Volume XXII 2019
ISSUE no.1
MBNA Publishing House Constanta 2019

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Aspects of human weaknesses in cyber security

To cite this article: R. Moinescu, C. Răcuciu, D. Glăvan, N. F. Antonie, S. Eftimie, Scientific Bulletin of Naval Academy, Vol. XXII 2019, pg. 163-170.

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-19-I1-022

Aspects of Human Weaknesses in Cyber Security

Radu Moinescu, Ciprian Răcuciu, Dragoș Glăvan, Narcis-Florentin Antonie, Sergiu Eftimie

Military Technical Academy "Ferdinand I" – Systems Engineering for Defense and Security
radu.moinescu@gmail.com

Abstract. Along with the development of information technology in recent years, awareness about the security of computer systems is also increasing. Because the human factor is often guilty of the vulnerabilities to which an information system is exposed, this paper will research and evaluate disparate attack vectors which are being utilized today to successfully exploit human weaknesses. We will also try to create a mechanism to mitigate against these attack vectors.

1. State of affairs

The issue of cyber security also includes those attacks that are designed to exploit users' weaknesses and naivety. In some situations, people's behavior tends to differ from their normal behavior and take actions that they wouldn't normally do if they judge better. The human factor is often guilty of the vulnerabilities to which a system is exposed, in this case the security breaches. Apart from certain external circumstances such as blackmail, physical constraint etc., most cyber-attacks are performed using social engineering techniques.

Social engineering is any act of using the influence, manipulation, or lying, so that a person performs an action that may or may not be in its interest. These techniques of deception have been used in the history of mankind either for financial gains, access to power and espionage, but especially as war techniques for winning the battlefield against a stronger opponent or fortification. Since ancient exists story using Trojan horse the Greeks to enter the walled city of Troy and win the war, which had erupted after Paris, prince of Troy, were abducted Helen, wife of Menelaus, king of Sparta. We can also refer to Basarab I (~ 1310-1352), ruler of Wallachia, victorious in the Battle of Posada (November 9-12, 1330), against Charles Robert of Anjou, king of Hungary.

Social engineering can be divided into various types of attacks such as:

- pretexting;
- trapping;
- quid pro quo;
- phishing and its variations.

Pretexting attacks tend to appeal to the sense of urgency. When people feel pressured and have to perform a task at a given time, they can react irrationally. An example of exploiting this weakness in information security was the 2015 scandal, involving CIA director John O. Brennan. A hacker has managed to access his private e-mail account and evict a number of classified documents, among them the data of several US government officials. The hacker would have used a social engineering technique, calling for an emergency, to trick Verizon employees, to provide him with the personal information of the CIA chief. Thereafter, the hacker said he persuaded AOL to reset Brennan's account. [1]

Phishing is the most effective mechanism of social engineering. Verizon's 2018 report on data breach investigation, claims that 93% of social engineering attacks involved phishing. According to the same report, between 2017-2018, more than two-thirds of cyber-spying cases were phishing attacks. [2] This form of attack takes more and more forms, trying to trick users through techniques that include:

- link manipulation – users can be fooled by similar or misspelled links;
- link spoofing – the way a link is displayed could send the user to an alternate address;
- the use of the "@" symbol within a link does not always mean that it is an email address;
- the use of URL shortening services and link management platforms such as Bitly, TinyURL, 1URL, or Cli.gs to ensure linking to a malicious website;
- use of IP addresses instead of links;
- adding elements before legitimate links;
- sending pre-compiled pages in e-mails;
- sending seemingly legitimate attachments but containing malicious content.

To make a phishing e-mail to appear as legitimate as possible, spoofing the sender's details, it increases the chances of success of the attack. An example of using these techniques in a real attack can be found in the case of Hillary Clinton's campaign chief, John Podesta. On March 19, 2016, it was the target of a phishing attack. At first sight, the email seemed to be legitimate communication from Google that warned him that someone would use his password to connect to Google from Ukraine. The e-mail message prompting the recipient to immediately change his password contained a link created with Bitly that once clicked loaded a website similar to a Google login page but under the control of the attackers. In this way the attackers persuaded the victim to disclose his credentials. [3] The phishing attack involving Hillary Clinton's campaign chief was not complex and did not require sophisticated skills, he only exploited the human weakness associated with the sense of urgency. Loss of email account control for this category of people may sometimes have disastrous personal and professional implications, but it can also mean compromising your political career.

