After reviewing different models in this study, a risk matrix has been developed to allow organizations to scientifically assess how vulnerable an organization or individual is to phishing attacks.

Chapter 3 is an overview of this study's research methodology. It has provided the methods, techniques of coding, type of software, and organizational and categorical approaches that will be used in this study. The first step in this section was the collection of data from various sources. The second step was the identification of literature. The third step was the implementation of Grounded Theory Coding. The fourth step was the elaboration of patterns. During the third and fourth steps, NVivo software was used when needed. The fifth step was the Model Development. The sixth and final step was the interpreting and reporting of the results. The outcome of this research was a new model of a phishing scenario. This study started by building a framework to develop a model which would include risk management and the use of human views which became part of the framework resulting in a risk cube.

NVivo proved to be an asset to help understand how the two methods can be effective. In this study, NVivo categorized and created a database of all the articles reviewed in this study. It played a major role in identifying training and awareness. Although NVivo did not categorize training and awareness as one of the larger categories in the phishing articles. Other tools within NVivo (word tree, word search, word frequency, and explore diagram) clearly identified training and awareness as an essential category and component. While using NVivo, looking for mitigation strategies, the human factor aspect was discovered to be very significant. Furthermore, the human factor aspect was addressed by two components known as training and awareness. These categories define the basis for creating a systematic phishing matrix. Since

two main categories were defined, it makes it clearer to develop a 3D risk Matrix to define whether it would be more evident for a company to invest in more training or awareness or both. The Human View model helps to capture how the phishing training and awareness categories would be captured in this model to increase the performance of the human factor perspective during a phishing event. This led to a systematic model that has been developed to theoretically determine whether a company could use this model as a basis for a systematic phishing tool to mitigate phishing in an identified company.

This study contributes to the body of knowledge in Risk Management and Cyber-Systems Engineering by introducing a new systemic approach to mitigate phishing. Using methods from Human View, Risk management and System Engineering, the methodology in this study has produced a systematic model that will aid in the mitigation of phishing. This study has also produced an idea for a systematic tool that would be implemented in the security system of an organization that uses will use the model to help an organization mitigate phishing. Two main characteristics of phishing mitigation (training and awareness) is incorporated into the methodology of this study to produce the systematic model in this study.

CHAPTER 8

FUTURE RESEARCH

This study is only the beginning of future research into training and awareness and its effects and use into mitigating phishing. There are many promising future research prospects for this study. Mitigation of phishing is an intensive and constant process. There are multiple phishing techniques, and the attacks are persistent and varying every day.

The development and creation of a systematic phishing mitigation tool using this model that can systematically balance awareness and training to mitigate phishing is a favorable prospect. The tool would help organizations systematically decide which phishing mitigation techniques would be more protective against constant and persistent phishing attacks. The tool would help enhance an organization phishing defense and aid the organization in becoming more resilient.

Other future research projects:

- Creation of a systematic tool using this model that can systematically balance awareness and training to mitigate phishing.
- Developing Awareness in its use to systematically mitigate phishing. The development
- Developing Training in its use to systematically mitigate phishing.
- Configuring Training and Awareness and Training to work together to mitigate phishing.
- Development of Training and Awareness Programs can be costly. A study can focus on the cost of the development of either Training, Awareness or Awareness Training Programs.

