Dogana

ADVANCED SOCIAL ENGINEERING AND VULNERABILITY ASSESMENT FRAMEWORK

The role of Social Engineering in evolution of attacks

Work Package:	WP2
Lead partner:	CEFRIEL
Author(s):	E.Frumento, R.Puricelli, F.Freschi, D.Ariu, N.Weiss, C.Dambra, I.Cotoi, P.Roccetti, M. Rodriguez, L.Adrei, G.Marinelli, G.Kandela, B.Pachego
Submission date:	1st February 2016
Version number:	1.1 **Status:** Final

Grant Agreement N°:	653618
Project Acronym:	DOGANA
Project Title:	Advanced Social Engineering and Vulnerability Assessment Framework
Call identifier:	H2020-DS-06-2014-1
Instrument:	IA
Thematic Priority:	Trustworthy ICT
Start date of the project:	September 1st, 2015
Duration:	36 months

Dissemination Level	
PU: Public	✓
PP: Restricted to other programme participants (including the Commission)	
RE: Restricted to a group specified by the consortium (including the Commission)	
CO: Confidential, only for members of the consortium (including the Commission)	

Horizon 2020 European Union Funding for Research & Innovation

Project co-funded by the European Commission under the Horizon 2020 Programme.

Revision History

Revision	Date	Who	Description
0.1	21/12/2015	R. Puricelli/CEFRIEL	First draft that integrates all contributions from partners
0.2	10/01/2016	P. Roccetti/EII	Revision of the document
0.3	15/01/2016	E. Frumento/CEFRIEL	Revision of the document
0.4	31/01/2016	M-Rodriguez/EII	Revision of the document
1.0	01/02/2016	E. Frumento/CEFRIEL	Final editing
1.1	16/11/2016	E. Frumento/CEFRIEL	Addition of Executive Abstract and Conclusions and general revision

Quality Control

Role	Date	Who	Approved/Comment

Disclaimer:

Table of Contents

List of figures

List of Tables

Definitions and acronyms

CC	CyberConnector
CyberConnector	An internal knowledge collaboration site and social network that is used to share all the information among partners. Referred to also as CC.
DOW	Description of Work
MST	Management and Support Team
PC	Project Coordinator
SC	Scientific Coordinator
OSINT	Open Source Intelligence
OCG	Organized Crime Group
SE	Social Engineering
CI	Critical Infrastructure
ECI	European Critical Infrastructure
CNI	Critical National Infrastructure
SEO	Search Engine Optimization
ASE	Automated Social Engineering
TA	Targeted Attacks

1. Executive Abstract

The problem of Social Engineering (SE) is evolving since few years at an incredible pace. What, till the end of the past century, was an advanced, but niche, way of attacking specific systems, is nowadays mainstream in cybercrime and terrorism. The complexity level of attacks that are actively exploiting the human element is incredibly high and often the exploitation of the human element is the enabler element for the following technological part[1]. However, also SE evolves and today we are talking of **SE 2.0 vs old-school SE**.

The old-school SE is an adaptation of the ageless art of deception to the modern communication media (e.g., mainly phone and early use of email, beside physical intrusions), where the level of personal talent involved and effort required, limited this type of attacks to the capabilities of few famous attackers, who were concentrated on valuable targets. Hence, traditionally the Information Security considers the "human factor" a potential threat only in those systems requiring «SECURITY-IN-DEPTH», because for these situations any possible threat, also the less common one, is evaluated up to the innermost levels.

The reason behind such evolution is the utter increasing relevance of the Targeted Attacks (TAs) as also reported by all nowadays attacks' statistics. TAs are the most popular and most widely used in today's attack strategy, also for SMEs. TAs are a type of attack which takes advantages of a complex Human Attack Vector combined with a technological exploit mixed into a unique targeted and specialized ad-hoc attack which exploits (deceives) both the humans and the IT systems. Targeted Attacks are often confused with APTs (Advanced Persistent Threats), but even though they share the techniques, they do not have the same intent (TA are usually not driven by government agencies).

Modern SE includes and extends the former SE concepts into a wider vision. Probably the cornerstone that splits between old-school and modern SE is the possibility to exploit the SE techniques on a larger scale, using automated attacks on a potentially large number of victims. The transition from old school to modern SE was triggered by the large amount of machine-readable data that is freely available today. This trend has been exponentially strengthened by the advent of Social Networks and the new social trends of information sharing. Another important aspect was also the involvement, in the planning of the attacks, of competences for never previously seen in the cybercrime world, required to better understand how to "exploit the humans". Competences such as psychologists, marketing experts and in general all the human sciences are becoming requested by the Organized Crime Groups (OCG).

The aim of this document is to present the evolution of modern social engineering and to discuss its relationship with modern cybercrime and cyberterrorism trends. The aim of the

[1] As an example, about the recent Pawn Storm attacks, see E. Frumento, "The real story behind the latest pawn storm attack and the windows zero-day patch release," in *Blog DOGANA Project*, 2016. [Online]. Available: http://www.dogana-project.eu/index.php/social-engineering-blog/11-social-engineering/27-real-story-behind-pawn-storm-attack. Accessed: Nov. 16, 2016.

document is to be a funding document for the whole project, giving a clear and complete view of the Social Engineering influence on modern cybercrime tactics, technologies and trends. D2.1 documents the refence model for SE across DOGANA.

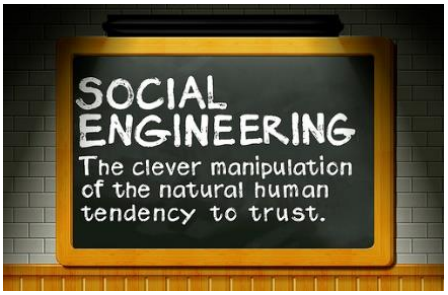
1.1. Deliverable Structure

The document will explain the concepts presented in this introduction. In particular:

- Chapter 2 “Introduction to the Social Engineering” introduces the problem of social engineering with details of how it is used by OCG in todays’ attack strategies, and presents also the ground theoretic model of which are the driving forces of SE 2.0. These elements are the real ground foundation of how SE in considered in DOGANA.
- Chapter 3 “The importance of the Human Element in Social Engineering 2.0” introduces the motivations that made attacking humans so important in the current digital environment.
- Chapter 4 “Social Engineering within the modern Cybercrime” reports an overview of the leading trends in cybercrime, it shows SE 2.0 as the most remunerative tool that is at disposal of cybercriminals today
- Chapter 5 “Attack Process” describes how attacks are performed and which are their most relevant phases
- Chapter 6 “Critical infrastructure and other vulnerable industries” presents a list of the most vulnerable industrial sectors with examples of assets that need to be protected from SE attacks.
- Chapter 7 “Countermeasures and trends” discusses the plethora of countermeasures that are nowadays either on the market or still in the research area. SE 2.0 is still an open point in security.
- Chapter 8 “Foreseen Evolutions” presents the evolutions of this area of security, advances foreseen for the following years.

2. Introduction to the Social Engineering

The best way to open such document is to report a classic definition of Social Engineering (SE onward in the document), to better underline the difference between what is commonly perceived as SE and what is the current state of this “art”. There are many different definitions of SE, but the following is interesting because it is classic and belongs to the so-called old-school SE and at the same time it is also generic enough to contain hints on what is nowadays SE 2.0.



Social Engineering (SE), in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme. The term "social engineering" as an act of psychological manipulation is also associated with the social sciences, but its usage has caught on among computer and information security professionals[2].

Traditionally, the world of Systems Security mostly focuses on technological threats coming from the compromised technological systems. Nonetheless, an information system is not composed merely by a technological factor, but also by the "human" factor. When dealing with Information Security the "human" factor refers to the often-forgotten user who plays an important role in a cyberattack. Traditionally Information Security considers the "human" factor a potential threat only in those systems requiring «SECURITY-IN-DEPTH» [1] because for these situations any possible threat, also less common one, is evaluated up to the innermost levels[3].

Old school SE requires very talented hackers and often directly involve attackers. Old school SE is an early adaptation of the ageless art of deception to the modern communication media (mainly phone and mail beside classic presence).

The main characteristic of this type of SE attacks was the high level of ability required by the attacker (very few talented hackers in those years) and the direct involvement in all the phases of an attack. The old-school SE is an adaptation of the ageless art of deception to the modern communication media (mainly phone and early use of email, beside classic presence) allowing these few talented SE experts to concentrate on very valuable targets.

This approach is called **old school** mostly because the assumptions mentioned above are not true anymore: the SE threat is becoming increasingly simpler for attackers and the required knowledge is less than in the past.

A basic bibliography of the old SE school includes (e.g., the ability of D. Mitnick or Frank William Abagnale Jr. to trick humans) [2][3][4][5].

At its roots, the early social engineers were all IT experts or talented hackers. Despite being well prepared in hacking logics and personally talented, their results were not comparable to the results achievable nowadays due to the involvement of professionals such as psychologists, marketing experts or cognitive scientists in the hacking attacks.

The modern Social Engineering includes and extends these concepts into a wider vision explained in this document in the following chapters.

[2] See Wikipedia, *"Social Engineering"*

[3] For example Mitnick K D and his famous Social Engineering twisted incursions, narrated in his books (e.g. The art of deception: Controlling the human element of security, 2002; Ghost in the wires, 2011)

2.1. A practical definition of Information Security

"Information Security" is a term related to old-school SE and, in the context of the current document, it is useful to understand what it means. According to the US Code[4] it can be defined as:

(1) The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(C) availability, which means ensuring timely and reliable access to and use of information.

This definition is based on the concept that a person, business or government will suffer harm if there is a loss of **confidentiality, integrity or availability of information.** Therefore, the role of information security is to minimize the possibility of such harm occurring.
A more concise definition is the one reported in the ISO 17799: "*Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities*".

According to the previous definitions SE is used to disrupt Information Security by violating the confidentiality, integrity and/or availability of an asset. This disruption is exploited through techniques and methods that leverage on the natural human tendency to trust systems, other humans, ICT devices, etc.

2.2. Theoretic model of the social engineering threat

The definition of Information Security given in the previous section implies the protection of assets that belong to a specific Information Space, which leads to the following assumption:

- Assets $\in$ information space $\Rightarrow$ The whole information space must be protected

Figure 1 reports a schematization of the components of an information space, which is composed by two important elements, the **humans and the technics**. Both, from the information science point of view, store (i.e. knows) the assets that need to be protected (e.g., credentials).

[4] US Code Title 44, Chapter 35, Subchapter III, § 3542

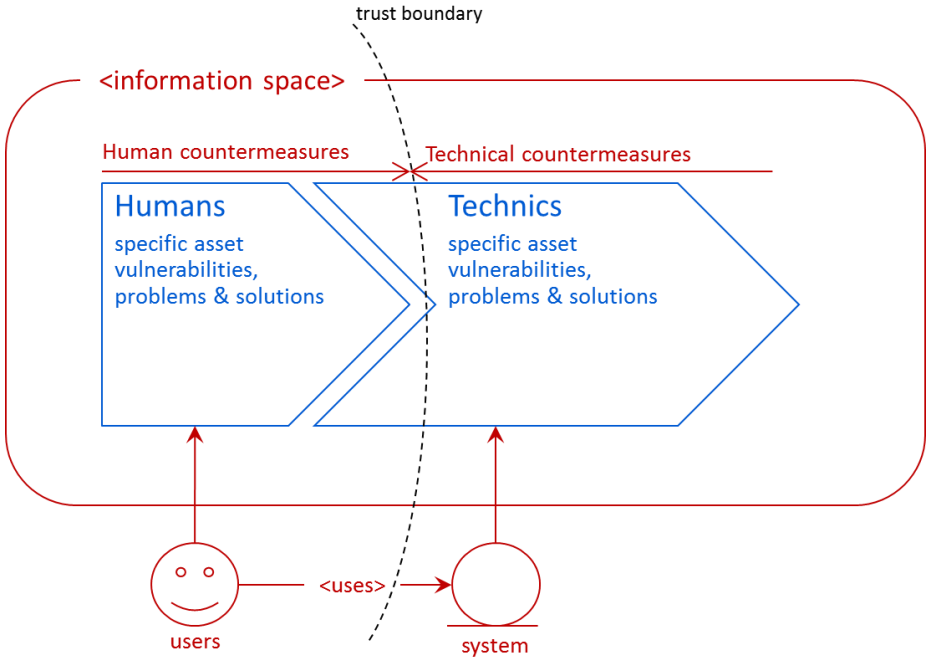


Figure 1 - A general model of information space that includes the technological and human dataspaces

> The essence of human and technological attacks is to create collusions in the information elaboration system represented in Figure 1 or, in other words, to abuse the trust-chain between humans and technics.

At the conceptual level, these information elaboration sub-systems interact through a transitive trust chain [6] that essentially can be described as: *the technical and the human sub-systems trust that the other one is able to protect their information space, which means to offer integrity, confidentiality and availability*.

The presence of a trust chain in any information elaboration system implies the following assumption: the node granting trust to another one does not have by design the instruments to check when the trust is misplaced or broken [7]. Like any other system based on transitive trust, the system described in Figure 1 is vulnerable to infiltration and Sybil collusion. The essence of human and technological attacks is to create collusions in the information elaboration system represented in Figure 1 or, in other words, to abuse the trust-chain between humans and systems.

Just as specific countermeasures in the technological domain have been largely explored by the security community, it is now important to fully investigate the human domain. One of DOGANA's main challenges is to investigate countermeasures and their capacity to mitigate vulnerabilities present in the human domain. Figure 2 reports the situation that particularly DOGANA but also the rest of the society are facing today

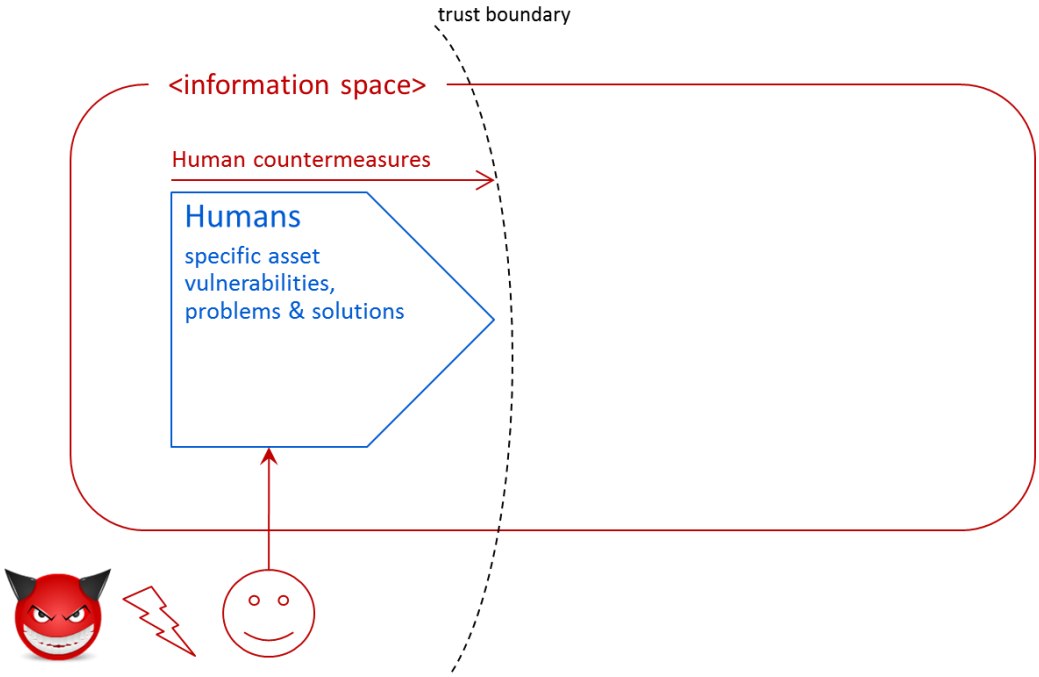


Figure 2 - Modern Hackers concentrate on the human side of the information space with specific techniques and methods

One of the biggest problems, highlighted in the attack scheme shown in Figure 2 is that the number of automatic attacks exploitable against a large number of people at the same time, have increased alarmingly in the recent years. Nowadays many of the mainstream security companies[5] are focusing on how the "Human OS" could be hacked [8][9] and more importantly how it can be protected [10].

Probably the cornerstone that splits between old school and modern SE is the possibility to exploit the social engineering techniques on a larger scale, using automatize attacks.

The transition from old school to modern SE was triggered due to the current large amount of data that is freely available and easily machine-readable, the new trends in sharing information and the advent of social networks. Traditionally the SE is associated to cyber espionage or APTs, but thanks to the improvement in the execution of SE attacks the number of targeted attacks has increased substantially[6].

The following approach, at a model level view, could also be represented using a triangle where the three corners are **Social** (groups of people), **Human** (single humans) and **Technology**. These corners shape a space where the asset exists and where all possible attacks fall (Figure 3 shows real examples of concepts and how they are mapped in this theoretical model). The old-school SE is confined into the space between the human and social corners, slightly closer to the human, and its "classic" approach keeps it far from the technology corner.

[5] For example: http://www-03.ibm.com/software/products/en/x-force-threat-intelligence

[6] targeted attacks must not be confused with APTs, they share techniques but not intents and are a result of commoditization and diffusion of SE techniques (see http://securityaffairs.co/wordpress/40228/cyber-crime/targeted-attacks-vs-advanced-persistent-threats.html)

Other section, further down in the document, describes how strategies used in modern attacks' could fall into this triangle.

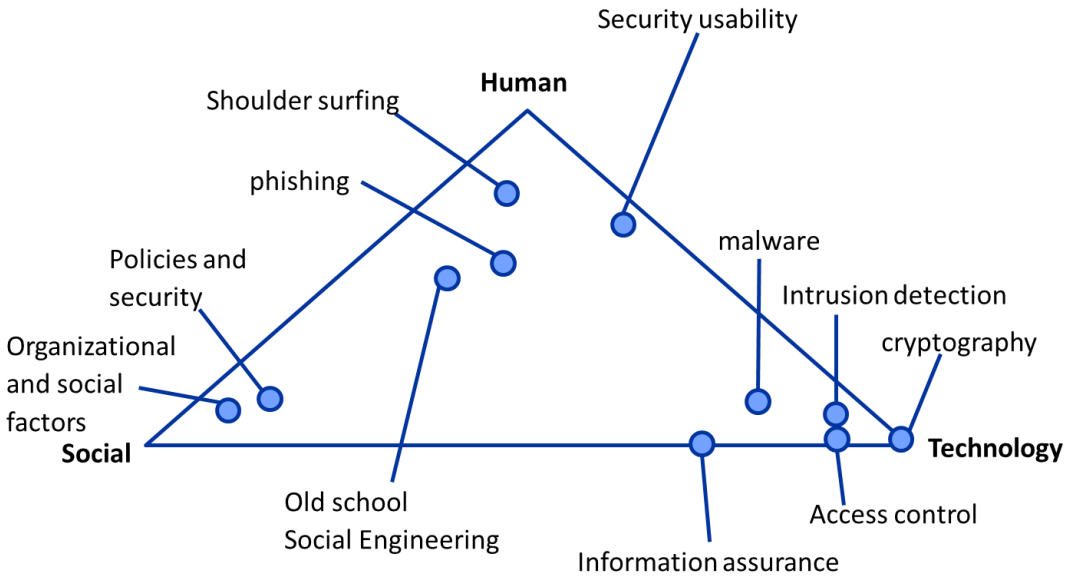


Figure 3 - A triangle of security made of three corners Social-Human-Technology with some real examples of mapping

2.3. Impact of Social Engineering on the modern security

Since most of cyberattacks include non-technological exploits, the impact of SE on modern information security has increased significantly. Recent statistics [11][12] provide additional and relevant insight such as the following:

- 1 year is the medium time to discover an attack performed via SE.
- 5 is the average number of emails needed to create an entry point in a company.
- Attacks are typically discovered by third parties.

Attacks have become narrower, involving less generic victims at the same time. This is on the one hand a consequence of improved hiding tactics, whose aim is to keep the attack "under the threshold" reducing the risk of being detected, but it is also a sign of a better a-priori selection of the potential targets and thus a more aggressive usage of SE techniques.
As mentioned in a previous section the **current protection strategies address information systems**, whilst, in practice, both humans and information systems can be considered as access points to major assets.
For instance, login credentials are considered as critical information, either directly, they are an important asset or indirectly, they need to be stolen because they are the main entry point to that important asset.
Credentials are often stored as encrypted information in one or more systems. However, they are also "stored" in personal devices, sheets of paper, etc. as well as memorized by users. The approach of SE is to acquire the credentials by focusing the attack on humans rather than

systems. The last ones can be easily hardened and improved, making attackers work harder and dedicate more resources to access them, while human behaviour is more complex, subjective and harder to "patched" [13].

In this context, enterprises have become extremely vulnerable, even large companies that have made significant investments in security and often operate worldwide have experienced attacks that exploit the human element of (in)security [14][15][16].

> Enterprises have become extremely vulnerable and recent attacks have had major societal impact. Good old days of (in)security are back.

This situation shows that the strategies used in modern attacks influence the way attackers plan and focus their actions against citizens and enterprises. These strategies originate from the logics of Advanced Persistent Threat (APTs), detailed in section 5.1.1) and are directly associated with Targeted Attacks (TAs). They are becoming more popular thanks to the continuous improvements registered in the SE domain.

TAs are an important vector during the initial phases of infiltration and the early phase of such attacks is usually spear-phishing or context-aware phishing, it depends on the level of sophictication of the hook. Targeted phishing attacks are customized to reach a specific user or community, and the customization is implemented using social engineering and especially crafted malware. This issue integrates the human, technological and conceptual concepts that are currently present in the real-world and that must be addressed.

Research in security is lagging behind, and fully operational solutions that address this problem (at an integrated level) are still not present on the market [17][18][19]. Therefore, companies currently face a major challenge due to the lack of established countermeasures [20].

"Good old days of (in)security are back".

This sentence builds up the following phrases regarding information security, where SE is one of the main factors included in the greatest part of the most relevant trends:

- Main stream entities demonstrated to be incredibly weak against SE based attacks [21]
- Crushing attacks can be launched even by a single attacker [22]
- Awareness programs demonstrated to be incredibly inefficient along the years [23][24]
- Classical protection technologies (e.g. antivirus, firewall, etc.) are less and less efficient against these new types of attacks [17][25].
- All the sectors of society and less targeted markets are increasingly attacked (e.g., health, insurance, SCADA, mining industry, manufacturing, small enterprises, etc.)[7]

2.4. Definition of the Social Engineering 2.0

SE is a well-known method of deception already used for a very long time, but the following evolutions were very important to change the current landscape:

[7] See latest IBM X-Force Threat Intelligence Quarterly http://www-03.ibm.com/security/xforce/downloads.html

- The evolution of social network and its scalability through mobile platforms and the naive behaviour by users.
- The evolution of new technologies that make SE attacks more sophisticated, such as automation. This means that attacks can reach and impact a large number of people/victims at the same time.

These two factors contributed to the evolution of the social engineering into a new multifaceted phenomenon that we call Social Engineering 2.0 (SE 2.0). It increased the number of potential victims directly exposed on the internet.
It uses advanced automatic methods to gather and elaborate the information needed to carefully select the "victims".
Social Engineering 2.0 is indeed a complex field that involves several heterogeneous technologies and competences. Figure 4 shows the most important technological and scientific areas involved.

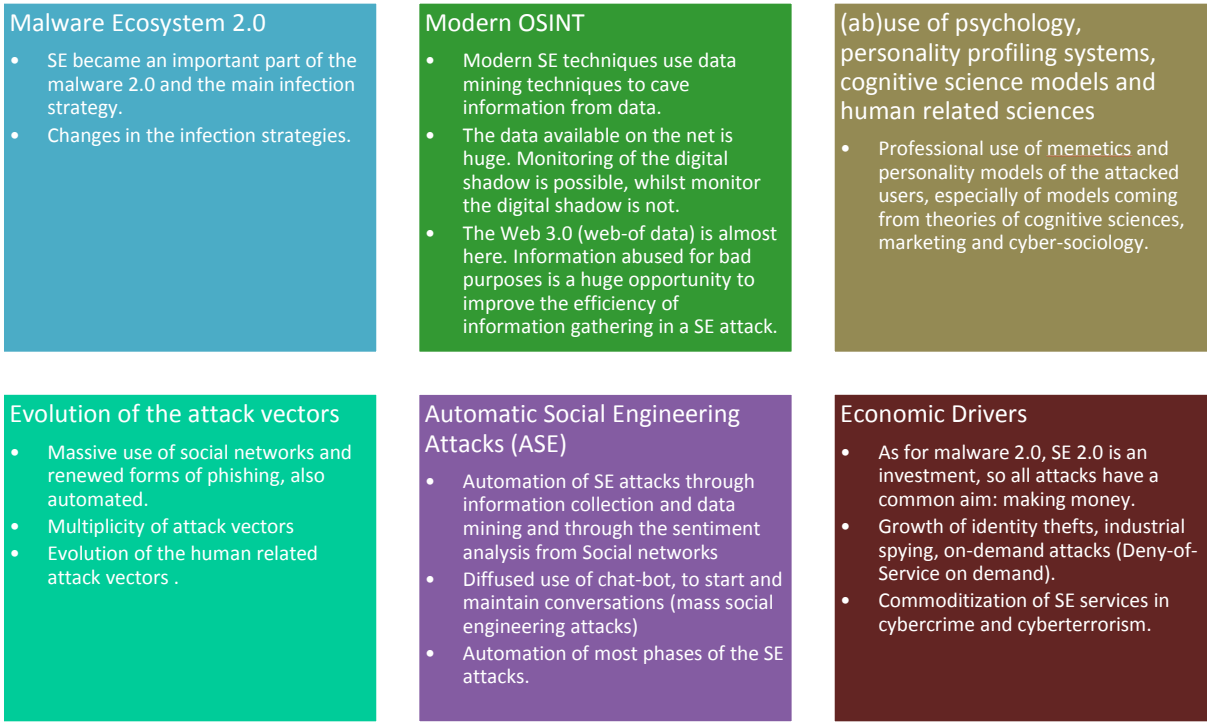


Figure 4 - Overview of the main characteristics/competences of Social Engineering 2.0

- **Malware Ecosystem 2.0**. SE became an important part of the malware and its main infection strategy; this implies changes in the infection strategies and in the development process of new malware.
- **Modern Open Source Intelligence (OSINT)**. Modern SE uses data mining techniques to cave information. This builds up the large amount of data that people or enterprises

share intentionally or inadvertently on the network[8]. OSINT is used to collect information before the attack, hence beside digital shadows and footprints, there is another interesting source of data that is increasingly exploited: The Web 3.0 (web-of data) [26]. Abuse of information publicly available for bad purposes is a huge opportunity to improve the efficiency of information gathering in a SE attack.

- **(Ab)use of psychology, personality profiling systems, cognitive science models and human related sciences**. SE means hacking humans using the most efficient ways available; therefore, psychology and all human sciences are frequently used to gain knowledge of the "vulnerabilities" present in the attacked system (i.e., the human). Reports have noted that cybercriminals in becoming more professional, are increasingly using memetics [27][28] and personality models of victims[29][30], especially models from cognitive sciences [31], marketing and cyber-sociology theories [32][33].
  Psychological profiling (for example, identifying the most vulnerable victims) [34][35], use of memetics [27][36] and sentiment analysis [37][38][39] are used to rapidly contextualize and tailor attacks around selected victims with a localized approach[9].
- **Evolution of the attack vectors**. Understanding victim's psychology and how they think has leaded to change the way hooks are crafted and delivered.
  The massive usage of SPAM is a technique that is not very used anymore. Nowadays SPAM is mainly used to collect the so called "*low hanging fruits*" supplying the cybercrime world with a low but constant flow of incidents.
  On the other hand, Advanced Persistent Attacks (APTs) are the ones with the highest results and they use massively social networks and renew forms of phishing (spear phishing, context aware phishing, collectively called *-phishing). As result, attack vectors are multiplied and the modern *-phishing are not anymore tied to specific channels.
- **Automatic Social Engineering Attacks (ASE).** One of the most interesting points in the evolution of SE has been the possibility to automate most of the attack's phases, this fact increases the efficiency of mass social engineering-based attacks.
  Automation of SE occurred thanks to the automated information collection and data mining from social networks, also because of the improvement of algorithms for sentiment analysis [39].

