Stephen Giorgi

CYSE 495

Dr. Saltuk B. Karahan

8/2/2024

Effects of Social Engineering in Cyber Incidents: The Role of Human Factors in Organizational Cybersecurity

Introduction

Cybersecurity threats abound in the digital era of today and have profound impacts on companies. Among these threats, social engineering has become especially destructive since it uses human psychology instead of technological weaknesses. Supported by cases from recent cyber incidents, this essay investigates the degree to which human variables affect the cybersecurity of an organization. Analyzing academic studies and practical cases make clear that recognizing and reducing social engineering attacks depends on human elements.

Fundamentals of Social Engineering

Social engineering is the process of guiding people into revealing private information or engaging in behaviors endangering security. These kinds of attacks penetrate beyond technological protections by using human emotions including trust, curiosity, and dread. Common strategies include phishing, pretexting, baiting, and tailgating, each of which uses different psychological triggers (Mitnick & Simon, 2011).

The most often used technique of social engineering, phishing is sending false messages seeming to come from a trusted source. Many times, these communications cause receivers to

share private information or download dangerous programs. Creating a fabricated scenario to entice a victim to disclose information or execute an action is known as pretexting, another form of social engineering. The act of baiting involves the use of deceptive promises to arouse the curiosity or greed of a victim, thereby causing them to download malware or compromise their credentials. Piggybacking, sometimes known as tailgating, is the practice of a threat actor following an authorized person into a restricted area (Grange, 2002).

Human Factors' Part in Cybersecurity

Attacks in social engineering depend much on human elements. The human element still stands as the weakest link in the security chain regardless of technical developments. An organization's sensitivity to social engineering is significantly influenced by the awareness, training, and behavior of its staff.

Training and Awareness

Employee education and training is among the best strategies available to fight social engineering. Companies with thorough cybersecurity training initiatives see less successful social engineering efforts. By enabling staff members to identify and react properly to suspicious behavior, training serves to lower the possibility of effective breaches (Parsons et al., 2014).

For instance, a lack of staff training contributed in some measure to the 2013 Target data breach, among the most serious in history. Attackers used a phishing email to trick a third-party HVAC contractor into exposing credentials, therefore gaining access to Target's network. The hack exposed 40 million credit and debit card records, underscoring the vital necessity of staff awareness and training in cybersecurity (Riley, Elgin, Lawrence, & Matlack, 2014).

Training needs to be constant and adaptable in order to accommodate new threats. Programs for static training soon become obsolete as attackers learn new, novel approaches. Gamification and simulated attacks are among interactive and interesting training tools that have shown higher success in maintaining high degrees of awareness and preparation among staff members (Jansson & von Solms, 2013).

Behavior and Psychological Aspects

Social engineering mostly depends on psychological elements and human behavior. Attackers manipulate others by using their emotions and cognitive biases. Phishing attempts frequently make use of the authority principle, which holds that individuals often follow leaders. Emails supposedly from top executives are more likely to get responses than those from unidentified senders (Alseadoon, Chan, Foo, & Gonzales Nieto, 2012).

Another often-used method is the scarcity principle, whereby people act quickly out of fear of missing out. Claiming that a limited-time offer or essential security update needs immediate action, attackers may instill urgency in their targets and cause them to click on dangerous links or disclose sensitive information without thinking (Workman, 2007).

Another instance of how human behavior could potentially be used is the 2017 Equifax hack. Attackers gained access to a web portal comprised of private data by means of social engineering. Primarily from human error and neglect to deploy an established software patch, the hack revealed the personal information of 147 million people. This event emphasizes the need to include human elements in cybersecurity policies (Mcmillan & Knutson, 2017).

Organizational Culture

The sensitivity to social engineering attacks also depends much on organizational culture. The likelihood of successful assaults can be greatly lowered in a society that gives security first priority, promotes awareness, and supports reporting of suspicious activity. On the other hand, a society that minimizes or ignores the need of security might foster an atmosphere in which social engineering finds great flourishment (Hadnagy & Fincher, 2015).

Social engineering attacks may go unreported and unattended in companies when staff members fear consequences for reporting possible security incidents. Crucially, we should encourage a culture of openness and support whereby staff members feel free to document suspicious behavior without worrying about repercussions (Ashenden & Sasse, 2013).

Practical Social Engineering Case Studies

Several well-publicized cyberattacks show the terrible impact of social engineering and the significance of human elements in cybersecurity.

2020 Twitter Bitcoin Scam

Targeting Twitter staff members in July 2020, a coordinated social engineering effort obtained access to internal tools and compromised well-known accounts including those of Elon Musk, Bill Gates, and Barack Obama. The Bitcoin scam was promoted by the perpetrators through tweets, which resulted in losses exceeding $100,000. This instance emphasizes how attackers may use human weaknesses—such as poor training and sensitivity to manipulation—to carry out advanced attacks (Newman, 2020).

The breach happened because the attackers fooled Twitter staff members into granting access to internal systems via social engineering. This case emphasizes the importance of strong access restrictions and staff training to identify and handle attempts at social engineering. This underscores the significance of restricting access to sensitive systems to only those who have a legitimate need (Matherly, 2020).

The 2011 RSA SecurID Breach

Leading cybersecurity company RSA became the victim of a social engineering attack in 2011. Targeting staff members with phishing emails disguised as recruitment offers. Once opened, the emails loaded malware that let the attackers get onto RSA's network and pilfer data linked to their SecurID authentication tokens. Many companies that rely on RSA's security technologies suffered this hack, demonstrating the broad impact of effective social engineering (Gallagher, 2011).

The attack emphasizes the complexity of social engineering campaigns and the need for thorough security policies outside of technological protections. It emphasizes the importance of a multi-layered security strategy including strong access restrictions, staff training, and ongoing observation of odd activity (Grimes, 2011).