REFERENCES

- Aldiabat, Khaldou M. (2018) The Mysterious Step In Grounded Theory Method, TQR Vol. 23
- Armerding, Taylor (2018, January 26) The 17 biggest data breaches of the 21st century. CSO.
Retrieved from: <https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html>
- Baily, Janet L., Parrish Jr., James L., Courtney, James F. (2018) A Personality Based Model for Determining Susceptibility to Phishing Attacks.
- Baker, Kevin, & Stewart, Andrew, & Pogue, Chris & Ramotar, Rudy (2008). Human Views. Extensions to the Department of Defense Architecture Framework. CAE Professional Services (Canada) Limited
- Benishti, Eyal (2017, September 26) Devastating phishing attacks dominate 2017. SCMedia.
Retrieved from: <https://www.scmagazineuk.com/devastating-phishing-attacks-dominate-2017/article/685213/>
- Berr, Jonathan (2017, May 16) "WannaCry" ransomware attack losses could reach \$4 billion. CBS News. Retrieved from: <https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/>
- Boulton, Clint (2017, April 19). Humans are (still) the weakest cybersecurity link. (CIO)
Retrieved From: <https://www.cio.com/article/3191088/security/humans-are-still-the-weakest-cybersecurity-link.html>
- Borsboom, Denny, Mellenbergh, Gideon J., Herden, Jaap van (2004). The Concept of Validity. Psychological Review, Vol 111, No. 4, 1061 - 1071
- Bruseberg, A. (2011). The Human View Handbook for MODAF, System Engineering & Assessment Ltd. On behalf of the MoD HFI DTC, First Issue,

- Buller, David B., Burgoon, Judee K. (2006, March 17) Interpersonal Deception Theory. Communication Theory, Volume 6, Issue 3, 1 August 1996, 203–242
- Buller, David B., Burgoon, Judee K. (2015, December) Interpersonal Deception Theory. Research Gate
- Buller D.B. & Burgoon, J.K. (1996). "Interpersonal deception theory". Communication Theory. 6 (3): 203–242. [doi:10.1111/j.1468-2885.1996.tb00127.x](https://doi.org/10.1111/j.1468-2885.1996.tb00127.x).
- Buller, D. B., Burgoon, J. K., & Burgeon, J. K. (1996). Interpersonal deception theory. [Article]. Communication Theory, 6(3), 203-242.
- Burton, Graeme (2016, December 12). Top-five biggest spear-phishing email frauds (V3) Retrieved from: <https://www.v3.co.uk/v3-uk/news/2479388/top-five-biggest-spear-phishing-email-frauds>
- Burton, Graeme (2016, December 12). Top-five biggest spear-phishing email frauds (V3) Retrieved from: <https://www.v3.co.uk/v3-uk/news/2479388/top-five-biggest-spear-phishing-email-frauds/page/3>
- Chaiken, S., & Trope, Y. (Eds.). (1999). Dual-process theories in social psychology. New York: The Guilford Press.
- Chaudhry, Junaid Ahsenali and Chaudhry, Shafique Ahmad and Rittenhouse, Robert G. (2016) Phishing Attacks and Defenses. International Journal of Security and Its Applications. Vol. 10, No. 1, pp.247-256
- Chyung, Seung Youn (Yonnie) Systematic and systemic approaches to reducing attrition rates in online higher education, American Journal of Distance Education, 15:3, 36-49, DOI: 10.1080/08923640109527092 Referenced from: <https://doi.org/10.1080/08923640109527092>

- Crow, Jonathan (2017, July). Must-Know Phishing Statistics 2017 (Barkly) Retrieved from:
<https://blog.barkly.com/phishing-statistics-2017>
- Crucial Research (2014, September). People's Role in Cyber Security: Academics' Perspective. White Paper.
- Davies, D., & Dodd, J. (2002). Qualitative research and the question of rigor. *Qualitative Health research*, 12(2), 279-289.
- Department of Defense Architecture Framework Working Group, (2004) DoD Architecture Framework Version 1.0 Deskbook, Department of Defense, Washington, DC, February
- Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes*. Orlando, FL: Harcourt, Brace, & Janovich. Brace, & Janovich.
- England, Rupert (2017, March). Human Factors for System Engineers. INCOSEUK Z12 Issue 1.0
- Frauenstein, Edwin D. and Flowerday, Stephen V. (2016). Social Network Phishing: Becoming Habituated to Clicks and Ignorant to Threats? Department of Information Systems University of Fort Hare East London, South Africa
- Golafshani, Nahid (2003). Understanding Reliability and Validity in Qualitative Research. *TQR*, Volume 8 | Number 4 Article 6, 5
- Godman, Jeff (2016, January 25) University of Virginia Breached by Phishing Attack Retrieved from: <https://www.esecurityplanet.com/network-security/university-of-virginia-breached-by-phishing-attack.html>
- Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet. *Group Decision and Negotiation*, 13(2), 149-172.