[8] The amount of data intentionally shared on the network is usually called "*digital footprint*". This concept is paired with the corresponding one of "*digital shadow*"; a *digital shadow* is composed by all the data spread or shared on the network, not intentionally and often inadvertently. The sum of digital shadow and footprint is a big source of information for attackers. Monitoring of the digital footprint is by definition possible because the potential victim is aware of its existence, whilst monitor of the digital shadow it is not.

[9] Refer to the latest Symantec Internet Threat Report, http://www.symantec.com/it/it/security_response/publications/threatreport.jsp

- **Economic Drivers.** There is one important difference between malware and social engineering, creating malware could be done for fun, to prove the technical skills of the author, as a matter of fact, the early generations of malware were born with this intention, but on the other hand, using social engineering for fun makes less sense; social engineering has only one single goal: deceive persons.
  This difference led SE 2.0 to become an efficient instrument to carry serious attacks and a fruitful investment. The growth of identity thefts, industrial spying, on-demand attacks (Deny-of-Service on demand), commoditization of SE services in cybercrime and cyberterrorism are all consequences of the evolution of SE [40].

The modern social engineers use a large and complex mix of different competences (technological, cyber-sociology, psychological, marketing, design, etc.) to create a complete attack. However, at the same time the technological and cybercrime evolutions lowered the level of complexity required to perform an attack, exposing a larger number of potential victims to this threat.

In SE 2.0 most of the technologies previously mentioned have been developed originally in different contexts, like the ones coming from social marketing to help catching and influencing social trends. However, at its core, Social Engineering intents to influent people's way of thinking, similarly to marketing, but with malicious intentions.
All cited technologies, originally, are design, develop and used legitimately, but they also are abused by social engineers to perform attacks and collect information, which afterwards are exploited in highly contextualized attacks.
Summing up, **the real criticism of SE 2.0 is the abuse versus the use** of these technologies. Hence the problematic is not only limited to the technical world, it includes the psychology and cyber-sociology[10] areas.
Science (i.e. human science) and technology (e.g. social network scanning) help to identify the three factors that define SE 2.0 as illustrated by Figure 3. Figure 5 shows the characteristics mentioned above, which are then described in following sections.

[10] A fundamental evolution in the attack techniques is the application of cognitive sciences and semantics technologies in the modern social engineering attacks, in order to automatically profile personalities and find potential victims on large mass of online persons.

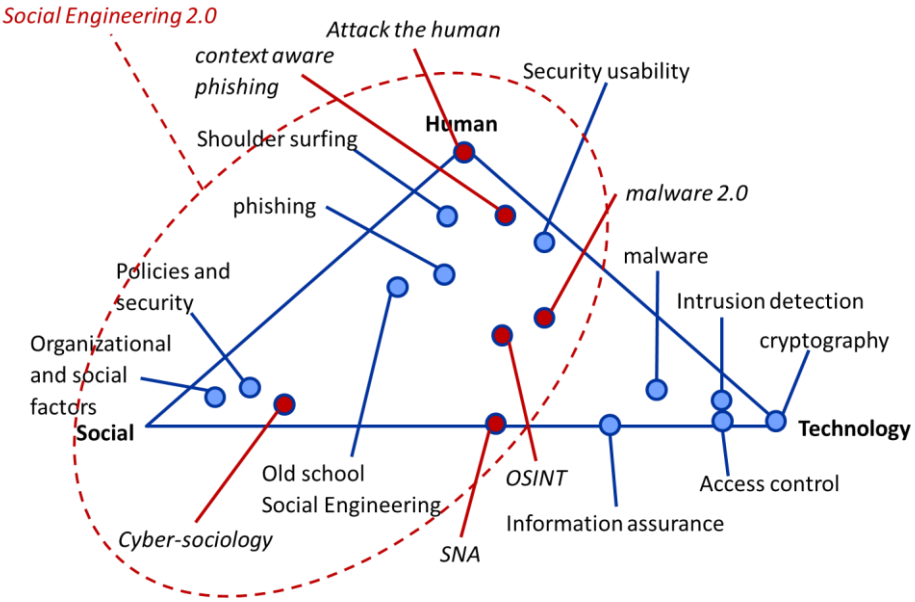


Figure 5 - A triangle of security made of three corners Social-Human-Technology with evidence of Social Engineering 2.0

2.4.1. Malware Ecosystem 2.0

SE 2.0 is nowadays the most efficient and economically relevant instrument used in cybercrime. Malware has been particularly affected and it has become extremely different compared to the malware that was identified in recent past.
The main Malware 2.0 characteristics are the followings [41]:

- Lack of a single control centre and ability to adapt the infection to the attacked machine
- Extensive use of methods to fight AV systems
- Victim machines take the role of servants and attacks get more discrete
- Intense production on syntactic – not logical - variations
- Short and targeted attacks from many directions
- Intense and advanced use of SE techniques[11]
- Modularity and complexity of infections
- Malwares and SE follow the markets laws governed by supply and demand (MaaS) [42].

[11] Common web based attacks include malicious URLs, compromised web pages (aka watering hole attacks), drive-by attacks, drive-by-download, drive-by-infection, web backdoors and browser exploits.

Once the human "firewall" is bypassed, the Trojan has direct access to the PC without having exploited the technological system yet, and this is usually simpler than writing automated viruses.

Since 2000, the statistics of malware reported by McAfee [43] show a clear predominance of Trojans versus two other categories: Potentially Unwanted Programs (PUPs) and Virus and BOTs. This predominance lies behind the definition of Trojan: a Trojan is a malicious program unable to infect a machine on its own, it requires a user that executes it (i.e. click over a link or open an attachment). The user must be convinced to do it, and usually is convinced through a hook[12]. The creation of a hook must be an efficient and reliable process in order to deal with the challenges of cybercrime industry, and Social Engineering has become the right instrument to achieve it.

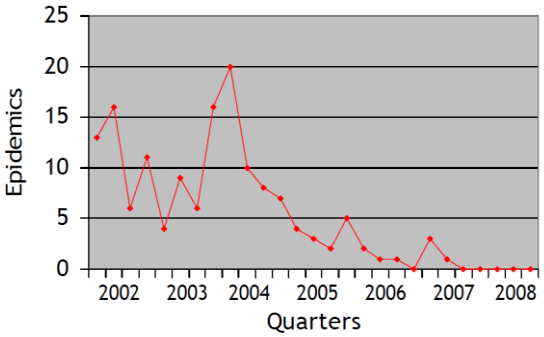


Figure 6 - The number of Epidemics is decreasing, also today (source: Kaspersky)

In the information space model (Figure 1), the main characteristic of a Trojan is that the exploit starts in the human side and continues in the technological one. Counted as 100% the overall vulnerability abused by malware, resulting by a sum of human and technological exploits, what differentiates the malware today is the relative complexity of the human exploit, which simplifies the technological one.

Once the human "firewall" [44] is bypassed, the Trojan has direct access to the PC without yet exploiting the technological system, this is usually simpler than writing automated viruses. The technological exploits that follow are logically a consequence of the initial human-side exploit.

Thus, nowadays[13] approximately 76% of the overall malware produced are Trojans.

Beside the absolute predominance of Trojans, there is another interesting trend, reported by Kaspersky up to 2009 [45], the progressive disappearance of global epidemics in malware (Figure 6).

The assumption aboveis that malware creates profit as long as it stays undetected, which implies the following concepts that are almost the same from the definition of malware 2.0 reported above:

- The victims are more targeted improving the selection process prior the real attacks
- discretion of attacks, hence reducing the number of infected machines, digital shoulder surfing, short-lived attacks on multiple channels
- increased the interest in keeping systems compromised but infected and responding to remote controllers

[12] The hook is the element that catches the attention of the victim

13 Source: PandaLabs Report Q1 2015, http://goo.gl/3gZEdn

- reducing the time to develop new malware and increase the availability of efficient exploit-kits[14]

Figure 7 shows a comparison between the structures of two generic malwares: malware 1.0, on the left and malware 2.0, on the right.
The left side shows that a malware typically consists of three different routines: hiding, seek & search and infection, which is the common structure of an automated infection malware. It should be able to infect any type of system because its infection business plan is flat: malware infects any system that is vulnerable, without much discretion and/or selection. This type of malware was common in automated infections and it is the equivalent to SPAM emails.

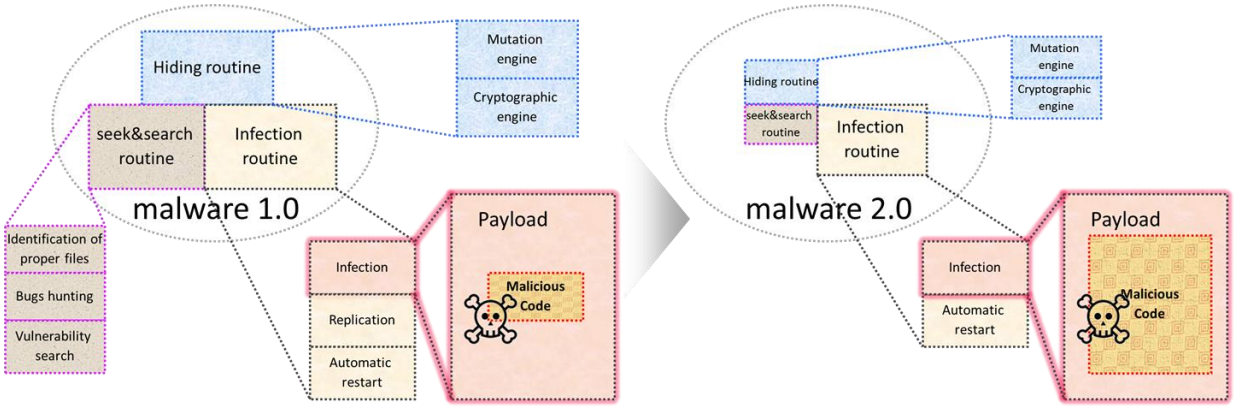


Figure 7 – Comparison of the structures of malware 1.0 and modern malware 2.0

Modern malware 2.0 (right side) has a different structure because of the crucial role of SE in the infection process, the consequences are the following:

- There is no need of privileges escalation in the infected system
  - The attacker gets in touch directly with the person who handles the target asset because managing the virus in the user's system is technically easier to exploit
- Asymptotically the infections are 1:1 with carefully selected victims/targets
  - Ad-hoc malware, no families, custom writings even using high level languages, no epidemics
- Less need to hide
  - Users allow the malware to enter the system, because they are convinced beforehand
  - The malware needs less polymorphism and mutations because it does not need to abuse the cracks of the protection
- Large infections are not used for most of the remunerative attacks anymore, they are used mainly to produce low level constant incomes and often to create noise, to better hide ad-hoc infections

[14] Angler, which is the most prevalent exploit kit today, is a good sample of the sophistication level Achieved (https://threatpost.com/analyzing-angler-the-worlds-most-sophisticated-exploit-kit/110904/), accessed November 2015.

    - Seek & search is almost useless because the right system is directly targeted
    - (Automatic) Replication is not an issue anymore
- Extremely big malicious payload. It is now quite common to find payloads with a dimension of 20Mb or more. They are often written in high level languages.
    - One of the most challenging tasks for modern malware is the crawling of the victims' information space: after selecting a user and infecting their system with an ad-hoc process, the malware needs to understand which data the victim really accesses.
    - There are many more "script-kids" writing payloads with high level languages instead of using Assembler where it is difficult.
    - Attackers use multi-stage infection processes and increasingly use droppers in order to update the scripts

This vision of how malware evolved positions the problem of SE 2.0 into a wider scenario: mitigating SE attacks would also mitigate modern malwares.
The technical skills required to develop a new malware are reduced[15]: having SE in place before exploiting the technological attack implies the possibility of attacking the few useful victims with 1:1 customized ad-hoc attacks[16].
Thus, Malware 2.0 does not need to spread across a network or to escalate privilege or even use unknown 0-day bugs. It needs a strongly customized behaviour to hit just one user on one machine[17], concretely the user that owns the asset that the attacker wants. This situation recently led Symantec to declare that standard defence systems as anti-viruses are dead [17]. This is the same concept expressed many times across the latest years and referred by the AVID buzzword (Anti-Virus is Dead) [25][46].

2.4.2. Modern Open Source Intelligence (OSINT)

OSINT is used in the preparation phases of an SE attack and its goal is the measurement of the digital footprint and shadow, with licit or illicit (e.g., fake identities) methods.

Open source intelligence (OSINT) solutions provide access to a wealth of internal and external data from millions of sources with the intention of helping both governmental agencies and private sector businesses make informed decisions every day [47] , which demonstrates that it is used not only for malicious intents.

15 Source: PandaLabs Report 2013, http://goo.gl/MjFYBm
16 Therefore the watering pool attacks and the malware ad-hoc infections are nowadays one of the most actively exploited techniques of infection [10].
17 Two recent sample are the Trojan.VikNok.2014 (http://thehackernews.com/2014/05/beware-cyber-criminals-spreading-click.html) and the Trojan.PoSeidon.2015 (http://thehackernews.com/2015/03/poseidon-point-of-sale-malware.html), but also CARBANAK and TURLA share these general characteristics.

In the information security sector OSINT is used to gather knowledge of the system under attack (e.g. via google hacking [48] or dumpster diving[18] or extraction of documents metadata[19]). It is a classic method that has been used for a few years now and it could be named "OSINT of classic sources", see Figure 8.
Apart from this, the increased amount of data shared on social networks (see Chapter 3) and the fact the processing it is not complicated have made Social Intelligence[20] and Social Data Mining techniques mainstream.
One of the last additions to the long list of OSINT technologies is the Linked-open-Data, that that is being increasingly used across the web, even vertically for specific web giants (e.g., the Google universe of services) which allows to cross-correlate also other data and enrich the digital footprint and shadow previously defined in this document[21]: large data can be mined for intimidation such as facts of malware, anomaly, or phishing.
As said above, the OSINT could be abused to gather knowledge in the preparation phases of a SE attack, for example, using an aggressive information gathering process. The information could be collected in two ways:

- Actively: Creating of a fake profile on a social network and request friendship to victims in order to access information shared privately
- Passively: Collecting information that has been freely shared across the web and correlating it to different cyber profiles (this operation is called remediation).

[18] Es. http://searchsecurity.techtarget.com/definition/dumpster-diving
[19] Es. OSINT with FOCA 2.6, https://holisticinfosec.org/toolsmith/pdf/march2011.pdf
[20] The term SNA (Social Network Analysis) is also used
[21] For example, an attacker can use the GPS position of posts (e.g., Foursquare) to understand the places visited by the user and cross these information with Google Maps to collect information on victims' real-life contexts.

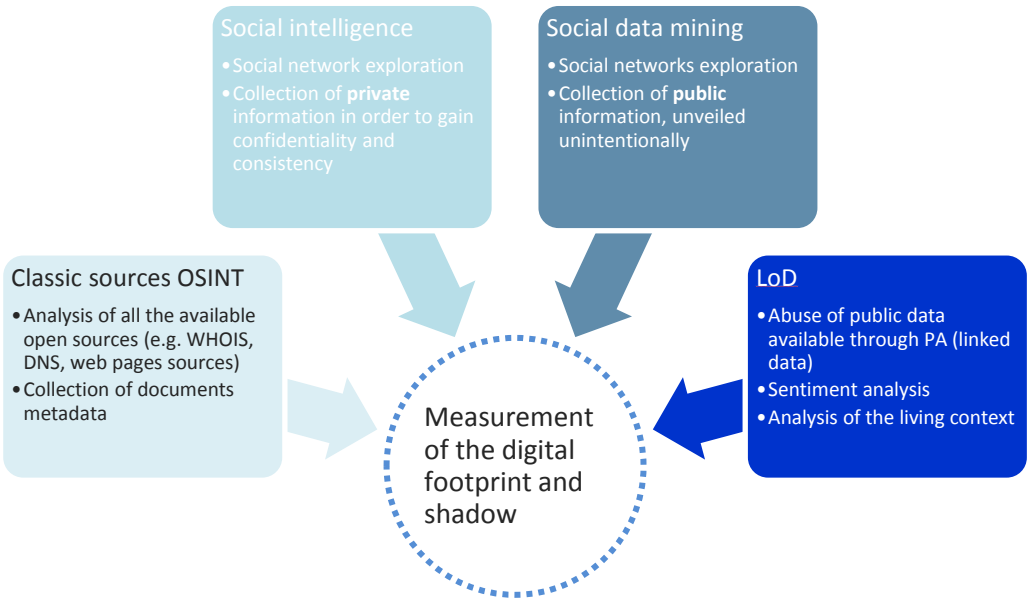


Figure 8 - The role of OSINT in the Social Engineering 2.0

OSINT is one of the most powerful tools used in SE 2.0, it is efficient because of the large amount of data that people voluntarily or inadvertently share on the Internet [49]. This modern tendency to over-share information on the network is one of the most interesting aspects about this topic. Social Network operators incentivize this behaviour because it is beneficial for their marketing strategies (see section 4.4.1 Intelligence or information Gathering)[22].

2.4.3. (Ab)use of psychology, personality profiling systems, cognitive science models and human related sciences

This document defines SE as a set of arts and techniques that can be used to hack humans' OS in order to violate their information space, gain access to some specific assets or facilitate the exploitation of a technical system.

One of the most important areas of improvement is the introduction of advanced psychological methods in the process of an attack. However, extending the concept, if the attacker wants to find ways to exploit the users' brain (e.g., [50]) it could get inspiration from all the sciences listed in Figure 9, which are all human sciences.

Nowadays psychology and cognitive sciences are among the most used, either to improve the defence systems (e.g. behavioural security [51]) or to improve the effectiveness of the

[22] For example refer to the fearless and frictionless sharing of Facebook and the changes in the privacy habits [53][54]

attacks[23]. However, there is still little investigation (in terms of people investigating and money spent) of other sciences in the area of security. These are open questions:

- Which psychological models do hackers of Informative Systems apply to deceive users?
- How much are psychology and cognitive sciences abused to perform modern attacks?
- How do other human sciences contribute to the creation of modern attacks?

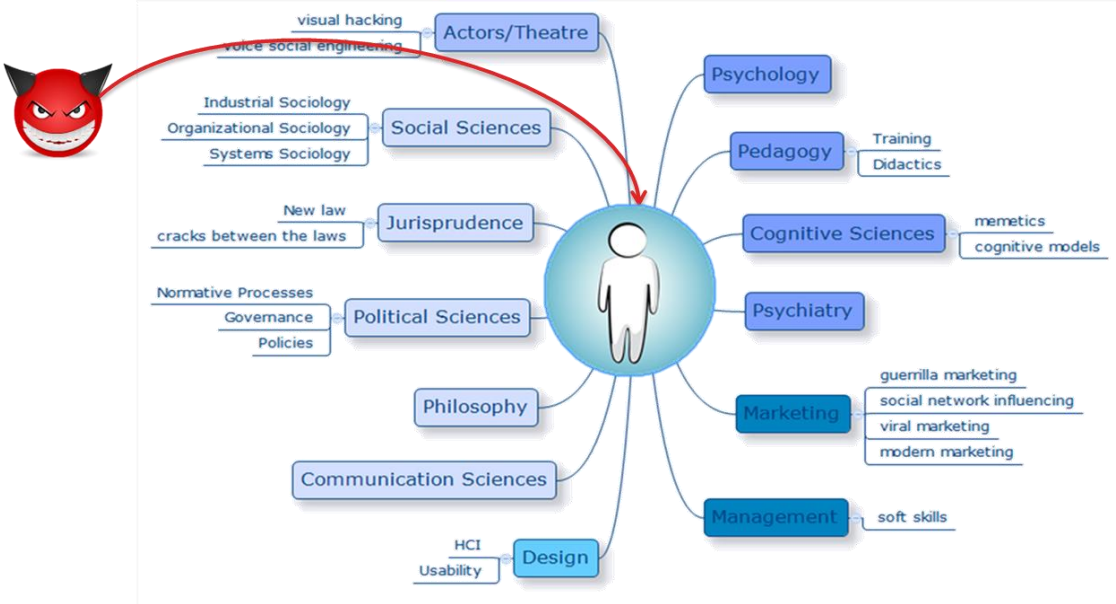


Figure 9 - Hacking the Human OS means to (ab)use all the human related sciences

2.4.4. Evolution of the attack vectors

An attack vector could be defined as the method used to penetrate the trust zone of a user or a technological system in order to gain access to its information space.
An attack vector, at its technical level could be a 0-day bug, at the humans' level it is what in the literature is called a "hook": the element that catches the reader's interest [55][24]. ~~We~~ The concept of an attack vector is generally extended so it includes everything that violates the information space, for example, a phishing email with its attachment or an infected link are all together considered an attack vector.
The following list of attack vectors is sorted from the most challenging (physical presence) to the easier (social networks) to deal with.

1. **The physical presence** is the most complex attack vector, where apart from the hook, the attacker must control all the non-verbal elements (also the unconscious ones): e.g., not revealing their final intentions through non-verbal behaviour.

[23] These same techniques are used also in marketing, the *Behavioral targeting* is a marketing technique where people's online behavior is tracked and the collected information is used to display individually targeted Web advertisements to people [52].
[24] For a better adaptability usually SPAM have a tripartite structure (hook, threat, request)

2. **The voice** is a real-time communication channel through which also some non-verbal behaviour is transmitted (e.g. the tone of the voice, the pronunciation). It requires some specific skills to control them.
3. **The chat and instant messaging systems** are real-time interactive media, but through a virtual channel. The communication channel is controllable and no non-verbal messages are filtered (the attacker's non-verbal behaviour is not communicated).
4. **The email** is not a real-time interactive media; therefore the attacker needs to create the attack completely offline and (try to) convince the victim in "one shot": convince the victim just by looking at the email.
5. **The social network** it is not a real-time media but it allows interaction among users, therefore the hook of the attack can be adjusted according to the victim's reactions. This is typically the easiest attack vector and the most abused today.

2.4.5. Automatic Social Engineering Attacks (ASE)

The diffusion of large amount of machine-readable data via social networks has been the turning point that speeded up the evolution of the automatic social engineering attacks. Chapter 4 will further address this issue; the evolution of ASE is the element that opened the door to mass social engineering. Figure 10 reports the "classic" 6 phases of a social engineering attack, from the initial gathering of information up to the final steal of a valuable asset (see Chapter 5 for further details). The interesting point here is that the phases from 1 to 4 could be often easily[25] automated [39][56][57].

[25] Typically thanks to relatively simple scripts

Figure 10 - The six phases of a typical SE 2.0 attack with evidence of automated steps

(1) **Generic information Gathering**: An example of this phase is the creation of a fake profile in one or more social networks, both for leisure and for business. The profile must be trustworthy and studied starting from a preliminary information collection to increase the likelihood of being accepted by the victim

(2) **Develop all the possible relationships**: This step could be done either automatically or manually, the profile gains new friends (potential victims) aiming at entering the group or gathering further information

(3) **Select victim and target asset**: The profile of the potential victim is based on what the hacker wants to steal (i.e. the attacker needs to find a single person or a recently hired employee, etc.). The phase ends when the goal is achieved (i.e. a good number of potential victims has been achieved)

(4) **Preliminary actions on the selected victim**: The relationship with the chosen victims gets deeper in order to gain the confidence needed and enough reliability to attack

(5) **SE Attack**: A direct attack is launched to the targeted source. The aim is to gain access to a specific asset (i.e. credentials). The methods can be: spear phishing, contextualized phishing or even targeted exploits. This phase needs the specific competence of a social engineer and cannot be automated.

(6) **Asset Stolen**: It is the acquisition of an asset, (i.e., credentials for systems access, digital ID theft) the intrusion into the company's premises or even the acquisition of someone's assets (i.e., withdraw someone else's registered email or cash in a money order)

The possibility of automating these steps is extremely important. The dynamics of modern SE-enabled attacks indicate that a social engineer is directly involved in the execution of almost all the steps of an SE attack compared to how they were performed in the past. Thus, the number of SE attacks were extremely limited, and the targets were carefully selected prior phase 1. Nowadays this is no longer the case.

2.4.6. Economic Drivers

Criminals are obviously focusing on efficiency, rather than complexity. Malware 2.0 and SE 2.0 have become an investment where all attacks have a common goal: making money. This causes a dangerous growth of identity thefts, industrial spying and damages of on-demand systems (Deny-of-Service on demand).
SE 2.0 is effectively integrated into the modern cybercrime economy and it is one of the best instruments available today for attackers. The evolution of SE follows the same path of viruses: they were the passion of a few and now they are a professional tool.
Several economic models have become quite popular in the cybercrime world[26]. However, one aspect that has been increasing in the latest years is the establishment of cooperation among cybercriminals, they use "affiliate programmes" that are some sort of crime-ware-as-a-service approach[27].
As a matter of fact, from the efficiency point of view, it has been said that a targeted attack may bring ten times the revenue of one thousand phishing mails [49][58]. Stories of groups like FIN4[28] or PAWN[29], among others, clearly show how difficult it is to detect these types of attacks and how lucrative they can be. Chapter 4 will dive into these aspects.

3. The importance of the Human Element in Social Engineering 2.0

This chapter aims to argue how nowadays cybercrime is focusing on attacking humans. The evolution of social networks and the fact that people share more and more information about their social lives on the Internet may be the reason that explains this fact.
Social Engineering is not a recent threat: the Institute of Management and Administration (IOMA), in fact, reported that this was the top security threat in 2005. The reasons behind this rising trend are mainly related to the continued improvements in protection against technology-based threats on one hand, and little attention paid to recognize the dangers inherent in human hacking on the other hand [77][78].

---

[26] For example Exploit-as-a-service (https://wkr.io/assets/refs/grier2012compromise.pdf) and Pay-per-install (http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/pay_per_install.pdf)
[27] For example in the area of RaaS (Ramsonware as a Service) http://www.darkreading.com/partner-perspectives/intel/franchising-ransomware/a/d-id/1321148, accessed November 2015.
[28] https://www2.fireeye.com/fin4.html, accessed November 2015
[29] http://www.securityweek.com/operation-pawn-storm-cyber-espionage-campaign-hits-organizations accessed November 2015

As mentioned in chapter 1, information security threats can come from technological vulnerabilities or people's vulnerabilities, the systems to be secured also include the people who use them [71].
People's vulnerability is based primarily on their naivety and lack of cybersecurity knowledge, such as how to use ICT tools in a safe way. Hence, these kind of attacks (e.g. stealing bank codes and passwords) exploit the behaviour habits and trusting nature of users. Nowadays, by focusing on manipulating humans, SE attacks pose the most significant security risks since they are more challenging to detect [74][76][75].
As described in detail in this chapter most popular types of attacks could be split in two main categories:

- *Context Aware Phishing or Spear Phishing*: it consists in a highly-targeted phishing campaign, crafted using collected context information, towards a specific goal.
- *Penetration via Social Networks*: it exploits access to the circle of trust of corporate employees, establishing credible relationships on Social Networks, possibly through a credible fake profile.

This chapter does not concentrate specifically on the ICT improvements that made the information collection easier (improvements of OSINT, big-data collection and semantics for example), but rather on the increased importance that the human element gained in the overall complex scenario of SE today.

3.1. Psychological Foundations of the Social Engineering

As mentioned above, psychology and cognitive science are among the most used ones in Social Engineering attacks. Humans are susceptible to various forms of social influence by nature and, as certain theories explain, sometimes resisting is almost impossible.

The ***Theory of Gullibility***, for example, explains the susceptibility to persuasion as an extension of credulity where the victim has a willingness to believe someone or something even in the total absence of reasonable proof [60].

The ***Theory of Optimistic Bias*** states that people believe that positive events are more likely to occur to them than to other people [61]. The inverse is also true: people believe that negative events are more likely to occur to other people than to themselves.

Optimistic bias together with gullibility implies that people think that they (a) will not be selected as a social engineering target and (b) are more likely to resist than others. Once a person is a target, offenders can use persuasion techniques to change the odds in their favour. The six principles of persuasion (*reciprocity*, *conformity*, *liking*, *scarcity*, *commitment*, and *authority*) and the two kinds of social influence (respectively **Compliance** and **Persuasion**) defined by Cialdini's categorisation [62] can be leveraged to increase the offender's probability of success.

