Social engineering cyberattacks can be considered a kind of psychological attack that attempts to persuade an individual (i.e., victim) to act as intended by an attacker. These types of attacks exploit weaknesses in human interactions and behavioral/cultural constructs and occur in many forms that will be discussed further later. The effectiveness of current security technologies has made social engineering attacks the go to gateway to exploiting cyber systems. Most research in social engineering has mostly focused on understanding and/or detecting the attacks from a technological perspective, however there is currently no systematic understanding of the psychological components of these attacks which perhaps explains why these attacks are roughly eighty percent effective.

In order to further understand this, we must acknowledge and treat social engineering cyberattacks as a particular kind of psychological attack. If we look at this with this new perspective, it lays a foundation that could be used as a precedent for many others to follow. This approach could later pave the way for designing effective defenses against these attacks and making sure that these attacks are built based on psychologically valid assumptions. This could potentially lower the effectiveness rate of social engineering attacks by understanding why these attacks work so often and later, using this information to counter and protect ourselves.

Analyzation of Social Engineers

Before discussing psychological attack vectors, we should also take moment to look at how social engineers study people. This often means that these professional social engineers are more like actors and actresses versus the classic 'computer nerd'. They understand and are well acquainted to studying body language, voice control, and group dynamics. Social engineering depends on the victim's logical thinking toward the information given by the cybercriminal and how well the victim can be persuaded. The victim's actions after receiving the information are determined by a psychological trigger. Triggers are psychological principles that exhibit power to influence or persuade people. Gragg (2002) extracted seven psychological triggers: strong affect, overloading, reciprocation, deceptive relationships, diffusion of responsibility, authority, and integrity and consistency. Strong affect applies when the cybercriminal makes a statement or provides information that triggers strong emotions. If the victim is feeling a strong sense of surprise, anticipation, or anger, then the victim will be less likely to think through the arguments that are being presented or develop a counter argument (Gragg, 2002). Often these social engineers focus on developing a trustworthy identity to later manipulate this to get what they want. These attackers combine the target's personal information, the context, and their goals. This includes a potential engineer to act and impersonate a member of your IT team or a bank representative, a new coworker etc. Often, doing this requires dedication and time, which will further enforce the credibility of the relationship.

Examples of credible behaviors include: Knowing your name, knowing what department you work in or interact with, basic knowledge of your technology usage, knowledge of personal and/or professional relationships to impersonate mutual friends or colleagues, incorporating environmental sound clips to enforce life-like situations (Abouzeid, 2019). One can see that a social engineer will gather as much information as they can about your life and behavior. This is commonly known as Open-Source Intelligence which according to United States public law is produced from publicly available information and is collected, analyzed, and disseminated in a timely manner to an appropriate audience. These social engineers will create a database of information that is specific to the victim. This can be thought of as a game of connect the dots in which each dot represents some sort of information about your life (Abouzeid, 2019).

After the social engineer collects this database of information they will focus on psychological influences. As humans we naturally pay attention to key details when someone first interacts with us. Based on our first interaction with someone new we can sense if we can trust this person or not. In doing so, we might ask ourselves some basic questions. These include whether it makes sense for this person to reach out to me, whether this person behaves in a trustworthy manner, or whether this person has any authority (Abouzeid, 2019). These characteristics like consistency, commitment, and obligation is what social engineers focus on for the sake of making sure their target is more susceptible to manipulation. This can be a trial-and-error type of process in which the engineer needs to portray confidence in each of the characteristic they choose. Lastly, these attackers focus on building rapport with a target. This includes a successful utilization of factors: Validation, Asking questions, Time constraints, and Ego suspension (Abouzeid 2019). These types of factors help build this idea of a false relationship by creating a sense of comfort that humans naturally are attracted to. This could include a threat actor potentially employing sympathy as their subtle attack by requiring help from the target.

Another common method used by social engineers is exploitation. This is where a social engineer exploits a person's natural tendency to avoid doing something wrong or getting in trouble. If an attacker can make an employee feel that he or she caused a problem or performed a task incorrectly, then the employee may become open to suggestion and thereby agree to compromise a policy or standard in order to correct the perceived error, which then leads to a breakdown in information security protocols (Chubb 1). Some countermeasures for combating this is to conduct a data classification assessment to make sure each employee has access to things they need access too, and to make sure you can identify which employees are prime candidates for these attacks due to the access they hold to sensitive information. On top of this, psychological tests could be performed to make sure your employees can handle all types of scenarios that might be thrown at them.