- Griffin, E. (2006). Interpersonal deception theory of David Buller & Judee Burgoon. *Communication: A first look at communication theory* (pp. 97-109): McGraw-Hill.
- Hackett, Robert (2017, July 13) Beware of These Top 10 Phishing Emails. Would You Fall for Them? Fortune Retrieved From: <http://fortune.com/2017/07/13/email-security-phishing/>
- Handley, H. A. H. (2019). *The Human Viewpoint for System Architectures*. Springer International Publishing, Switzerland.
- Handley, H. & Smillie, R. (2008). Architecture Framework Human View: The NATO Approach. *System Engineering* 11(2), 156-164
- Handley, Holly A. H. (2010). Human Factors Engineering [Power point Slides]
- Handley, Holly A. H., PhD. PE & Houston, Nancy P., PhD. (2010) NATO Human View Architecture and Human Networks. Pacific Science & Engineering Group, NATO Allied Command Transformation.
- H. Handley, T. Sorber, and J. Dunaway (2006) Maritime headquarters with maritime operations center, concept based assessment, Human Systems Performance Assessment Capability Final Report, Pacific Science & Engineering Group, San Diego, CA
- Handley, Holly A. H., PhD, PE & Tolk, Andres, PhD (2011). A Human View Model for Socio-Technical Interactions. MODSIM Conference, October 13, 2011
- Herzberg, Amir and Gbara, Ahmad (2004, November) TrustBar: Protecting (even Naïve) Web Users from Spoofing and Phishing Attacks. Computer Science Department, Bar Ilan University
- Internet World Stats (2017, December 31) Usage and Population Statistics. Retrieved From: <https://www.internetworldstats.com/stats.htm>

- Iuga, Cristian, Nurse, Jason R. C. and Erola, Arnau (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences*, 1-20. DOI 10.1186/s13673-016-0065-2
- Jakobsson, Markus (2007). *The Human Factor in Phishing*. School of Informics, Indiana University at Bloomington.
- Johnson, B. R. (1997). Examining the validity structure of qualitative research. *Education*, 118(3), 282-292.
- Johnson, S. D. (1995, Spring). Will our research hold up under scrutiny? *Journal of Industrial Teacher Education*, 32(3), 3-6.
- Keizer, G. (2007, 12 18). Phishers pinch billions from consumer' pockets. Retrieved 2 25, 2008, from Computerworld UK:
www.computerworlduk.com/management/security/cybercrime/news-analysis/index
- Kelly, Rhea (2017, August 31) Phishing Attack Scams Canadian University for \$11.8 Million. Retrieved from: <https://campustechnology.com/articles/2017/08/31/phishing-attack-scams-canadian-university-for-11-8-million.aspx>
- Kinetz, Erika (2016, March 29) Mattel fought elusive cyber-thieves to get \$3M out of China (AP) Retrieved from: <https://apnews.com/f50ded283c41465d9bdfef393732ce1/mattel-fought-elusive-cyber-thieves-get-3m-out-china>
- Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Beverly Hills, CA: Sage.
- Litan, A. (2007). Phishing attacks escalate, morph and cause considerable damage.

Luo, Xin (Robert) & Zhang, Wei & Burd, Stephen & Seazzu, Alessandro (2012). Investigating phishing victimization with the Heuristic Systematic Model: A theoretical framework and an exploration. Anderson School of Management, University of New Mexico, 1924 Las Lomas NE, MSC05 3090, Albuquerque, NM 87131, USA University of Massachusetts Boston, USA

Mathews, Lee (2017, May 5). Phishing Scams Cost American Businesses Half A Billion Dollars A Year. (Forbes) Referenced from:
<https://www.forbes.com/sites/leemathews/2017/05/05/phishing-scams-cost-american-businesses-half-a-billion-dollars-a-year/#15c85bc33fa1>