The outcome of a social engineering attack is highly influenced by several factors that can be manipulated by both the target and the offender to obtain a more desirable outcome. The offender may use the knowledge of the principles of persuasion to increase the likelihood of a successful attack while the target can use the knowledge of the social engineering

techniques as a form of defense. Even other factors like the gender, real or presumed, of the target and victim can alter the context, as well as if the social interaction is ***Face-to-Face (FtF)*** or ***Computer-Mediate-Communication (CMC)***.

Social scientists have been studying the impact of Internet on human behavior in several contexts, from long distance relationship building to decision making in computer mediated groups and even online shoppers behavioral patterns. Although Internet is used for plenty of different applications, it remains primarily a tool for communication [59] and it has a huge impact on the nature of our interactions with others. According to researchers [63] there are four novel and important aspects regarding online interactions:

- **Anonymity** – the Internet allows for a general greater anonymity since individuals can choose how much information to disclose in regards of their name, age, appearance, sex and other details. Normally readily visible characteristics are no longer our most salient feature. On the other side, our professional email address or email signature can convey a lot of information like our full name, place of work and other details.
- **Physical appearance** – in a context where the communication is usually text-based, physical appearance naturally loses its importance compared to a classical face-to-face form of communication. This aspect of online interaction is the main force behind the reassuring feeling that we can communicate with others with no concern about different treatment because of our physical appearance.
- **Physical distance** – physical distance disappears and the users are allowed to create bonds with a wider pool of people than before the advent of the Internet. Online communities allow for an easier access to other people with similar interests.
- **Time and place** – communications can be established with a greater control over the time and place where they happen. While empowering and positive, this experience has a negative side as it blurs the line between professional and personal life.

There is also a fifth novel aspect that needs to be considered, the lack of social cues. Face to face human interaction is a rich experience where all five senses are involved, as consequence the message is conveyed not just by words but also by body language and physical appearance factors like clothing, voice tone, etc. This phenomenon could be extended to its pathological consequences just looking at the social withdrawal among young, due to the (ab)use of non-physical forms of communication, which is present in Japan since few years and today appearing also in Europe[30]..
These four, or even five, novelty aspects can affect the human behavior in CMC context. Anonymity, for example, has been related to a decrease in self-focus on internal standards for behavior [64] and is considered one of the reasons behind the increased tendency of engaging in non-normative behavior, such as making offensive and rude statements, in a CMC interaction compared to FtF interactions [65]. It has also been proven that an individual whose nickname denotes the membership to a certain social category is likely to exhibit a behavior

[30] For example see M. Suwa, K. Suzuki, K. Hara, H. Watanabe, and T. Takahashi, "Family features in primary social withdrawal among young adults," Psychiatry and Clinical Neurosciences, vol. 57, no. 6, pp. 586–594, Dec. 2003

consistent to normative expectations for that social category even if the individual does not actually belong to that group at all.

3.2. Evaluation of Social Networks role

The advent of Social Networks (SNs) can be seen as one of the event that most influenced modern society in terms of relationships management among the humans and sharing habits in their digital lives.

Considering them as a cultural phenomenon, social media reshaped the information and communication ecosystem [72]. Online social networking sites are an increasingly popular place for people to interact with families and friends, colleagues, business contacts and even meet new people to share interests, feelings and emotions at any time and remotely [83].

The result of this is that people do not think of the computer as a “Analytical Engine” any longer, but as a “Machine for intimacy” [97].The incredible spread of Social Networks during the last decade has radically changed the way humans communicate.

Users’ information is the most valuable element for SNs providers, since it is fundamental to better profile users or groups for marketing or advertisement purposes [71]. Consequently, SNs providers keep on encouraging users to reveal and share more personal information. It is easy to understand how this information constitutes a “gold mine” for social engineers that are able to exploit news, stories, hyperlinks, photos, videos, and applications [79] shared by users.

As mentioned in Chapter 1 SNs are able to provide machine-readable and classified information, which can enable more contextualized attacks, and “automated social engineering” attacks (see Figure 11)

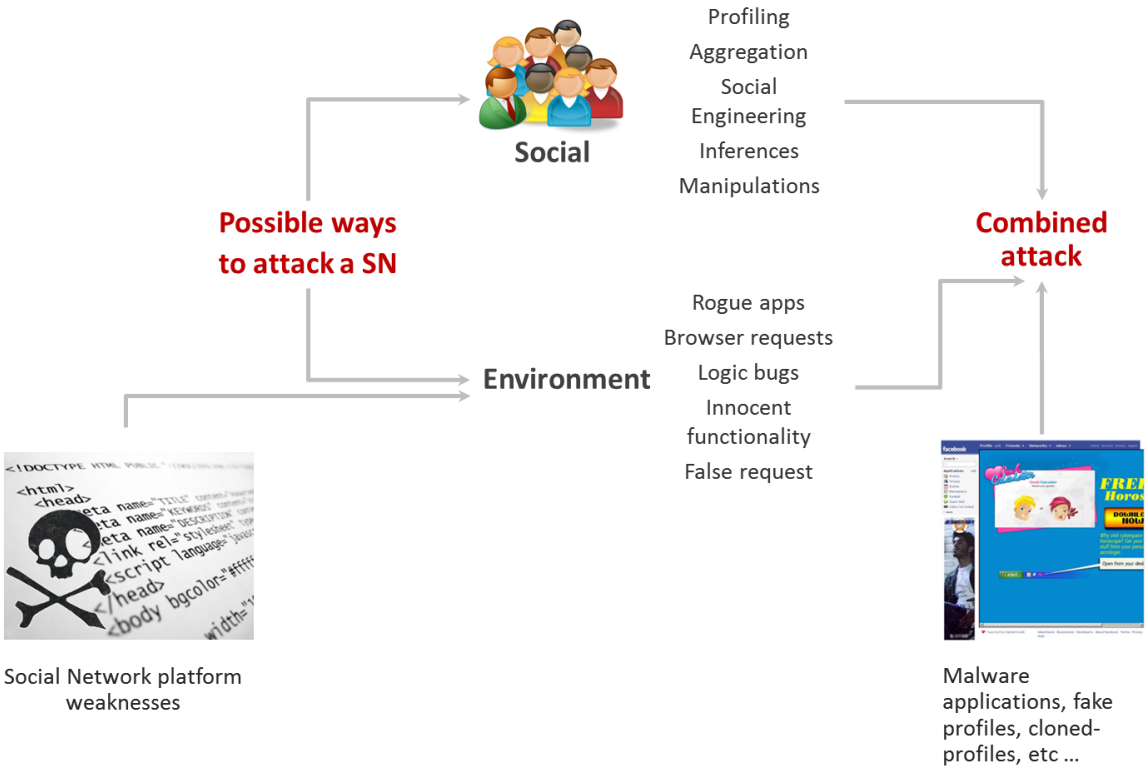


Figure 11 – Automatic Social Engineering Attacks - Attacking the Social Networks

Social networking sites are the main source of social engineering attacks that can be carried in two different ways. The first way involves information gathering about the victims in order to understand their vulnerabilities. This is an important step in order to choose a perfect tactic and develop a good plan [80]. The second way involves reaching the victim: SNs also offer a cheap and effective method for reaching victims and applying effective tricks [82].

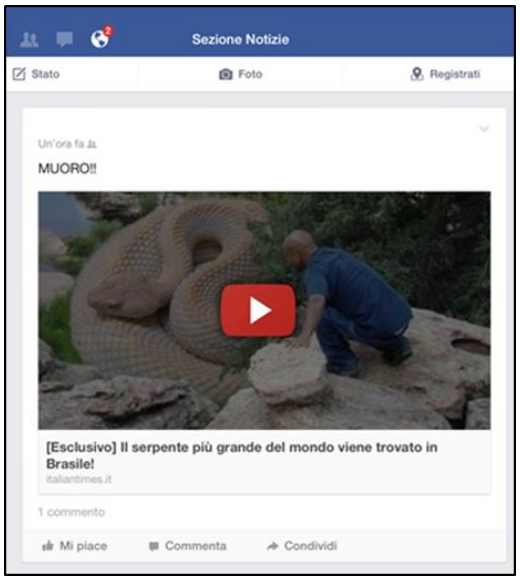


Figure 12 Click-jacking scams uses "Like", "Share" and "Play" buttons on social networking sites

Social networks operations imply specific behavioural and communication paradigms which have great influence in information security field.

The first aspect to be considered is that information access and interaction are based on trust and users generally share a lot of personal information with other users. Even if a user decides not to have a public profile, (in this case the access to it is regulated by a network of trust and the information regarding the person is available only for the user's community), critical issues may raise.

Social networking sites do not provide yet strong authentication mechanisms, and it is easy to pretend to be someone else and sneak into a person's network of trust substituting the original identity with an impersonation attack (e.g., ID theft) [84]. Moreover, it often happens that people, to increase their popularity on the platform, accept any friendship request they receive, exposing personal information to unknown people [85]. This situation alters the base of the Social Network, where the implicit trust is broken by potentially exposing the user and their contacts.

Another important characteristic of social networks are the different levels of awareness about threats that users have. While most users have become aware of the common threats that affect the Internet, such as e-mail spam and phishing, they usually do not show an adequate understanding of the threats hidden in social networks. For example, a previous study showed that 45% of users on a social networking site readily click on links posted by their "friend" accounts, even if they do not know that person in real life Figure 12 [86]. This behaviour might be abused by spammers who want to advertise web sites, and might be particularly harmful to users if spam messages contain links to malicious pages [85].

Referring to what was expressed above, regarding the level of awareness about information security threats, it's worth doing some more general considerations. Another interesting aspect to be considered is the discrepancy existing between online and offline human behaviour. In the "offline dimension" people seem to be quite capable of not subjecting themselves or their property to unnecessary risk, while in the "online dimension" there is an epidemic of poor security-related decisions [68].

The majority of users continuously employ risk analysis heuristics to plan both their online and offline actions. The overwhelming problem of online security is that these analyses are based primarily on entirely wrong assumptions, intuitively derived from incorrect interpretation of GUI elements and processes.

Today's typical computer user actively engages in casual browsing, carrying out financial transactions via Web and email, exchanging documents over email, sending instant messages, and similar activities. Such a user's security situation, however, is nothing somewhat

deplorable. At the heart of the matter are bad trustworthiness decisions. Users' incorrect assumptions about processes involved in computer transactions lead to false or incomplete models of these transactions, which then result in decisions that more informed users would classify as obviously bad [68].

Trust and confidence are a fundamental part of the interactions with any system. This concept will be further discussed in Chapter 7 but at this stage, it is important to underline the importance of trust in the social network as a service in its entirety. The sharing habits of users are a direct consequence of the trust they lend to the SNs. The impact of trust toward the SNs and of course the ways to abuse is an interesting area of investigation [99].

These results suggest that in online interaction, trust is not as necessary when building new relationships as it is in face-to-face encounters. They also show that in an online site, the existence of trust and the willingness to share information do not automatically translate into new social interaction. This study demonstrates that online relationships can be developed in sites where perceived trust and privacy safeguards are weak.

3.3. Evolution of modern workforces

Another important element regarding the role of humans in the information systems is related to the evolution of the workforces, which nowadays affect the way people live.
Among the aspects arising from the wide adoption of the mobile technologies, but more in general, from the diffusion of digital technologies there is the evolution of the workforces. Figure 13 reports a simplified user-centric model of the modern way of working. The schema has four directions surrounding a worker that impact their working habits: Dataspace, Enabling Technologies, Use Cases and Context.
A worker can be defined as a person that owns a Dataspace where all their data are stored. What the worker does is to extend, elaborate and create new elements in this dataspace, even with the collaboration of other workers (shared dataspaces) or objects (internet of things).
A simple definition of a working dataspace is a virtual place where to store and access the data, that could either be strictly personal, shared or both. To access the dataspace, a worker can use several Enabling Technologies with different usability characteristics. Choosing any of these technologies is in general just a matter of usability and easiness for the worker. Nowadays, the market is constantly offering new "methods" to access user's dataspace: Google Glasses are just the newest one, but others are just behind, like for example the expected revolution of the wearable electronic [89][90][91].
A Use Case is the "invariant" portion of this scenario where technologies and social trends do not affect. For example, in a span of several years a user could have written a commercial letter in different ways: using a typewriting machine, a video terminal with a word processor, more recently a tablet or in the future wearable smart glasses that understand speech or thinking [92], but what remains always the same is the way of writing a commercial letter.

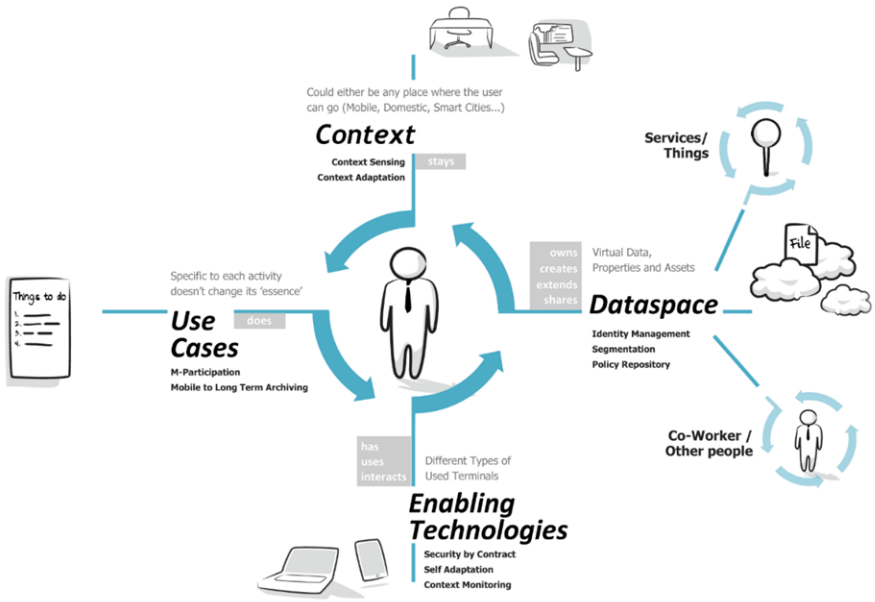


Figure 13 - Schematization of modern mobile work forces (source: CEFRIEL)

The recent global recession directly influences labour market adding new paradigms, more flexibility and more mobility. In the following list, we summarize the concepts that can be considered as key elements of the modern workforces and are expected to influence the development of future scenarios in this area:

- **Mobile devices**: widespread distribution of mobile and wearable devices. Thanks to mobile and ubiquitous terminals, a user could complete a task in any possible place, home, public spaces or company premises.
- **Blending life**: a world where physical and virtual meetings seamlessly merge.
- **Social platforms**: widespread distribution of social networking platforms.
- **Ubiquitous workforces**: solutions that allow users to complete a task in any possible place, home, public spaces or company office.
- **Usability:** characteristic related with user experience and easiness for a worker to access the dataspace through different tools.
- **New data space**: improvement of the traditional personal dataspace, moving towards a complete dematerialization on centralized cloud services.
- **Communication service provider**: availability of large and long bandwidth.

Within this environment, sensing the context of a user becomes important in order to adapt the enabling technologies' usability [72]. The Context helps to define which data of the personal dataspace a user can access, in a specific place: to protect identity, privacy or to respect some security policies.
Nowadays, in order to verify users' identity (and decide whether to grant access or not) machines collect personal data from users accessing to services. Users want to use those

services and therefore are willing to reveal personal data, following a data-for-(free) services logic. At the same time, humans' identity, trust and privacy constraints are not the same for every environment (business identity, cultural identity, administrative identity etc.).
From a technological point of view, it is a digital ecosystem: a community of people who interact, exchange information, combine, evolve in terms of knowledge, skills and contacts, in order to improve their lives and meet their needs.
Among cloud services the concept of federated cloud is emerging, where there are common standards for both hardware and software companies. An important issue emerging from this scenario is the change in trust chains that are growing in number and are influenced by logical and physical contexts. In this kind of environment, the essence of cybercrime is to abuse the trust chains to steal assets. Hence, changes in trust models and importance of assets implies changes in cybercrime.
Starting from assertions made so far, going further into detail and based on different studies on the topic, it is easy to speculate on the trend of workforces' evolution in terms of cybersecurity.
According to a McAfee Labs' five-year look ahead [95], the predictions on how the types of threat actors will change and how the industry will meet these challenges over the next five years could be briefly summarized as follows:

- **Below-the-OS attacks**: applications and operating systems are hardened against conventional attacks so attackers could look for weaknesses in firmware and hardware. The consequence could be a broad control performed by the attackers.
- **Detection evasion**: it means the attackers' attitude in trying to avoid detection targeting new surfaces and using sophisticated attack methods and actively evading security technology. Difficult-to-detect attack styles will include fileless threats[31], encrypted infiltrations, sandbox evasion malware, exploits of remote shell and remote control protocols.
- **New devices, new attack surfaces:** when IoT and wearable will reach a significant level of market penetration, also the necessity to have user safety guidance and precise industry best practices in order to accomplish appropriate information security needs for the devices will arise.
- **Cyberespionage goes corporate:** the dark market for malware code and hacking services could train cyberespionage malware used in the public sector and corporate attacks to be used for financial intelligence-gathering.
- **Privacy challenges, opportunities**: we will assist to the increase of volume and value of personal digital data. The availability of this amount of extremely attractive data (in cybercriminals perspective) will likely promote the development of new privacy regulations around the world. Concurrently, individuals will seek and receive compensation for sharing their data.
- **Security industry response.** The security industry will develop more effective tools to detect and correct sophisticated attacks. Behavioural analytics could be used to detect

[31] For example look the following report "McAfee labs threats report," McAfee, Nov. 2015. [Online]. Available: http://www.mcafee.com/kr/resources/reports/rp-quarterly-threats-nov-2015.pdf. Accessed: Feb. 1, 2016.

irregular user activities that could indicate compromised accounts. Shared threat intelligence is likely to deliver faster and better protection of systems. Cloud-integrated security could improve visibility and control. Finally, automated detection and correction technology promises to protect enterprises from the most common attacks, allowing IT security staff to focus on the most critical security incidents.

3.4. Why people share: towards a fearless and frictionless sharing world

In this paragraph, considerations concerning content sharing on social media are provided in order to investigate the main reasons leading people to share information online. It is a state-of-art requirement to describe current trends and set the correct pointers.
Each year the number of people "addicted to Internet" grows. People store important data in their phones, as well as access social media and Internet bank information from their mobile devices. The downside to this is that many of users neglect security of these devices.
Kaspersky Lab has conducted a research and found out that more than a half of respondents do not use remote block or find-my-device features. Only a quarter of respondents behave carefully when connected to a public Wi-Fi. About a third of the people surveyed take their phones to bathrooms, and even go to bed with their smartphone [101].
According to a recent New York Times three-phase research initiative [66] technology has enabled consumers to share more contents with more people more often, and the willingness to share and the enjoyment of sharing are also increasing. When consumers encounter great content – useful, enlightening or simply entertaining – they feel an instinctive need to share it, as sharing is considered half the fun of finding information, therefore is right to say that online sharing is changing the way humans process and manage information.
According to the study mentioned above, 73% of respondents assert that they process information more thoroughly as a result of sharing it with others. The reasons for sharing can be divided into the following categories [66]:

- Interesting information: bring valuable and entertaining information into the dimensions of people they care about in order to improve their lives.
- Self-definition: many people share information on SN's to define themselves to others. They consider sharing as a help to cultivate an idealized online persona.
- Growing and nourishing relationships: sharing maintains other users connected, strengthens relationships and potentially create new connections.
- Self-fulfilment: Users have satisfaction from bringing valuable information into the lives of people they care. Moreover, they enjoy getting credit for doing so.
- Sharing information about causes that they believe in because they think is a way to support them.

All these motivations for sharing have one thing in common, the relationships consumers have with one another. Even more self-directed motivations, such as self-fulfilment and identity, are ultimately defined in relationship to others.
When talking about new habits and trends concerning the propensity for sharing online contents, it's worth reporting some interesting considerations about the so-called "Millennials" generations depth in the article of Steinmetz, *'Help! My Parents are Millennials'*

[67]. Millennials generation is defined as the one composed by those 20- and 30-somethings born from the late ’70s to the late ’90s. This growing cohort of parents is digitally native, ethnically diverse, late-marrying and less bound by traditional gender roles than any generation [67]. Many of the Millennials entered the job market during one of the worst economic downturns in modern history. This factor has surely contributed in shaping a culture where everyone is expected to be on all the time— for their bosses, co-workers, family and friends. Social-media platforms have also become places where it is acceptable to “brag”, as parents have done since they had kids to brag. Indeed, every post or tweet invites opinions on one’s choices from the typical millennial’s network of 500 Facebook friends (at least half of whom are likely to be loose acquaintances). Moreover, the pseudo anonymity that people feel behind a keyboard can lead them to make comments online that they’d never make to another parent’s face [2].

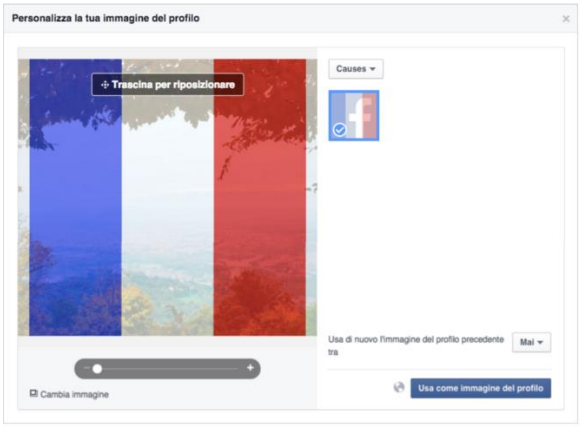


Figure 14 – Following the terrorist attacks in Paris, Facebook has enabled the option to change profile photo applying the colors of the French flag. The phenomena became viral in few hours.

Concerning what has been discussed so far dealing with the reason why people share, it seemed appropriate to mention a phenomenon happened in social networks after the recent terrorism happenings that took place in France. As the tragic events started to have a certain resonance on social media, a sudden transformation of Facebook homepages could be observed. Many users decided to express their solidarity applying the background of the French flag to their profile picture using a special feature provided by Facebook [100] (see Figure 14). Since social media users feel closer to the victims of attacks even very far from them, more if compared to what happened before Facebook which makes it very easy to get in the shoes of the victims. Understandably, these expressions of solidarity were also a source of much criticism especially if considered as a perfect example of a psychological mechanism that combines empathy with narcissism [100]. *"There is a principle of psychology that explains that people huddle together when they have a common enemy and the world feels rightly united against terrorism,"* said Karen North, professor of communication and social media expert at the University of Southern California. *“So, every tragedy of our time, people are looking for ways to express their solidarity and often do so through hashtags and memes. But this psychological mechanism is not the only one to have played a role, explains North: there is also the principle called "self-presentation". "People are motivated to control and shape their public image. These events provide an opportunity to present themselves as "good" and informed "*. This case is mentioned because it clearly show how much time and energy is spent today to shape ones personal digital image, and how many things about lives it can reveal.

3.4.1. The young generations

The aim of this sub section is to address some initial thoughts on the influence of the new sharing habits of younger generations, which will become workers in the near future.
As mentioned in 2.3, the widespread use of smartphones in recent years has radically changed the way people approach to mobile devices. Today, especially for youth generations, they are seen as a key enabler for a broad range of social communications that were not provided until a few years ago. The importance of mobile phones for young people as the device with a continuous network connectivity, raises key issues of risk-taking behaviours in the form of privacy concerns and lack of awareness towards data security implications associated with mobile phones.
The research '*Young People and Smart Phones: An Empirical Study on Information Security*' [69], which concerns students from four UK universities, has shown that there were significant differences in the perception on mobile phone data security among young people depending on different factors. Results from comparative analysis indicated that IT literacy is the variable that most influences the approach to mobile risk among young people. It was found that those who are more concerned about the threats on their mobile phone security were more expert in information technology, less likely to allow applications to access their personal details and more regular in using password security measures on mobile phones. Therefore, those who are less IT literate tend to be more likely to use their mobile phone for activities such as shop online, connect to free Wi-Fi in public areas with their mobile devices allowing applications to access their private information. In terms of gender differences, it has been found that young men are more likely to behave this way than young women.
Beyond how they are accessed, Social Networks and their use is another topic to be deepened when considering young generations and their communication habits. While in the 1990s, young people interested in computers were just a small niche of individuals who shared idiosyncratic interests that were typically born from dissatisfaction with their local community, today things have completely changed.
Nowadays, teens are attracted to social media like Facebook and Twitter or mobile technologies for entirely different reasons. Unlike the previous generations called "early adopters" who avoided the local community by hanging out in chatrooms and bulletin boards, most teenagers now go online to connect to the people in their community. Their online participation is not eccentric; it is entirely normal, even expected [72] so it is right to say that SN's play a crucial role in the lives of networked teens.
According to Danah Boyd point of view in her book "It's complicated" [72], young people today look for public spaces to hang out and express themselves and, since traditional public places such as parks, squares and malls are more regulated and controlled than before, they flock to SN's.
The consumption of digital contents among teenagers has reached very high levels, they do many types of activities, from passive to interactive consumption and content creation, during the time they interact with digital devices. According to a new report from group Common Sense Media [96],
For tweens (those between the ages of 8 and 12), tablets are more popular, with 53 percent of respondents in this age group owning their own device. However, it is also found that both

tweens and teens, are most familiar with passive consumption of media, performing activities like listening to music, watching videos, watching TV, or reading. Slightly less popular are activities like browsing the Web, playing games, or even chatting online [96].
Among the most interesting topics to be discussed about the use of SNs by the younger generations, it is necessary to mention the so-called FOMO, the “Fear of Missing Out”. It means the fear of being excluded from the group of friends and the events that are shared. A recently published English article [97] defines that it as the new "disease" that has been identified in the groups of teenagers. The phenomenon refers to anxiety induced in those who frequent social networks, to be traced and connected 24x7 hours a week, always waiting for the revelatory share or the news that changes the day. The person with FOMO, first suffers the intrusiveness of information overload, then is transferred to a step of addiction and finally becomes in a certain way “dependent” on the virtual dimension.
Another aspect that is worth to focus when talking about the relationship existing between new generations and social media is the evolution of the privacy concept. Always referring to the optimistic interpretation that Danah Boyd expresses in “It’s complicated”: the teenagers are not merely passive consumers, but are cultural creators with a good control of the script of their lives and their experiences in the digital world.
Teenagers develop innovative strategies to achieve privacy, instead of acting by limiting the visibility of some content, they develop other strategies to obtain it in public. Danah Boyd uses the example of "social steganography", a sort of interpersonal encryption, which encrypt the guys creatively their messages public sharing a secret grammar to hide private communications. In other words, rather than seeking privacy by controlling access to content, many teens do that by controlling access to the meaning of what they decide to share.

3.5. The progressive disappearance of the enterprise’s trust zones

The context described in the current document shows that nowadays the traditional concept of a corporate trust zone does no longer exist. While in the past it was relatively easy to separate “personal” and “corporate” information space, nowadays there is an overlap between these two spheres. The continuous evolution of tools and services, indeed, enabled access to corporate information systems from almost everywhere (and not more limited to the internal perimeter), through different devices that are always less owned by the company itself. This is a problem from an information security point of view, mainly because the risk mitigation processes and techniques may not be so effective outside the company perimeter and because users have lack of knowledge regarding how to secure tnheir devices.
Moreover, this context is going to expand again, enabled from a multitude of new technologies such as IoT and wearable devices. The adoption of such technologies will probably enable new scenarios [70], which will improve work procedures, but will also introduce new risks and vulnerabilities [102].