While it is natural to focus on threats from external actors, it is often forgotten that part of cyber-risk can also come from within the organization. Internal staff is a unique threat vector for any organization, given its privileged position in terms of physical and logical access to the organization's information system. In contrast to someone outside the organization, an insider has a better knowledge of the situation (*for example: knowledge of weaknesses*), more time available, fewer security measures to overcome, and legitimate privileges of access to secured areas, access to the information system, by virtue of the position it occupies in the organization. These factors, combined with the possibility that a person inside has to commit any type of malicious act, implicitly lead to an increase in the impact of any incident. (*Fig 1.1*)

The most prominent targets for quid pro quo attacks are unhappy employees (*they have not received a salary increase, have conflicts / do not reconcile with their boss, have lost their trust in the organization or something that has disliked*) or who are considered frustrated. Financial motivation is largely due to the employee's avidity, whether it is generated by aggressive motivational factors, which induce negative feelings and reactions about the position occupied within the organization. In this respect, the main factors determining the act of betrayal may be:

- the appearance of the impression of inequity;
- collective / hierarchical relationships;
- the individual status that gives a certain position in the organization;
- low salary / salary reduction;
- job insecurity;
- the influence of the job on personal life (free time vs. busy time).

However, internal risk can also be accidental, generated by some people's weaknesses such as curiosity. Under the impulse of this weakness, people often do not think about possible future effects, some notorious examples where USB flash drives caused significant damage are Conficker, Stuxnet, or Flame malware. To give an example, in 2006, as part of a security audit carried out within a bank, USB flash drives containing various Trojans, designed specifically for the audit activity, were placed in the parking lot, smoking areas and in recreation rooms. When the USB flash drives in question was introduced to an employee's workstation, the Trojan informed the auditor of this fact. Steve Stasiukonis, the founder of Secure Network Technologies Inc.'s information security consulting firm, has established that out of the 20 USB flash drives placed in various areas of the bank, 15 were found and connected to the workstations of the bank's staff over a three-day period. [4]

