

Decomposing the Social Engineering Threat: A behavioral science perspective

By Tohru Watanabe – ISSA member, Minnesota, USA chapter

The purpose of this article is to provide a behavioral, cultural, and structural view of the social engineering threat.

Many articles present social engineering as an emerging and current threat, and most authors have concluded with similar recommendations for mitigating the risk of the social engineering threat. Compared to technology-specific vulnerabilities, the scientific basis of exploiting behavioral patterns in humans is not very well understood by many information security professionals. Sure, people often present anecdotal evidence and hypothetical scenarios, but the majority of published articles are not backed by empirical studies of behavioral traits.¹ Technology vulnerabilities are often based on weaknesses in implementation of logic or poor exception handling routines that lead to an exploitable attack vector. Since the output of hardware or software technology is repeatable and reproducible given the same input variables and conditions, exploit code can be generated and distributed for use against similar hardware devices or software applications. The purpose of this article is to provide a behavioral, cultural, and structural view of the social engineering threat.

So what is social engineering?

Social engineering is the exploitation of basic behavioral and cultural constructs to achieve an objective. By its definition, social engineering includes both intentional and non-intentional acts of coercion. For example, parents apply the basic constructs of social engineering when coercing their children to eat a healthy diet or when a foreign call center employee identifies himself as “Joe” in an attempt to build rapport with an American caller. Social engineering is neither a human

weakness that must be patched nor a thought process easily brought into conscious decision making processes.

The social engineering threat is a concern to both individuals and organizations because successful exploitation enables an attacker to circumvent technical and administrative controls. Technology implementations, in general, operate as designed and do not stand to reason against a user, barring directed application-level attacks, to dump information at will. Although social engineering attacks alone may not realistically be an effective means for an attacker to attain the “keys to the kingdom,” when combined with weaknesses in technology controls, social engineering can provide the right leverage to gain deep access into organizational information systems.

Andrew Jaquith posits the importance of relevant metrics in information security.² Without good measures, it is difficult to quantify the cost of a well-executed social engineering attack and benefit of interventions to mitigate risk of threat. Although there are several threat risk management models available for public consumption, the information security industry has not standardized on any specific methodology. Similarly, although there have been directed efforts to empirically study behavioral traits as relating to susceptibility to social engineering attacks by practitioners,^{3 4 5} the academic and theoretical basis, based on empirical studies to develop-

1 M. Workman, “Gaining access with social engineering: An empirical study of the threat,” *Information Systems Security*, 16 (2007), pp. 315 – 331.

2 A. Jaquith, *Security metrics: Replacing fear, uncertainty, and doubt*, (Upper Saddle River, NJ: Addison-Wesley, 2007).

3 M. Workman, “Gaining access with social engineering: An empirical study of the threat,” *Information Systems Security*, 16 (2007), pp. 315 – 331

4 E. Shaw, K.G. Ruby, and J.M. Post, “The insider threat to information systems: The psychology of the dangerous insider,” *Security Awareness Bulletin*, 2 (98).

5 M. Rogers, “Psychology and computer crime,” retrieved from <http://homes.cerias.purdue.edu/~mkr>.

Social engineering is neither a human weakness that must be patched nor a thought process easily brought into conscious decision making processes.

ment of a common practices statement, are still absent aside from a per-organization basis.

Past articles on social engineering

The *ISSA Journal* has published three articles in about social engineering dating back to mid-2003. In the November 2003 issue of the *ISSA Journal*, John Bumgarner⁶ classified social engineers as internal, external, and trusted, and described four attack vectors: ego attack, sympathy attack, intimidation attack, and technical attack. Bumgarner concluded with four recommendations: establishment of a security policy, creation of security awareness program, establishment of a policy and procedure education program, and feedback of program effectiveness through testing and evaluation.

In October of 2005, Mathieu Gorge,⁷ a consultant and security auditor based in Ireland, took one step further to include two different but similar classifications of factors, the first being conformity, situational, personal persuasion, co-operation, and involvement, in addition to Rusch's⁸ four factors: authority, scarcity, linking, and similarity. Gorge's proposition described these behavioral factors as weaknesses and proposed a back-to-basics approach to security, the application of the CIA triad, promotion of education and awareness training, and staff training to create a feedback mechanism for suspected suspicious behaviors.