Maxwell, J. A. (1992). Understanding and validity in qualitative research. Harvard Educational Review, 62(3), 279-300

Milletary, Jason (2005). Technical Trends in Phishing Attacks. CERT Coordination Center, 1-17

Mishra, Sushma and Harris, Mark A. (2006) Human Behavioral Aspects in Information Systems Security. Proceedings of the 5th Annual Security Conference

Muniandy, Lalitha and Muniandy, Dr. Balakrihnan. (2013, August). Phishing: Educating the Internet users – a practical approach using email screen shots. IOSR Journal of Research & Method in Education (IOSR-JRME) Vol. 2, Issue 3, PP 33-41

Negil, Pritam Singh, Negi, Vineeta, Pandey, Akhilesh Chandra, (2011) Impact of Information Technology on Learning, Teaching and Human Resource Management in Educational Sector. International Journal of Computer Science, Volume 2, Issue 4, July 2011

Pagliery, Jose (2015, August 5) The inside story of the biggest hack in history (CNN) Retrieved from: <http://money.cnn.com/2015/08/05/technology/aramco-hack/index.html>

- Parker, D. (1998) *Fighting Computer Crime: A New Framework for Protecting Information*. New York, NY: John Wiley and Sons.
- Patton, M. Q. (2002). *Qualitative evaluation and research methods* (3rd ed.). Thousand Oaks, CA: Sage Publications, Inc.
- Paulsen, Celia and Coulson, Tony (2011). *Beyond Awareness: Using Business Intelligence to Create a Culture of Information Security*. *Communications of the IIMA*, Volume 11 | Issue 3 Article 4
- Petty, R. E., & Cacioppo, J. T. (1986). *Communication and persuasion: Central and peripheral routes to attitude change*. New York: Springer-Verlag.
- Petty, R. E., & Cacioppo, J. T. (1981). *Attitudes and persuasion: Classic and contemporary approaches*. Dubuque, IA: W. M. C. Brown.
- Petty, R. E., Barden, J., & Wheeler, S. C. (2009). *The Elaboration Likelihood Model of persuasion: Developing health promotions for sustained behavioral change*. In R. J. DiClemente, R. A. Crosby, & M. C. Kegler (Eds.), *Emerging theories in health promotion practice and research* (pp. 185-214). San Francisco, CA, US: Jossey-Bass.
- Petty, R.E., Brinol, Pablo (2012, January) *Handbook of theories of social psychology* (Vol.1), Chapter: *The Elaboration Likelihood Model.*, Publisher: London, England: Sage., Editors: P. A. M. Van Lange, A. Kruglanski, E. T. Higgins, pp.224-245
- Programming-Idioms (2023, January 31) Rust
Retrieved from: [Create a 3-dimensional array, in Rust \(programming-idioms.org\)](https://programming-idioms.org)
- Radar, Marc A. Rahman, Syed (Shawon) M. (2013). *Exploring Historical and Emerging Phishing Techniques and Mitigating the Associated Security Risks*. *International Journal of Network Security & Its Applications*, Vol 5, No. 4

Raymon, Alison DuNisco (2018, April 9) Ransomware reigns supreme in 2018, as phishing attacks continue to trick employees. Retrieved from:

<https://www.techrepublic.com/article/ransomware-reigns-supreme-in-2018-as-phishing-attacks-continue-to-trick-employees/>

Reuters Staff (2016, May 25) Austria's FACC, hit by cyber fraud, fires CEO. Technology News.

Retrieved from: <https://www.reuters.com/article/us-facc-ceo/austrias-facc-hit-by-cyber-fraud-fires-ceo-idUSKCN0YG0ZF>

Sargent, R. G. (2009). Verification and validation of simulation models. In Simulation Conference (WSC), Proceedings of the 2009 Winter (pp. 162–176). IEEE.

Sargent, R. G. (2009). Verification and validation of simulation models. In Proceedings of the 2009 Winter Simulation Conference, ed. M. D. Rossetti, R. R. Hill, B. Johansson, A. Dunkin, and R. G. Ingalls, 162-176. Piscataway, New Jersey: IEEE.