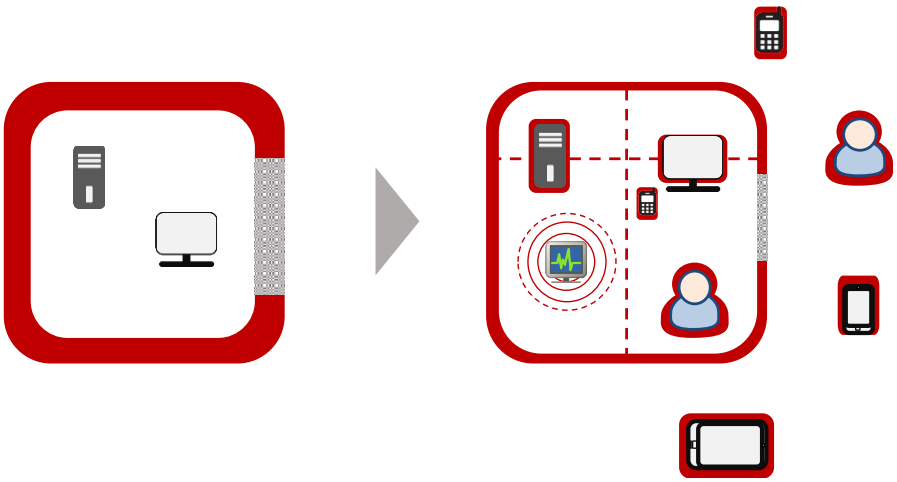


Figure 15 – Evolution of Enterprise Trust Zone.

Figure 15 shows the evolution of Enterprise Trust Zone. In the past, enterprise Trust zone consisted of the internal network, which was separated from the public Internet through firewalls or other security components, such as antivirus (AV) and anti-spam (AS) filters, intrusion prevention systems (IPSs) or intrusion detection systems (IDSs). The resulting internal perimeter is the user trusted zone, where enterprise assets located inside are considered completely safe from any untrusted access and the security is provided as a hidden layer by IT departments.

This approach gradually evolved following technology evolution including themes as improved connectivity, bring your own device (BYOD) cloud based services and Internet of Things (IoT). Therefore, it is necessary to redefine the perimeter, which is no more limited to a central location any longer, but it is totally decentralized and might include different kind of devices out of the enterprise's control and from the traditional perimeter. Enterprises are implementing new security mechanisms, which most of time consist in embedding specific controls aimed at protecting corporate information into the devices, but the scope is now totally decentralized and might include different kinds of devices out of the enterprise's control and from the traditional perimeter

The disappearance of the Trust Zones introduces some weaknesses, exposing enterprises to a new series of threats. Perimeter break-ins are diminished, because, from an attacker's perspective it is enough to obtain access to one of the devices or services outside the perimeter, which might be successfully targeted.

In modern Advanced Persistent Threat schema, it is enough to establish remote access to corporate network through any of the connected devices, in order to allow exfiltration of critical information.

In this threat scenario, social engineering is one of the most used attack vector, since users play an important role in contributing to maintain a correct security posture where technological countermeasures could not be effective. Anyway, from the user perspective, it has become much more difficult to understand the impact of these threats, thus it is required to extend existing security audits and controls in order to consider and manage also this kind of risk.

4. Social Engineering within the modern Cybercrime

Recent developments in the cybercrime trade have brought several major innovations that transformed the ecosystem in which computer crimes are planned, executed and exploited. Whereas past activities in the field were mainly the result of the efforts of technically skilled individuals seeking personal revenue, current trends suggest the existence of a decentralized, diverse system in which multiple actors contribute to the underground economy[32]. Each bringing value either in the form of experience and skills, or resources which can be shared and exchanged for services making use of dedicated and well-known communication channels.

Therefore, most modern cybercrime activities are the result of coordinated efforts, emerging from multiple interests and yielding numerous profit sources [103][104][114].

4.1. Services available on the black market

In this heterogeneous context, the traditional figure of the lone hacker has been replaced by an industry that offers illegal activities as services [116], some of which are briefly listed in Table 1

Table 1 - a short list of most common cybercrime services offered in the black market (Source [116])

Cybercrime Services			
Research	Crimeware	Cybercrime Infrastructures	Hacking Services
• Vulnerability discovery • Exploits brokerage • Selling of emails' address list	• Professional services (e.g. malware outsourcing) • Malware services (Trojans, Rootkits, Ransomware) • Exploit Services	• Botnets • Bulletproof Hosting • Spam Services	• Password Cracking • Denial of Service • Financial Information

This business model is guided by Economic Drivers: "customers" requests and needs have also radically changed and shaped the kind of services offered. Modern variants of malware (the so called Malware 2.0, see section 2.4.1) are often specially-crafted and chosen for the particular aim of the plan being carried out as explained in section 2.4.1 of this document. Just like vendors of legitimate software, programmers working in this field set fees for the production, rental and sale of these commodities, and provide their customers with technical support and updates [104].
Everything on this market has, of course, a price: Zero-Days[33], email Databases, DDos Attacks, Crypters, VPN services (see, for instance [120]) like shown in Figure 16.

32 "Cybercrime as a business: The digital underground economy",*Europol*, http://mcaf.ee/5hykf4
33"Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits", *Forbes*, http://mcaf.ee/jknoe

ADOBE READER	$5,000-$30,000
MAC OSX	$20,000-$50,000
ANDROID	$30,000-$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000-$100,000
MICROSOFT WORD	$50,000-$100,000
WINDOWS	$60,000-$120,000
FIREFOX OR SAFARI	$60,000-$150,000
CHROME OR INTERNET EXPLORER	$80,000-$200,000
IOS	$100,000-$250,000

Figure 16 – Left : Zero Days Exploits Pricelist (Source: Forbes). Right: Florida residents emails for sale. (Source: McAfee [116])

Among the different kinds of actors that are part of this complex system there is also room for those interested in providing simple human labour which can be exploited in those fields in which automatic and electronic systems are still lacking, for example in the case of farms of CAPTCHA's solvers [129]. Despite common belief, these actors do not really need to resort to digital and crypto currencies, as most transactions can easily be processed via regular credit card circuits, see Figure 17.

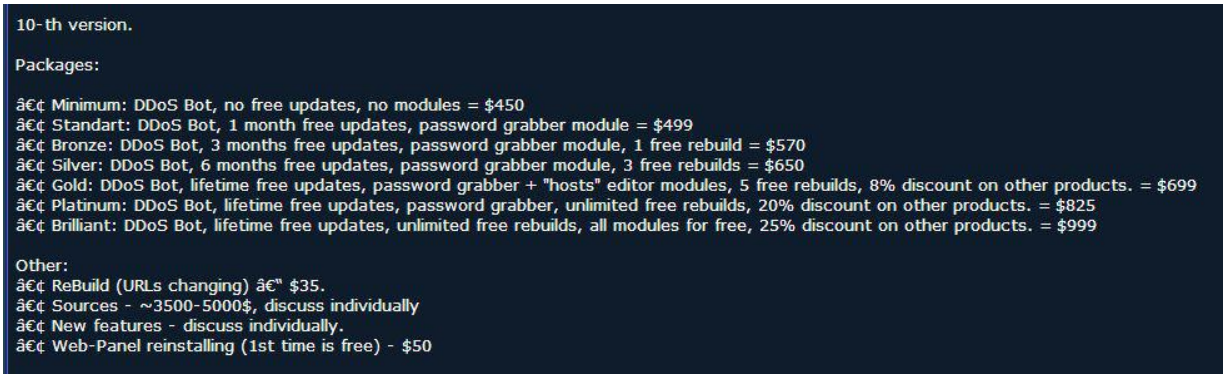


Figure 17 - Example of botnet facilities offered on the black market. Source: McAfee [14].

This scenario clearly shows that, while technically proficient individuals contribute to this economy, relentlessly feeding the underground market with more sophisticated facilities and innovative malicious software, they are not the sole recipients of the advantages and profits. The evolution of the cybercrime industry made this process attractive for new actors willing to leverage these commodities. It is thus necessary, when attempting to give an accurate picture of the current status of cybercrime, to classify as cybercriminals figures and groups belonging to more traditional and well-known crime fields, such as financial fraudsters, terrorist groups, industrial espionage agents, drug dealers.

The lack of know-how or technical skills are not an obstacle anymore. Everybody can enter the cybercrime trade adding assets to the market value-chain (e.g., selling of financial assets, lucrative targets, renting or selling whichever service, skill or intelligence). This makes the cybercrime economy extremely diversified and thriving: numerous specialized, geographically-distributed actors, each contributing to the system's value-chain, bring in new

ideas and new means of profit in an attempt to monetize whatever intelligence they can gather and the skills needed to obtain it. Novelty is an extremely important factor in determining its value for the other participants: nothing limits or specifies what may or may not be considered valuable, and therefore advertised and put on sale to pursue criminal activities.

The overall model, which is quite well organized, has been recently analysed within a number of different research papers, tech reports, and books [103][104][114][117]. We report here, in Figure 18 and in the following text, an example taken from [114].

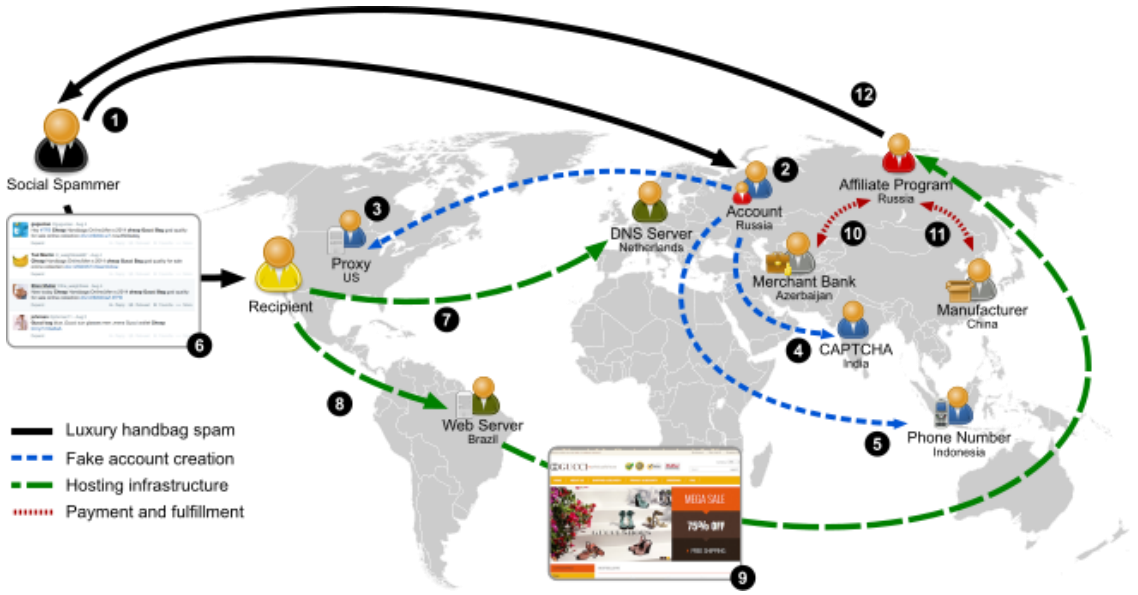


Figure 18 – Specialized roles in the underground economy that underpin extracting wealth from victims. This represents just a single abuse monetization value chain to serve as a motivating example.

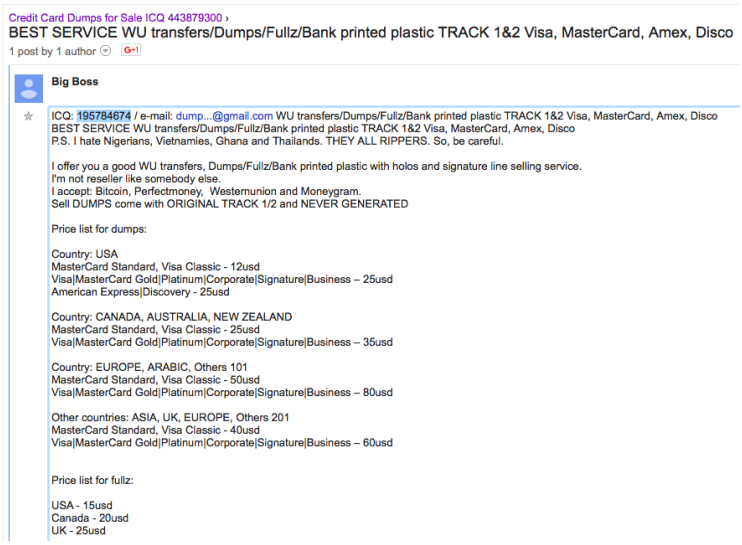
An example of a complex value chain capturing the flow of capital between actors in the black market in Figure 18 where a spammer seeks to monetize user interest in trademarked products on Twitter by selling knock-off replica handbags (1).The spammer first requires a multitude of fake accounts to post messages, in order to engage with Twitter users. This is satisfied by a subset of the underground that coordinates all the components required to bulk register accounts in return for a fee (2), including paying parties with access to dynamic proxy infrastructures to evade IP blacklisting (3), human workers solving CAPTCHAs (4) and SMS verification challenge farms reliant on foreign SIMs (5). With the accounts in hand, the spammer posts links to Twitter, which ultimately land in a legitimate user's timeline (6). When the victim clicks on the URL, an entirely independent set of components is required to provide domain resolution (7) and Internet hosting (8). In turn, the victim is handed off to an affiliate program (9) that handles order placement, including processing the victim's credit card for payment (10) and coordinating delivery from illegal manufacturers (11). Ultimately, the spammer receives a cut of this sale from the affiliate program (12), while the victim receives the intended replica handbag.

Probably one of the best synthetic definitions of the modern black market comes still from paper [114]: *the underground economy is a loose federation of specialists selling capabilities, services, and resources explicitly tailored to abuse ecosystem*. However, like any system based on transitive trust, the ecosystem is vulnerable to infiltration and Sybil collusion. In response, underground markets have become increasingly insular.

4.2. Social Engineering in the underground economy

In a criminal ecosystem, so well diversified and driven by the goals set by non-technical entrepreneurs, the process of intelligence gathering becomes focused. What actually matters nowadays is to set up an attack based on quality and not quantity [115], as an example a huge database dump is not anymore useful to create an efficient phishing, if few key pieces of information are enough. There is clearly some kind of asymmetry between the dark market value of information versus the value perceived by the victims. One of the biggest examples of this asymmetry is the common misunderstanding that, contrary to common belief, the human factor is one of the most profitable targets.

The SE enlarged then the context of cybercrime-as-a-service because competences commonly associated with other, seemingly unsophisticated types of crimes and frauds have been able to enter the cybercrime market successfully with specific skills. Either resorting to direct interpersonal contact when needed, making use of the capabilities offered by the tools supplied by hackers, or even silently and passively exploiting common, publicly accessible data repositories and services.


Credit Card Dumps for Sale ICQ 443879300 ›
BEST SERVICE WU transfers/Dumps/Fullz/Bank printed plastic TRACK 1&2 Visa, MasterCard, Amex, Disco
1 post by 1 author

Big Boss

ICQ: 195784674 / e-mail: dump...@gmail.com WU transfers/Dumps/Fullz/Bank printed plastic TRACK 1&2 Visa, MasterCard, Amex, Disco
BEST SERVICE WU transfers/Dumps/Fullz/Bank printed plastic TRACK 1&2 Visa, MasterCard, Amex, Disco
P.S. I hate Nigerians, Vietnamies, Ghana and Thailands. THEY ALL RIPPERS. So, be careful.

I offer you a good WU transfers, Dumps/Fullz/Bank printed plastic with holos and signature line selling service.
I'm not reseller like somebody else.
I accept: Bitcoin, Perfectmoney, Westernunion and Moneygram.
Sell DUMPS come with ORIGINAL TRACK 1/2 and NEVER GENERATED

Price list for dumps:

Country: USA
MasterCard Standard, Visa Classic - 12usd
Visa|MasterCard Gold|Platinum|Corporate|Signature|Business – 25usd
American Express|Discovery - 25usd

Country: CANADA, AUSTRALIA, NEW ZEALAND
MasterCard Standard, Visa Classic - 25usd
Visa|MasterCard Gold|Platinum|Corporate|Signature|Business – 35usd

Country: EUROPE, ARABIC, Others 101
MasterCard Standard, Visa Classic - 50usd
Visa|MasterCard Gold|Platinum|Corporate|Signature|Business – 80usd

Other countries: ASIA, UK, EUROPE, Others 201
MasterCard Standard, Visa Classic - 40usd
Visa|MasterCard Gold|Platinum|Corporate|Signature|Business – 60usd

Price list for fullz:

USA - 15usd
Canada - 20usd
UK - 25usd

Figure 19 – A credit card dump seller advertising his ICQ account on Google Groups. ICQ is a well-known platform among the sellers and buyers of stolen credit cards. Sellers usually accept either payments with money transfers or bitcoin.

What makes a social engineer's skills so profitable for the black industry is the change in the scope of the adopted strategies: from the traditional cybercrime activities, which are directionless, targeting extremely large and nondescript groups of people, to new carefully focused attacks. Even an attack brought on a large corporation might be accomplished targeting only a small group of individuals, or even a single persons[34,35].

[34] "CARBANAK APT: The Great Bank Robbery", *Kaspersky Lab*, http://mcaf.ee/fg6bes
[35] "The Interview: A guide to the cyber attack on Hollywood", *BBC News*, http://mcaf.ee/7hrl6y

Some data of high importance for attackers can often be disclosed on company websites and on employee profile pages. Management and personnel at all levels of an organization typically present themselves stating their abilities, their roles within the organization, the areas, facilities and data they have access to without realizing that all of it could serve as a foothold for the criminal looking for clues about the direction its efforts should take. This problem goes generally under the definition of "**unintentional insider threat**" [128]. This type of disclosure not only happens through company websites but also through link to external pages published by associates, collaborators and partner companies or even employees' social network profiles.

4.3. A data driven economy

It seems clear that more and more cybercriminals make money from the data harvested from people. "*The Hidden Data Economy*" report [115], recently published by Intel Security, identifies four kinds of "profitable" data:

- Financial Data. The headlines are still dominated by data breaches involving the theft of financial data, particularly payment card information. Credit cards and bank accounts are priced on the black market based on the amount of information provided (Figure 20) or the country of issue[36].
- Login Access to systems within organizations' trusted networks. Login access refers to systems within organizations' trusted networks. Depending on the systems, the types of entry vary, from very simple direct access (such as login credentials) to those exploitable with specific competence (such as vulnerabilities).
- Access to Online Services, including music, videos, loyalty programs, and others. Stolen credentials could be used to access assets which are sold separately[37]
- Identities. Identity theft refers to either physical (e.g. Passports, Social Security Numbers, Healthcare records) or the digital identities. Depending on where the data was stealed, the stolen data is shared without cost in a moment[38]. As a recent example of this, the collective Rex Mundi Hackers has for instance revealed private customer information to punish a medical company (Labio) for not paying a ransom of € 20,000[39]

[36] For the sake of clarity, it is worth to remark that cards provided with "*Fullzinfo*" are those where the seller supplies all of the details about the card and its owner, such as full name, billing address, payment card number, expiration date, PIN number, social security number, mother's maiden name, date of birth, and CVV2.
[37] An example is the fappening exploit "I explored the dark side of the network behind the nude celebrities hack" *The Guardian*, http://mcaf.ee/34hrez
[38] An example is the Ashley Madison data breach "The Ashley Madison Hack -- A Timeline", http://mcaf.ee/sb0rxv
[39] "As threatened, Rex Mundi dumps Labio patients' diagnostic test results", http://mcaf.ee/oke9ia

Payment Card Number With CVV2	United States	United Kingdom	Canada	Australia	European Union
Software-generated	$5–$8	$20–$25	$20–$25	$21–$25	$25–$30
With Bank ID Number	$15	$25	$25	$25	$30
With Date of Birth	$15	$30	$30	$30	$35
With Fullzinfo	$30	$35	$40	$40	$45

Figure 20 – Estimated per card prices, in US$, for stolen payment card data (Visa, Mastercard, Amex, Discover). Source: Intel Security [13].

4.4. A taxonomy of the Social Engineering Attack Techniques: Yesterday and Today

Greitzer [118] Social Engineering taxonomy reported in Figure 21 highlights in grey, which are the most profitable techniques for the modern cybercrime. Despite simple is a good model to frame some of the most interesting techniques of SE[40].

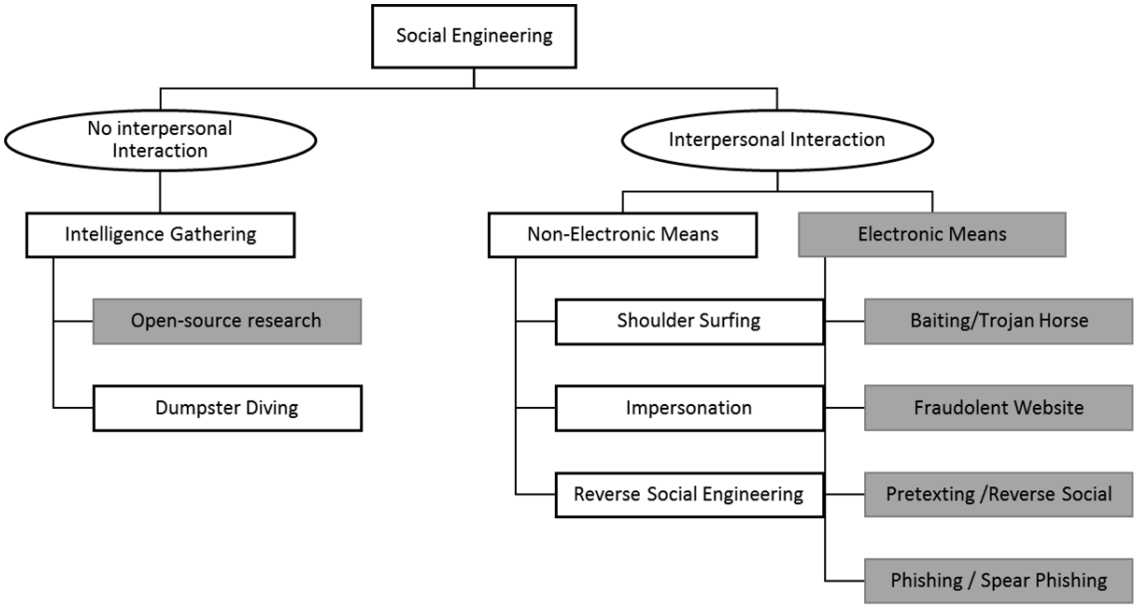


Figure 21 – Social Engineering Taxonomy proposed by Greitzer et. Al.[16]. Grey boxes highlight elements relevant to the modern cybercrime.

[40] Due to its importance for DOGANA, Phishing is managed with a section on its own

4.4.1. Intelligence or information Gathering

Automatic **Intelligence Gathering**[41] has been already introduced in section 2.4.2. Most common tools that can be used to perform the gathering are the search engines that allow to perform very powerful searches, even focused only on a certain website or single data type. There are online databases of predefined queries to use on Google to find vulnerable servers, unprotected storage repositories[42], or also reverse image searches. Beside generalist search engines, services as SHODAN[43] allows searching specific information such as the SNMP manifests of networked devices. Additionally, a typical process is to use personal bits of information leaked on the web (e.g., pictures of the profiles) as keys to discover more details (e.g., one tool that does this service is *Maltego*[44]).

4.4.2. Baiting and Trojan Horses

Baiting[45] **and Trojan Horses** are examples of malware, which is SE-enabled (see section 2.4.1, Malware Ecosystem 2.0). This means that it is not able to infect a system on its own, like the viruses do, but includes in its attack strategy the "cooperation" of the victim (e.g., who click on a link or executes an attachment or even uses an USB-key).

As described in section 2.4.1, a known vulnerability in a web browser's multimedia plugin coupled with a well-crafted viral video guarantees a huge number of infected devices in minutes. Carberp, Citadel, SpyEye, and especially Zeus[46] are a well-known example of such piece of malware.

Mobile platforms with their sudden rise as primary, or even sole, access points to the web are as well an interesting target for malicious software. Their highly-diversified software ecosystem, made of a plethora of operating systems and apps, makes it very difficult, if not totally impossible, to protect them against attacks. Repackaged applications [119], distributed along third party marketplaces are very often trojanized and implement data theft functionalities.

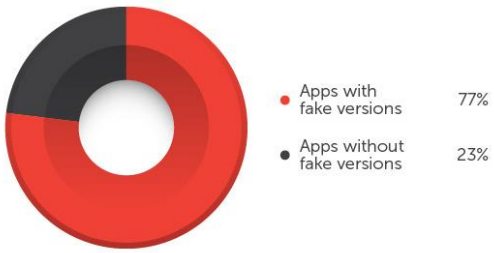


Figure 22 - Breakdown of free apps available in Google Play with and without fake versions. Source: Trend Micro.

[41] The term "Open Source Intelligence" is usually used to refer to the intelligence, which can be gathered from publicly available sources.
[42] Es. "Google Hacking for Penetration Testers", *Black Hat Europe*, http://mcaf.ee/lbz5tu
[43] https://www.shodan.io
[44] https://www.paterva.com/web6/products/maltego.php
[45] Also called piggyback
[46] http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-repackaged-apps-and-its-role-in-the-mobile-threat-landscape/.com/the-big-four-banking-trojans/2956/

A 2014 Trend Micro study estimates that about 77% of the free applications available in the Google Play Store have a fake version distributed in third party marketplaces[47], see Figure 22. Simple and new attack vectors are discovered like, for example, the QR code: a matrix barcode whose original purpose of directing the user's device to a predefined URL or content has been hijacked and turned into a way of delivering malware[48].

4.4.3. Fraudulent Websites

The typical resources for a phishing attack are a shared web host owned by the phisher, a legitimate website in which some phishing content is uploaded, or a number of infected end-user workstations in a botnet [112].
Today most of the phishing sites are created with ad-hoc toolkits, which require only indicating the legitimate webpage to copycat and where to direct the stolen data. Fake sites are usually hosted on free web space or compromised machine (e.g., defaced vulnerable real sites). The new domains involved often use typosquatting[49] i.e., sound domains created to increase the likelihood of the site (e.g., something not easily associated to a common spam site). The most innovative approach is anyway through the "fast-flux" networks, i.e., a network where the IP address are rapidly reassigned to other customers as fast as they are released. This affects the blacklisting and/or taking down of offending sites, but also the possibility to backtrack attack sources for forensics means [110].

4.4.4. Pretexting and Reverse Social Engineering

Pretexting techniques allow exploiting early intelligence gathered about a targeted individual to set up a scenario in which the attacker appears to know enough information to be deemed trustworthy, so that the victim may easily and even spontaneously decide to disclose details about sensitive data.
Reverse Social Engineering is just a special case of pretexting, in which the attacker manages to create (through advertising) an environment in which the victim believes the attacker can help solve a problem and can be fully trusted not to reveal the required sensitive information. Typical cases are offers to assist in preventing or addressing outside attacks, solving bank account problems, or supporting system operations.

4.5. Phishing

Phishing is commonly considered as a type of technology-based SE attack [112][127], which exploits "the weakness found in system processes as caused by system users" [10], and in particular the vulnerabilities of human intellect [132]. Although different definitions exist in literature, phishing can be broadly defined as "a type of computer attack that communicates socially engineered messages to humans via electronic communication channels in order to persuade them to perform certain actions for the attacker's benefit" [112].

---

[47] http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-repackaged-apps-and-its-role-in-the-mobile-threat-landscape/
48 http://resources.infosecinstitute.com/security-attacks-via-malicious-qr-codes/
[49] "What is Typosquatting?", *McAfee*, http://mcaf.ee/a08gpb

Usually, phishing is carried out by an email that is camouflaged to appear as a legitimate request for personal and sensitive information [131]. However, despite the typical phishing attacks flows through emails there are other possibilities. Nowadays the suffix **shing* is used in conjunction with different prefixes to distinguish phishing-like attacks performed through different media (SMS, Instant Message, social networks etc.) For example, when the content is delivered by SMS or exploiting the private messaging systems provided by most online social networks and communities it is called *Smshing*, when the content is delivered via a phone call it is called *Vishing*[50].

Whatever media is used to deliver the content the main goal of phishing most of the times remains to steal consumers' personal identity data and financial account credentials [113][121]. This allows phishers to achieve a financial gain, either by directly exploiting the stolen information (email and banking credentials), or by selling them to others.
The latter is a recent trend related to specialization and perceived risk [110][112]. For instance, people good at creating phishing sites might not be good at, or willing to take the risk of, stealing money from the accounts, also due to increasing vigilance, so they may thus prefer to sell on the black-market the stolen information to less risk averse criminals [110]. For instance, stolen identity data can be purchased and used for identity hiding [112].
Historically, the term "phishing" was introduced in 1996 after on-line social engineering attacks against America on-line accounts by scammers who attempted to impersonate support staff in order to steal passwords and account information from other users. In subsequent years phishing attacks moved to more profitable targets, such as on-line banking and e-commerce services [112], becoming a major problem since about 2000 [121].
It is worth noting that "traditional" non-targeted phishing bears some resemblance with the spam phenomenon. Indeed, it includes sending out a large number of non-targeted emails, hoping that a few recipients will respond [122], whereas such emails do not carry useful information for the recipients [123]. However, differently from spam, phishing emails, which are fraudulent, need to look like they come from a legitimate organization [123] or from contacts known by the victims on social networks or similar [110][111].