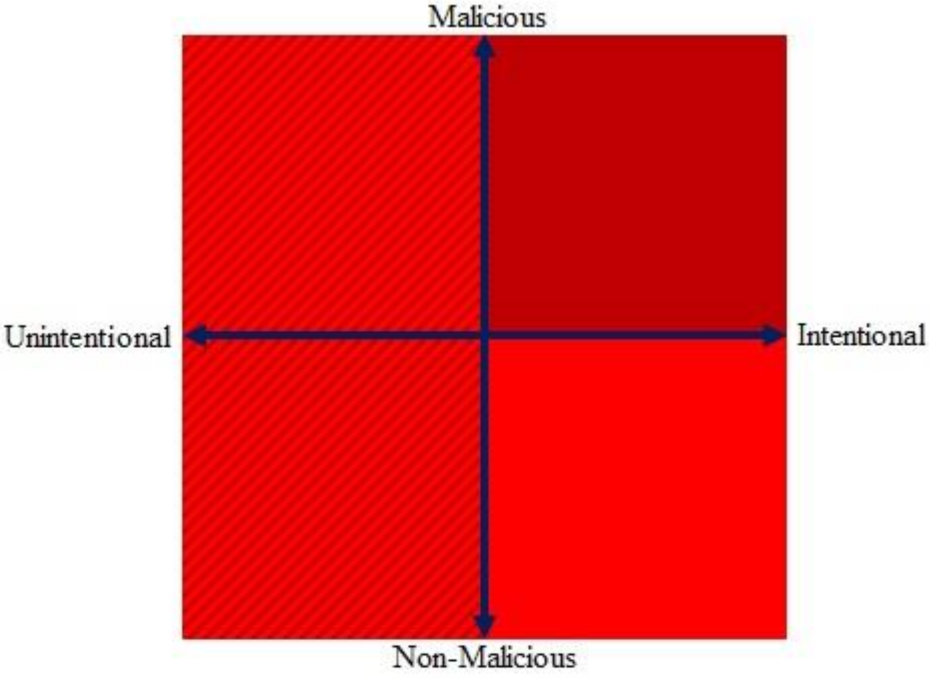

Fig. 1.1. Dimensions of insider threats

Another technique commonly used in social engineering attacks is trapping. Although classic, this technique always finds opportunities that are attractive to the victims. Torrent sites have been a simple way to download free software, video games, movies and music from the outset, thus violating copyright. For example, when the release of an anticipated video game is nearing, these sites are flooded with fake links whereby users, due to their ardent desire to play that game before its official release, actually download entire packages of malware. In order to be as credible as possible and to be downloaded by as many users as possible, files are added comments and positive feedback from fake users. [5] The malicious goal is either to exfiltrate data from computer or to create backdoor platforms that allow subsequent download of malware. Exfiltrated data may be sold on the black market, and compromised systems may become part of botnet networks. Frequently trapping is continued through blackmail.

2. Qualitative research on awareness-raising of social engineering threat

For a qualitative research into the awareness of these social engineering threats, security questionnaires should not be confined to those responsible for the security of information systems. The method of selecting the subjects must be done randomly for each department. Social engineering attacks don’t always target users with privileged or extended rights in the organization's information system, but can also target users with minimum privileges. An example of this may be the 2011 successful cyber-attack on the well-known security company RSA. Hackers have managed to achieve their goal by combining traditional hacking technical skills with social engineering techniques. They sent several spear-phishing emails to company employees with relatively low privileges and without a technical training. It took a single employee to open the malicious e-mail attachment for the attack to be successful.

An example of a societal-based level of awareness-raising questionnaire can be as follows:

- *Question 1* – Do you know the term "social engineering"? Do you know it's meaning?
- *Question 2* – Does your organization have internal policies on social engineering?
- *Question 3* – In your organization, are there any rules for maintaining security through social engineering awareness?
- *Question 4* – What kind of correspondence is received by e-mail?
- *Question* 5 – If you received an e-mail with attachment, are you concerned about its content?
- *Question 6* – Have penetration tests been conducted within your organization?
- *Question 7* – If yes with the previous question, have security breaches been identified?
- *Question 8* – If yes with the previous question, did the intrusion method been identified?
- *Question 9* – Was the security breach due to social engineering?
- *Question 10* – Do you think this questionnaire is a social engineering technique?

The questionnaire can be part of the awareness program about the risks posed by social engineering techniques and has the role of educating employees about the importance of security. It also lowers the potential of phishing attacks. It cannot eventually reduce the risk of internal threats by announcing the existence of the security structure and security mechanisms that monitor user activities and hence identify the culprits for the emergence of security breaches.

3. The implementation of security policies for reducing social engineering-based attacks

As organizations often fail to make employees aware of the concept of social engineering and how they can be manipulated, it becomes necessary to establish a security policy to solve this problem.

Security policy is a set of rules, requirements, and guidelines applicable to an organization that underpins security infrastructure and sets limits to acceptable behavior in the use of the organization's information and communication resources.

In any organization information security is a team effort and requires the participation and support of all employees working with computer systems. Managers of functional structures within the organization are responsible for implementing security policies, as well as initiating corrective and improvement / refinement measures, in line with the changes in the existing functional framework.

Implementation of security policy planning and development is followed by: strengthening and constantly improving it; integration of security actions at departmental level; analyzing and monitoring security incidents; periodic assessment and reporting of security at the organization level; adjusting policy and ensuring upgrading and compliance with legal requirements; popularizing policy among employees; assisting managers of functional structures to formulate their own information security plans.