Sargent, R. G. (2015). An introductory tutorial on verification and validation of simulation models. In 2015 Winter Simulation Conference (WSC) (pp. 1729–1740).

<https://doi.org/10.1109/WSC.2015.7408291>

Seale, C. (1999). Quality in qualitative research. *Qualitative Inquiry*, 5(4), 465-478.

Schruben, L.W. (1980). Establishing the credibility of simulation models. *Simulation* 34 (3):

101-105. U. S. General Accounting Office, PEMD-88-3. 1987. DOD simulations: improved assessment procedures would increase the credibility of results.

Shaw, Soojah (2016, June 03). Top 5 biggest phishing scams (the Inquirer) Retrieved from:

<https://www.theinquirer.net/inquirer/feature/2460065/top-5-biggest-phishing-scams>

Spork, Lauren (2016, January 18). 8 of the Largest Data Breaches of All Time (OPSWAT)

Retrieved from: <https://www.opswat.com/blog/8-largest-data-breaches-all-time>

- Stanwick, Peter A. and Stanwick, Sarah D. (2014, November) A Security Breach at Target: A Different Type of BullsEye. *International Journal of Business and Social Science*. Vol. 5, No. 12 Pg. 63
- Stenbacka, C. (2001). Qualitative research requires quality concepts of its own. *Management Decision*, 39(7), 551-555
- Symantec (2018, May 1) Internet Security Threat Report | Symantec. Retrieved from: https://www.symantec.com/security_response/publications/monthlythreatreport.jsp
- Thompson, Nathan A. (2013). Reliability & Validity. *Assessment Systems*
- Ting Li Shan, Ganthan Narayana Samy, Bharanidharan Shanmugam, Sami Azam, Kheng Cher Yeo, Krishnan Kannoopatti (2016). Heuristic Systematic model based guidelines for Phishing victims. 13th International IEEE India Conference, 1-6.
- Tran, Phong (2017, June 26). Anthem Data Breach Will Cost Record Fine of \$115 Million. Retrieved from: <https://www.paubox.com/blog/anthem-data-breach-will-cost-115-million>
- Vishwanath, Arun, Herath, Tejaswini, Chen, Rui, Wang, Jingguo, Rao, H. Raghav (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems* 51 pg. 576 – 586.
- Vroom, C. and R. Von Solms (2004). Towards information security behavioral Compliance. *Computers & Security* 23: 191-198.
- World Economic Forum (2016). Understanding Systemic Cyber Risk. Global Agenda Council on Risk & Resilience. REF 181016
- Websense Security Labs. (2008). State of Internet Security. Retrieved From:http://www.websense.com/securitylabs/docs/WSL_Report_1H08_FINAL.pdf

Xu, Zhengchuan and Zhang, Wei (2012). Victimized by Phishing: A Heuristic-Systematic Perspective. *The Journal of Internet Banking and Commerce*, 1-15.

Zhang, Wei, Luo, Xin, Burd, Stephen D., and Seazzu, Alessandro F. (2012). How Could I Fall For That? Exploring Phishing Victimization with the Heuristic-Systematic Model. 2012 45th Hawaii International Conference on System Sciences.

GLOSSARY

Actors: This is anything that acts negatively on the system. This contains criminal hackers, cyber criminals, viruses, malware, worms, phishing, Trojans, and key loggers. This includes any software which is used by aggressor to their benefit.

Attacker: A Criminal hacker, cybercriminal, or any person that uses phishing to exploit or deceive people into giving up sensitive and private information of the organization or oneself or other individuals.

Cyber Security Risk: The chance that a system could get compromised or infected by an unwelcomed cyber intruder or cybercriminal.

Database: The physical system in which a structured set of sensitive data is stored.

Human: The individual that phishing mainly affects. This is the person that is targeted by phishing exploits and is truly considered the weakest link in the system. Not all humans are the same and therefore they may be considered the weakest link. Humans have many different characteristics, response, and feelings which can make them unpredictable.