4.5.1. Evolution of the "Phishing problem" size

The following statistics summarize the phishing phenomenon evolution, extent and consequences.
In the USA alone, the number of clients that had lost money due to phishing attacks raised from 2.3 million in 2006 to 3.6 million in 2007 [122]. The estimated total losses for US victims were around U$ 3 billion per year in the mid-2000s [110][122]. In 2009, the largest fraction of complaints (21%) received by the Federal Trade Commission from Internet users was related to identity theft attributed to phishing emails, which resulted in a loss for consumers exceeding US$ 1.7 billion [122].

[50] For the sake of readability the text refers always to phishing, with the tacit inclusion of the other forms of *shing.

In 2005 the estimated number of unique phishing messages per week was 33 million [113]. According to the Anti-Phishing Working Group, in the first half of 2009 more than 55,000 phishing attacks (corresponding to unique phishing websites) occurred. Between mid-2009 and 2011 a drop in the number of attacks was observed, due to the switch in the activities of the Avalanche gang[51] (which is held responsible for many phishing campaigns) from traditional into malware-based phishing campaigns; in particular, Trojan horses were the most popular type of malware deployed by phishing attacks in 2011 [112].

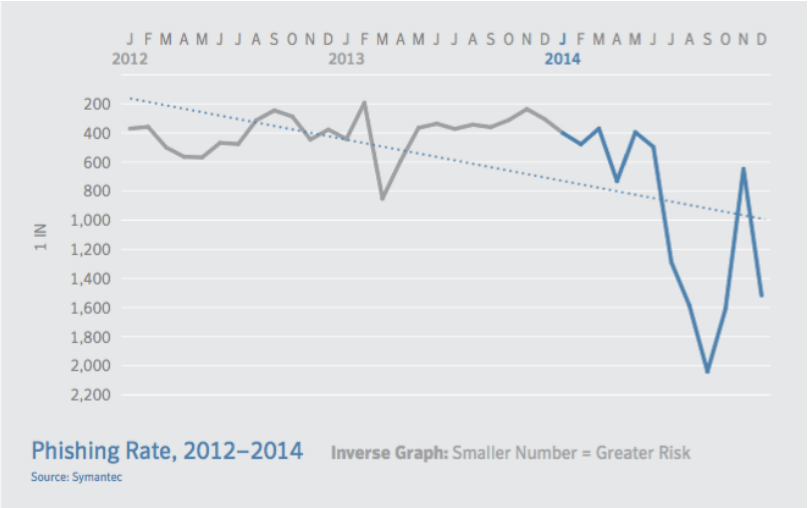


Figure 23 - Phishing Rate in the Period 2012-2014 (Source: Symantec [22])

As shown in Figure 23 a significant reduction of the email phishing rate has been observed in recent years, whereas phishing emails are more and more used to phish for professional account logins such as banking details, LinkedIn accounts, cloud file storage, or email accounts[52].

Around 2005, the main consequences of phishing attacks were financial and productivity losses for corporations, with corporate espionage being a minor concern; such losses came also from attacks that loaded software to turn computers into zombies, enabling hackers to engage in other illegal activities like spamming and further phishing attacks [113]. Even worse, the cost of managing anti-phishing efforts and maintaining trust among users were deemed to be much larger than users' losses [109]. Subsequently, identity theft became another major concern, as it can damage personal reputation of victims, e.g., by reducing their credit rating or linking them to illegal activities [110][121]. A further consequence is the reduction of consumer trust in email-based business communication and in online shopping, the increase of the cost of doing business and financial transactions online, and a damage of corporate reputation [110][121][131]. This can also be a kind of denial of service for large financial services institution [109]. Another issue pointed out by Epstein [133] is related to legitimate but phishing-like messages, often due to the laziness of the sender (e.g., the human resources department of a company). This can be considered as another kind of insider threat: its harmfulness consists of teaching employees to trust messages that look modestly legitimate, thus lowering their guard if a real phishing email appears.

[51] Avalanche Gang is a criminal syndicate involved in phishing attacks. In 2010, the Anti-Phishing Working Group (APWG) reported Avalanche to be responsible for two-thirds of all phishing attacks in the second half of 2009, describing it as "the world's most prolific phishing gang".

[52] http://www.symantec.com/connect/blogs/linkedin-alert-scammers-use-security-update-phish-credentials

4.5.2. Spear Phishing

Phishing has recently evolved into a kind of attack known as “spear phishing”, which is widely used in current SE attacks. It usually targets employees or members within an organization rather than system end-users. Spear phishing is characterized by the use of context-specific messages, based on specific knowledge of individuals and their organizations (including social-network information), which can deceive also individuals who would recognize a traditional phishing attack; spear phishing also uses more sophisticated techniques than in early generations of phishing scams [111][112][131]. This requires the attacker to spend time in understanding the target, with the aim of creating an effective spoofed email and phishing site [106].

Spear phishing is increasingly being used against high-level targets (aka “whaling”, [110]), and is responsible for some recent, high-profile corporate data breaches; accordingly, it has become a key part of the Advanced Persistent Threats (APTs) that companies and governments are facing today [106]. For instance, in 2011 notable attacks occurred against well-known security firms such as RSA, which resulted in further hacks against their client Lockheed Martin [112].

A 2011 CISCO report [125] pointed out that spear phishing need not occur on a massive scale to be effective: using far fewer emails than mass phishing attacks, spear phishing attackers need only a quarter of the victims to click in order to yield more than 10 times the financial benefit [106].

Estimates of direct costs to the public also fail to capture the damage from specialized spear phishing attacks. In many cases, attackers stole source code and other intellectual property. However, there are no good estimates as to the damage caused by spear-phishing, due to victims’ unwillingness to share information and the basic difficulty in assessing damages [110].

No specific countermeasures against spear phishing have been proposed so far, beside the ones mentioned above for traditional, non-targeted phishing attacks. Caputo et al. [106] argue that making embedded training effective in a corporate setting is more difficult than earlier studies suggest; immediate feedback and tailored framing appear insufficient, and other factors must be considered, including perceived security support, information load, and preferred notification method.

5. Attack Process

This chapter describes the most relevant aspects of social engineering attacks process. The aim of this chapter is to understand better these attacks from the attacker's point of view (see section 5.2), their motivations and most common "modus operandi". To achieve this goal this chapter covers different levels of information: from general use cases to more specific ones. Understanding the attacker's point of view is an open problem, which mainly has been addressed in three ways:

- Modelling the attack process with specific models, see Section 5.1.
- Understanding attackers using threat agents modelling, see Section 5.2.
- Modelling users, using a model that establish how their trust and confidence processes are deceived, see Section 5.2 (see also Chapter 7 as part of the countermeasures strategies).

Threat agents modelling is the base for a reactive defence strategy, while the users modelling is the base for a proactive defence, usually through awareness techniques. Attack models are instead useful for both approaches.
Beside these models, also the modelling of victims is extremely important, because from the attackers' point of view users are indeed victims. The victim modelling is part of the attack process in general terms.

5.1. Attack models

One of the common efforts in scientific literature is to implement a model with attacks involving SE. This effort is quite challenging because these attacks are often not fully documented and collected evidences are usually limited. Part, if not all, of the exploits happen in the human side of the Information System, which has limited possibilities to gather evidences using a forensic approach. This is complicated because most users do not understand how security works, so they build their own models, very often incorrectly [135]. Merging the definition of the attacker, the defender and the victim into a descriptive model is useful to:

- Help educate other users about social engineering,
- Create social engineering vulnerability assessment frameworks
- Improve incident reporting
- Understand the effect of implemented defense strategies.

One of the early models of SE is the SEAC (Social Engineering Attack Cycle), proposed by D. Mitnick in 2002 [136], which is reported in Figure 24 and is made of four phases:

- **Information Gathering (Research).** This phase initially requires the Social Engineer (SE) to select a source of information then to pick the right tool to "harvest" it and finally find a way, or a tool, to organize everything collected into a coherent result. The number of possible sources of information is huge and listing them all is a challenging task; nevertheless, it is still possible to give a broad description of the most relevant ones. Primarily, sources should be divided into two major groups according to the

method user to collect the information: physical sources require some sort of hardware and some "physical involvement" (e.g., steal of USB keys or drives) from the Social Engineer while technical sources usually just require a computer with Internet access and some software (e.g., steal of assets on servers).

- **Development of Relationship (Developing rapport and trust).** This phase requires the SE to earn the trust of the victim. There is not just a unique way to achieve this goal and it depends on the kind of attack the social engineers are interested in and how much time and skills they have. A weeklong friendship on a social media, a well-crafted fake blog or website and even just few well-written sentences on a forum can be enough. In some specific situations, this phase may require a more physical involvement, like casually meeting the victim in a pub or in a gym[53].
- **Exploitation of Relationship (Exploiting trust).** The victim is ready, trust has been earned and the SE can finally obtain the information he is looking for. Trust is usually exploited to make the victim reveal some information or to compromise a computer the victim is using by suggesting the download of a certain software or visiting a certain website.
- **Execution to Achieve Objective (Utilize information) Operations.** This phase is the final one only if the SE goal was to achieve this piece of information but very often this is just a step before the begin of a new attack cycle where the information can be used to attack another victim. Sometimes the information needs to be "transformed" or quickly saved/stored. This phase also requires that the SE decides how to handle the relationship previously built, if it is still useful it can be kept alive otherwise it has to be terminated and all the traces must be erased.

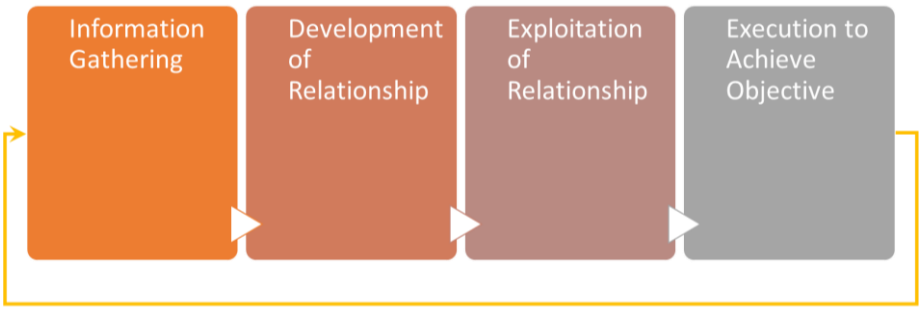


Figure 24 – SEAC model, from Mitnick, 2002

However, despite this model has been used to explain the real nature of SE for a long time, it is overly simplistic. It is quite common to use the model to describe the step-by-step approach while giving little support for the iterative reality of most attacks. Moreover, SEAC does not provide any suggestions for protection strategies, making the model of limited use.

A more recent model proposed by Nohlberg and Kowalski is reported in Figure 25 [137]. It is based on the observation of grooming crimes, which follow a similar deception model.

[53] This specific way of attacking is called "visual hacking"

Figure 25 - The Attack circle proposed by Nohlberg and Kowalski, 2008

This attack model is composed of five phases:

- *Goal & Plan*: at the beginning of the attack, the attacker must have a purpose with the attack, a goal, and a plan how to reach it. In particular, the attacker must possess a method, a motive, an opportunity, and means [138].
    - The method is required, in order to know about what kind of attacks are possible;
    - The motive is usually driven by the value of the asset that could be stolen (directly or indirectly);
    - The opportunity and the means could be casual (for example misconfiguration of a system, a data breach, etc.) or carefully planned (seek a weakness in the social network of the employees by means of an over sharing of information).
- *Map & Bond*: This is where the attacker tries to get information needed for the attack. An alternative is to use pure deception strategies: the attacker creates a deceptive relationship, for example using the six Cialdini's principles [139] (see also section 3.1). In other words, the attacker manipulates the victim into trusting the attacker.
- *Execute*: The execute-step is where the attacker launches its exploit by doing something that is illegal or not allowed, for instance when the target is asked to submit their log-in information in a website, or when the phishing e-mails are sent.
- *Recruit & Cloak*: Cloak are the actions performed after the execution in order to hide the illegal activities. They can be used to continue with the established "friendship", or use more advanced techniques in order to hide the crime and "restore" the trust in the relationship. In some cases, the victim can be recruited to either work for the attacker or as an ambassador/reference for the attacker (as a trampoline to gain access to the real target in the expansion phase).
  Evolve/Regress: This phase is where the attacker learns from the process and creates an internal justification for what happened. There are two possible ways where this may evolve to: learn from the mistakes made and let the attack improve or move to another phase of the attack.

This is just a short argument because the trust theory is a huge area of investigation, which is not only important for security [141].

Two important aspects are missing from the model most used in SE: the dynamics of the attacks and the victims.

- The representation of temporal data such as flow and time of the attack schema [140], are aspects often not considered, however the models existing in literature trying to overcome this limit[54] are, in many occasions, complex and not very useful for the defenders. The problem with a successful attack, as described in , is that always implies a violation of the trust boundaries of the victims, which by mistake grants the attacker access inside a trust zone they own.
- Another common mistake of these models is that they focus too much on the attacker, and forget the victims. This is still a gap in SE models that, if properly addressed, could help to understand better some preventions mechanisms, such as proper awareness methods. A proper model of the victims is useful for defense strategies, because victims can evolve into someone harder to victimize in the future, but it is also possible that victims regress, turning into someone easily deceived.

5.1.1. APT Attack model

Despite the limitations mentioned in the previous section, one of the most referenced models is the one proposed by RSA, which is used for modelling the Advanced Persistent Threat (APT) attacks or Targeted Attacks that normally involve SE techniques [142]. However, this model also focuses most on the attack process and less on its dynamics or the victims.
The APT model, depicted in Figure 26, is probably the most common cyber-attack model, which include Social Engineering as core part. APTs are targeted attacks, which mean that there is a well-defined goal and victims are specially selected. The goal is typically used to obtain critical information, which can be valuable itself (e.g. Intellectual Property, or digital money), or may enable further attacks (e.g. knowledge on internal procedures, that could allow effective fraud schema). This kind of attacks are mainly built to circumvent the existing technological countermeasures, obtain privileged access to the company infrastructure and then expand in order to reach the final goal.
There are a lot of examples regarding this kind of attacks, which are different for exploits or attack vectors, but they all have something in common: the core part of the attack is related to Social Engineering.
In order to obtain a privileged access inside the company network, attackers exploit humans deceiving them to conduct a dangerous behaviour. The combination of technological and "social" attack vectors with certain techniques makes APTs dangerous, as a matter of fact, all kind of companies can be potentially targeted: even RSA, one of the most famous information security firms [143]. In this example, it is interesting how the analysis outlines a possible typical attack model that begins with a social engineering attack and ends with the data exfiltration.
Figure 26 describes an Advanced Persistent Threat model with further information than the one proposed from RSA, it also includes specific phases executed before the SE attack itself

[54] For example. A. Algarni, Y. Xu, T. Chan, and Y.-C. Tian, "Social engineering in social networking sites: Affect-based model," presented at the 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), Dec-2013.

with the purpose of retrieving specific information in order to create a highly contextualized and potential effective attack [144].

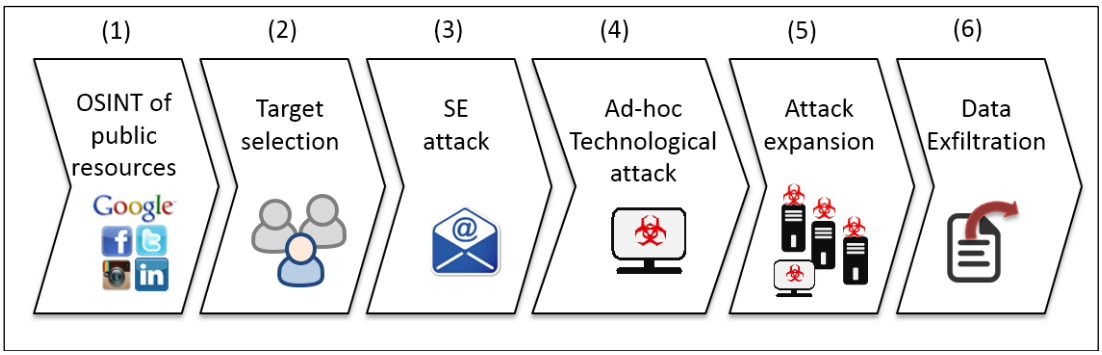


Figure 26 - Advanced Persistent Threat Model

The typical steps involved in Advanced Persistent Threat are:

1. **Open Source INTelligence (OSINT)**. As mentioned above, APTs involve targeted attacks: this implies the use of Intelligence Gathering techniques, already introduced in section 4.4.1.
2. **Target selection**. The effectiveness of the attack is also related to the potential victim; therefore, selecting the most vulnerable target is a crucial step.
   Possessing knowledge about the company role or department of a potential target is relevant information since it allows understanding the potential effect of the following attack, in terms of possibility to expansion. For example, selecting a target in the finance department, or a system administration can easily provide privileged access to critical information, or other internal systems.
3. **Social Engineering Attack**. The central phase is the SE attack, which exploits the SE attack techniques like: Pretexting, Reverse Social Engineering, Spear Phishing, etc. These techniques have been already introduced in sections 4.4 and 4.5.
4. **Ad-hoc Technological attack**. The SE attack aims to deceive users making them to perform a risky behaviour, then enabling the execution of a technological attack. This behaviour could be, for example, to visit and/or insert credentials in a fraudulent website (see section 4.4.3), or to install Trojan software (see section 4.4.2). In most part of the cases, a technological follow-up is necessary to allow the attacker gain a privileged access inside the company network, this can leverage a well-known or 0-day vulnerability, depending on the company targeted.
5. **Attack expansion**. Once a backdoor inside the target perimeter is established, the attacker may need to expand his knowledge of the internal network, evaluating which assets are accessible by the victims, or looking for other vulnerable systems that may provide relevant information. This can be considered the “persistence” phase of the attack, since it is executed until the attacker reach the final goal.
6. **Data exfiltration**. The last step is related to data exfiltration, which is performed once the attacker finds the targeted information, which is relevant for the goal of the attack.

Among the attack models, APT is the most interesting within the context of DOGANA. The reason is the completeness of techniques and tools used: it covers all topics related to the human factor (i.e. external analysis of information and direct social engineering attack), the potential technological consequences that constitute the actual damage for companies (i.e. technological attack and data exfiltration) and the afore mentioned earlier models.
Other models, for example those exploring the Social Network attacks (e.g. "Social Engineering in Social Networking Sites: Affect-Based Model" [145]) are probably too specialized for the aim of DOGANA.

5.2. Motivation and Targets

This section describes which are the attacker motivations and considerations when choosing targets. After reading this section readers should be familiar with common types of Social Engineers, which are the typical goals, and the type of human vulnerabilities that attackers try to explore when they choose their targets.
As reported in Figure 27, and documented in Chapter 1, the victim modelling provides guidance to three fundamental questions of how to attack:

- behavioural model that can be used to deceive users,
- data needed to efficiently run an attack against several victims at the same time,
- sustainable economic models for the attacks.

These questions belong to what is called the **victim modelling**, but at the same time, there are two other areas that are tied to the humans modelling, but more on the defence side. These two areas of investigation are the **threat agents modelling** (TA-modelling) and the **users modelling**. TA-modelling is part of the reactive defence strategies, while users modelling is a proactive method of defence. The TA-modelling tries to answer these questions:

- Which characteristics make a service ambitious for an attack?
- Which are the real motivations behind an attack?
- How can defenders improve security knowing why services are attacked?

The users' modelling instead tries to answer these questions:

- Which characteristics make a good boy recognizable?
- How can the system be secured of who is really using it?
- How can defenders improve users' performances?

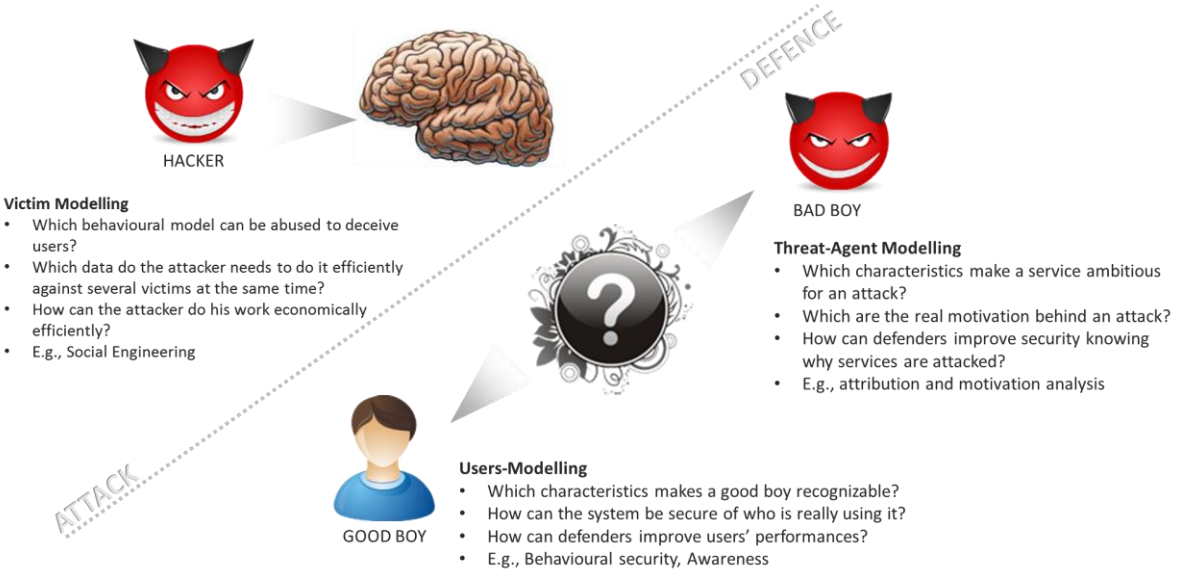


Figure 27 – Area of security where the modelling the humans is useful, for either attacking or defending systems.

All these areas of security are important to define the attack processes: Threat-Agent Modelling is behind attackers motivations, Victim Modelling is behind attacks logics and User-Modelling is behind efficiency of the countermeasures.

5.2.1. Attacker's Motivation: Threat Agents modelling

Threat Agent modelling (TA-modelling) is one of the emerging areas of security and consists in understanding which are the motivations of the attacker and which are the deep a-priori logical processes that would led to the security attack. Despite TA-modelling is a problem approached for a few years now, understanding the motivations that drive attackers is still fundamental for preventing cyber-crimes. There is one early project in this area called the Hacker Profiling Project and it is funded by UNICRI [146]. Advances in the TA-modelling could be helpful not only to understand the motivations of an attacker, but also for the following two reasons:

a) Understand how an attack occurred could help in preventing similar ones
b) Create less attractive services with reduced visibility and attractively.

This problem became urgent with the explosion of the attacks involving SE and has been identified as one of the areas of improvement in security [147].

It is important then to underline that the cyber-security community needs to understand the whereabouts of the threat agents present out there. This involves many aspects, starting from proactive activities, such as TA-modelling, to reactive ones related to attribution of incidents or analysis of currently active threat agent groups (i.e., the cyber gangs). The problem is that TA-modelling is naturally linked to the problem of attribution of a security incidents in general and to the cybercrime logics (e.g., how gangs works, which are their code of conduct, etc.).

Attribution consists in the association of a security incident to its TA motivations and help to understand their rationale.
One of the most interesting recent contributions to TA-modelling comes from Intel with a detailed analysis of threat agent motivations [148]. This work provides strong argumentation to understand the drivers behind threat agents and helps understanding their rationale. Figure 28 shows why the Motivation is one of the important elements of defence planning.

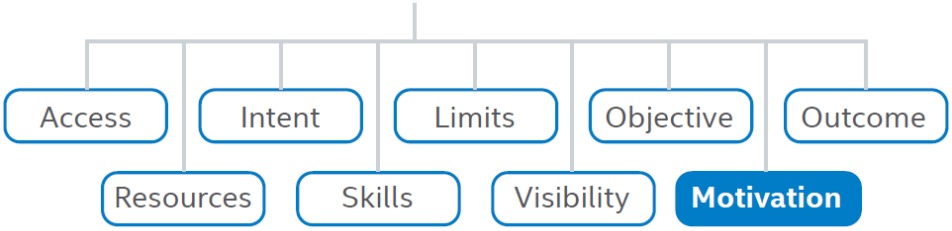


Figure 28 – Intel added Motivation in their threat taxonomy after realizing that it has a significant impact on defence planning

Quoting from Intel report: "when applied to threat agents, the word "motivation" can have two meanings: cause, the reason a person commits an act, or drive, which describes the level of interest or intensity a person acts on". The modelling of the agents is therefore a psychological modelling and one of the two most important areas of application for psychology, being the former one the application of psychology as a mean of attack in Social Engineering.
The Intel model is based on 10 personality traits, as reported in Figure 29. According to Intel, these elements describe all the major motivations relevant for describing threat.

Figure 29 10 elements for the Motivation parameter (Source: Intel)

As mentioned above, one of the more problematic issues of the TA-modelling is the attribution of the security incidents. This happens because the attribution helps to find real agents moved by real motivations that can be "studied". The relatively low number of identified threat

agents, is compensated by the existing correlation between the threat agents and the insider threats. Insiders follow more or less the same motivation patterns of real agents. Incidents caused by insiders have been analysed and more detail insights have been published into the structure and motivations of this threat agent group [149].
With the increase of SE attacks, the problem became also interesting for media. For example, The Telegraph recently published a classification [150] where six types of threat agents were defined and correlated with some real attacks. Between them, only the type "cyber thief" is reported to use SE, but it is reasonable to suppose that the latest evolutions in the area of Automation of the SE attacks will extend the "users" of this attack strategy. There is an increasing trend towards what is being termed the 'hacker for hire', or so-called Espionage-as-a-Service (EaaS) attacks [151]. With the possibility of new legislation coming in to play, this is likely to continue to grow. The increasing consumerization of these services also, has been influenced by the evolution of the threat landscape.
The first influential element is the **consumerisation of cyber-crime**. The offering of inexpensive cyber-crime services is a reality [152]. Cyber-crime "franchising" with affiliate programmes is a recently registered phenomenon that allows Cyber threat agents to be in the position to achieve maximum impact at low prices (see also Chapter 1).
Another important element driving the TA landscape is the relatively **low entry level barriers for technically novices**. It was never easier to launch a ransomware campaign (e.g., thanks to RaaS services), to make a successful malware [153] or to launch a phishing campaign. These facts ease motivated individuals to become cyber-criminals [154].
The last important element driving the TA-modelling is the **low rates of attributions**. It is still difficult to catch attackers in cyber-space. Attribution levels in cyber-space are very encouraging for threat agents. For most of the known security incidents, the number of attributions and consequently the risk of being captured are very low [155].

5.2.2. Definition of targets

As reported in Figure 27 together with TA-modelling there are the **victim and users modelling**, which are the two opposite sides of the same coin: at the centre, there is the user of an information system, which is seen either as a victim or as a user. Both sides of security (attack and defence) are influenced by the same trends and use the same techniques to correctly identify the targets.
As reported in Chapter 3, the evolution of the way of living and the different social and sharing habits changed these models aspects. This happened not only thanks to the ICT improvements that made the information collection easier (improvements of OSINT, big-data collection and sentiment for example[55]), but rather because of the changes in daily habits and the evolution of the workforces.
The selection of the victims is usually based on a set of key elements that may include:

- How much information the attacker knows about the victim

[55] The Social Network Sentiment is the analysis of the positive or negative opinions, of the emotions and opinions expressed on a specific subject among those discussed and shared on the social networks, the blogs and the network in general. It is used to perform automatic profiling and network sensing, of single persons or groups, over the social networks (for example see [156])

- The estimated asset managed in the enterprise
- The role in the enterprise (e.g. thanks to the clever use of social graphs[158][159]) for example as a trampoline to find more interesting victims
- The psychological profile of the victim (e.g. if it is a super target[160])
- The susceptibility to the chosen human attack vector.

