# Social Engineering and the Value of Data: The Need of Specific Awareness Programs

Isabella Corradini[1,3](✉) and Enrico Nardelli[2,3]

[1] Themis Research Center, Rome, Italy
isabellacorradini@themiscrime.com
[2] Department of Mathematics, Univ. Roma Tor Vergata, Rome, Italy
nardelli@mat.uniroma2.it
[3] Link&Think Research Lab, Rome, Italy

**Abstract.** In the field of cybersecurity human factor is considered one of the most critical elements. Security experts know well the importance of people's security behaviors such as managing passwords, avoiding phishing attacks and similar. However, organizations still lack a strong cybersecurity culture to manage security risks related in particular to the human factor. In this paper we describe the results of a study involving 212 employees belonging to two companies operating in the service sector. Within a cybersecurity awareness project executed in each company, employees participated in workshop sessions and were asked to evaluate the credibility and the success probability of a list of the most common security risk scenarios based on social engineering techniques. Cyber-attacks based on these techniques are considered among the most successful because use psychological principles to manipulate people's perception and obtain valuable information. The comparison of results obtained in the two companies shows that awareness training programs pay off in terms of raising people's attention to cyber-risks.

**Keywords:** Human factors · Cybersecurity · Social engineering · Cyber hygiene · Awareness

## 1 Introduction

Cybersecurity is a hotly debated topic all over the world, and the protection of information is a priority for institutions, companies and individuals. A data breach can have a high financial impact on a company, considering that in the range of 1 million to 50 million records lost, breaches can cost companies between $40 million and $350 million respectively [1]. In addition, companies have also to consider other significant consequences for their business, such as the loss of intellectual property and reputational damage [2].

Cyber threats have been growing over the last few years and they are going to be based on the exploitation of new opportunities.

On the one hand, security international reports stress the impact of the old cyber threats, such as ransomware, phishing, spear phishing, data breaches (e.g. [3–5]). Moreover, they highlight the importance of human factor, since mail and phishing

T. Ahram and W. Karwowski (Eds.): AHFE 2019, AISC 960, pp. 59–65, 2020.
https://doi.org/10.1007/978-3-030-20488-4_6

represent the primary malware infection vector [3] while social engineering is a critical launchpad for email attacks [5].

On the other hand, new threats are made possible by the application of Internet of Things and Artificial Intelligence [6]; furthermore, these technologies can strengthen the existing threats, such as improving the frequency of phishing attacks.

Notwithstanding the fact that more and more innovative technical solutions are available on the market to provide protection to companies and institutions, the problem of cybersecurity is far from being solved.

The role of human factor in cybersecurity is a fundamental topic to gain a better defense against cyber-attacks. Many authors indeed stress the importance of adopting a holistic approach, given that cyber defense cannot be considered only from a technical perspective but requires also a human-social viewpoint (e.g. [7–9]).

This paper is focused on workers' perception of cyber-attacks based on social engineering (SE), which is a method using psychological principles to manipulate people's perception to gain their confidence and lead them to disclose sensitive information or to do something else (e.g. opening an e-mail attachment), for the benefits of those who use these strategies (e.g. [8, 10]). SE is a successful technique because it exploits human nature bypassing technological measures [11]. In fact, as reported in [10], «We, as human beings, are all vulnerable to being deceived because people can misplace their trust if manipulated in certain ways».

SE can be used for several purposes and by different actors, targeting people through information directly posted by Internet users. SE can be executed in different forms. *Phishing*, a massive distribution of emails to solicit personal information, and *spear phishing*, targeting victims individually, are a form of SE. Moreover, SE can exploit physical devices (*baiting*), for example an infected USB stick left unattended in order to be found and used by people, with the consequence of installing malware onto the computer. Finally, SE can be executed by phone (*vishing*) to trick people or by exploiting information collected during a *face to face conversation*. Even though the actual modalities of execution can cause different reactions in people [12], the focus of SE is the social interaction.

## 2 Methodology

The study has involved 212 employees belonging to companies operating in the service sector (94 in company X, and 118 in company Y). In each company, we have carried out a cybersecurity awareness project aimed at the building of security culture. We used an interactive approach to actively involve participants and discuss with them security problems, and how to manage them.

More specifically, within each project we gathered 3–4 groups belonging to the same company for a half-day workshop where we tackled some of the most common security risk scenarios related to human behavior (e.g. choosing secure password, using unsecure wi-fi services). We repeated this half-day workshop with different sets of groups until all involved employees had attended. There were in total 13 groups for company X and 16 for company Y, with an average of 7 per group.