Dan Timko⁹ published the third article on social engineering in January 2008 where he reiterated the importance and criticality of social engineering threats to organizations. Timko built on Rusch's article by citing Robert Cialdini's¹⁰ work in social psychology of persuasion as human weaknesses and attack vectors for social engineering threats. Timko's recommendations for defending against social engineering attacks included a back-to-basics approach, similar to that proposed by Gorge, to security to include defense-in-depth, creation and maintenance of a security policy, user education, and reiterated consideration for technical defense as an example of a layered security approach.

The common theme that underlies recommendations posited by Bumgarner, Gorge, and Timko is the importance of

security awareness and education programs and a back-to-basics approach to information security. Although training and education are important and security practitioners espouse the value of training, the 2008 CSI Computer Crime & Security Survey¹¹ reports 53% of respondent organizations allocated 5% or less of IT budgets to security and 42% indicated that less than 1% of security budgets were allocated to training. As an example, an organization with a \$10 million dollar IT budget allocated \$500,000 to security and only \$5,000 or 0.05% of total IT budget to security awareness and education. Based on the results, organizations are not budgeting for sufficient funds to reach desired audiences to reiterate an important point about security. Based on survey results, one could argue that recommendations to provide security awareness and education programs have been and will continue to be ineffective at achieving the goal of raising awareness for security issues. Reasons for low budget allocation could be because the value of training programs is difficult to quantify and social engineering attacks do not receive sufficient visibility by IT and business executives. Although continued recommendations for security and awareness programs resonate with information security professionals, it is unlikely that woefully-underfunded awareness training and education programs will make any impact resulting in greater budgets. Instead, the author believes in a need to take a different approach to managing the risks associated with social engineering and insider threats.

Review of persuasion-based tactics

Robert B. Cialdini, a Regents Professor of Psychology at ASU, and perhaps the most widely cited author on the psychology of persuasion, defines six "weapons of influence." The list of six persuasion tactics includes reciprocity, commitment and consistency, social proof, liking, authority, and scarcity. An example of reciprocity includes the distribution of free gifts in return for a charitable donation. The most dangerous type of reciprocity is "reciprocal concessions" whereby as the initial request is denied, a less obtrusive alternative is proposed for consideration. Reciprocity in an unstructured attack is less effective than when used in a structured attack. The impact of reciprocity in a social engineering attack increases with the level of trust and rapport.

Commitment and consistency are also strong motivators that keep people in line. Commitment and consistency are often applied during sales meetings and parental discussions with children. For example, a car salesperson might ask the buyer to commit to closing a deal if certain conditions are met. If the buyer agrees with the salesman, the persuasion technique of commitment has been established and the salesperson will push the prospect towards consistent compliance with previous commitments. A hypothetical application of commitment and consistency in a social engineering attack include securing a commitment for assistance and influenc-

6 J. Bumgarner, "A hacker will be with you shortly: Social engineering 101," *ISSA Journal*, (Nov. 2003).

7 M. Gorge, "Social engineering: What you need to know to be able to foil attacks," *ISSA Journal* (Oct. 2005).

8 J. J. Rusch (n.d.), "The 'social engineering' of internet fraud," Retrieved from http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm#s3.

9 D. Timko, "The social engineering threat," *ISSA Journal* (Jan. 2008).

10 R. B. Cialdini, *Influence: The Psychology of Persuasion*, (New York: Quill, 1993).

11 R. Richardson, "CSI computer crime and security survey," (2008), Retrieved from <http://www.gocsi.com>.

ing compliance to the commitment when making subsequent requests.

A common persuasion technique used on a daily basis is the use of “best practices.” Best practices, without considerations for fit and relevance, are often accepted solely on the basis of social proof. Although best practices may be relevant, applicable, and timely given appropriate conditions, accepting best practices without considerations for fit is consistent with groupthink as an example of social proof. A hypothetical attack situation, similar to attack scenarios for use of commitment and consistency, is the use of social proof to minimize resistance to a questionable act by establishing a history and acceptability of what should be a dubious and questionable request for information or action.