5.3. Attack anatomy – How an attack is performed

The models of SE, described in Section 5.1, help to understand how the attacks are performed. Beside the models, it is also interesting to understand which the competences required for a Social Engineer are. Among the presented models, SEAC, despite being over simplistic, excels for its understandability. This section refers then to the four phases of SEAC.

A successful SE attack requires different kinds of competences. Regarding the four attack phases of the SEAC model exploitation and execution require mainly technical skills, as well as gathering information; establishing relationship and rapport demands instead several soft skills of human hacking, based on some knowledge of psychology and communication.

- **Information gathering.** It is crucial for a successful attack, and can be the most time-consuming and laborious phase. Many information-gathering techniques require technical skills, as they do not involve any relationship with people. Knowing where to look for information and how to carry out a search are fundamental aspects. Once social engineers have determined what information is relevant, they must have the capability of conducting a search across many possible technical or physical sources; moreover, since each source is likely to provide only small pieces of information, the capability of combining such bits into a larger and coherent picture is also required.
  About technical information gathering methods, seeking publicly available information about specific individuals (usually, the employees of an organization) through social media sites, or other accessible online locations, through either generic search engines or specialized ones (OSI/OSINT tools) is necessary. Physical methods cannot be used remotely, instead, but only on-site (e.g., shoulder surfing and dumpster diving); this often means interacting with people, which requires the ability to build a relationship (see below) early in the information gathering stage.
- **Development of Relationship**. The quality of relationship built with the target determines the level of his cooperation and the extent to which he will help the attacker. The capability to develop an *instant* rapport is also relevant, as the success of an attack can depend on *quickly* developing a positive bond with the target.
  The main skill in this stage is building trust with the target, which is one of the most important aspects of social engineering. This requires several communication and psychological skills.
  An important psychological skill is knowing and being able to apply the principles of *influence*, leveraging on some general rules of peoples' behaviour to manipulate them [161]. Among such principles, the fact that often people like to be helpful; desire to appear consistent in their behaviour, and value consistency in others, feeling obliged and exercising reciprocity; and are more prone to be influenced by things or people

they like. Social engineers should be able to use tactics like authority and fear, and make the victims believe that they will run out of time or miss the opportunity win some scarce item.
Manipulating people also requires understanding the incentives behind human actions upon which to leverage, which can be broadly categorized into financial, social, and ideological incentives.
Elicitation skills are also important, i.e., the capability of getting information without directly asking for it; this requires in turn communication skills.
Another essential skill toward building trust with the target is pretexting, i.e., the practice of impersonating other people to obtain private information.
Some of the skills useful to a social engineer are at the border between psychology and communication, e.g.: the nonverbal capability of accommodating; modulating the speaking speed as well as the tone and volume; recognizing micro expressions (involuntary movements of facial muscles when the body is under stress) and the corresponding emotion.
More specific communication skills are based on understanding the communication model and its components, e.g., how a message is perceived and evaluated by the receiver, based also on his psychosomatic state and on the context in which the communication occurs. A social engineer must be able to understand the *frame* of the target (the mental filters through which every individual understands the world, built through biological and cultural influences), so that the message perceived by the target closely approximates the intended message.

- **Exploitation of Relationship.** This stage requires technical skills, such as the capability of crafting spear phishing emails (see section 4.5.2 Spear Phishing), or compromising a legitimate website (see section 4.4.3 Fraudulent Websites).
- **Execution to Achieve Objective.** This stage mainly relies on technical skills. In particular, social engineers should plan a smooth "exit strategy": they should be able to erase digital footprints left during the attack, and to remove any item or information that may allow the target to identify the attacker. Even better, they should be able to conceal the fact that an attack has taken place, and to leave the target believing he did something good for someone else that allows possible future interactions to continue.

5.4. Attack automation

With computer-based attack tools, social engineers can automate most parts of their attacks, and consequently increase the efficiency of mass social engineering-based attacks. Nevertheless, nowadays automated mass SE attacks are limited to generic phishing attacks and to the usage of some chat bots to lure victims into malicious sites.
Social Networks (SNs) are present on people's daily life and it is common for someone to use more than one SN (see section 3.2). One of the most challenging areas in SE automation is the usage of chat-bots to exploit SNs. In this section, we will briefly present two proof-of-concepts with different approaches for chat-bots. The first approach uses a chat-bot to mimic human behaviour trying to play his role on a conversation with another human. In an alternative

approach, a chat-bot execute a man-in-the-middle-attack trying to control the conversation between two real humans.

5.4.1. Automated Social Engineering

As described in Section 2.4.5 it is possible to automate several parts of a social engineering attack using an ASE approach [162], which involves the chat-bots to mimic the human role. Regarding Nohlberg and Kowalski model introduced in Section 5.1 (see Figure 25), the attack involves the following phases:

- **Goal & plan:** During this phase, the SE will prepare and configure the attack. Configuration needed to prepare the succeeding phases to perform an attack against a Social Network account are:
  - Facebook account information –The account used by the bot to access the SNs. It should be configured according to the character to impersonate. The choice will depend on pre-acquired information about the target organization's members;
  - Target organization to attack – The target organization from where information is expected to be retrieved as a result of a successful attack;
  - Selection criteria for victims – The victims' profile preferences to be easily attracted and cheated by the bot's account profile;
  - chat logic – This includes the chat logic implementation (rules used to mimic the human behavior) and the criteria to define the minimum numbers of members that ASE bot should map in the nest phase;
- **Map & Bond:** This is the automated phase. Within it, the ASE bot tries to map an organization and bond with future victims. Actions in this phase are carried on in the following order:
  1. Fetching of basic information related with all members that belong to the specified organization's network in Facebook;
  2. Search for a group of victims matching the predefined selection criteria and sample size. In order to access the full profile the bot incrementally uses predefined fetching strategies (i.e. open profiles, geographical networks, add as a friend). In the case the bot is unable to find the specified group of victims, it will terminate;
  3. If the sufficient number of victims have been identified, the software starts creating a relationship with the victims by communicating through Facebook Chat according with its pre-defined chat-logic;
  4. Once the bonding goal has been reached, the bot moves on to the next stage.
- **Execute:** The predefined attack will be executed. The actual attack could consist of asking the victim to follow a link or to reveal some confidential information of interest for the attacker.
- **Recruit & Cloak:** After the attack execution, the bot can delete the account used to carry out the attack (if cloak was enabled on post-attack actions) and, if recruit was selected, the bot tries to recruit the victim and her/his circle of friends for future attacks, e.g. asking the victim if he could forward the malicious link to their friends.

- **Evolve/Regress:** In this phase, the success of the attack must be evaluated, depending on what was defined in the planning phase. After a successful attack the bot can use the information gathered to start another attack and after a failure the bot can stop or try a simpler attack.

5.4.2. Honeybot

Traditionally, ASE uses chat-bots to mimic human behaviour in conversations with the victims. Honeybot is a proof-of-concept [163] for a different approach, similar to a man-in-the-middle attack, in the sense that it tries to take control of real conversations between human users to implement ASE. According with their authors, Honeybot has the following features:

- Automatically bootstrap a conversation between two human users
- Influence the topic of the ongoing conversation
- Make the participants click on links that we inserted into the conversation
- Apply techniques to make conversations last longer

There are five tasks identified on a Honeybot attack:

- **Conversation Bootstrapping** - To initiate a new conversation, Honeybot contacts its victims when they are joining to the Instant Messaging channel by sending a generic hello message (such as hello, wanna chat? or simply hi there). Replies to this message are forwarded to a second user chosen at random from the entire channel population. Each user that does not reply to Honeybot messages is marked as unresponsive.
- **Maintaining Conversations** – After establishing a new conversation, Honeybot must ensure that it will be maintained until the opportunity to launch the real attack arises, without the users suspecting. During a conversation Honeybot is connected with the two human users and he forwards all messages between the users to the appropriate user. For example, when the first user says something about cinema, Honeybot forwards this message to the second user. After receiving the answer from the second user, Honeybot will forward this message to the first user. With this method, Honeybot can maintain a conversation without trying to mimic the human behaviour. Each time Honeybot forwards users' messages, it has to replace the original nickname by the one Honeybot is using. Gender consistency is maintained with an algorithm that is capable of modifying the perceived gender of the users talking to each other.
- **Attacking** – Attacks are carried out by sending a link or a question to one of the two users. To introduce a link in a conversation, Honeybot uses three different strategies: Keyword links (responding to keywords found in messages), Random links (randomly insert a new message with a link into the conversation) or Replacement links (replacing a link introduce by one user with a compromised one). To convince the victim to disclose information, Honeybot tries to influence the topic of the conversation.
- **Message Filtering** - During Honeybot tests, some victims where themselves spamming or sending malware links in their messages. To prevent Honeybot usage as a spam or malware dissemination tool, some heuristics were introduced. Honeybot has a blacklist with suspicious users (e.g. if the first three private messages sent by that user

contain links, email addresses or advertisements) and also generally filters messages that contain a link (http://, www) if that link is not replaced with a bot-generated link.

- **Stealth** – The effectiveness of Honeybot attacks depend on its how well it can avoid detection. For this reason, Honeybot never contacts users that have administrative privileges (when contacted by such a user, it just forwards the messages) and sends at most one link and/or question to every user. To be realistic, Honeybot simulates typing by varying the inter-message delay based on the length of the message.

5.5. Identification and choice of attack vectors

This section aims to describe how attack vectors are identified and why intruders choose them to carry their attacks. The first step for identifying an attack vector is to understand its definition and purpose in the context of social engineering. According to TechTarget *"An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome" [164]*
Viruses, emails, web sites, chat rooms, phone calls, social networks and so on are considered means to identify an objective, target the most vulnerable victims and finally deliver the attack, in other words, they are attack vectors. They can be used independently in different phases of the attack, for example social networks can be used to target potential victims but also to deliver the ad-hoc infections or even extract valuable information. However, each attack vector is more effective in one phase of the attack than another, which looking at the positive side could make it easier for social engineers to identify them, based on the standards. On the negative side, attack vectors are continuously updated becoming more and more sophisticated and harder to detect even if social engineers are aware that most likely that are going to be used in those phases.
In social engineering, there are two types of attacks vectors: the technical which have a computer or technology based deception and the non-technical which are purely human based deception [165]. The following list contains these vectors and for each of them there is a short description and two other sections: how to identify them and why and when they are selected by attackers.

5.5.1. Technical attack vectors

This section, moving from the taxonomy of Sections 4.4 and 4.5, adds some details useful to describe the technical attack vectors and their related identification methods.

Spam Mails
Description. Spam is a generic mail sent identical to millions of victims with a flat approach. The revenue model is simply tied to the probability to hit a vulnerable person (someone who falls into the hook). Could be graphic or not, but the discriminant is always that the hooks are generic being applicable possibly to anyone. It is a blind massive form of attack.

Attacker's choice. The main reason why hackers choose these types of attacks is because they provide a high relative success rate when considering the associated risk of the crime being discovered. The protagonist with minimal knowledge can create these type of emails and launch a large number of attacks per day, and remain anonymous.

Phishing

Description. Section 4.5 describes phishing as a weakness "*found in a system and caused by system users*" but there are different types of phishing:

- Phishing is a more sophisticated form of SPAM that, thanks to graphics, delivers a more sophisticated hook, specialized for a subsample of users belonging to the targeted company (e.g. targeted Bank customers are falling more into this hook than those who are not). The business model is not flat. It is usually sent to less people as SPAM but also to people not belonging to the users' category chosen, supposing for them the hook just does not work.
- Spear Phishing is a specialized form of phishing which is sent only to the customers of the company which the mail pretends to come from (for example a bank), the return of this type of phishing is greater because the victims are selected because are real customers of the targeted organization. Victims are selected on the Social Networks using OSINT techniques or setting up customers' assistance un-official pages on the social networks. Spear phishing is the most common attack on internet today, accounting 91% of the attacks [166].
- Context Aware Phishing (also called Whaling[56]), is an extremely targeted phishing where the semantic distance with the real mail is minimal, meaning that the real mails and these phishing mails are similar. The context aware phishing mail are crafted around the few selected victims of the attack, which are found using OSINT operations. It is a technique common in APT or Targeted attacks.

Attacker's choice. Phishing is the attack vector most commonly used among hackers, it does not require great skills or resources to create it and the rate of success is very high. Partially a phishing attack rely on the participation of the user, which means that there is no need to deploy a sophisticated software in order to acquire the desired information, the user is giving it up unconsciously if the persuasive tactics are well delivered.

Vishing

Description. This Social Engineering concept is a combination of "voice" and "phishing". It consists of using the telephone to acquire information or attempting to influence actions via the telephone. With Voice over Internet Protocol (VoIP) technology the attacker can "spoof" his outgoing number to exploits the public's perceived trust in traditional analogue telephone services.

Attacker's choice. These attacks are less used in social engineering because they require an extra effort from hackers, they are personally involved in the scam and the risk is much higher.

[56] For example see "What is 'whaling', and what's the difference from phishing," [Online]. Available: https://business.kaspersky.com/whaling/5009/. Accessed: Feb. 1, 2016.

Also the process is less automatized, require more resources and specific technology such as VoIP, which makes it more expensive than just simply send an email. These attacks are often used when it is essential to acquire information from a specific person, and is considered worth the risk in order to complete the scam.

Popup Window

Description. This attack consists of software delivered to the end user's terminal. The attacker's rogue program creates a pop up window, instructing the end-user that the application connectivity was dropped due to network problems, so the user must re-enter their username and password to continue with the session. The unsuspecting user promptly does as requested and the attacker will therefore have gained access.

Attacker's choice. These attacks are more elaborate and sophisticated, they require specific knowledge from the attacker and there is software development behind them, but the risk is also low and they are a fast way to acquire information directly from the user's computer. The fact that they look very real and that non-expert users will most likely fall for the trick make them a very effective attack.

Interesting Software

Description. These attacks are constantly present on the Internet, users are persuaded to download and install a very useful program or application such as CPU performance enhancer, a great system utility or a crack to an expensive software package. In this case, when the user voluntarily downloads the program that appears to be legitimate, malicious software is installed.

Attacker's choice. These attacks are commonly used by hackers because they do not need to be very active in the scam, they just need to develop the malicious software and the design of the appearance to make it look like a legitimate program, then they place it in a server and wait for people to download it. Many users download these programs because either they are not aware that they may be fake or because they are trying to avoid paying for the official ones. Hackers are aware of this situation and they use it to fill the Internet with all these malicious programs.

5.5.2. Non-Technical Attack Vectors

Pretexting/ Impersonation

Description. This category of SE attacks involves creating and using an invented scenario (the pretext) to persuade a victim to release information or perform an action. It is more than a simple lie as it most often requires a prior research or organization to know better the victims, their vulnerabilities and specific details that will enable a degree of legitimacy in their minds.

Attacker's choice. These attacks generally have a specific target that is going to provide a great return, they are not random and they are not carried very often. These attacks also required a direct involvement of the attacker which represents a higher risk, so that is why benefits must be worth all the trouble of researching the target and building a consistent pretext to make the victim fall into the trap.

Dumpster Diving

Description. In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes, but also information like a phone lists, calendars, or organizational charts that can be used to assist an attacker using social engineering techniques to gain access to the network.

Attacker's choice. Organizations dispose a lot of valuable information believing that it is never going to be used again, but while for these organizations the information is obsolete, in the context of social engineering it may be provide the necessary knowledge to hack into the company and steal more valuable assets. From the hackers' point of view this process does not represent a big risk, as they are almost not traceable (no one looks what is going on in the dumpster) and they can be the key to a successful attack. Hackers use them as the first stage of social engineering attacks to gather useful information that may help them to carry the next phases of the attack.

Spying and Eavesdropping

Description. Not all attacks require the deployment of a complex software or any other complicated process. Being a clever spy could be enough to get the id and password by just observing a user typing it in, this is known as shoulder surfing. Carrying an attack during a daily event such as withdrawing money from the ATM, all that the attackers must do is to stay behind their victims and observe how they enter the pin code. Another example of this attack that may affect organizations are the protocols established. For example, if the company policy states that the helpdesk can communicate the password to the user by a simple request via phone, the hacker can easily eavesdrop or listen into the conversation and acquire the password compromising it.

Attacker's choice. These attacks provide solid and valid intel, sometimes key for the purpose of the attack, and they do not require an specific knowledge or any particular skills, just to be in the right place at the right, perhaps a prior study about which is the most vulnerable target but nothing very elaborated, but the risk of getting caught is very low, which means is a good way for hackers to acquire sensitive information without risking themselves too much. But at the same time if users are trained and follow the protocols the rate of success of these attacks is very low.

Acting as a Technical Expert

Description. This attack consists of an intruder pretending to be a member of the IT support team working on a network problem, the intruder asks for the credentials in order to access the workstation and 'fix' the problem. The unsuspecting user, especially if not technically savvy, often does not question the IT Technicians authority and agree to give up the credentials facilitating direct access for the hacker.

Attacker's choice

Like the previous mentioned techniques, the way these attacks are carried represent a low risk for the hackers and they return very valuable information

Support Staff

Description. This is more of a general technique but essentially, it consists of posing as a member of the staff working for the targeted organization. For instance hackers, may pose as members of the facility support staff or dress like a member of the cleaning crew, step into the offices and walk around looking for password (for example written on post it notes) or any other type of valuable information.

Attacker's choice. These attacks may represent a higher risk because impersonating another person is considered a felony, also in this case the physical presence of the hacker is required at the scene of the crime and the risk of getting caught is higher, but the process of stealing information is more reliable and could be very useful. Sometimes attackers choose this attack because there is no other way of getting the information.

5.6. Attack tools

Depending on the aimed targets and its skills, the Social Engineer will choose the most convenient attack vectors, as well as the appropriate tools to execute them. Nowadays, with SE 2.0 (see Chapter 1), computer based tools are predominant and massively used, but phone-based and physical SE attacks are still common and effective [167].

5.6.1. Physical Security attacks tools

The effective execution of physical SE attacks requires impersonation and deception skills. Besides these skills, attackers may use some tools to capture, record and exfiltrate information, or to track someone's location.

- **Listening devices**: Hidden microphones or long distance directional microphones are used to covertly listen to conversations, and for a social engineer they can be useful to learn about a potential victim and prepare the attack more thoroughly;
- **Cameras:** They can be used to capture information by taking photos or recording videos, for example:
  - Cell phones – Nowadays cameras are commonly present in cell phones and are an easy to use
  - Covert/ hidden – There are some compact and covert cameras that look like a button or a screw and some of them can even be hidden in a pen [168][169];
  - Streaming services are used to send captured data directly to a hard-to-trace web location.
- **GPS Tracker:** GPS trackers open up the possibility of tracking the victim's location and learning about their routines. This kind of device is usually attached to some vehicle and can be triggered by the vehicle movement. Data can be transmitted remotely (using embedded cell data or SMS modules) or offline (local access after recovering the device) [170];
- **Malware on smartphones and personal computers:** This is another possible way to acquire valuable information. If there is something that the social engineer can guess the possibility that his victim has a smartphone and possibly often uses a personal computer. Those devices are present in our daily lives and they are powerful tools with integrated cameras, microphones and position tracking capabilities, a part from

internet access. Applications used on smartphones and personal computers that have been given permission to access device features can be infected with malware allowing potential control of the victim's device. If a social engineer can convince a victim to install a malicious app, they can activate to be able to intercept communications and/or remotely activate audio, video, etc.

5.6.2. Phone attacks tools

Phone calls were always a useful technique to execute SE attacks. Currently it is still common and effective technique but call tracking and caller identification can reveal the real identity of the attacker. To avoid this, social engineers have some tools available such as:

- **Burner phone:** This is a disposable phone that cannot be traced to the user. With this kind of phones, an attacker can make anonymous calls and avoid tracking. Anonymous phone numbers can also be obtained through mobile VoIP applications available for smartphones.
- **Caller ID Spoofing:** This is the technique that provides false information about the origin of a phone call. To spoof the caller-ID the attacker has to control the caller ID sent by his telephone company to the victim. Some VoIP (Voice over Internet Protocol) service providers allow to freely setting the caller ID, so the attacker can use open source tools for manipulating the caller ID information that is associated with outbound calls [171][172].

5.6.3. Computer based attacks tools

The amount and variety of information that people share online (intentionally or not) and the reliance on online services for end-users or corporations, places computer-based attack tools on the top of the list for SE attacks.
A Social Engineer can find tools for different proposes such as to start and maintain conversations on Instant Messaging applications (chat-bots), information gathering, email attacks (mass email or spear phishing attacks) or web-based attacks. Some of the most common tools are the following:

- **Maltego** [173] can be considered as an OSINT being used to gather and mine information. Maltego has a powerful graphical interface that shows contents in an easy to understand format and highlights links between bits of information. With Maltego, Social Engineers can save hours of search engines usage, looking for information and determining how it correlates. This type of information can be useful to define/refine the attack vector, and eventually increase the user's trust on the attacker's request;
- **SET** (Social Engineering Toolkit) is an open source toolkit, created and written by David Kennedy and is included in the Kali Linux distribution. The attacks built into the toolkit are designed as targeted and focused attacks against a person or organization to be used during a social engineering vulnerability assessment. SET supports several attack vectors that are constantly updated.
- **A.L.I.C.E.** –[174](**Artificial Linguistic Internet Computer Entity)** is a natural language processing chat-bot (see section 5.4) using AIML (Artificial Intelligence Markup

Language) for specifying heuristic conversation rules. A malicious implementation of ALICE based chat-bots can be used on a mass deception scheme attacking instant messaging channels' users.

6. Critical infrastructure and other vulnerable industries

Cybercrime is nowadays widespread affecting both people and businesses. Regarding the cyberattacks targeting businesses, as a matter of fact all industries are vulnerable, but it is interesting to analyse which are the most vulnerable ones. Since cyberattack vulnerability metrics are not a defined standard, it is necessary to consider other information such as high ICT dependence, level of consequences following attacks, level of associated risk and others may be useful to determine which industries are most vulnerable to cyberattacks.

As certain industries contribute to the cohesiveness, prosperity and security of society, they are increasingly relevant to cyber attackers interested in disruptions or theft of information.

These industries are often categorized as Critical Infrastructure (CI) or "the pillars of society", and successful attacks will often have debilitating and long lasting consequences for the population.

The fact that CIs are so attractive to attackers is a key part of them becoming vulnerable. Another factor is the level of interdependency and complexity characterizing CI and their connected industries; this makes it hard to protect CI since attacks can have unpredicted cascade effects on connected infrastructures (critical, or not).

Other industries appear to be increasingly vulnerable as well. The impact of an attack here might not be as devastating to society, but it might still impact, or even compromise, businesses.

Although the scope of this section is not to provide an exhaustive list of the industries that are more vulnerable to cyberattacks, the chapter will list a few amongst them that are considered especially vulnerable and whose assets need to be protected.

The chapter will give commented examples of such industries, discussing also the reasons behind their reluctance to testing their resilience against social engineering cyberattacks.

6.1. Definition and role of CI

Definitions of critical infrastructure exist on national levels in most European countries today. These definitions, while not identical, are very similar. The regional definitions, such as the definition from the European Commission, are equally similar:

> *Critical infrastructure is an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural*

disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the EU and the well-being of its citizens.[57]

EU member countries are obliged to designate which of their national CI should also be considered European critical infrastructure (ECI) . As countries vary on numerous aspects, their relevance to this discussion is expected to vary as well. The following list (contracted) covers fundamental examples of CI and ECI [179]:

- Energy sector (gas, oil, wind, solar, electricity)[58]
- ICT (Information and communication technology providers)
- Financial industry (banking, investment)
- Transportation (roads, rails, harbours, airports, public transport)
- Food and water supply (agriculture, water purification)
- Emergency services (police, health care, military)
- Production industry (chemicals, weapons)
- Government (administration, buildings)

6.2. Interdependency and complexity of Critical Infrastructure

Societies are becoming more and more interdependent and processes are increasingly automated. Although this is a progress for our societies, the risks that arise for the functioning of CI cannot be overlooked. The fact that CI are becoming more and more dependent of one another, as shown in Figure 30, increases the complexity of the system making the consequences of successful cyberattacks almost unpredictable.

As an example, the impact of a regional electricity outage covering parts of a country just 20 years ago, should be considered. Besides affecting the faulty CI (energy sector), such an outage would impact and potentially paralyse or disrupt a range of other CIs, such as hospitals, railways or financial institutions.

Consider now a similar regional electricity outage occurring today and provoking a nation-wide ICT malfunction shutting off Internet access. Although difficult to assess precisely, it can be easily argued that the impact on an interconnected system of CIs and industries would increase exponentially.

The fact alone, that all industries rely heavily on broad and swift integration of Internet-based solutions, contributes to the vulnerability towards cyberattacks. The constant and rapid development of ICT technology and possibilities only enhances this trend.

[57] Citation from http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm

[58] See http://www.securityweek.com/oil-and-gas-industry-increasingly-hit-cyber-attacks-report

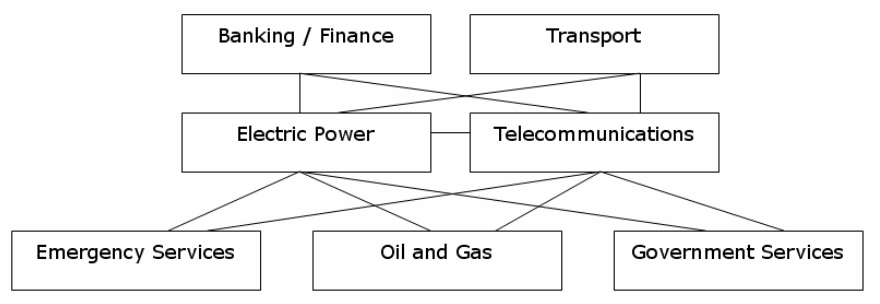


Figure 30 - Basic illustration of identified CI interdependency [180]

The fact that ICT has become such a fundamental part of society and in relations to CI makes the following quote very relevant:

> *A central problem in relation to cyberattacks is that ICT is both a part of CI and ICT also supports IC. Cyberspace is both an overall entity, covering almost the entire possible CI as well as a subset of this and can, based on this, be compared to e.g. electricity [181].*

Another factor increasing the complexity of CI is that key industries are often owned and managed by a range of different configurations comprising public authorities and private actors or corporations. The heterogeneity of these actors' interests, objectives, procedures and metrics for assessing the risk, further increases the level of vulnerability of the system as a whole.

Overall, the interdependency and constantly increasing complexity of CI's are primary reasons for the connected industries' vulnerability to cyberattacks.

Successful cyberattacks carried out against CI hold the potential to disrupt and seriously harm society. The potential for exploiting such industries for profit through stealing and selling intellectual property or secret information also continues to be a serious threat and risk.

6.2.1. Critical Infrastructure assets

Critical Infrastructures are a first class target for cybercriminals and cyberterrorists because of the importance of the assets (information and/or infrastructures) they maintain. Not surprisingly, recent attacks to Critical Infrastructures, like those carried by the "Operation Pawn Storm"(OPS)[59] and "Cleaver" groups[60], includes the usage of S.E. 2.0 techniques described in section 4.4 and 4.5, like **spear phishing** and **watering hole[61].** These were used in combination with advanced technology tricks to extensively compromise target systems.

[59] For further details refer to the following whitepaper http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf
[60] For further details refer to the following link https://www.lancope.com/blog/operation-cleaver-what-it-who-it-affects-and-what-it-means-everyone-else
[61] For further details refer to the following whitepaper https://www.symantec.com/content/en/us/about/media/pdfs/b-istr_18_watering_hole_edits.en-us.pdf

These facts indicate that these groups have access to large economic resources that allow them to fund their activities, resources that are only partially motivated by the revenues generated by the attacks. Beside financial motivations, other interests (political, strategical, etc.) drive the action of these APT groups. This is also reflected by the political targets attacked by OPS, as well as on the kind of information stolen by Cleaver.

The available information about attacks shows that the usage of S.E. in these attacks mostly relies on information (facts, topics and contacts) publicly available in the web, and well-known by targeted employees. This poses an additional difficulty in protecting CI from this kind of threats, because of the natural trust that targets have on renowned topics and contacts.