In each workshop, group participants were presented with the list of considered security risk scenarios and were asked to assign a mark to the **credibility** of each of them (i.e., how plausible the scenario is) and to its **success probability**, using a scale from 1 (low) to 5 (high).

At the beginning of each workshop we explained, to all groups present, each of these security risk scenarios, by showing videos in the public domain or short excerpts from well-known movies depicting the specific scenario and by illustrating real life examples of them (e.g. actual phishing emails). Subsequently, groups split and each of them separately discussed the presented scenarios, in order to estimate its credibility and success probability in the light of their personal experience, both in business and in private life.

After each group internally discussed and provided a consensus evaluation on both the credibility and the success probability of the scenarios, we united all groups together and a representative from each of them declared their conclusion. Next, we conducted a discussion and a comparison among all participants in that workshop of the various conclusions. Finally, we trained participants on the best behavioral practices to manage the presented security risk scenarios.

Some of these security risk scenarios were based on social attacks and engineering techniques (e.g. phishing), still a relevant problem given that social attacks are very frequent and can compromise data, secrets, and credentials [4]. The security risk scenarios discussed in the paper are the following:

- Receiving emails asking for data or to perform some action (Phishing and spear phishing)
- Receiving a phone call asking for information (Vishing)
- USB dropped in obvious places to employees (USB baiting)
- Face to face conversation

Note that the first three above listed scenarios refer to situations that intrinsically constitute direct risk scenarios, in the sense that they directly lead to jeopardize valuable assets. On the other side the last scenario describes a situation where there is not an immediate danger but the consequences of careless behaviors may provide a social engineering attacker with the information on which to successfully carry out the above three scenarios.

## 3 Results and Discussion

We now report and discuss the main outcomes of our study related to the above listed scenarios, also in the light of the different situations existing in companies X and Y.

In Figs. 1 and 2 we compare credibility and success probability results obtained in each of the two companies. Reported numbers are, for each risk scenario, the average across all groups involved of the consensus evaluation provided by each group.

As you can see, the success probability has an average mark slightly lower than credibility in all scenarios apart from “Vishing” in both companies. This scenario refers to a kind of interaction where people are naturally aware of the risk of being unconsciously manipulated by astute people. Even without training or previous experience, it

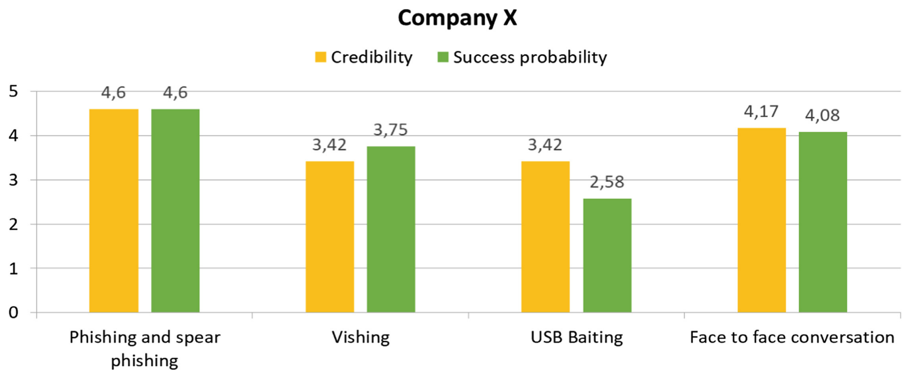

**Fig. 1** Results for Company X.

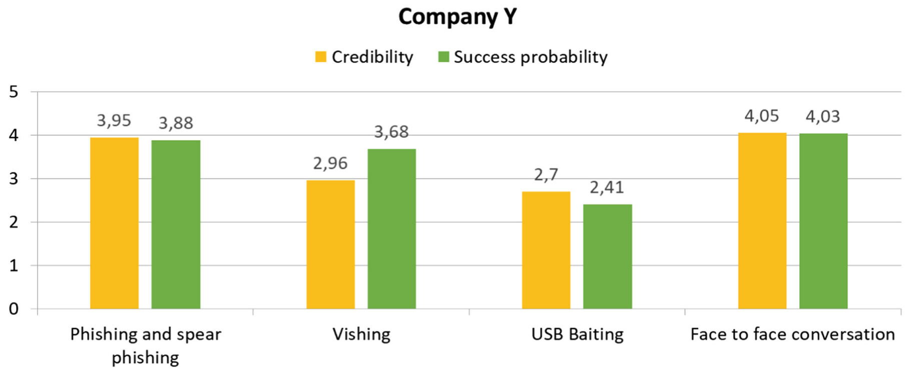

**Fig. 2.** Results for Company Y.

appears highly plausible to many that an able and empathic speaker can persuade others during a phone conversation.

