# Chapter 3
# Redefining the Approach to Cybersecurity


**Abstract** One of the most critical issues in cybersecurity is represented by social engineering attacks. These threats have been known for years, but it is very difficult to handle them effectively, because they are strictly related to human nature. Social engineering is not just a phishing email; indeed, it is possible to distinguish several forms of attack which combine different elements, from human to social to physical and technological. According to a psychological point of view, social engineering is a powerful means of gaining information exploiting individuals' weaknesses. Moreover, due to the mechanisms of persuasion, widely studied in literature, it is easy to imagine how complicated the management of this threat is. Appropriate training of employees, especially of key roles of the company, can be an effective antidote to social engineering. Given the current scenario and the future perspective in cybersecurity, it is clear that the approach used to manage cybersecurity requires a radical change. Currently, the preferred cybersecurity strategy is still based on technological solutions, without brilliant results, since cyberthreats keep growing. Many are convinced that Artificial Intelligence (AI) will be an opportunity for managing cybersecurity; whether true or not, it is however evident that AI has also the power to generate new threats and to strengthen the existing ones. Therefore, we should be very prudent when technologies are presented as a miracle solution for cybersecurity problems. The starting point is that technology has to be deployed under full human control. Then, critical thinking is needed to develop alternatives to improve the current approach to cybersecurity. In short, we need to develop a multidisciplinary vision of cybersecurity, involving other disciplines and assuming different perspectives.

## 3.1 Social Engineering: The Real Trojan Horse of Cybersecurity

In the era of social media and digital communication, it is strange to admit that communication can become a threat: the more we are connected, the more we have to face dangers. One of the most critical issues in cybersecurity, based on communication techniques, is social engineering.



I. Corradini, *Building a Cybersecurity Culture in Organizations*,
Studies in Systems, Decision and Control 284,
https://doi.org/10.1007/978-3-030-43999-6_3

This concept seems to have been used for the first time in politics, and then migrated into cybersecurity (Hatfield 2017).

From a psychological viewpoint and in the context of cybersecurity, social engineering can be defined as a tactic which, using a persuasive communication, aims at gaining people's confidence in order to lead them to disclose sensitive information or to do something dangerous, e.g. to click a malicious link or to open an infected file.

If in this context social engineering has a negative meaning, we cannot say the same when applied to other fields. For example, a vendor frequently uses social engineering techniques to convince a potential buyer to acquire his products or services. A vendor needs effective communication abilities to appeal to individuals' emotions and persuade them. Hence, he uses empathy to understand clients' feelings. Also, empathizing with others in different life and work situations is a fundamental communication skill (Chap. 5).

The main element which characterizes social engineering is its power to manipulate people's perception by using different approaches. When communication is face-to-face, facial expressions and gestures are powerful means of persuasion. When the medium is digital technology, as in the case of phishing email, social engineering aims at generating a believable situation in order to capture people's attention.

Previously, phishing emails were easily identifiable, because of grammar errors or of the strange language used. Now, they are becoming more and more accurate with respect to contents and style; it is not therefore easy to recognize them, especially for inexperienced people, but even expert users can be confused by visual deception attacks (Dhamija et al. 2006). Currently, phishing represents a core attack method for all cybercrime (Europol 2019) and requires human interaction to succeed.

However, social engineering is not just a phishing email; we can distinguish several forms of attacks which may combine different aspects (Salahdine and Kaabouch 2019; Krombholz et al. 2015), i.e. human, physical, social and technical. In the following we describe some of them.

- Phishing: This is the most popular application of social engineering. It is the fraudulent practice of sending emails, usually appearing to come from a well-known source (e.g. an important organization) to steal sensitive information, like passwords, credit card numbers, etc.
- Spear phishing: It is a form of phishing tailored to the target recipient (individual or groups). Attackers study the behaviour of their targets and collect information to make the attack believable, in order to increase the likelihood of its success. When victims receive a spear phishing email, they think that the communication comes from a trusted source. For example, Business Email Compromise (BEC) is a fraud where the attacker impersonates an organization executive to lead an authorized employee in that organization to perform a wire transfer to an account controlled by the same attacker.
- Pretexting: Social engineering needs to achieve trust to be successful. For this purpose, it uses an appropriate scenario fabricated in order to convince a targeted victim. Pretexting consists, for example, of impersonating someone else, e.g. a police officer, or an insurance investigator.