Another psychological mechanism social engineers use is distraction in persuasion and manipulation. People typically have a limited range of attention in sight, hearing and thought. Distraction facilitates persuasion mainly by disrupting the counter-argue process and increasing the effort to communication. It is effective both online and on the scene. Distraction may force the target to exert high effort so that to hear and understand the persuasive message. Experiments show that moderate distraction does facilitate persuasion, and moderate distraction produces more persuasion than strong distraction because targets are less inclined to suspect the persuasion is intended. The present distraction increases participants' yielding to propaganda by inhibiting counter arguing. Online advertises that frequently disrupt people's web surfing actually do have a persuasive effect even when people do not actively attend to them. ''Although consumers maintain illusory beliefs that they can tune out such ads, the ads have substantial persuasive and subtle distracting effects" (Sagarin 20). Distracted persons who have a low propensity to counter argue will be the least resistant to persuasion. Distraction is often used in malicious manipulation attacks. The thought process regarding security will be inhibited and disrupted if the target's focus is transferred to elsewhere.

In addition to this social engineers also use source credibility and the fact that users will obey to authority in certain persuasion attempts. People have a tendency to comply with authoritative figures automatically. In most cultures, especially the collectivist culture, people are told that to believe who are authoritative, expert and familiar, since these characteristics signify the credibility, trustworthiness and low-risk. For individuals low in need for cognition, when the message source was assumed to be relatively honest, persuasion are less dependent on message scrutiny. Experiments on obedience to authority show that, authority is so powerful that our independent thinking and rational behavior are often suppressed. Even the symbols of authority can trigger the individual's compliance. For instance, in the experiment conducted by study (C. K. Hofling "An experimental study in nurse physician relationships") , the hospital nurses were ordered by an unknown physician (who stands for expert and authority) to administer patients an obvious overdose drug. Although almost all the nurses and nursing students in the control group claimed they would not to obey, in the experimental group, all 22 nurses but one obeyed without a delay despite the order was given by the phone, until they were intercepted on their way to the patients. This explains why the symbols that reflect the authority, expert and credibility, such as uniform, badge, lingo and insider terminology, are frequently used in social engineering attacks. Study also shows that authority is effective to convince targets that the phishing URLs in emails are secure.

Lastly, we must propose a conceptual model which can provide an integrative and structural perspective to describe how the attacks work in terms of entities. There are three core entities in which include, effect mechanism, human vulnerability, and attack method. These are identified to help the understanding of how these attacks start up. A common psychological fact is that similarity invites liking,

whereas dissimilarity leads to dislike. The more someone's attitudes are similar to our own, the more we will like the person. On the contrary, we tend to decrease liking when getting to know someone and discovering the person is actually dissimilar. Thus, it may be less effective that a social engineer (attacker) attempts to over-persuade the targets in a manner obviously against their inclination or thought (Wang 11897). This is how an attacker will use psychological play in order to relate to the victim and trick them into believing things that are not true.

Now that we understand the human cognition behind the social engineering attacks, we can further deep dive into four distinct psychological attack vectors. The four distinct attack vectors that have been defined thanks to Lively's paper titled, "Psychological Based Social Engineering" are as follows: Careless Attack Vector, Comfort Zone Attack Vector, Helpful Attack Vector, Fear Attack Vector. Since we have categorized these attacks into four distinct subcategories, we can help create a Defense in Depth Strategy that can effectively defend against them later.

Careless Attack Vector

The first vector named, the Careless Attack Vector, is made "exploitable due to the indifference of implementing, using, or enforcing proper defensive countermeasures. It is often the first phase of a more complex overall attack. The attack escalates as the attacker's knowledge expands about the target. Reconnaissance is often seen in this vector" (Lively 2003). This definition of a carless attack vector help give way into common techniques used by social engineers that lead to real world attacks. Some examples of this include dumpster diving, and password theft. Dumpster diving is the act of taking trash from commercial dumpsters outside of office buildings. This helps the attacker build a rapport, as mentioned earlier, to gain intelligence on an individual or organization which they can later exploit. Password theft is as its name suggests, a common careless vector where passwords are written down and left out in the open. This could be a sticky note on a monitor to a note hidden in a drawer, both of which are obvious security risks. This deals with psychological factors as well, as this vulnerability is very prolific due to the innate sense of security many users feel in their office space. This false sense of security is actually the very foundation for the next group of attacks (Lively 2003).