The 2014 Sony Pictures hack

Still another noteworthy illustration of the consequences of social engineering is the 2014 Sony Pictures breach. Attackers gained access to Sony's network by means of phishing emails, therefore disclosing a great volume of private emails, staff data, and unreleased films. For Sony, the hack significantly damaged its reputation as well as finances (Perlroth, 2014).
This incident serves as an illustration of the potential for social engineering to serve as an impetus for more extensive and detrimental intrusions. It underlines the significance of companies to use thorough security policies covering technology as well as human vulnerabilities. It also emphasizes the need of resilience and incident response strategy in lessening the effects of successful attacks (Sanger & Perlroth, 2014).

Scholarly Perspectives on Human Factors

Studies confirm how important human elements are to cybersecurity. More efficient training programs and security policies can be derived from knowledge of how people view and react to security challenges (Bada, Sasse, & Nurse, 2019).

Essential is a multidisciplinary approach to cybersecurity including ideas from behavioral science, sociology, and psychology. For instance, knowing the psychological triggers that expose people to social engineering allows for more effective training programs to be designed. Research indicates that under stress or time constraints people are more prone to fall for social engineering attempts; so, it is advisable to lower such situations to increase security (Parsons et al., 2014).

Developing a security-conscious culture inside companies is truly vital. This entails not only teaching but also creating an environment in which staff members feel accountable for and dedicated to cybersecurity. Modeling and reinforcement of responsible behavior depend critically on leadership, therefore security becomes a shared organizational priority (Hadnagy & Fincher, 2015).

Studies by Bada, Sasse, and Nurse underline the need for ongoing education and modification of cybersecurity training courses. Programs for static training soon become obsolete as attackers pick up new strategies. Maintaining high degrees of awareness and readiness rests on frequent updates and interactive training approaches including simulated attacks and real-time feedback (Bada, Sasse, & Nurse, 2019).

Reducing Social Engineering Risks

Given the substantial influence of human factors on social engineering, it is imperative that organizations implement a comprehensive cybersecurity strategy.

Effective strategies include:

- Regular, **interactive training courses** covering the most recent social engineering strategies and including useful exercises can help staff members identify and stop attacks (Bada, Sasse, & Nurse, 2019).

- Frequent **simulated phishing attempts** help to find shortcomings and evaluate the efficacy of training efforts. These drills also give staff members useful feedback, thus supporting security procedures (Jansson & von Solms, 2013).
- Establishing **clear standards and practices** for managing confidential information and reporting suspicious activity is vital to security. Should employees come across possible social engineering attempts, they should know who to call and what to do (Ashenden & Sasse, 2013).
- Reinforcement of **open communication** about security issues and recognition of staff members who exhibit effective security practices will help foster a culture of awareness and responsibility (Hadnagy & Fincher, 2015).
- **Strict access controls** to restrict the level of access to critical systems and ongoing monitoring for abnormal activity will help to identify and respond to social engineering attempts more precisely (Grimes, 2011).
- Reducing stress and time strain on staff members will help to lessen their vulnerability to social engineering attempts. Important elements of this approach are keeping reasonable workloads and encouraging **a good work-life balance** (Workman, 2007).
- Having a well-defined **incident response strategy** in place will enable companies to minimize the impact of instances of social engineering by reacting swiftly and effectively (Matherly, 2020).

Conclusion

The cybersecurity of an organization depends on human elements, especially concerning social engineering attacks. The human factor is still the most easily exploitable weakness. Cybersecurity measures' efficiency greatly depends on awareness, training, behavior, and company culture. Organizations can better defend themselves against the constantly shifting threat of social engineering by knowing and resolving these human factors.

Dealing with human elements in cybersecurity calls for both a holistic and flexible strategy. Companies have to make continuous investments in training, create a security-aware culture, adopt strong security policies, and constantly monitor and change to match novel threats. This helps them to improve their general cybersecurity posture and greatly lower their risk of social engineering attacks.

References

Alseadoon, I., Chan, T., Foo, E., & Gonzales Nieto, J. (2012). Who is more susceptible to phishing emails? A data analysis study. In *2012 International Conference on Security and Management*.

Ashenden, D., & Sasse, M. A. (2013). CISOs and organisational culture: Their own worst enemy? *Computers & Security*, 39, 396-405.

Bada, M., Sasse, M. A., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Gallagher, S. (2011). Lessons of the RSA breach. Retrieved from https://arstechnica.com/information-technology/2011/03/lessons-of-the-rsa-breach/

Granger, S. (2002). Social engineering fundamentals, Part I: Hacker tactics. *Security Focus*.

Grimes, R. (2011). RSA SecurID: The hack that shook the world. *InfoWorld*.

Hadnagy, C., & Fincher, M. (2015). *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails*. John Wiley & Sons.

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, 32(6), 584-593.

Matherly, M. (2020). The Twitter Hack: Lessons Learned from a Major Social Engineering Attack. *Cyber Security Review*.

McMillan, R., & Knutson, R. (2017). Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed. *The Wall Street Journal*.

Mitnick, K. D., & Simon, W. L. (2011). *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons.

Newman, L. H. (2020). The Twitter Hack Could Have Been Much Worse—and It's Still Bad. *Wired*.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165-176.

Perlroth, N. (2014). Sony Pictures Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm. *The New York Times*.

Riley, M., Elgin, B., Lawrence, D., & Matlack, C. (2014). Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It. *Bloomberg Businessweek*.

Sanger, D. E., & Perlroth, N. (2014). Obama Vows a Response to Sony Cyberattack, but Warns of Overreaction. *The New York Times*.

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security*, 16(6), 315-331.