- Tailgating: In this physical form of social engineering, someone gains access to a building or to a restricted area without proper authentication, but exploiting a convenient situation, for example, following another person entering the property.
- Whaling: In this form of phishing the main characteristic is the type of target, represented by senior executives, representative people of government agencies, politicians, and celebrities. Given the relevance of the target (big fish), the value of information is particularly attractive to cybercriminals. Like spear phishing, the scam email is tailor made, and appears to come from a business partner.
- Vishing: This is a phone scam which combines phishing and voice. Vishing can be considered the telephone equivalent of phishing. Here, given that the fraudulent action is over the phone, empathy and the ability of handling conversation are needed for the success of the attack.

We underline the multiplicity of the methods used in social engineering attacks, as well as the different levels of sophistication. For example, reverse social engineering (e.g. Irani et al. 2011) points to the active role of the victim: the attacker does not start the contact with her, but the victim herself is tricked and led to initiate the relationship with the attacker.

Apparently, social engineering techniques seem to be carried out spontaneously, especially when associated to the sending of massive amount of emails; there is always someone who falls for a phishing email.

Several phases define a social engineering attack (e.g. Mouton et al. 2016; Segovia et al. 2017); typically, it includes:

- target identification and information gathering;
- relationship development to gain the trust of the selected victim;
- execution, in order to exploit the trust achieved;
- exit, to avoid leaving proof and, at the same time, maintaining a good relationship with targets for future activities.

Whether or not it is happening through physical or technical means, the focus of social engineering is social interaction and manipulation. Understanding the mechanisms of persuasion is fundamental to handle phishing threat, since people tend to ignore the critical warning messages (Gupta et al. 2017), thus contributing to the success of the attack.

## 3.2 Persuasion in Social Engineering

Digital technologies and social media offer many opportunities to interact socially. Hence, a social engineer can interact with targeted people through social media platforms, and collect information directly posted by Internet users.

In investigating the psychological aspects of social engineering, we can say that this technique exploits both social and cognitive vulnerabilities (Corradini and

Nardelli 2020): if the social relationship can be -by its nature- a risk, the cognitive element[1] is represented by manipulation of people's perception.

In this sense, two forms of interaction can be identified for the manipulation, depending on how explicit the interaction is. When a victim gets in touch with the attacker (direct interaction), such in the case of phishing, spear phishing and vishing, email or telephone are the means which connect the two actors. In the indirect way, instead, manipulation works without starting an explicit relationship with victims. Posting false information on a website or on a social media, for example, can attract certain individuals or groups particularly interested in the published information. Here, the number of potential targets can be very high, even if false information is posted with the goal of capturing the attention of specific groups.

We know the effects of spreading fake news on the Internet and the difficulty of restoring proper communication. We also know how manipulation of information can alter people's perceptions and generate collective inadequate behaviour (Sect. 1.5). False and negative information on the financial market, for instance, could cause people's hysterical reactions, disrupt the economic balance and affect the financial relations among countries.

Threats based on social engineering have been known for years, but they continue to have high chances of success, because they are strictly connected to human nature. In short "[…] we, as human beings, are all vulnerable to being deceived because people can misplace their trust if manipulated in certain ways" (Mitnick and Simon 2002).

Indeed, investigating victimization in the case of phishing, we observe that individuals can have an active role in the success of social engineering attacks, given that for them it is usual to receive emails and phone calls, while it is difficult to judge messages in full detail to find markers of fraud (Jansen and Leukfeldt 2015).[2] Moreover, stress, pressure, and other factors can facilitate the lack of accurate control and ensure the success of the attack.

From a psychological point of view, it is interesting to explore how effective psychological principles of persuasion (Cialdini 1984, 2000) are. In this sense, understanding their function and promoting awareness on this subject should be included in cybersecurity education programmes.

In Table 3.1 we describe some principles characterizing social engineering attacks and some specific points of attention translated into simple questions.

The principles listed above work effectively because they are based on heuristic processes easily available to human minds (Sect. 2.3). They can count on the peripherical route of persuasion, which points to incidental cues, rather than to the strength

[1] In literature, social engineering is considered a form of cognitive hacking, that is "as gaining access to, or breaking into, a computer information system for the purpose of modifying certain behaviours of a human user in a way that violates the integrity of the overall user-information system" (Cybenko et al. 2004).