Also, scenario “USB Baiting” has in both companies the lower mark, most probably because the specific situation where a memory stick is dropped in obvious places for employees is not a common happening. Moreover, it depends on the security policy adopted by organizations, given that the use of a USB stick could be prohibited.

Finally, scenario “Face to face conversation” has received the highest mark in one company and the second highest in the other one, which is reasonable given that face to face interactions are common in any kind of job and people are aware that these situations can be a very good opportunity to collect sensitive information.

In Figs. 3 and 4 we present the same data but arranged to compare the situation between the two companies.

Figure 3 presents credibility marks. You can see that, in general, employees in Company Y are less convinced by the plausibility of the presented risk scenario than in Company Y. This may be explained by the fact that company X has been working on a security culture project for a few years and their employees have been participating in

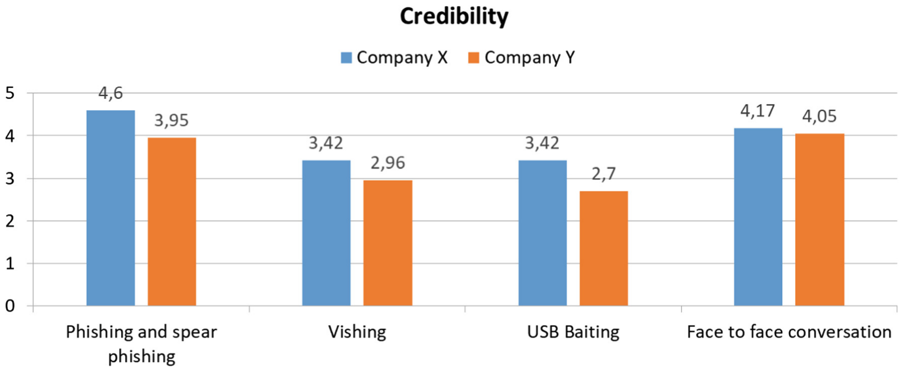

**Fig. 3.** Results for credibility.

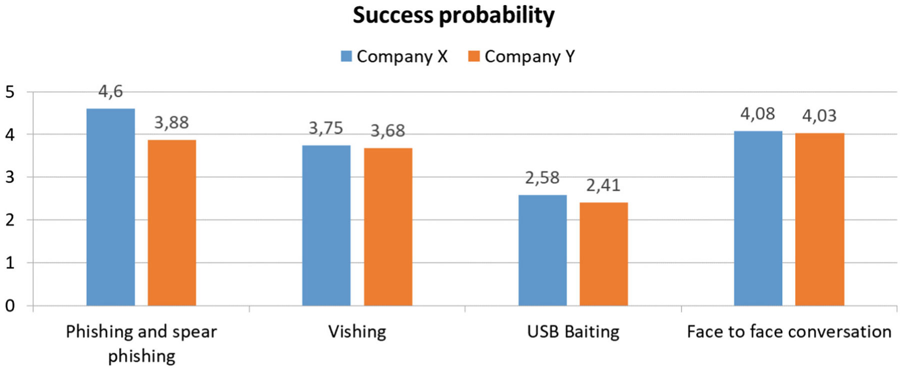

**Fig. 4.** Results for success probability.

specific training sessions, while company Y is at its first experience. Moreover, most participants of the company Y are not aware that an email can be sent to targeted individuals such as spear phishing, as well they were not aware of the psychological aspects of these security risks.

Moreover, as reported by periodical reports on the most common types of cybersecurity threats and cited above, phishing is actually the preferred vehicle for SE attacks.

For what regards the success probability, whose comparison of the marks between the two companies is shown in Fig. 4, there is no published data – to the best of authors' knowledge – about the actual success rate of the various threats. Annual cybersecurity reports usually provide indications on the top threats and whether a threat has become more or less common compared to the previous year [4, 5, 15]. This is understandable since data about failed attacks are usually not disclosed, while successful attacks cannot be usually hidden, for both their visible consequences and data protection laws (e.g. GDPR, General Data Protection Regulation) that requires companies to notify an authority data breaches when they occur.