3.1. Identity Manual – Tool to reduce social engineering-based attacks

The organization's Identity Manual provides a unique, strong and consistent picture of the organization in the minds of all parties involved in the organization's work (employees, partners etc.). The Identity Manual sets out how the organization is to be presented. (*Fig 3.1*)

The visual elements of an organization include:

- *the logo* – is the most representative element of identity of any organization. It is the sign that produces in the public mind the association between the communication materials of an organization and the organization itself. It is extremely important for the logo to be used correctly and consistently by all the emitters of an institution's messages. Among the features of the logo are the minimum acceptable dimensions, safety area, positioning, correct use etc.;
- *colors* – the organization sets a color set, being the only ones that can be used with the logo represented as color codes in CMYK (for print), RGB (for screen), and Hex (websites). The correct use of colors is essential to preserve the coherence of the organization;
- *characters (fonts)* – Is another important element of identity due to the high frequency of use. These, used correctly, appear almost everywhere: official documents, promotional materials, emails etc.

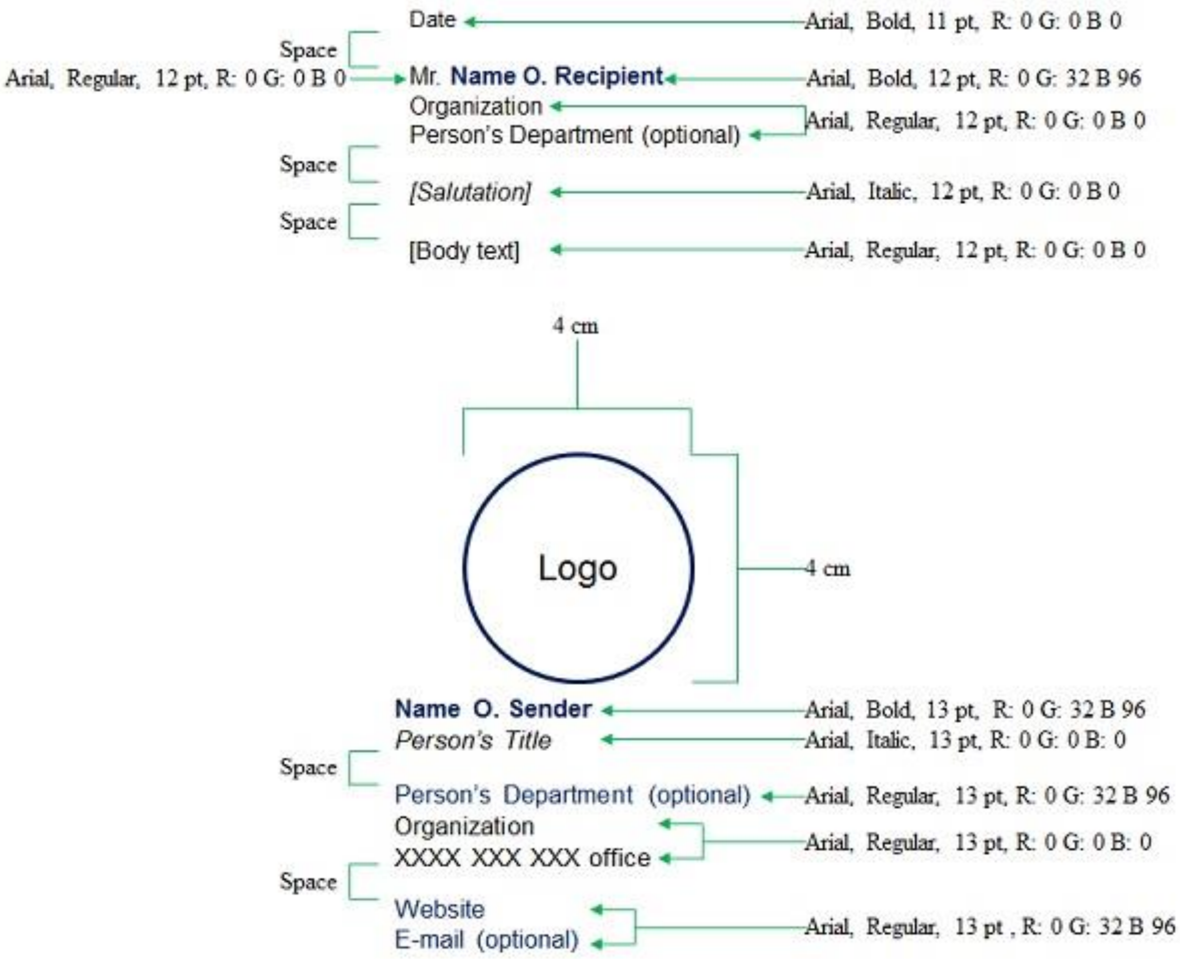
Date
Arial, Bold, 11 pt, R: 0 G: 0 B 0
Space
Arial, Regular, 12 pt, R: 0 G: 0 B 0
Mr. Name O. Recipient
Arial, Bold, 12 pt, R: 0 G: 32 B 96
Organization
Person's Department (optional)
Arial, Regular, 12 pt, R: 0 G: 0 B 0
Space
[Salutation]
Arial, Italic, 12 pt, R: 0 G: 0 B 0
Space
[Body text]
Arial, Regular, 12 pt, R: 0 G: 0 B 0
4 cm
Logo
4 cm
Name O. Sender
Arial, Bold, 13 pt, R: 0 G: 32 B 96
Person's Title
Arial, Italic, 13 pt, R: 0 G: 0 B: 0
Space
Person's Department (optional)
Arial, Regular, 13 pt, R: 0 G: 32 B 96
Organization
XXXX XXX XXX office
Arial, Regular, 13 pt, R: 0 G: 0 B: 0
Space
Website
E-mail (optional)
Arial, Regular, 13 pt , R: 0 G: 32 B 96