[2] The study consisted of an analysis of 600 phishing and malware incidents involving a Dutch bank, and focused on the behaviour of the customers victims of fraud. Despite the limitations of the study (regarding one bank), the authors underline how the combination of phishing (social engineering) and malware (technical skills) is becoming a more common method to commit fraud.

**Table 3.1** Persuasion principles and points of attention

| Persuasion principles | Description | Points of attention |
|---|---|---|
| Reciprocity | According to a social norm, individuals tend to return a favour: if someone gives something to others, they feel obliged to repay that debt | How selfless is the helper? |
| Commitment and consistency | People need to appear consistent in their behaviour. Hence, they act in line with their words or agreements, so as not to be perceived unreliable | Am I sensitive to people's judgment? |
| Social proof | People tend to do what the others do, especially in uncertain conditions | Do people behave in a certain way just for conformity? |
| Authority | People feel an obligation to obey figures of authority, even if they don't agree with them | Is the source reliable? |
| Liking | People tend to comply with requests made by those they like, because of physical attractiveness, familiarity and similarity | Is it really empathy? |
| Scarcity | People tend to consider things more valuable if less available. For example, finding offers available for a "limited time only", sales are encouraged | Do I really need it? |

Persuasion principles (Cialdini 1984, 2000) and points of attention in social engineering (Corradini 2017)

of the contents.[3] The power of persuasion is well-described in literature, especially in social psychology (e.g. Petty and Cacioppo 1986; Kruglanski and Thomson 1999).

The main factors of persuasion include:

- the communicator (*who*),
- the message content (*what*),
- the channel of communication (*how*),
- the audience (*whom*).

[3] According to literature, it is possible to distinguish two different methods of persuasion: the central route is characterized by the strength of the messages or of the arguments; to be effective, the person receiving the message must have a high motivation to listen to. Peripheral route, instead, do not require thinking carefully. For example, when we are distracted, we cannot be concentrated on the contents of a message, but we are attracted by superficial cues (depending on the context).

However, in investigating the persuasive process, we have to consider other many factors, such as: the characteristic of the source and its reliability; logical or emotional contents of the message and what they inspire; motivation and need of cognition; the flood of influence generated by the channels of communication.

It is evident that when factors are combined in a digital context (*where*), the space of influence is larger and more powerful (Corradini 2017). Digital technology has changed the nature of persuasion (Perloff 2014), increasing complexity and blurring the lines between three different concepts, such as information, influence and entertainment.

People are not often aware of the reliability of sources, and—unless they do a particular job—they do not bother to verify them. It is a fact that nobody is immune, to the point where even security experts can become victim of social engineering.[4]

Organizations have to consider this threat seriously, and to review training and awareness programmes to fight it (Aldawood and Skinner 2019): despite of their efforts, social engineering is still a significant problem for companies. Indeed, social engineering activity can be finalized to different targets with the purpose of stealing useful information. Specific positions can be targeted for this goal, for example executive assistants to the CEO, general managers, drivers, receptionists, the cleaning staff: according to their different roles, they handle sensitive information which needs to be protected.

Appropriate training combined with social engineering penetration testing can be a strong antidote to this persuasive form of communication; moreover, the points of attention identified in Table 3.1 are useful questions to invite people to reflect on the situation they experience, in order to ponder the different circumstances they have to face.

## 3.3 What Happens with Artificial Intelligence and Internet of Things?

As discussed in Chap. 1, the growth of Internet of Things (IoT) and Artificial Intelligence (AI) applications are defining a new technological environment, which produces advantages but also further security risks. Currently, many countries are more and more interested in deploying AI systems, to the point where the estimated business for 2030 is impressive.[5]

---

[4] See, for example, how Kane Gable, a 15-year-old, using social engineering, gained access to the personal and work accounts of some of America's most powerful spy chiefs.

The teenager persuaded call handlers at an internet giant that he was John Brennan, the then director of the CIA, to gain access to his computers and an FBI helpdesk that he was Mark Giuliano, then the agency's Deputy Director, to re-gain access to an intelligence database https://www.telegraph.co.uk/news/2018/01/19/british-15-year-old-gained-access-intelligence-operations-afghanistan/.