Another important aspect concerns data protection related to the use of social media, which has been tackled during the discussion of the "face to face conversation" scenario, by relating what happens on social media to what happens in a person interaction. Discussing their behavior on social media, employees tend to minimize the risks associated with certain behaviors. From their words it emerged that while company's data protection is considered fundamental to business, their awareness of the value of personal information is not so high: an often repeated comment was "I have nothing to hide", while in reality each person has some information to protect. This dichotomy between attitude and behavior concerning privacy, which emerged with higher frequency in Company Y, is well-known in literature as the privacy paradox (e.g. [13, 14]).

## 4 Conclusions

It is clear that while digital technology is spreading everywhere security risks are growing and have to be seriously tackled. Criminals tend to exploit every vulnerability they can find; in addition, they will be able to exploit the advantages of Artificial Intelligence and Internet of Things.

If technical solutions are adequate to solve technical problems, they are inappropriate to manage security cyber threats related to human nature based on social engineering technique, e.g. phishing and spear phishing attacks. Hence, companies have to adopt a holistic approach, able to include and balance "People, Process and Technology" [15].

The lack of security awareness represents a vulnerability for every organization, making SE attacks easier to carry out. Hence, people using digital technologies have to be more and more aware of the risks involved with their use. In fact, even though cybersecurity is considered by governments and institutions as a priority, the actual behavior of people represents a challenge for any organization [16].

Therefore, building a cybersecurity culture in organizations [17, 18] is the best way to develop and reinforce effective security practices [19].

In this paper we have described the outcome of a study involving 212 employees, belonging to two companies in the service sector, who participated to a cybersecurity awareness project aimed at the building of a security culture within the organization. Employees had to evaluate the credibility and the success probability of each security risk scenario presented.

In one company the project was carried out for the first time, while in the other people had already participated in cybersecurity awareness training sessions. The analysis shows that people in the latter company have a better comprehension of risks related to the use of digital technologies.

Our study therefore provides support for the fact that without adding people to a company defense arsenal, effectiveness of its cybersecurity is weakened. This is in line with recommendations of recent cybersecurity reports [3, 5].

## References

1. Ponemon Institute: Cost of a Data Breach Study: Global Overview (2018). https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf
2. Allianz: Allianz Risk Barometer. Top Business Risks for (2018). https://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2018_EN.pdf
3. ENISA: Threat Landscape Report. 15 Top Cyberthreats and Trends (2018). https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
4. Verizon: Data Breach Investigation Report (2018). https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf
5. CISCO, Cisco 2018 Annual Security Report (2018). https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf
6. Brundage, M., Avin, S., Clark, J., et al.: The malicious use of artificial intelligence: forecasting, prevention, and mitigation (2018). https://arxiv.org/abs/1802.07228
7. Schultz, E.: The human factor in security. Comput. Secur. **24**(6), 425–426 (2005)
8. Corradini, I.: Human factors in hybrid threats: the need for an integrated view. In: Zorzino, G., et al. (eds.) Hybrid Cyberwarfare and The Evolution of Aerospace Power: Risks and Opportunities, pp. 85–96, CESMA (2017)
9. Ki-Aries, D., Faily, S.: Persona-centred information security awareness. Comput. Secur. **70**, 663–674 (2017)
10. Mitnick, K.D., Simon, W.L.: The Art of Deception: Controlling the Human Element of Security. Wiley, New York (2002)
11. Schneier, B.: Secrets and Lies. Wiley, New York (2000)
12. Bullée, J.W.H., Montoya, L., Pieters, W., Junger, M., Hartel, P.: On the anatomy of social engineering attacks: a literature-based dissection of successful attacks. J. Invest. Psychol. Offender Profiling **15**(1), 20–45 (2018)
13. Barnes, S.: A privacy paradox: social networking in the United States. First Monday, **11**(9) (2006). https://firstmonday.org/article/view/1394/1312_2
14. Barth, S., de Jong, M.D.T.: The privacy paradox: investigating discrepancies between expressed privacy concerns and actual online behavior – a systematic literature review. Telematics Inform. **34**(7), 1038–1058 (2017)
15. Schneier, B.: https://www.schneier.com/blog/archives/2013/01/people_process.html
16. De Bruijn, H., Janssen, M.: Building cybersecurity awareness: the need for evidence-based framing strategies. Gov. Inf. Q. **34**, 1–7 (2017)
17. Enisa: Cyber Security Culture in organizations (2018). https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations
18. Corradini, I., Nardelli, E.: Building organizational risk culture in cyber security: the role of human factors. In: AHFE 2018, pp. 193–202. Springer, Cham (2018)
19. Wilson, M., Hash, J.: Building an information technology security awareness and training program. NIST Special Publication 800-50, USA (2003)