6.3. Critical Infrastructure vulnerability exemplified

In April 2007, the Baltic country of Estonia was attacked through numerous DDOS attacks on a large number of Estonian websites (ICT infrastructure). The attack was initially focused on political parties and the Estonian government, but within a short period of time Estonian news publishers were also hit and related websites were taken offline.

Next on the attackers list was the Estonian banking industry. After several days of being attacked, at least one key financial institution in Estonia purposely shut down all its Internet-based activities and by doing so basically shut down most of its operations, leaving its customers with no way to transfer funds or use their credit cards (at least while abroad).

After nearly a month of being attacked, and with no successful countermeasure, the Estonian government shut down all international Internet traffic going in and out of the country. They managed to stifle the attacks, but at huge costs for its businesses and industries.

The example of the 'Estonian Cyber War' [182] is an example of attackers targeting CI and succeeding in exploiting vulnerabilities and interdependency of the various CI sectors. The attack on the Estonia's banking industry, by attacking websites, is an example of how one CI (banking) heavily depends on others (e.g. ICT).

6.4. Other vulnerable industries

Apart from CI industries, other industries are also being victims of cyberattacks. While these industries might not be vital for the well-functioning of society, they nevertheless contribute economically with jobs, products and services.

The list of successful attacks these days seems never ending. A recent Security Response report [183] by the IT-security company Symantec points to the following industries as recently being the targets of very advanced cyberattacks:

- Pharmaceuticals
- Technology
- Law
- Commodities

The described attacks appear aimed at stealing intellectual property or other information of confidential nature (assets). Such information is then either sold by the attacker to third

parties or used for spying, see chapter 4 for details. Given the advancing in the level of attacks and the seemingly high success rate, all the mentioned industries are vulnerable.

6.5. Types of attacks

Attacks to the Industry domain can be categorized in different ways, depending on the aspects considered. Two aspects are considered in this section because they are key factors for the selection and implementation of countermeasures. When the effect of attacks is considered, two main categories can be identified:

- **Information Theft**: a.k.a. "data exfiltration", its final aim is to violate the confidentiality of information. Usually, attacks motivated by Cyber-espionage, hacktivism, etc. fall in this category.
- **Destructive attack**: its final aim is to violate the integrity of information and systems. Usually, attacks of cyberwarfare, cyberterrorism or industrial unfair competition such as Stuxnet, German steel plant attack, attacks against industrial control systems, fall in this category[62]. Among Destructive attacks, two subcategories can be considered, depending on the kind of assets they aim to destroy:
  - **Physical assets**, i.e. attacks targeting physical systems run by the target organisation
  - **Informational assets**, i.e. attacks aiming at destroying information owned by the target organisation

In turn, when the attack duration is considered, attacks can be partitioned in two different categories:

- **Cyber Assaults**, i.e. quick attacks carried out in a short timeframe and with a well-defined purpose (e.g. defacement of a website), the attacks from Anonymous are a clear example.

[62] For further details on the mentioned category refer to the link http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/german-steel-plant-suffers-significant-damage-from-targeted-attack

6.5.1. Data Exfiltration

As mentioned earlier in this document, attackers will often direct their efforts to steal sensitive data from their chosen targets. The term *data exfiltration* is commonly used to designate the techniques employed to take advantage of a successful intrusion on an organization's communication system to steal information stored on its servers, transferring the data to an external repository through an unauthorized connection while trying to avoid detection. Attacks targeting data storage systems and making use of advanced persistent threats (APT) are carried out over long time spans and often go unnoticed for months or years before being finally discovered by information security personnel, and even then, the initial symptoms might not even reveal the full scope of the breach, its duration and the relevance of the resulting damage. Groups engaging in this kind of attacks, characterized by the employment of sophisticated tools and a continuous control over the flow of information, are normally classified as APT groups, and they will often be driven by motives of political antagonism or international, military or industrial espionage. In these contexts, data exfiltration can cause significant and irreparable damage. Social engineering techniques are employed to infiltrate the network,[63] typically delivering specially-crafted phishing messages to individuals either employed by an organization or temporarily granted special privileges and access credentials, such as contractors [202]. As soon as a file containing the malicious payload is opened, attackers gain a foothold within the organization's systems, which they can then rely on in order to escalate privileges and start collecting whatever intelligence they are after. The actions required to make the breach and carry out the theft will often go unnoticed, appearing as perfectly legitimate activity performed by authorized personnel. A famous example of this procedure is the Carbanak[64] case [209].

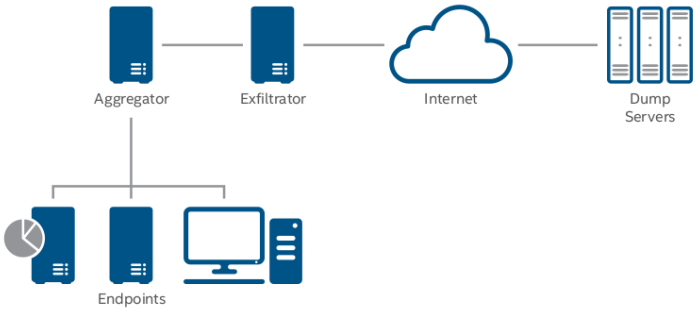


Figure 31 – A typical data exfiltration architecture: data found on endpoints and collected by an aggregator is transferred to a set of external dump servers [200]

[63] In July 2015, the United States government revealed the discovery of a major breach in the computer systems holding data pertaining to the activities of the Office of Personnel Management. Almost 20 million records were stolen, containing private sensitive data belonging to current and former federal employees, including social security numbers, health, criminal, financial and employment histories, and in some instances even fingerprints.

[64] Carbanak is the name of a malware family which was used to infect banks and several financial institutions during the last year. The malware was delivered via a carefully planned spear-phishing campaign. Once the attackers gained control of internal systems, they could perform exfiltration of sensitive data, transfer funds to their own bank accounts and even use ATMs to dispense cash at certain times.

Whenever data exfiltration techniques are designed to make use of readily available outgoing data channels, such as those used by a company's employees to access their own private accounts on popular public services, like social networks or cloud-based storage[65], the miscreants' activities become even more difficult to detect, as sensitive data might even be stolen out of the company's systems by embedding it within files containing pictures, videos and other seemingly innocuous documents. In other instances, the theft might be carried out quickly, often with the aid of an insider threat. For instance, an employee might misuse his or her access credentials intentionally, acting as an accomplice, and thus exploiting a flaw in the company's security systems which will not limit an employee's action range or signal anomalous activity [199]. The subject might also act unintentionally, not being fully aware of the possible repercussions of performing potentially insecure operations or carelessly disclosing confidential information.[66] While the theft's traces and consequences might be immediately noticeable in the aftermath, the damage caused by the data breach and such a fast flow of exfiltrated information will still be, in most cases, beyond repair.[67]

6.5.2. Destructive Attacks

Apart from targeting companies and government agencies for information theft, cybercriminals in recent years also seem to have regained interest in acting with the sole aim of disrupting services, causing data loss – not necessarily following a theft – or even producing persistent, visible, physical damage to infrastructures and facilities, thus hampering an organization's activities with attacks from which they might

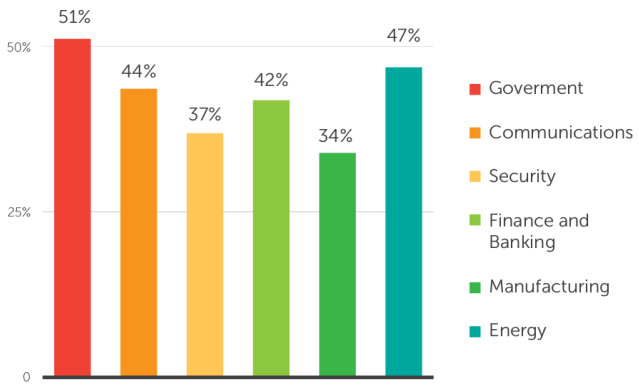


Figure 32 – Percentages of organizations operating in the Americas which suffered a potentially destructive attack in 2014, divided by sector

[65] In the case of the attack carried against Anthem Healthcare, one of the largest health insurance companies in the USA, miscreants stole social security numbers over the course of a prolonged effort, which was finally discovered in early 2015. The sensitive information gathered by cybercriminals could be sold on the black market, or used to perform identity thefts. Such unrestricted access to the company's systems became possible thanks to a stolen set of credentials belonging to an employee with administrator privileges, probably obtained because of a well-crafted spear-phishing attack.

[66] In late 2013, during the span of just a few weeks, attackers could collect details about some 40 million debit and credit card accounts, having successfully broken in the data centres of the American retail chain Target. The breach was made possible by stealing network access credentials from a company's subcontractor, who had been given access to the systems to manage refrigeration, heating and conditioning appliances.

[67] The personal data of up to 50,000 drivers belonging to the international transportation network company Uber were stolen after an unauthorized access to their database occurred on May 13, 2014.

never be able to recover. Such destructive attacks receive much less attention by the press, as the details and consequences are often not disclosed by the victims, who would rather try to quickly regain control and salvage their businesses than make public statements admitting to having lost part of their assets due to an attack of this type. Nevertheless, recent surveys and research confirm that this type of attack is becoming increasingly common, especially targeting government agencies, energy and communications firms [204]. Notable, documented incidents belonging to this category [197] include those involving Sony Pictures Entertainment.[68]

6.6. Role of Social Engineering in Critical Infrastructure cyber attacks

Some types of attack, among those which can be delivered exploiting social engineering techniques, are especially noteworthy and have been increasingly prevalent in news stories describing the methods used by cybercriminals to break security systems and circumvent policies and regulations imposed by organizations and governments to safeguard their assets.

News about notable cases have surfaced in recent times, sometimes years after the incidents occurred, and they fully exemplify the potential risks which an increased feasibility of this sort of attacks, delivered with the aid of social engineering techniques, would bring. In 2014, a German steel mill was attacked by intruders gaining access to the facility's internal systems thanks to a successful spear phishing attack delivered by email. The miscreants sabotaged industrial regulators, causing vast physical damage to machinery and other equipment [195].

Cyber-physical attacks hardly ever make the headlines, due to the victims' secrecy policies concerning incidents of this scope and seriousness. The most famous example of this type of attack is the one related to the development and diffusion of the Stuxnet malware. Stuxnet is the name of a malware which was used to attack several industrial sites in Iran, including a uranium-enrichment plant. The malicious software was particularly sophisticated, targeting workstations as well as industrial equipment such as programmable logic controllers. Having gained control of these systems, attackers could physically damage industrial machinery, modifying the settings used to ensure stability during standard operation [204]. The malware managed to replicate itself and infect systems in other countries.

Oil and natural gas company Saudi Aramco, owner of most of Saudi Arabia's oil reserves, was the target of an attack in 2012 which used a malware called Shamoon to wipe data from over 30,000 workstations used by the company's employees. The attack lasted just a few hours, and security personnel reacted fast to disconnect the company's networks from the internet; the damage, however, was already done. The recovery process required major expenses and a tremendous effort over the course of several days. It seems that attackers took advantage of the extra time off Islamic employees took during Ramadan, providing another example of how intelligence gathered through social engineering can reveal precious details about the

[68] The famous hack targeting Sony Pictures Entertainment occurred in November 2014. Intellectual property and personal data belonging to employees were stolen and published online. However, the attackers (a group calling themselves “Guardians of Peace”) decided not to limit their objectives to information theft: the company's systems were attacked using the Wiper malware, which caused serious data losses and forced SPE to temporarily shut down its networks.

weaknesses of the human factor. The energy sector is among the most targeted by this type of attacks, and Saudi Aramco's case illustrates the potential of cyber criminals in influencing market prices and destroying business activities [198].

6.7. Vulnerable industries exemplified

The following examples will elaborate on the potential impact of SE attacks on critical infrastructures and society at large. The selection will showcase threats and vulnerabilities to current and future CI organizational assets and operation.

6.7.1. Public transportation sector

Urban Public Transport Systems are very vulnerable to cyberattacks, because their networks cover the entire cities' surface, having different locations with sensitive functionalities, processing personal, economic and technical data, which are “eye-catching” for different groups of cyber criminals. The dynamic development of the “smart” component of Public Transport Services generates vulnerabilities to cyberattacks.

Public Transport employees are required to have a permanent e-mail and internet communication with their clients, with other professionals and institutions. Therefore, the vulnerability of this organization is high even if employees are aware of the threats.

Taking into consideration that Public Transport is an important support to the local economy especially for large cities, the functional perturbation of this service can affect the entire local economic system.

The staff of Public Transport Operators and Public Transport Authorities exchange different kinds of sensitive or critical data in external and internal communication at all levels. The following items describe the kind of information available to typical public transportation staff, highlighting the possible interest as target of cyber-attacks:

- **Human Resource staff** works with a dedicated data-base which contains detailed personal data of thousands of employees and their families. There are specified names, residential addresses, revenues, holidays programs/schedule, health conditions, family information, etc. These sources of data can be exploited by cyber attackers motivated by economical (money stealing), political (people manipulation) or social interest (people behaviour and affiliation).
- **Commercial staff** works with a dedicated customers’ data-base: seasonal tickets users, free passes users, reduced mobility and vulnerable users, etc. Certain teams of ticket inspectors have mobile devices (smart phones with a dedicated software installed) for verifying the different types of transport smart-cards. The information stored in such database includes personal data regarding the movements within public transport networks, economic data, etc. – which can be exploited by cybercriminals for planning attacks and blackmailing strategies.
- **Technical staff** uses dedicated software for keeping records (accounting) of materials, stocks, technical procedures and needs, internal codes, etc. This information includes

statistics regarding vehicle operation and traffic control. Misuse of this information might for example negatively influence the economic performance of the company and manipulation of public procurement process.

- **Operational staff**, in case of special events and in accordance to the law, collects and uses the video images recorded inside the vehicles. The personal data contained in the recordings of certain events can be modified, erased or misused to influence criminal investigations.
- **Other staff**, such as the majority of bureaucrats which are working in Public Transport Companies have Internet and e-mail access and they can offer other hundreds of "doors" open for hacking attacks. Even if a large part of employees has no direct access to sensitive data, they are connected to the same local network, and their computer can be used as an "access door".

6.7.2. Healthcare sector

A long-term radical change of perspective happened in the health services since few years that goes under the name of "***Patient Ecosystem***". It consists in the evolution from the simple hospital care to a network of services for patients provided in home environments, mobile contexts through different channels and new technologies.

The **Patient Ecosystem** consists in the evolution of Hospitals from the place of care to a network of services for patients, provided in home environments and mobile contexts through different channels and new

The development of *Assisted Living Systems* is one of the evolutionary aspects that the healthcare is facing since few years to support the creation of such ecosystem. "**Moving to the Humans is the new wave**", referring both to the many technological developments, whose common characteristic is to "centralize" the user (wearable systems, natural interfaces, and emotional design for user-centred innovation, etc.), and, above all, the way in which the access to services is provided. See Figure 33.

Figure 33 – Patient centred health system

Until a few years ago, healthcare ecosystems were understood as limited within the hospital walls. The expected evolution relies instead on knocking down the localization attribute, in favour of a fully outsourced network of services. Consequently, the hospital will ideally keep its traditional role for healthcare services that cannot be relocated and will keep being the institution where clinical competence is maintained and medical required professionalism can remotely operate (see also section 3.3, the evolution of the modern workforces).

The most relevant threats for security in the health sector are the increasing trend in attacks to secondary markets, not usually targeted by cybercrime until now. Health is gaining a lot of attention because it is a simpler target than banks, hospitals security landscape is jeopardized and their employees are significantly less trained [186]. This problem is getting even harder with the raise of mobile Health. In 2014 over 90 percent of healthcare organizations suffered a data breach and 40 percent had over five incidents in the last two years [186]. This trend also explains why healthcare industry sees 340 percent more security incidents than the average industry [187]: "*The rapid digitization of the healthcare industry, when combined with the value of the data at hand, has led to a massive increase in the number of targeted attacks against the sector*".

The most common threats within the healthcare world are the followings:

- Physical theft/damage/loss is maybe one of the most usual cases in areas where there is the presence of very sensitive data, such as health and government. In healthcare, the physical theft ranks first among the breach methods (over 50%), compared to hacking (ca 17%). Combined with all the recorded methods to attack a hospital

institution, recorded in cybercrime this threat ranks 4th in the statistics. As such it is more likely than network intrusion and denial of service [188]

- Information theft is another important element of incidents in medical/healthcare industry. Identity theft in this sector has received attention [189][190]. The increase of data breaches if seen in combination with internet of things/wearables developments, makes a lot of potential misuse in healthcare obvious [190][191].
- Targeted Attacks are among those that more efficiently are exploiting SE techniques (see Chapter 1) to facilitate data breaches. Despite not being one of the most abusive attacks, nowadays in the Hospitals the likelihood of an attack of this type is very high for data breaches, Due to the structural and security problems of several Patient Ecosystems [192]. A mitigation for such attacks could be to identify the critical roles in the organization and the estimation of their exposure to espionage risks, based on their internal role and their digital footprint and shadow.
- Threatening of the hospital users and infiltration through the external nodes. The problem of a distributed informative system like Hospitals 2.0 is that the security of the overall ecosystem is equal to the security of the weakest node. In a distributed system, like that of Figure 33, the weakest nodes are several: patients, wearable things, peripheral ambulatories, untrained security knowledge of physicians and nurses, etc. An interesting menace comes from the abuse of patients' dataspace and medical information, for example through specialized ransomware [194], which uses SE techniques against weak targets (elderly, patients etc.) [195][195].

Why is social engineering such a problem in healthcare? Social engineering is hard to identify, especially in larger organizations where workforce members do not always know their fellow co-workers. This happens despite the existence of security policies (e.g., HIPAA in the US or HITEC Act which enforces the encryption of healthcare data) and employee training programs. Social engineering attacks of any kind tend to be highly successful, but against an organization with uneducated and untrained employees, these attacks are lethal, an example are the multifaceted social engineering attacks [193] which combine phishing and vishing attacks and works well in healthcare.

6.7.3. Information and Communications Sector

The information and communications sector refers to the sector handling all satellite, wireless and terrestrial broadcasting and handling of electrical signals over metallic wires, radio waves through the air and space, and light signals through optical fibres [218]. The fundamental principle of the communications sector is the ability to transmit information over a distance (Ibid). The communications sector thus includes the broadcasting of TV signals, mobile networks and the Internet (Ibid).

The sector is typically owned and operated by the private sector, which provides the expertise for building, maintaining and improving the sector, though with governmental oversight. The communications sector is an integral component of critical national infrastructure (CNI) as it provides an enabling function across the entire critical infrastructure [211].

Societal importance

The communications sector has evolved from a provider of voice services into an extremely complex and diverse industry that is interconnected through all layers of society, utilizing satellite, wireless and terrestrial communication transmission systems.

Social life in a country is thus highly dependent on the communications sector in terms of being able to broadcast television in private homes and for people to be able to text each other or surf the Internet on their handsets or home devices [212].

Impact of an attack

The impact of an attack against the communications sector would be particularly devastating due to its enabling function concerning other critical infrastructure sectors; e.g., the information and communications sector is closely linked to the energy sector, the financial sector and the emergency services [213].

An attack against the communications sector could therefore potentially mean a disruption in communication services, where the consequences are as follows:

- loss of life about emergency services
- serious social consequences for people to communicate
- serious impact on the national economy because of the financial sector's need for communication
- Be of immediate concern to national governments (Ibid.)

6.7.4. Critical Components

The communications sector is comprised by various critical components that are key for maximizing security and resilience: assets, systems, networks and cyber infrastructure, which the sector is all highly dependable on for transmitting and enabling services such as Internet, telecommunication and broadcasting of TV [213].

- *Assets* - Assets include equipment facilities, systems shared by network operators and equipment operated or located at the end user's facility (Ibid).
- *Systems* - Systems refer to the signalling services that exchange information to establish connections and control systems that manage the network. These systems access the local part of the network infrastructure, which handles the connection between end users and the core network allowing for the exchange of information, e.g. when sending a text messages [213]. These systems include public switched telephone network (PSTN), asynchronous transfer mode (ATM) switches, and IP routers for Internet service providers (ISP) (Ibid.).
- *Networks* - The key components of the networks can be divided into (1) the core network, and (2) local networks that are critical to serve other societal functions. The core networks are high-capacity elements that service nationwide, regional and international connectivity, thus being a vital function in the communications sector

[213]. The local networks might be deemed a critical component in the communication sector if they serve other critical societal functions, such as providing the ability for communication to emergency services or energy suppliers.

- *Cyber Infrastructure* - The cyber infrastructure can be divided into three respective aspects concerning the communication sector: (1) People, (2) processes, and (3) technological elements, all of which enable an efficient and functional sector. People include computer emergency response teams (CERTs), processes include sector and enterprise policies, operation plans and response plans, and technological elements include routers, switches, protocols and related hard/software [213].

Sector Vulnerability

The U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) evaluated on 200 incidents across all critical infrastructure sectors in the first half of 2013 fiscal year (October 1, 2012 - May 2013). They found that the information and communications sector accounted for 5% of all incidents recorded [214].

In 2015, Trend Micro did a survey in the Americas to evaluate, which experiences critical infrastructure had with incidents where information was either deleted or destroyed. Interestingly, the communications sector responded to have experienced in 44% of the cases destructive attacks, surpassed only by the government and energy sector (see Figure 8).

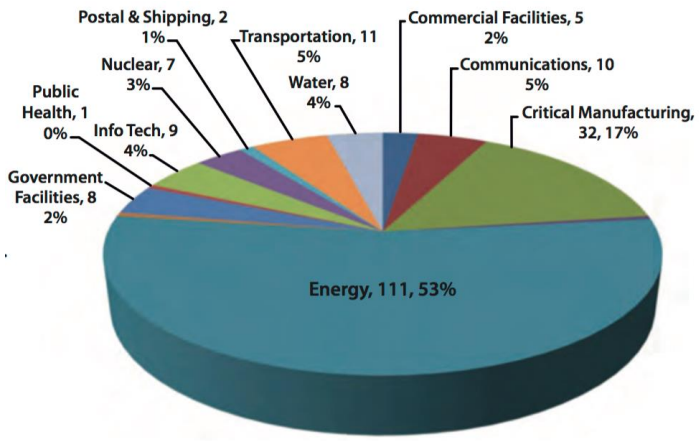


Figure 34 American continent CI's experiences with incidents where information were either deleted or

The previously described case of the Estonian cyber war is most likely the best example of the consequences of an attack to the communications sector (The Guardian, 2007). There were many consequences deriving from the cyber-attack against Estonia, though most relevant in the communication sector remains the necessity to completely cut off access to the Internet, as reactive approach to stopping the waves of DDOS attacks [216].

6.7.5. Security and Safety – Military

A small and very likely targeted group of military attaches across the world was targeted with a malicious attachment (word document) containing a well-known Trojan. The sender was an unused account and the recipients were selected users with valid email accounts which indicated that the attacker had some degree of access to this information. Additionally, the email content was very relevant to the normal information exchange between attaches as it was referring to an updated recipient list.

It is obvious that the target was the military attach's account/system seeking for sensitive information that may be shared between attaches and their countries' capitals. Even unclassified information at this level could be very useful and valuable for an adversary as it could reveal foreign affairs policy issues.

The malware was successfully detected and quarantined by an Antivirus alert. However, it is important to mention that this could be evaded and after a successful compromise the impact could really be severe.

The biggest concern was, though, the well-structured content of the email and the precise list of the recipients. Both facts show that the attack was prepared very carefully and the following analysis revealed that it was part of a broader APT campaign.

The conclusion is that social engineering with relevant cyber-attacks proves to be a significant threat against military environment where a huge amount of sensitive information is being transferred and processed with not always safe and secure ways.

6.8. Challenges of testing social engineering resilience in industries

All security aware organizations should test their security measures. Even well executed security planning and policies, following international standards, have the potential to fail if it is never tested in realistic unscheduled simulated attack scenarios. This is perhaps even more vital in regards to cyberattacks.

Testing industries against cyberattacks with SE 2.0 elements is a process where resistance from the industries is to be expected. As such tests, will mean conducting security and social vulnerability assessments most organizations and companies will be reluctant to participate, as several considerations immediately will come into play. Concerns and uncertainty are elements that will always arise when organizations undertake testing of the security performance. Basically, the results will have potential consequences for the organization as well as for key positions.

To efficiently approach organizations and convince them of the necessity of testing their level of resilience and preparedness against cyberattacks, we need to be aware of the concerns and uncertainties. They should then be addressed immediately, so they don't grow into a too large hindering challenge.

6.8.1. General concerns

As some of the CI industries have a long history they might have static processes in place for working with security. These processes might work for a range of security related situations, but they might not be dynamic or proactive enough to enable them to work in the field of securing themselves against advanced cyberattacks.

The general concern could be rooted in the uncertainty of testing security proactively. The following questions should be anticipated and addressed:

- "are we sure the attack won't cause disruption of our operation/production?"
- "how do we ensure confidentiality?"
- "do we run the risk of exposing ourselves?"
- "are the simulated attacks even realistic?"

6.8.2. Financial concerns

Actively testing security readiness, attack resilience and contingency plans are traditionally a costly affair. Even if conducted in-house, it is a process that demands resources in relation to planning, executing and evaluation.

Budgets might not be ready for new or changed processes, and if the test setup becomes too demanding in terms of involved personnel, it might impact normal business operation.

6.8.3. Security concerns

Professional security teams will always be concerned about adopting and using external procedures and consultants, as it will increase the risk of a security breach.

Management will consult the security team about the risks of changing security procedures. This means that security teams will seek assurances towards the continuity of business operations before, during and immediately after the testing situation.

Additionally, the security team will be concerned of the final results of the testing process, as it might reflect badly upon them.

6.8.4. HR concerns

Both HR and staff associations will have overlapping concerns regarding employees and their rights and possible implications of security testing.

HR will be concerned of the legality of an unannounced testing setup and whether it can be considered an offence to test e.g. employee reactions. Potential lawsuits against the organization will be a main concern.

Staff associations will be concerned of the consequences for individual employees, who do not live up to security policies or who, in some form, become negatively exposed because of the security testing. Basically, staff associations will be concerned about employees being

punished or ultimately fired as a result of bad performance in an unannounced security testing.

7. Countermeasures and trends

This chapter focuses on three different, somewhat complementary, aspects:

1. the existing and studied countermeasures to SE2.0 attacks (from those presented in literature and in the sector's white papers to those recently offered as products or services by commercial companies);
2. the security metrics necessary to estimate SE2.0 security risks and the costs and effectiveness of countermeasures;
3. the main legal aspects posed by the adoption of SE2.0 countermeasures and the current trends of EU legislation on SE2.0 related matters.

The aim is not to provide a complete analysis of the state-of-the-art in the above areas, but to provide an overview of the main approaches currently adopted to face SE2.0.

7.1. The Social Engineering mitigation dilemma: reactive vs proactive approaches

As a form of SE, and as computer security issues in general, it is widely acknowledged that the phishing phenomenon involves both the technical and the human factors [112]. Accordingly, two main kinds of countermeasures have been put in place so far: technical countermeasures, which mainly follow a reactive defence approach; and user education, which is a proactive approach [110][112][122][130].

Technical countermeasures mainly consist of [110][122]:

- Network level protection, to prevent phishing attacks from reaching users; e.g., DNS blacklisting and packet filtering. A more specific tool was proposed by Yue [126]: it transparently feeds many bogus credentials into a suspected phishing site, which makes it more difficult for the scammer to identify the real victim and to exploit its credentials.
- Approaches based on authentication at the user and domain level; e.g., a user-specific login webpage [133].
- Client-side tools, aimed at making phishing attacks more obvious. To this aim, user profile filters and browser-based toolbars are widely used, relying on black- and white-listing.
- Server-side software tools. Content-based filters and classifiers are widely used; they often use machine-learning tools, which are considered as the best option to detect zero-day attacks. A different approach was proposed by Wang et al. [131]: detecting web pages visually like those of known legitimate institutions or companies.

Techniques used by the industry also include attack tracing and analysing, phishing report generating, and network law enforcement [130].
Specific countermeasures were also proposed by Epstein against legitimate but phishing-like emails: leveraging keys and digital certificates, if they are already issued to all employees; modifying email clients to require an extra level of confirmation before opening attachments if the message isn't signed by a known insider (e.g., solving a CAPTCHA); using software that warns users if their message is phishing-like (although the latter could be exploited by attackers to craft their messages to minimize the risk of detection) [133], see Figure 35.