Fig. 3.1. Simple e-mail signature – Corporate Identity Manual[1]

Visual consistency can help distinguish phishing emails as long as the organization defines certain strict e-mail rules in different situations. E-mail messages sent internally between departments will differ in appearance from those sent to partners, customers etc. by appearance.

The organization's Identity Manual may be part of the content-based filter. The filtering algorithm inspired by the identity manual contains features such as:

- the header form;
- the proportions of elements in the message body and their location (such as the size of the logo and its location);
- characters used (including special ones), spacing, colors, spelling etc.

The filtering algorithm (*Fig. 3.2*) is an improved version of the phishing detection charts proposed by Sophos cyber security company and Login Helper blog. [6] [7] The proposed algorithm analyzes incoming e-mails and separates them into headers, message body, and attached file. Because the header contains information about the sender, recipient, e-mail subject and date, it can be compared to existing data and whether it can be correlated. The algorithm then verifies whether there are links in the body of the message, and if so, they are extracted and analyzed separately. The result of this analysis results in the blocking of the email, or the verification of the appearance of the message, according to the identity manual. In collaborating with third parties, the organization will have to implement their filtering algorithms and their identity manuals. The algorithm can take into account a multitude of features such

[1] Inspired by Graphics Standards at Fermilab, http://www.fnal.gov/faw/designstandards/email-instructions.html

as font, font size, color, spacing, contact elements, logo, etc. If the ID policy is respected, then the e-mail can be considered safe.