Use of authority is a simple persuasion technique that affects people on a daily basis. The application of authority in social engineering tests legitimate against illegitimate authority figures in coercing desired action. For example, people generally look for direction from their bosses, thought leaders, or consultants. Leader-member relationships are based on identified role prototypes and identities. Therefore, the attacker will assume the role of a leader or a figure of authority to drive compliance with directives.

The general tendency to help people we like is a common part of our daily lives whether the attraction be based on physical, similar background, experience, or beliefs. Similarly, people may have a desire to fit in and be liked by others. It is no wonder that sales and marketing professionals often attempt to identify common grounds of interest, experiences, and pay compliments as conversation openers in hopes of establishing favorable rapport. Although liking alone does not yield compliance, it helps to increase the persuasiveness of an attacker when combined with any of the five other weapons of influence.

Scarcity is also a commonly exploited trait whereby a limit, be it time or quantity, creates a sense of urgency towards action. Scarcity is often used on infomercials with the visible placement of a timer or quantity limits. Similarly, certain brands realize benefits by limiting production of products in an effort maintain favorable prices. Similar to liking, scarcity alone may not be a compelling attack vector. However, when combined with other weapons of influence, the introduction of time limits helps to drive action by reiterating a sense of urgency.

There are other behavioral attributes that describe behavior. Festinger’s theory of cognitive dissonance suggests that when a person is confronted with contradictory information that creates internal tension, the person will change her beliefs or behavior to reduce this tension.¹² There are also common behavioral biases such as confirmation bias and the drive towards cognitive closure. One study found that waiters are better able to remember the total bill for open tabs than paid

tabs.¹³ An astute social engineer will combine multiple behavior traits and biases to increase her chances of success.

Each set of behavioral attributes do not serve, in itself, as motivators for action. Behavioral science research does not attempt to describe and infer future causal relationships between cause and effect. So, scarcity, by itself, is not likely an effective social engineering tactic. However, an astute social engineer will be capable of executing a structured attack by combining tactics to influence the environment towards a favorable outcome. As an example, an attack scenario involving telephone communication might be made more effective by creating a sense of authority and liking in favor of the attacker. The attacker may first establish authority by introducing himself as an executive. The attacker may also involve additional parties to act as his subordinates in an effort to reiterate his authority status as well as to establish social proof of legitimacy of authority. The attacker may further apply liking by relating to the target to build rapport.

It is also important to consider external influences such as structure and culture on the target. External influences may or may not be attributes that the attacker can directly influence. As an example, if the target is influenced in a high power distance culture¹⁴ or has a strong desire to be liked, these factors will also influence susceptibility towards a certain attack vectors. A victim with an internal locus of control may be driven to take action without consulting peers or their superior. Similar to how an external attacker may employ dumpster diving as a means to gather peripheral information about the target organization, an astute social engineer will make attempts to gather peripheral information such as names and titles, hobbies, and technical aptitude to structure an effective social engineering attacks. Thus, identifying as an executive who is not technically savvy may result in lower barriers to simple coercion.

Aspects of organizational culture

Social engineering threat has been described as a human factors weakness. Humans, by nature, are not susceptible to *weapons of influence*-based social engineering threats. Similar to a PC with only a basic operating system installed where the absence of additional applications or server services limits the usefulness of the PC but also the susceptibility to vulnerabilities, humans operating without the boundaries of cultural norms and constraints are not subject to behavior patterns and prototypes imposed by geographic, political, organizational, and other cultural identities. However, when organization-specific cultural dimensions such as low power distance and value placed on individualistic achievement creates a work environment high in intra- and inter-group competition, attackers can tailor an attack strategy

13 M. Hunt, *The story of psychology*, (Anchor Press, 2007).

14 “A low power distance culture is one in which the hierarchy is low and decision-making is shared. A high power distance culture is one in which the hierarchy is considered very important and bosses are not disagreed with lightly.” Don Rutherford, “Who’s in charge? Cultural value differences: the concept of Power Distance,” <http://www.entrepreneur.com/tradejournals/article/129814158.html>.