[5] According to McKinsey Global Institute AI has the potential to deliver additional global economic activity of around $13 trillion by 2030 https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy#part1.

It is evident that there is a strong reliance on automation; the application of AI in cybersecurity is accelerating: to fight against cyber-attacks, at least a third of Chief Information Security Officers (CISOs) have decided to adopt artificial intelligence (CISCO 2018). In addition, firms are more and more convinced that they need to implement AI systems to identity critical threats (Capgemini 2019).

It is more than likely that AI will re-design our lives, and that it will have a significant impact in a lot of fields. It is not very clear if this would have a positive or negative effect. Media and experts say that the growth of AI systems is going to improve our lives, because of the opportunities offered.

We always recommend great prudence when technology is presented as a miracle for our problems, before research clarifies benefits and risks. On the other hand, technology can be considered positively when human beings have its complete control.

Among recommendations on AI (Del Ponte 2018), it is recognized the need of discussing its societal risks, and the need of creating an ethical framework to regulate it, starting from the principle that this technology has to be developed under human control. In this sense, the Ethics Guidelines for Trustworthy AI by European Commission (2019) underlines the necessity of a full adherence of AI to humans' ethical principles and values (Sect. 1.1).

AI systems are developing rapidly, and the risk that their growth overcomes people's capacity of handling them is more than real. According to the approach of Machine Learning (ML), machines can "learn" without someone having to program them. And they learn rapidly, focusing on any data we, as humans, handle for our activities; so, if we search a certain product on different websites, we have to be aware that in the future similar products will be suggested to us.

It is obvious that humans cannot enter into competition with AI. The battle would be lost from the start. On the contrary, humans and machines have to work together respecting their own limits, because more and more in the future digital technologies will play an important role in our lives.

Hence, we have to exploit opportunities offered by the landscape of AI and, at the same time, we cannot ignore that AI increases relevant risks even in the workplace (Houghton and Green 2018), regarding health and safety, employee ethics, diversity and equality. One of the major risks is about discrimination: machine learning works on data, and there is no guarantee that this data is free from prejudice. Consequently, the algorithmic process of learning can build altered representations of reality on whose basis discriminatory answers are provided by the AI system.

Such an impact is significant when hiring people or promoting specific categories or genders for specific jobs; bias in predictive hiring tools is a relevant problem to be handled, since employers are more and more interested to use these predictive tools to reduce time and costs (Bogen and Rieke 2018).

In the meantime, precautionary measures are required when AI applications are proposed as the panacea for cybersecurity. They say that solutions based on AI will provide important support for the protection of organizations, ensuring effective security standards. AI will probably be able to identify new malware and cyberthreats, given its capacity to handle massive volume of data.

There are at least two considerations we should reflect on.

The first is that we are facing many threats not yet solved, despite using the most advanced technological solutions available on the market. Moreover, cyberthreats continue to evolve and improve, so every solution based on artificial intelligence needs to be constantly updated. Therefore, it is not clear why and how AI will be able to solve security problems without causing new ones.

The second issue is that, as with any innovation, everyone takes advantage. This means that criminals can also improve their "modus operandi" exploiting the scalable use of AI systems. We can assume an extension of the landscape of threats consisting of (Brundage et al. 2018)[6] a reinforcement of the existing menaces (e.g. expanding set of actors) and of the possibility of generating new ones.

From this point of view, we can say that social engineering techniques can be strengthened from AI systems. Indeed, since AI is able to mimic human voices realistically, a social engineer can create automated social engineering attacks, using recorded data and impersonating perfectly, even using the same style of language. No wonder that Facebook engineers have created a machine learning system named "MelNet" cloning the voice of Bill Gates,[7] and that a Canadian start-up introduced an AI system capable of synthesizing a person's voice from just a one-minute audio sample.[8]

In addition, the combination between AI and Internet of Things provides a powerful weapon for criminals. IoT devices make available a large amount of data, because their sensors are able to collect information about their environment. AI algorithms, on the other hand, can infer selected information from this data. Consequently, it is possible to produce accurate profiles of targeted people, as well as to identify further vulnerabilities.

Such a combination can also be useful for the implementation of social engineering attacks, where the ability of gathering information and profiling is essential for their success.