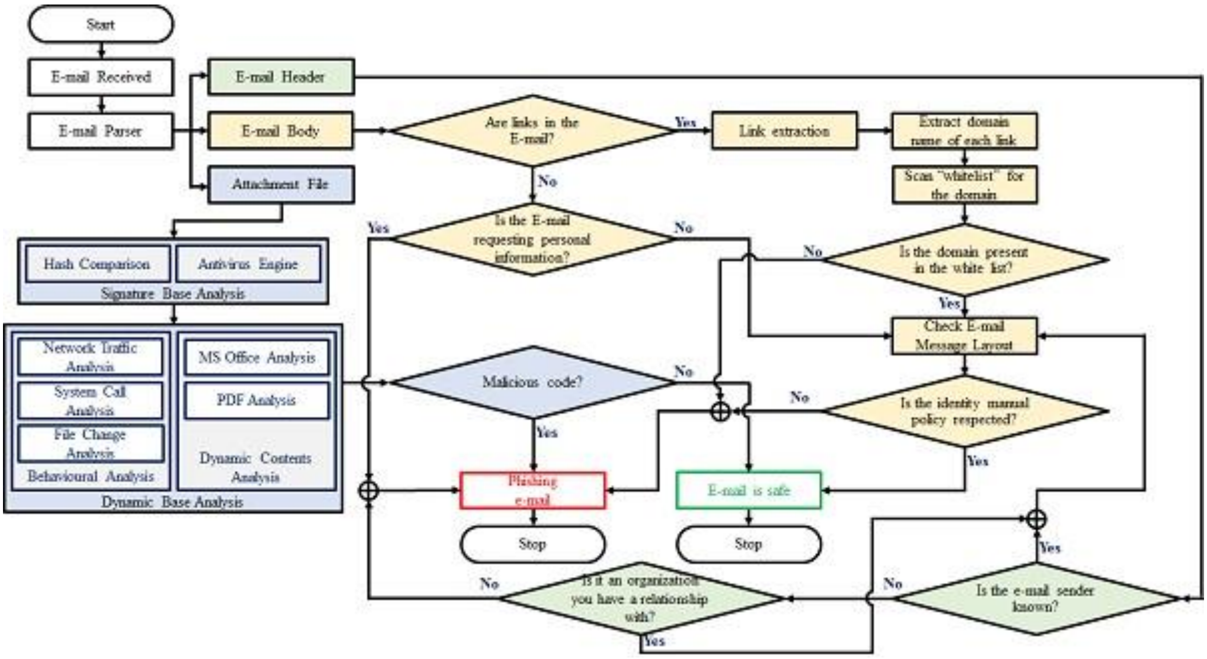

Fig. 3.2. E-mail filtering algorithm based on the identity manual

When the organization signs different protocols of cooperation / collaboration with third parties, it is absolutely necessary to establish a policy on how and rules of communication between the parties. The need for such a policy could be seen in the RSA security breach. It is important for each third party to provide the organization with a list of employees involved in the implementation of the protocol / partnership. The list must be permanently updated and any changes must be notified to the organization within 24 hours.

Because spear-phishing attacks, targeted phishing attacks, are becoming more and more difficult to detect due to the use of zero-day vulnerabilities, the algorithm first analyzes the attachments by comparing hash values of known malware codes with hash of the attached file to determine if it is malicious or not. Even if at this stage the attachment was not confirmed as malicious, or if it generated a "false-positive" alert, in the second step, the dynamic analysis, it analyzes its behavior through the virtual machine. Here are analyzed and monitored the dynamics of network traffic, the state of the network, such as communicating with the command and control server, downloading some malicious components to the attachment.

3.2. Reducing the intentional/unintentional USB storage device attack vector

The use of removable storage devices that connect via the USB port may be required by an organization but at the same time creates an additional risk. In this case, it is necessary to establish a policy for introducing / extracting data into / from the organization's network by using USB storage devices. This policy can be divided into three categories: USB port access control, data access control, and acceptable usage policy.

Access control of the USB port includes:

- disabling USB ports by physically disabling, BIOS, firmware, operating system settings, or installing applications to actively control access to these ports;
- group policy settings and editing of operating system registers;
- application of privileges to access USB ports by implementing dedicated applications;
- implement the USB driver in user mode to prevent escalation of privileges.

Access control of data includes:

- deactivating the "auto run" feature;
- restricting user privileges.

Last but not least, the acceptable use policy is more a management solution and sets out the terms in which USB devices can be connected to the internal network. Data coming from outside the organization will be scanned antivirus first. Optionally, stations dedicated to this purpose will be set up to enter / remove data to / from the organization's network via USB devices.