Comfort Zone Attack Vector

The next vector mentioned was called the Comfort Zone Attack Vector. This is where exploits often occur due to the fact that the user is in an environment, they feel comfortable in, therefore, leaving them to have a lower level of threat perception. A comfort zone could be anything from a user's corner

office to a lunch break room. In order to really gain access to this attack vector, it usually requires exploiting one of more of the other attack vectors. There are many examples of this including but not limited to, impersonation, shoulder surfing, direct approach, physical security, and insider threat. Impersonation is a common attack in which hackers impersonate everything from janitors to fellow co-workers from a victim's own IT staff. The attacker will use this to try to persuade the victim into following orders, to achieve the end goal. Shoulder surfing is the act of looking over a user's shoulder to observe the entries to the keyboard as the username and password are being typed. A direct approach, otherwise known as theft, is self-explanatory. The attacker will study the victims' habits, find them outside their workplace where they feel comfortable, and 'direct approach' them and take something personal like a wallet, purse or ID. Physical Security is self-explanatory as well as it includes a physical security of a structural building. For example, designated smoking areas within organizations. Due to the difficulty in securing these areas, they provide an easy point of physical entry into an otherwise secure facility (Lively, 2003). Lastly, an insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors, or business associates, who have inside information concerning the organization's security practices, data and computer systems.

Helpful Attack Vector

The next attack vector is called the helpful attack vector, which is used on the premise that people will generally try to be helpful, even if they do not know whom they are helping. Both examples for this attack vector are direct approaches, including piggybacking and impersonation again. Piggybacking refers to when a person tags along with another person who is authorized to gain entry into a restricted area or pass a certain checkpoint. It can be either electronic or physical. Impersonation could entail an attacker calling a number they might have gotten from dumpster diving earlier, and impersonating an employee, and trying to pressure and use their psychological tactics to get information or change passwords etc.

Fear Attack Vector

Lastly, is the fear attack vector which is an attack that is based on attacking the victim in such a way that the user provides the attacker with the information or access needed due to putting the user in a state of anxiety, pressure, stress, and fear. Here it is more evident that psychological factors are used, but in a way not seen before. There are many examples of this that all revolve around impersonation, including conformity, time frame, and importance. Conformity is a situation in which the attacker puts the user in the uncomfortable position of being the only user to not help them out as the others have in the

past. Time frame is an attack that uses a fictitious deadline to obtain user compliance from a Helpdesk Operator (Lively, 2003). Importance is a technique employing impersonation in which the attacker pretends to be someone important or someone who is acting on behalf of someone important.

Conclusion - Psychology

Social engineering attacks consist of four phases: information gathering, development of relationship, exploitation, and execution. The exploitation phase includes techniques that can be either human-based or computer-based. Social engineering depends on motivational and psychological triggers to be successful. Motivators that motivate cybercriminals to conduct 6 social engineering techniques include money, ego, entertainment, cause, entrance into social groups, status, revenge, external pressure, and wannabe. Psychological triggers that trigger victims to give away information or access to cybercriminals include strong affect, overloading, reciprocation, deceptive relationships, diffusion of responsibility, authority, and integrity and consistency. When a cybercriminal gains trust of the victim, the victim is very likely to give the information or access requested by the cybercriminal. Even though there are human-based and computer-based techniques, most of the techniques rely on the trust factor. By having a good relationship with the victim, a cybercriminal can be more successful using the following techniques: shoulder-surfing, tailgating, eavesdropping, watering hole, phishing, and vishing. Everyone has different personality traits causing everyone to react differently when presented with information from a cybercriminal. Social engineering is an attack vector that is going to be commonly used in years to come. With information and data reliant on technology, every organization needs to be prepared in the event of a cyberattack no matter how big or small. Every organization should have a policy and defense in place to combat cyberattacks like social engineering. Social engineering can have devastating impacts on a global scale. As seen with NotPetya and WannaCry, social engineering can disrupt economies or disable a nation's critical infrastructure. The number one reason why social engineering is effective and can cause massive damage is humans due to the lack of cybersecurity awareness training. By making individuals aware of social engineering attacks and tactics, individuals can prevent massive damage to organizations or nations.