We are convinced that human beings are essential in cybersecurity, regardless of the wonderful technological solutions used. Who thinks that the employment of AI will completely replace human beings in the activity of protection has not yet understood the nature of the issue. Once again, the tendency is to underestimate the importance of human factors and of well-trained people, and to rely on AI completely. This conviction is the biggest threat to overcome.

Even if AI is able to recognize threats more quickly than humans, thanks to its ability to analyse a large amount of data, originality and human experience are quite difficult to replicate. This is especially true when it comes to tackling cyber-attacks:

---

[6] In this report the authors identify three representative domains: Besides digital security, and the problems of cyberattacks, they also consider the domain of physical security (e.g. the deployment of autonomous weapon systems) and the political security (the use of AI for propaganda and deception).

[7] https://www.theverge.com/2019/6/10/18659897/ai-voice-clone-bill-gates-facebook-melnet-speech-generation.

[8] "Lyrebird" is the system realized by the start-up, on the basis of deep learning models developed by the University of Montréal https://www.nextnature.net/2017/05/lyrebird-api-copies-human-voice/.

if AI solutions are based on rule sets, people have the opportunity of using abstract thought (Hadley 2019).

Finally, delegating cybersecurity to machines and replacing humans in control activities can certainly solve technical vulnerabilities, but if people and technology become ever more distant, other critical issues will have to be handled.

## 3.4 For a Holistic Vision of Cybersecurity

As discussed in the previous chapters, we have to get used to living in a more and more connected and digitized world, since this trend will continue in the years to come. Consequently, the amount of data available on the Internet will tend to rise, as well as the need to protect them.

Hence, it is realistic to think that the threat landscape will get worse.[9]

Individuals and organizations will be exposed to new security risks, and they will have to improve their capabilities to handle them. Indeed, criminals will continue to exploit any possible vulnerability, whether it is technological, physical or human.

Considering the current and the potential future situation of cybersecurity, a strong and effective approach to the issue becomes vital for everyone and, above all, for decision makers.

The first thing to do is to admit that, as it is, cybersecurity does not work. Like in a therapeutic relationship, recognizing the problem is fundamental to achieve positive outcomes.

Critical thinking is needed to develop alternatives to improve the current approach. We can start from the enhancement of what has been done so far, recognizing errors and weaknesses, and move on. It takes a change of mentality, involving both decision makers and those who have to deal with security problems. For example, within organizations, we should have the courage of breaking away from old patterns that consider security as a set of products or, worse, a check list to tick off.

Critical elements in the approach to cybersecurity cannot be ignored anymore, and we urgently need to redefine it.

Since the digital aspect is now an integral part of our lives, we should accept the idea of considering cybersecurity as a "public good" (Mulligan and Schneider 2011), like public health. In this sense, cybersecurity should be handled in the public interest, by developing a strong cooperation between public and private sector, as well as users' responsibility regarding their cybersecurity awareness (Taddeo 2019).

So, at least three issues are important in this vision.

[9] Just think of the COVID-19 pandemic which probably is going to change our future habits and way of working: increasing the dependence on digital tools exposes to the risk of cyberattacks (WEF 2020).

### 3.4.1 Excessive Focus on Technology

The first issue concerns the general approach to security, based mainly on a technocentric point of view. We confirm the importance of technological view to clarify how cyberthreats work and what technological solutions are needed, but this is not enough. It has been proved that technological solutions are not sufficiently developed to respond to all the threats.

We need to adopt a multidisciplinary vision of cybersecurity. Other disciplines—also far from technical approaches—are capable of giving different views. Clearly, these perspectives should be integrated with the technological approach, because we are strongly convinced that humans and technology have to work together.

Similarly, the study of the human factor in cybersecurity requires different contributions from social science fields, such as psychology, sociology, anthropology, and so on. To best understand cyberspace and all criminal activities developing in this huge area, it is not sufficient to be trained in mathematics and engineering related approaches (Patterson and Winston-Proctor 2019), but it is necessary the expertise of individuals with knowledge in behavioural sciences.

On the other hand, several international security reports over the years[10] have shown how the most advanced technological solutions are not capable of solving all cybersecurity problems. They represent only one of the means, not the only one.