4. Conclusions

Social engineering is an evolving practice with many sources of inspiration. Even though the techniques used are not new, new ways of using human behavior are permanently found to exploit the weaknesses of people unable to distinguish lies from the truth of information. At present, technology is not capable of detecting social engineering in the online environment so people do not fall prey to it. IT security experts need to constantly assess and detect social engineering tactics, thus being able to provide a user warning, awareness, and training.

Adequate awareness and training in cyber security requires time, is costly and cannot cover all aspects of social engineering.

Awareness and training programs in the field of social engineering must ensure that:

- employees understand the way in which social engineering attacks are carried out;
- employees have the knowledge and training necessary to detect an attack, respond appropriately, and prevent any exposure wherever possible.

The first and most important line of defense against social engineering is organizational policies. The establishment and enforcement of information security policies shall provide clear indications to employees of the information that may be communicated, under which conditions and to whom. These policies must clearly specify the channels of information, the means of identifying the applicant and the means for transferring information. A mistake made by some organizations is to create these organizational policies, but without communicating them efficiently and clearly enough to employees. A strong policy can make an employee more resilient to attempts to exploit different human weaknesses.

The proposed filtering algorithm can be a good security check by monitoring compliance with the organization's identity manual policy, analyzing the links in the body of the e-mail message by comparing it with the "white list" and verifying both signature and dynamic of attachments. The information behind the decision to tag an e-mail as phishing is collected from the three e-mail plans: header, body mail, and attachment.

The limitation of the algorithm is that it cannot be used for correspondence with people outside the organization or with other organizations with which no co-operation agreement has been concluded. Messages from them will be considered phishing. Instead, the organization can define an e-mail address dedicated to public communication, to be monitored by dedicated staff. The goal of the algorithm is to fulfill the mission and interests of the organization, employees and partners under the usual operations.

The implementation of the filtering algorithm based on the organization's identity manual will ensure the intelligibility, consistency, availability, accessibility and quality of data for the benefit of both users and partners alike. It is also necessary to manage and continuously monitor the "white list" to add exceptions and the "blacklist" to reduce the number of false exclusions. Although the applicability of the algorithm is limited, it can be improved by adding encryption facilities, electronic signature and spell checking. We can conclude by saying that:

> Organization Security = (Informational Flow + Investment Power + Computing Power) x (Security Policy + Employee Loyalty)

Explanations:

Informational Flow = the information circuit within the organization or between several organizations
Investment Power = the ability to keep pace with technology
Computing Power = how fast an amount of information is processed
Security Policy = vulnerability identification, risk assessment, measures taken to counter cyber threats and minimize risks
Employee Loyalty = employee will, employee pride

References:

[1] Kim ZETTER, *Teen Who Hacked CIA Director's Email Tells How He Did It*, October 19, 2015, https://www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/

[2] Verizon, *Verizon 2018 Data Breach Investigations Report*, 2018, https://www.verizonenterprise.com/verizon-insights-lab/dbir/ore references

[3] Graham CLULEY, *This is the email that hacked Hillary Clinton's campaign chief*, Hot For Security – Bitdefender Official Blog, October 31, 2016, https://hotforsecurity.bitdefender.com/blog/this-is-the-email-that-hacked-hillary-clintons-campaign-chief-17039.html

[4] Steve STASIUKONIS, *Social Engineering, the USB Way*, Dark Reading, June 7, 2006, https://www.darkreading.com/attacks-breaches/socialengineering-the-usb-way/d/d-id/1128081?piddl_msgorder=asc

[5] Bitdefender, *Un cheval de Troie dans des kits GTA 5 : joueurs, attention aux mirages!*, Bitdefender France, September 10, 2013, https://www.bitdefender.fr/actualite/un-cheval-de-troie-dans-des-kits-gta-5-:-joueurs-attention-aux-mirages--2807.html

[6] Sophos, *Phishy Flowchart*, Oxford, UK, 2017, https://www.thiel.edu/assets/documents/offices/information-technology/Phishy_Flowchart.pdf

[7] Martin BRINKMANN, *The Phishing Flow Chart*, February 11, 2010, https://www.ghacks.net/2010/02/11/the-phishing-flow-chart/