12 Wikipedia - “Cognitive Dissonance,” retrieved from http://en.wikipedia.org/wiki/Cognitive_dissonance.

to specific behavioral patterns driven by cultural constructs towards desired objectives. For example, a hypercompetitive culture that breeds one-upmanship can lack intra- and inter-group coordination and overall policy compliance resulting in heightened sensitivity to threats based on scarcity and liking. Conversely, an environment that is risk averse that values tradition may suffer from bandwagon effect and be more susceptible to social engineering attacks based on commitment and consistency, social proof, and authority.

Since current security budgets only allocate minimal funds to security training and awareness programs, these tactical approaches can not address the inherent difficulty of managing security for a large user base. Instead, organizations should consider strategic interventions tied to each organization's unique culture. Given that culture helps to define morals, values, and other shared belief systems that serve as primary drivers for individual and group behavior, we should consider social engineering threats as a cultural phenomenon. When classifying social engineering threats as a cultural phenomenon, risk mitigation becomes a strategic issue and interventions have to occur at the cultural layer where an organizational intervention is led from the top down with senior executive support and helps to define *how things are done* between and within each department, division, or countries. This approach requires an assessment and understanding of the values and beliefs unique to each organization and further assessment of organizational structure to determine weaknesses in alignment between how people describe their work with the way people actually perform their work.¹⁵ And since organizational culture is a strategic business concern and closely associated with unique organizational strengths, cultural interventions may gain greater visibility to senior executives responsible strategic business planning.

Effects of globalization

Technological advances and globalization have affected both the industrial era and post-industrial digital era of American society. As business thought leaders had begun to shift low-value manufacturing processes to lower-wage and lower-cost nations in the mid 1900s, a similar trend has begun to affect knowledge workers. Low value and non-core operations have been outsourced to lower-cost countries in an effort to help contain costs. And since knowledge work transcends national or geographic boundaries, industrialized nations such as China, India, and Eastern European countries have begun to develop the intellectual capital of its citizens. In the near future, high-value knowledge workers may soon join the ranks of many organizations as the *virtual organization* begins to take shape. Although virtual organizations offer organizations the ability to attract and retain talent, there will be a greater need for cross-cultural training for existing workforce as well as those joining the workforce.

As with any systemic change, organizations will be exposed to greater risk of social engineering threats during the initial phases of operational and cultural integration. Similar to how M&A integrations create operational, cultural, and structural discontinuities that increase exposure to risks as people struggle to acclimate and assimilate into new organizational structure and cultures, globalization and cross-cultural integration results in similar discontinuities that increase overall exposure to social engineering threats.

Conclusion

The behavioral aspect of social engineering is an area less familiar to technologists and information security professionals than technical aspects. The multi-disciplinary nature of information security requires a multi-disciplinary approach to assessment, analysis, and management of risks of information systems. Past articles on social engineering have focused on tactical solutions to risk mitigation primarily through implementation a layered security model, establishment and enforcement of security policies and procedures, and implementation of security awareness and education programs. However, social engineering threat is a behavioral issue that is more nebulous than logic-driven technical threats. As the bidirectional influence of information security has shifted from a vertical focus to cross traditional business functions such as risk, legal, finance, and human resources, the emerging social engineering threat requires inclusion of behavioral, cultural, and structural components to construct a relevant and applicable threat mitigation strategy.

About the Author

Tohru Watanabe, CISSP, works as a solutions consultant for a privately held information security firm where he works with organizations to define, develop, and integrate information protection and compliance solutions. Tohru holds a Bachelors in business administration and is working to complete a Masters in organizational psychology. He may be reached at tohruw@gmail.com.



¹⁵ C. Argyris, "Effective Intervention Activity," in Joan V. Gallos (Eds.), *Organization Development: A Jossey-Bass reader* (pp. 158 – 184), (San Francisco, CA: Jossey-Bass, 2006).