There is a general overconfidence in emerging technologies as soon as they make their appearance, when instead they should not be seen as the magic bullet. Before relying on technologies completely, we should study their advantages and disadvantages.

On the contrary, it happens that technologies are immediately released on the market, while industry and media underline the pros of them. Unfortunately, the cons come after, when it is impossible to take a step back. Business is business, we know, and technological evolution must go on, but the basic question is: are we really willing to give up our ethical and social values for the benefits deriving from the use of technologies?

Differently from the past, we are now dealing with powerful technologies, but we are not sure that we will be able to control it, and this represents a serious problem for security too.

Other daily examples help us to understand how technology alone cannot offer a real solution to security. Besides a refined design, modern smartphones are becoming more and more equipped with highly advanced functions, such as sophisticated access to the device (fingerprint, facial recognition, etc.). Just pronouncing them, it seems that these technologies are able to keep hackers and criminals of all kinds away. However, being technologically advanced does not mean being protected from security risks. As security experts love repeating (and it is really true), an absolute security does not exist.

[10] See, for example, ENISA Threat Landscape Report (2019) and Verizon Data Breach Investigations Report (2017, 2018, 2019).

Nothing is impenetrable, considering that even a child can unintentionally overcome more or less sophisticated security protections.[11] Sometimes, people's false security perceptions are able to produce undesirable effects. Everyone knows the dramatic epilogue of the Titanic, marketed as unsinkable. Despite this assumption, things went differently, and unfortunately, consequences were tragic.

### *3.4.2 Physical Elements Are Neglected*

The second issue concerns underestimating the "physical" elements involved in cybersecurity. Behind an attack there are devices and human beings, not only Internet. For example, attacks can guarantee the access to national infrastructures, with the consequence of interrupting essential services, such as transport, energy and financial systems. Coordinated cyber-physical attacks on critical infrastructures can be devastating and produce severe damages (Xiang et al. 2017). The well-known cyberattack to Ukrainian power system in 2015[12] has shown that multiple approaches can be extremely effective, impacting remote assets both electronically and physically (Lee et al. 2016).

Then, thinking of Internet of Things, we know that this is made up of physical objects and connectivity; we already have evidence that the combination of the two elements can be critical for security.[13] We should not forget that even cities are implementing the adoption of smart technologies (smart cities), developing automation, remotely managed, and so on.

Looking at this scenario, we should realize that if the focus of cybersecurity remains anchored only to its cyber aspects, it is plausible to think that physical elements will be considered by cybercriminals as an attractive vulnerability to be exploited. It is no coincidence that criminal actions involve physical devices and that among criminal actions there are also theft and cards skimmer (Verizon 2018).[14] In

[11] See, for example, the news about a child who, at the age of 10, overcame his mother's i-Phone security block, consisting of the Face ID, the technology based on the recognition of the user's face https://www.wired.com/story/10-year-old-face-id-unlocks-mothers-iphone-x/. The episode is worrying, since if a child can unintentionally overcome security blocks, we can imagine what hackers can do.

[12] The Ukrainian power system cyberattack is the first publicly acknowledged incident to result in power outages. It left about 225,000 people without power for several hours.

[13] In 2016, a massive DDoS attack (distributed denial of service) hit the Internet. Important website platforms, like Twitter, Netflix, etc., took down. The company attacked was Dyn, that controls much of the internet's DNS infrastructure. The attack was realized through a specific malware (Mirai), which infected IoT devices (like DVR players, digital cameras), and accessing the devices using default password and usernames.

[14] The report refers to Payment Card Skinner, including all incidents in which a skimming device is physically implanted (tampering) on an asset that reads magnetic stripe data from a payment card.

addition, whether data is stored in a physical or digital form, physical access controls are required to prevent unauthorized access.

An effective approach to cybersecurity should involve actors and instruments coming from different security fields, together with people having a plurality of experiences in order to expand the breadth of analysis. On the other hand, analysing the new threats and the growing ability of criminals to exploit any vulnerability, it is evident that a traditional approach based on the separation of physical and cyber security is inadequate and should be overcome, since physical security regards the protection of personnel and IT infrastructures—hence hardware, software and data—from physical actions that could cause damages or loss to an organization.