Human Factor: The information related to characteristics, abilities, and limitations of humans that are applicable to a specific system design (Handley, 2010). Specifically, how human characteristics, abilities, and limitations will be viewed in a system geared towards security.

Trust is a characteristic that plays a big role in this system. Human View will be used to target specific aspects of Human Factor that will be relevant to this study.

Human Dynamics: The interaction between humans and technology (computer systems). This is the method of how humans interact with computer technology and how the interaction affects both systems. Specifically, how humans interact with computer security and technological security or cyber security.

Human System: This is the collection of human traits, personalities, skills, liabilities, and capabilities composed into a representative system. A representative system of 1 or more humans.

Models: A theoretical representation of a system that represents how an organizational unit will react to phishing attacks.

Risk: The chance or possibility that a negative action could occur on a system.

Risk Management: The process of prioritizing, recognizing, and evaluating threats to the system while trying to monitor and minimize the probability and impact to the system.

Risk of Phishing: The possibility or chance that an individual will be presented with a lure and get hooked by a cybercriminal.

Software & Defenses: This is software which is used by Stakeholder or Defender to protect the system being attacked. FireEye, McAfee Anti-virus and Anti-Malware, 2-Factor Authentication and Firewall's are a few examples of software. Defenses include software, physical systems, researchers, and defenders that protect the system.

Stakeholders: The mass majority that are victims of Phishing or affected by Phishing in a negative way. Businesses, Universities, Families, students, individuals, government, and businesspeople. Stakeholders are the victims of a phishing attack. Unlike actors, which are the attackers or Phishers (Cyber Criminals that use Phishing to commit cybercrimes).

System Components: The Physical components of the system such as the Internet, Intranet, Network, Cloud, Servers, Databases, Routers, and Desktops.

System: A set of interdependent components existing at different levels of complexity that is designed to work together for some common goal.

Systemic: A set or a group of components that are related to or represent a select system.

(Adjective) Relating to a system, especially as opposed to a particular part.

Systematic: A set or a group of components that work together to perform a specific task or have a specific goal.

(Adjective) Done or acting according to a fixed plan or system; methodical.

VITA

Curriculum Vitae for
Mark K. Guilford

EDUCATION

2023 Ph.D. Engineering Management & Systems Engineering, Old Dominion University
2011 M.E. Systems Engineering, Old Dominion University
2000 B.S. Mechanical Engineering, Minor in Chemistry, Old Dominion University

WORK EXPERIENCE

2019 – Present: Information Technologist III, Old Dominion University, Norfolk VA. 23529

- Virtual Desktop Support Engineer
- VMWare Horizon 7 VDI Administrator
- Virtual Software Support
- Lead Azure Virtual Desktop Infrastructure Administrator
- Dell Wyse Server Management
- Dell Wyse Thin Client Management
- Cloud Computing

2000 – 2019: Information Technologist II, Old Dominion University, Norfolk VA. 23529

- Research and evaluate server and large-scale operating system, hardware, and related application software.
- Research and testing of operating system upgrades and support modules to insure continued efficient operation of Enterprise Systems in the University Production Environment.
- Technical Lead in developing application deployment and support strategies for departmental and enterprise-wide applications.
- Testing and Evaluation of Emerging hardware and software technologies for possible implementation in the University computing structure.
- Windows / UNIX (Solaris and AIX) / MAC / Linux Systems Administrator
- Web Content Management and Mobile Technology Support and Configuration
- Virtual Software Support (VMWare, Hyper-V, Virtual Box, Parallels)
- Lead VMWare Horizon 7 VDI Administrator
- Software and Hardware Support, Configuration, Deployment, and Repair

Certificates

- Microsoft Certified Professional (MCP)
- Virginia Terrorism Awareness
- Responsible Conduct of Research (RCR)
- Azure Fundamentals
- VMware Horizon Fundamentals
- Cybersecurity Awareness: Phishing and Whaling