Perhaps, speaking of Cyber-Physical-Security instead of just Cybsersecurity could be a more appropriated approach to understand and manage threats. Even though the term cybersecurity is more fashionable and appealing, we should not forget the relevance of physical elements involved.

### *3.4.3 Human Factors and Cybersecurity Culture*

The third issue—strictly related to the others—regards the importance of social and human aspects of cybersecurity, and the need of raising awareness. The building of Cybersecurity Culture is a must for any organization. In this sense, the popular triad "People, Technology and Process" developed by the security expert Schneier at the end of last century is still a valid reference to handle security.

Between the cyber and the physical dimension there are always human beings: whether it is a physical theft or a data breach, the illegal action is carried out by individuals, and the consequences inevitably involve them. Furthermore, people can also be the vector of criminal actions, such as in phishing and social engineering attacks, as discussed in this chapter.

In a new approach to cybersecurity, we should not see human factor as a problem, but as a part of the solution, since individuals are essential to the functioning of the socio-technical system (Zimmermann and Renaud 2019).

While everyone agrees that the human factor is fundamental, in practice this conviction does not find application as a global strategy, and when it happens, its management is not effective. We must admit that it is not a simple matter, and in designing cybersecurity awareness programmes we have to consider the need of taking care of cognitive, emotional and social aspects.

What is necessary is the construction of high-reliability-organizations (Winnefeld et al. 2015) based on interconnected and fundamental principles: integrity, depth of knowledge, procedural compliance, forceful backup, a questioning attitude, and formality in communication.

We often forget that organizations are made up of people, who must be prepared to recognize risks and respond to them, but they have to be put in the right condition

to do so. Hence, investing in people also means paying attention to their well-being, since effective Cybersecurity Culture requires a receptive and a healthy workplace (Sect. 4.4).

Finally, working on prevention is still the best strategy. This concept is too often forgotten in favour of emergency management. Cybersecurity incidents happen constantly and it appears more and more difficult to prevent them, to the point where many are convinced that the only thing we can do is to be prepared to manage crisis events. We are aware that there are real hurdles in managing cybersecurity, since it touches every business process and function, and changing user behaviour requires considerable effort.[15]

On the contrary, we strongly believe that preparing employees to secure behaviour can prevent many security problems. After all, prevention is better (and cheaper) than cure.

## References

Aldawood, H., Skinner, G.: Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. Future Internet, Review **11**(3), Art no. 73, (2019)

Bogen, M., Rieke, A.: Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias, Upturn (December 2018)

Brundage, M., Avin, S., Clark, J., et al.: The malicious use of artificial intelligence: forecasting, prevention, and mitigation (2018)

Capgemini Research Institute: Reinventing Cybersecurity with Artificial Intelligence. The New Frontier in Digital Security (2019)

Cialdini, R.B.: Influence. The Psychology of Persuasion. Quill William Morrow and Company, New York (1984)

Cialdini, R.B.: Influence: Science and Practice, 4th edn. Allyn and Bacon, Boston (2000)

Cybenko, G., Giani, A., Thompson, P.: Cognitive hacking. Adv. Comput. **60**, 36–73 (2004)

CISCO: Annual Cybersecurity News Report (2018). https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

Corradini, I.: Human factors in hybrid threats: the need of an integrated view. In: Hybrid Cyber Warfare and The Evolution of Aerospace Power: risks and opportunities, CESMA (2017)

Corradini, I., Nardelli, E.: Social engineering and the value of data: the need of specific awareness programs. In: Ahram, T., Karwowski, W. (eds.) Advances in Human Factors in Cybersecurity, AHFE 2019. Advances in Intelligent Systems and Computing, vol. 960. Springer, Cham (2020)

Del Ponte, L.: European Artificial Intelligence Leadership, the Path for an Integrated Vision. Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Brussels (2018)

Dhamija, R., Tygar, J.D., Hearst, M.A.: Why phishing works. In: Proceedings of the 2006 Conference on Human Factors in Computing Systems (CHI), Montreal, Quebec, Canada, pp. 581–590. ACM (2006)

ENISA: Threat Landscape Report 2018. 15 Cyberthreats and Trends (January 2019) https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

European Commission: Ethics Guidelines for Trustworthy AI (2019). https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[15] https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/why-senior-leaders-are-the-front-line-against-cyberattacks.

Europol: The Internet Organised Crime Threat Assessment (IOCTA) (2019)
Gupta, B., Arachchilage, N.A., Psannis, K.E.: Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommun. Syst., 1–21 (2017)
Hadley, J.: In the Age of AI, The Human Factor Still Matters For Cybersecurity, Forbes, March 27 (2019). https://www.forbes.com/sites/jameshadley/2019/03/27/in-the-age-of-ai-the-human-factor-still-matters-for-cybersecurity/#7a9774725cc5
Hatfield, J.M.: Social engineering in cybersecurity: the evolution of a concept. Comput. Secur. (2017)
Houghton, E., Green, M.: People Analytics: Driving Business Performance with People Data. Chartered Institute for Personnel Development (CIPD), Global research, report (June 2018). https://www.cipd.co.uk/Images/people-analytics-report_tcm18-43755.pdf
Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., Pu, C.: Reverse social engineering attacks in online social networks. In: Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 55–74 (2011)
Jansen, J., Leukfeldt, R.: How people help fraudsters steal their money: an analysis of 600 online banking fraud cases. In: Proceedings of the 5th Workshop on Socio- Technical Aspects in Security and Trust, pp. 25–31 (2015)
Krombholz, K., Hobel, H., Huber, M., Weippl, E.: Advanced social engineering attacks. J. Inf. Secur. Appl. **22**, 113–122 (2015)
Kruglanski, A.W., Thomson, E.P.: Persuasion by a single route: a view from the unimodal. Psychol. Inq. **10**, 83–109 (1999)
Lee, R.M., Assante, M.J., Conway, T.: Analysis of the Cyber Attack on the Ukrainian Power Grid. SANS Industrial Control Systems, Santa Monica, CA, USA (2016)
Mitnick, K.D., Simon, W.L.: The Art of Deception: Controlling the Human Element of Security. Wiley Publishing, Inc., Indianapolis, IN (2002)
Mouton, F., Leenen, L., Venter, H.S.: Social engineering attack examples, templates and scenarios. Comput. Secur. **59**, 186–209 (2016)
Mulligan, D.K., Schneider, F.B.: Doctrine for cybersecurity. Daedalus **140**(4), 70–92 (2011)
Patterson, W., Winston-Proctor, C.E.: Behavioural Cybersecurity: Application of Personality Psychology and Computer Science. CRC Press, Taylor & Francis (2019)
Perloff, R.M.: The Dynamics of Persuasion. Communication and Attitudes in the 21st Century, 5th edn. Routledge (2014)
Petty, R.E., Cacioppo, J.T.: The elaboration likelihood model of persuasion. In: Berkowitz, L. (ed.), Advanced in Experimental Social Psychology, vol. 19, pp. 123–205 (1986)
Salahdine, F., Kaabouch, N.: Social engineering attacks: a survey. Futur. Internet **11**(4), 89 (2019)
Segovia, L., Torres, F., Rosillo, M., Tapia, E., Albarado, F., Saltos, D.: Social engineering as an attack vector for ransomware. In: Proceedings of the Conference on Electrical Engineering and Information Communication Technology, Pucon, Chile, 18–20 October 2017, pp. 1–6 (2017)
Taddeo, M.: Is cybersecurity a public good? Mind. Mach. **29**(3), 349–354 (2019)
Verizon: Data Breach Investigations Report (DBIR) (2017). https://enterprise.verizon.com/resources/reports/2017_dbir.pdf
Verizon: Data Breach Investigations Report (DBIR) (2018). https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf
Verizon: Data Breach Investigations Report (DBIR) (2019). https://enterprise.verizon.com/resources/reports/dbir/
WEF: Why Cybersecurity Matters more than ever During the Coronavirus Pandemic (March 2020). https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/
Winnefeld, J., Kirckhoff, C., Upton, D.A.: Cybersecurity's human factor: lessons from the Pentagon. Harv. Bus. Rev., 87–95 (September 2015)
Xiang, Y., Wang, L., Liu, N.: Coordinated attacks on electric power systems in a cyber- physical environment. Electr. Power Syst. Res. **149**, 156–168 (2017)
Zimmermann, V., Renaud, K.: Moving from a "Human-as-Problem" to a "Human-as-Solution" cybersecurity mindset. Int. J. Hum. Comput. Stud. **131**, 169–187 (2019)