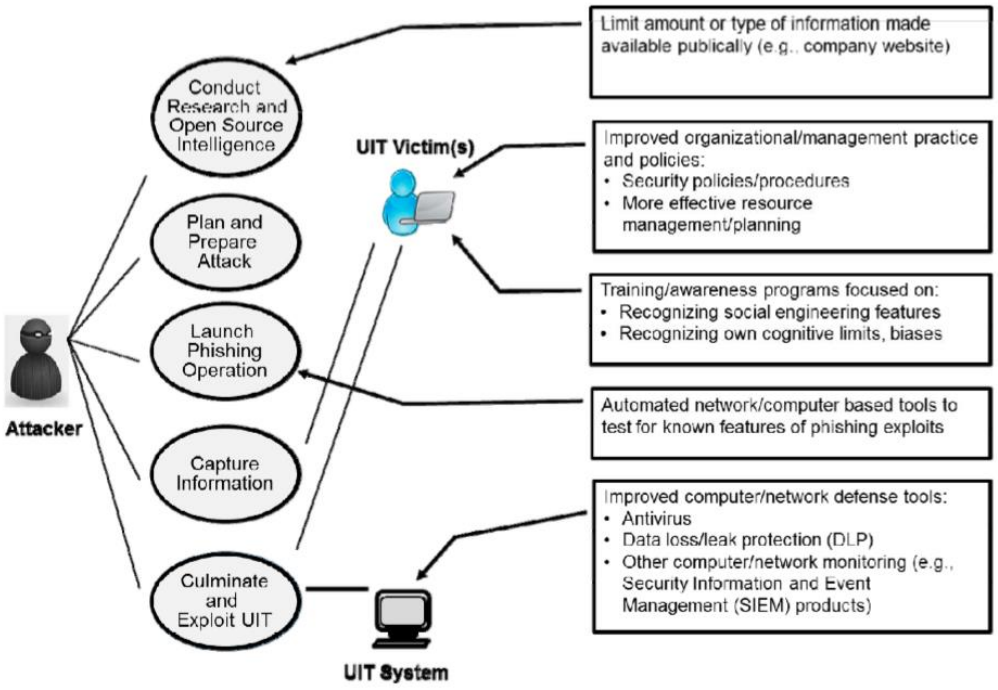


Figure 35 – The list of possible countermeasures for the different phases of a phishing attack. Source: [118]

All existing technical countermeasures exhibit however significant drawbacks. User- and domain-level authentication is not widely used, due to lack of agreement between email service providers [122]. Content-based filtering using machine learning tends to produce a high number of false positive or false negative detections, and can be manipulated by skilled attackers [122]; in particular, phishing is a semantic attack in which electronic communication channels are used to deliver content in natural languages, and automatically understanding the semantics of natural languages is still a challenge [112] [123]. Empirical studies showed that most browsers were opaque about ten years ago [107]; however, despite tools embedded in web browsers (e.g. Google Safe Browsing[69]) have been improved since then, they are still generally deemed to be ineffective, as the users often do not pay attention to warnings [122][130]. Kirlappos and Sasse report that a significant percentage of users still ignore passive anti-phishing indicators, or often do not understand their meaning; additionally, the position

[69] https://www.google.com/transparencyreport/safebrowsing/diagnostic/

of such indicators changes across different Web browsers, which makes even more difficult to identify a phishing site [121].
User education to increasing the level of awareness about phishing attacks is believed essential to complement technical countermeasures [112][121]. Early studies provided evidence that people tend to trust web pages based on their content and professional look, not realizing that they can be easily copied [107], and that basic, often incorrect heuristics in deciding how to respond to email messages are often used [108]. Governments, academic institutions, non-profit organizations and trading platforms have spent considerable effort in offering on-line information. On-line training and testing platforms are also available, that score user ability to identify phishing websites and emails [122]. For the specific case of legitimate but phishing-like emails, Epstein suggested to teach nontechnical staff (e.g., human resources personnel), payroll, and facilities organizations, to avoid sending unexpected messages that have the characteristics of a phishing message [133]. Behavioural research has also investigated the theoretical underpinning of phishing email processing, and attempted to empirically understand this form of deception [131]. Warning theory has also been advocated to study how individuals can be helped in noticing, accepting and acting on warning messages [105].
However, several studies have recently questioned the effectiveness of user education, based on empirical evidence. One of the issues is that all the publicly available studies have evaluated educational materials independently from software solutions [112]. Although phishing may be thought as a simple attack that can be effective only on naive end-users, the evidence shows that it can deceive also educated users, including security-aware engineers [107][112][132]. A possible reason is that systems' complexities are raising beyond the cognition limits of many humans [112]. Another problem is that education strategies assume that users are keen to avoid risks, whereas in reality most online shoppers are mainly looking for good deals [110][121].
To improve the effectiveness of user education, [112] suggested improving user interfaces (e.g., using active warnings) and enhancing the behaviour of the systems to automatically detect and quarantine the harmful messages. Kirlappos and Sasse proposed that, beside warning users of dangers, successful user education and training must target the misconceptions that underlie user actions: understanding how users make decisions, both in business and personal settings, and tailor new security solutions based on this (in fact, this suggestion can be valid for computer security in general) [121]. A deeper understanding of end-user motivations, beliefs, and mental models is believed essential to build effective countermeasures also by [110].

7.2. Mitigation processes

According to the paper [242], a definition of trust is "*the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party*".

This definition is applicable to a relationship with another identifiable party who is perceived to act and react with volition towards the trustor. Being vulnerable implies that there is something of importance to be lost because of this relationship. The concepts of risk, trust and vulnerability are therefore tightly connected to one another. However, trust is not taking risk per se, but rather it is a *willingness* to take risk. There is no risk taken in the *willingness* to trust, the risk is inherent the **behavioural manifestation of a willingness**. The **risk-taking** is therefore the correct term that can be used as a metric for evaluating the risks of SE operations.

This definition was neither written for the ICT security world nor for Social Engineering, it was meant for marketing. Nonetheless, it fits for the purposes of the present document, if one considers the trustor as the victim of the attack and the trustee the real attacker[70]. Using such a definition enlarges the classic concept of risk that used in security and regulated by the ISOs, including those human aspects that correlates the risk-taking to the personal attitudes or habits.

Risk-taking is broadly interpreted as risk taking concerned with information security. For the purposes of this document, we defined the information (and data) security as "*The safeguarding of an individual's data from unauthorised access or modification to ensure its availability, confidentiality and integrity*"[71].

Controlling the risk in the SE-enabled attacks is therefore a twofold operation.

- First, reduce the risk for a system to be compromised through attacks started in the human side of the information space (e.g., attacks that initiated through a phishing mail and terminated with a malware infecting the systems). To this extent, the risk management procedures are those already used in security and often adopted by the ISO regulations. This is the technological risk assessment and mitigation.
- Second, reduce the risk of humans to be compromised through attacks that violate their trust zone, purely inside the human side of the information space (i.e., the part of the attack that is purely "human" and uses social engineering). The mitigation process in this case is completely different and consists in finding ways to modify the behaviour towards **risk-taking**, and the risks associated with a lack of understanding towards data security implications, associated to the actions performed. In this case awareness is mostly the only mitigation instrument available. Assessing the risk-taking level of people means assessing behavioural and psychological traits of the persons to understand what drives their actions; mitigation instead means to influence their actions, through innovative awareness methods, for example.

7.2.1. Psychological hardening (or Human hardening)

The Willingness defined as one of the parameters that influence risks is connected to the confidence of the trustor in the actions of the trustee. Confidence is defined as "*the extent to*

[70] Becoming a trustee of a trustor implies the concept of **Trustworthiness,** which in its simplest formulation is assessed as the perception of a lack of motivation to deceit or lie [243]

[71] See http://ishandbook.bsewall.com/risk/Methodology/IS.html or the definition in Chapter 1

which one is willing to ascribe good intentions to and have confidence in the words and actions of other people" [244]. If the victim does not consider alternatives (every morning he/she opens the email without worrying too much) he/she is in a situation of confidence. Confidence hence is connected to the concept of risk-taking. Therefore, the confidence of people in the systems is one of the most abused elements in SE attacks, because it relates to the risk-taking. When users receive an email they need to decide if it is a menace or not, according to their confidence. Users choose to follow the instructions in the email or not, in spite of the possibility to be hacked, based on their level of trust or confidence[72]. The role of awareness is to influence this value, the confidence.

However, several factors influence the confidence. Mainly biases and habits but others are discovered everyday by cognitive sciences, such as the mirror neurons [245], co-dependent relationship [246], fear of missing out [247], reverse-psychology [248] etc.

This is not a simple problem: the ICT security experts have been debating it in the last years as one of the most challenging problems. The point is to measure the performances of the awareness programs and their correlation with the real risk reduction for the enterprises. All the SDVA performed clearly show that not all the awareness programs perform well, leaving the final risk for enterprise unchanged at a long distance. A recent whitepaper [250] reports that people clicked on test phishing campaigns in 2014 because they did not match the characteristics they had been trained to look for in 2013. Another paper reports the results of a phishing test run on a big sample of enterprise employees [251] before and three months after an awareness program. It clearly shows that the risk level reduced immediately after to increase again afterwards.

One aspect that complicates the matter is the propensity of people to trust or the propensity to have **confidence**. This propensity requires some sort of psychological profiling to tailor the awareness programs around each behavioural trait However, the propensity to have confidence is influenced by the personal culture, habits and age. As an example, a recent study [252] presents a co-dependent relationship: users perform better on cognitive tests when their smartphones are nearby (even if they are not using them) compared to when they are out of sight or far away. Other studies [253] [254], as discussed in Chapter 3, report an important change in everyday habits that affect risk-taking behaviour (e.g. extroversion and introversion).

For example, smartphones:

[…] for young adults, the importance of mobile phones as the device of choice coupled with continuous network connectivity raises key issues of risk-taking behaviours. The attitudes of young people towards data/information security are particularly important. Further, the

[72] Some authors [249] argue that trust differs from confidence because it requires a previous engagement on a person's part, recognizing and accepting that risk exists. This is exactly the type of distinction that exists in the phishing attacks because every user knows that the risk of being hacked exists, but often does not recognize it correctly.

gamut of communications styles and the range of activities that can be performed on a phone increases considerable risk arising from data security and privacy concerns […]

The question of how to train users or "patch the human side of security" still remains an open issue despite having being on the list of open problems in the last few years [255][256]. The lack of fully proven reliable and long lasting awareness methods is still pressing. Existing literature [257][258] highlights that to effectively solve these problems through awareness the best option is to have on the one hand fully customised training programs and on the other hand highly innovative methods, possibly mixing defence and awareness [259][260]. The problem of personalization means to understand which methods are most effective in which context, starting from the psychological evaluation of users and in some cases considering how the brain works and learns [261].

7.2.2. Technological hardening

Nowadays almost every operating computer is connected to a network, which means that it is constantly exposed to new threats and external attacks. In order to prevent and fight these attacks, systems must be technologically prepared. Many of them already offer security features to limit outside access, but even with these features in place, systems are still getting compromised, therefore they also must be hardened to minimize these security vulnerabilities.

Technological hardening consists of protecting sensitive data from internal and external threats by eliminating as many security risks that may affect the system as possible, always minimizing the risk of a successful attack. Bruce Schneier mentioned in one of his articles "Security is a process, not a product" [219]. Therefore, the **process** of eliminating these risks includes the removal of non-essential programs as well as the use of different techniques to prevent and/or mitigate threats that represent system vulnerabilities. Products can be implemented and be part of the process, but an effective security system is always based on a process or methodology.

So far, most of the security processes are reactive and they aim to detect and mitigate attacks, but new technologies are designed to be proactive and not just detect and mitigate but also prevent attacks by setting up the necessary measures. Some of these techniques for hardening systems are Big Data, predictive analytics or data shadow analysis among others.

- **Big Data**: This technology and its style analysis can be the answer for detecting and preventing advanced persistent threats. These techniques could play a key role in helping detect threats at an early stage, using a more sophisticated analysis pattern, and combining and analysing multiple data sources. Big data also provide the possibility of identifying anomalies by using feature extraction.
  Today, security logs are often ignored unless an incident occurs and the red flag is raised. Big Data provides the opportunity to consolidate and analyse logs automatically from multiple sources rather than in isolation. This could provide insight that individual logs cannot, and potentially enhance Intrusion Detection Systems (IDS) and Intrusion

Prevention Systems (IPS) through continual adjustment and effectively learning "good" and "bad" behaviours.
Integrating information from physical security systems, such as building access controls and even CCTV, could also significantly enhance IDS and IPS to a point where insider attacks and social engineering are factored in to the detection process. This presents the possibility of significantly more advanced detection of fraud and criminal activities [220].
In the context of social engineering, Big Data can be used to analyse enormous amounts of data about human behaviour to understand how attackers think and anticipate their movements, to understand how users behave when they are attacked is also vital to take the necessary measures and adapt new technologies to the human behaviour to increase their effectiveness.
In 2014, the SANS Institute [221] carried a survey where respondents reported difficulties in understanding, identifying and dealing with abnormal behaviours as well as supporting the security operations team. However, in 2015 the results seem to indicate slow but steady progress, which thought that processes and tools similar (or the same) to those used in Big Data could also be used in security data. However, the lack of maturity implementing and using analytics tools is still too low.
Now organizations are starting to collect more data from many different sources, the use of threat intelligence is increasing and analytics platforms are considered seriously and necessary. Visibility is increasing but detection and response times are still very low.
The same study shows that 50% of organizations are quantifying improvements in their programs thanks to the analytics tools. Some respondents (11%) stated that they had seen 100% improvement in their visibility into actual events or breaches, but most noted that improvements came in between 25% and 75% across all categories. The following are some relevant statistics for each area listed in Figure 36.

Table 4. Improvements Attributed to Use of Analytics Tools

	Percentage of Improvement		
	25%	50%	75%
Accuracy of detection/response (reduced false positives)	27.4%	24.2%	25.3%
Attack surface(s) reduction (as result of response/repair)	26.9%	28.5%	21.0%
Detection of unknown threats	23.1%	26.9%	19.9%
Duration of events	24.2%	21.0%	18.8%
Reduced time to detect and/or remediate	21.0%	31.2%	23.7%
Skills/staffing reduction for detection and response	16.1%	18.8%	18.3%
Visibility into actual events or breaches	23.1%	25.8%	23.1%

Figure 36 Improvements attributed to use of analytics tools

- **Predictive Analytics:** The Company SAS [217] describes predictive analysis, as "Predictive analytics is the use of data, statistical algorithms and machine-learning techniques to identify the likelihood of future outcomes based on historical data" [222].
  In the future of security, one of the goals is to go beyond descriptive statistics, reporting and monitoring to predicting what will happen in the future within a certain margin of

error. The aim is to produce new insights and anticipate patterns of behaviour that would lead to better actions and solutions.
Predictive models use known results to develop techniques that can be used to predict values for different or new data. These techniques come up with predictions that represent a probability of something happening based on an estimated and already studied set of variables. This is different from descriptive models that help to understand what happened or diagnostic models which aim is to explain key relationships and determine why something happened.
More and more organizations are using predictive analytics to increase their security by anticipating possible attacks and knowing how attackers behave per already determined patters. This allows companies to set up the best security systems and take the necessary security measures.

- **Data shadow analysis:** *Shadow System* is a term used in information services for any application relied upon for business processes that is not under the jurisdiction of a centralized information systems department. That is, the information systems department did not create it, was not aware of it, and does not support it[73]
  Shadow systems are also known as shadow data systems, data shadow systems, shadow information technology or in short: Shadow IT.
  Very often organizations do not have the resources to maintain an IT department that secures and provides data through the proper channels, but even if they do, sometimes business departments do not find an effective way to collaborate with them, either way the result is the same, the necessary data is not being acquired or processed. Ultimately, they have the need to access this data, so if they have an IT department, often they decide to bypass the security measures established, and if they do not they find their own way through the already mentioned shadow systems.
  The problem with these systems, even if they seem affordable, effective and decisive, is that they are not tested, documented or secured with the same rigor as the systems developed by the IT department, and they can show incompatibilities with other systems and not comply with the protocols established by the company bringing security issues in the long term.
  Even if the protocols are strictly followed, these systems are still going to be used by employees, either because they ease the day by day work or because they are faster solutions. The best way to harden organizations from leaking sensitive information or loosing critical data is to analyse these systems and have certain control over them.

  Price Waterhouse Coopers [223] reports: *"Many companies rely on spreadsheets as a key component in their financial reporting and operational processes. However, it is clear that the flexibility of spreadsheets has sometimes come at a cost. It is important that management identify where control breakdowns could lead to potential material misstatements and that controls for significant spreadsheets be documented, evaluated and tested"*

[73] Shadow system (2013) in Wikipedia. Available at: https://en.wikipedia.org/wiki/Shadow_system

7.2.3. Threat intelligence

As shown in Figure 37 Threat intelligence (TI) is a part of the modern defence systems. TI uses an initial shot of Big Data, mined to collect evidences of new attack patterns. The data used in the early steps of the funnel includes information coming from the anti-SPAM filters, or more recently from the SPAM traps, data collected from the Social Networks Analysis (SNA) or the enterprise digital footprint and shadow, and data collected from other sensors. The number of relevant sources is increasing. The intention is to fund these new systems on the principles of **early detection and agility,** which may come only from a big amount of information. One of the core parts of the Threat Intelligence is the simulator of the APT architecture, which copycats the known attack patterns using also the data mined.
The TI research also intersects with the definition of efficient Social Engineering attack models (see Chapter 5). A complete taxonomy of the attack processes is of help to improve the solution implemented in Figure 37. As described in Chapter 5, this is still an area of investigation because of the lack of conceptual models that represent SE attacks [262].

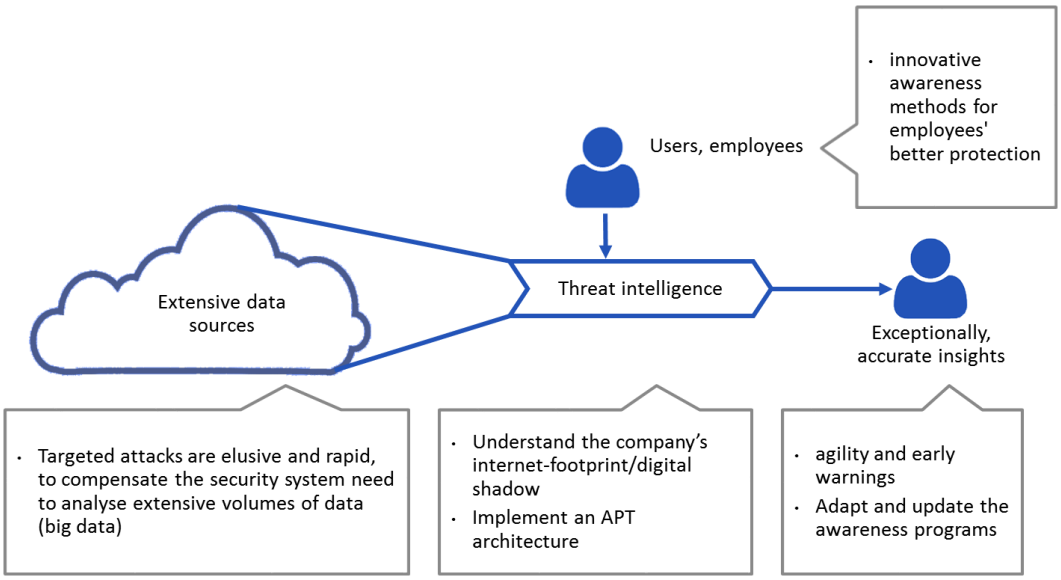


Figure 37 – Threat Intelligence based defence system (source: Encode)

7.3. Awareness strategies

Awareness is recognised as the most effective countermeasure against SE but, as reported in [233], the security awareness is still immature as demonstrated by the following facts:

- Despite a direct correlation between available resources (time and money) and maturity of awareness programmes, only 5% of company's security key personnel work on their security awareness program full time.
- A clear majority of security awareness programmes are led by IT technical people with little experience in psycho-social sciences, communications, and change management thus failing to properly address the human factor.

- Using the Security Awareness Maturity Model, SANS found that half of the organizations surveyed currently do not have an awareness program or have an immature program that is solely focused on compliance. Only 5% of respondents felt that they had a highly mature awareness program that not only was actively changing behaviour and culture, but also had the metrics to prove it.

Moreover, the current typical approach to awareness programmes is limited to standard training approaches without properly testing the human vulnerability. An example is the PCI checklist specific security training programmes[74] in Table 2 that is based on standard communication means and without a proper actionable metric.

Table 2 - PCI Security Awareness Programme checklist

Step 1 - Creating the Security Awareness Program	Step 2 - Implementing Security Awareness	Step 3 - Sustaining Security Awareness	Step 4 - Implementing Security Awareness
Identify compliance or audit standards that your organization must adhere to.	Develop and/or purchase training materials and content to meet requirements identified during program creation.	Identify when to review your security awareness program each year.	Document security awareness program including all previously listed steps.
Identify security awareness requirements for those standards.	Document how and when you intend to measure the success of the program.	Identify new or changing threats or compliance standards and updates needed; include in annual update.	
Identify organizational goals, risks, and security policy.	Identify who to communicate results to, when, and how.	Conduct periodic assessments of organization security awareness and compare to baseline.	
Identify stakeholders and get their support.	Deploy security awareness training utilizing different communication methods identified during program creation.	Survey staff for feedback (usefulness, effectiveness, ease of understanding, ease of implementation, recommended changes, accessibility).	
Create a baseline of the organization's security awareness.	Implement tracking mechanisms to record who completes the training and when	Maintain management commitment to supporting, endorsing and promoting the program	
Create project charter to establish scope for the security awareness training program.			
Create steering committee to assist in planning, executing and maintaining the awareness program.			
Identify who you will be targeting—different roles may require different or additional training.			

[74] Best Practices for Implementing a Security Awareness Program (2014) PCI Data Security Standard (PCI DSS)

Identify what you will communicate to the different groups.			
Identify how you will communicate the content.			

The need to set-up an appropriate level of security awareness in organisations is becoming a topic of broad and current interest, as demonstrated in many articles in specialised web sites and blogs (see for example [237] and [238]).

To this end, some innovative approaches are recently emerging from the literature:

- A specific **social engineering (Social-Ed) awareness portal** [227]. The proposed portal includes:
  - Awareness-raising material about a wide range of social engineering techniques.
  - Links to support material such as news reports regarding social engineering trends or techniques.
  - Quizzes allowing users to test their own ability to recognise and defend against social engineering attacks.
  - Online assistance to users who have difficulty in using the material provided (e.g. user guides to explain the general operation of the site).
- **Using Influence Strategies to Improve Security Awareness** [228]. The paper proposes to identify the conscious or unconscious, personal, environmental or social sources of influence to get people to act differently. The focus is on aspects like:
  - Vital behaviours, identifying the behaviours to be changed before start trying to change them (e.g. metrics around past incidents may put focus on the vital behaviours to target in an organization).
  - Personal motivation and ability, by linking people's actions to their values. By giving people an image of their best selves, and showing them how to stay true to that image, enacting "secure" behaviours can be made inherently satisfying.
  - Peer pressure. Whenever people are uncertain about how to act, they tend to assume a response is correct if many people are behaving that way (social proof). Concentrating on "influence leaders" will allow a better penetration of the correct message within the considered organisation.
  - Environmental Factors, by changing the environment (e.g. by putting photos of viruses on USB sticks to remind people to disinfect) thus making the desired behaviour easier to achieve.
- **Gamification**. Using the gamification theory and its elements (Autonomy – we like having choices – Mastery – we like getting better what we do – Feedback – we like getting feedback on how we are doing – Purpose – meaning amplifies what we do – Social – all this means more with others), Sedova [234] has proposed a new approach for security awareness based on the steps shown in Figure 38 to transform the security mindset of an organization.

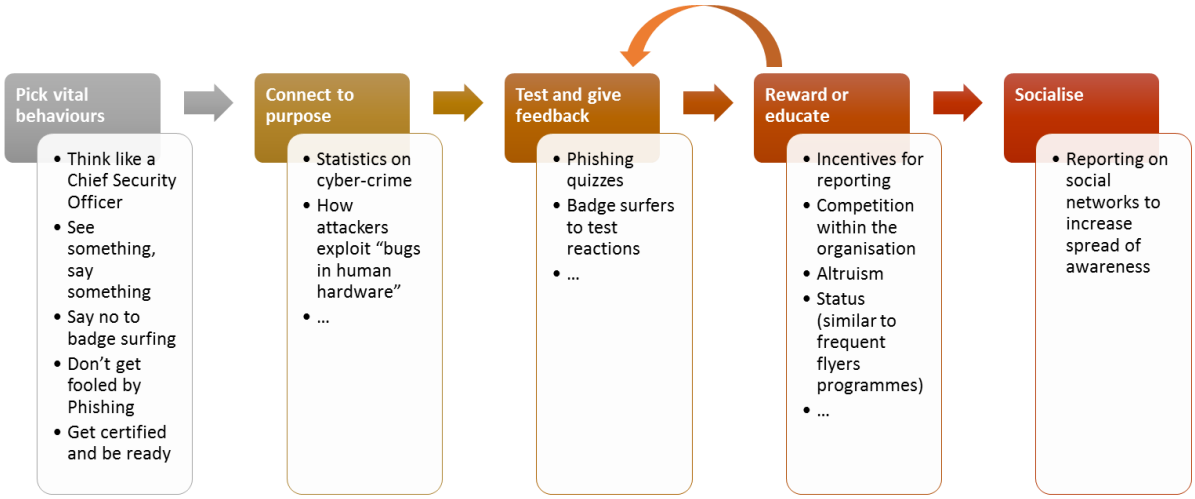


Figure 38 - The gamification approach to security awareness

- **Targeting misconceptions**. Kirlappos and Sasse [235], starting from a study on an anti-phishing tool, have discovered a "*significant gap between the signals security experts would like users to consider when assessing the legitimacy of a website, and those they actually use when faced with a tempting offer*". They propose a major rethinking in security awareness, education and training, starting from users' misconceptions and decision-making processes and trying to tailor innovative security solutions (e.g. challenging users' assumptions about trust signals, organising games in which users can collect or lose points by answering questions about the trust and assurance indicators, etc.).
- **High Reliability Organisation (HRO)**. A totally different approach, borrowed from the IT security management of US Navy nuclear-propulsion programme, is proposed in [239] aiming at building and sustaining a HRO culture. The HRO is funded on several principles:
    - Integrity. To reach a level of awareness bringing employees to eliminate deliberate departures from protocols and own up immediately to mistakes.
    - Depth of knowledge. Employees shall reach a deep level of knowledge of all aspects of their organisation/system to promptly recognise deviations from normal behaviours and to effectively handle anomalies.
    - Procedural compliance. To know - or know where to find - proper operational procedures and to follow them to the letter.
    - Forceful backup. Any action that presents a high risk to the system should be performed by two people, not just one, and every employee is empowered to stop a process when a problem arises.
    - Attitude. Employees shall be trained to listen to their internal alarm bells, search for the causes, and then take corrective action.
    - Formality in communication. To minimize the possibility that instructions are given or received incorrectly at critical moments, employees shall communicate in a prescribed manner.

  In this approach awareness is reached by making everyone accountable and instituting unified standards and centrally managed training and certification.

7.4. Current products and services

This section describes some examples of products and services aimed at providing countermeasures against Social Engineering related threats.

7.4.1. Alien Vault Unified Security Management

AlienVault Unified Security Management™ (USM)[75] is an all-in-one platform designed to ensure that mid-market organizations can effectively defend themselves against today's advanced threats.
The product[76] is an integrated platform including

- An Asset Discovery tool for network scanning and asset inventory
- A Behavioural Monitoring tool to identify suspicious behaviour and potentially compromised systems
- A Vulnerability Assessment tool that allow network vulnerability testing and continuous vulnerability monitoring
- A SIEM (Security Information and Event Management) tool that correlates and analyses security event data from across the network and
- A Threat Detection tool to detect malicious traffic on the network.

The tool is based on the analysis of network events and related vulnerabilities but it does not consider explicitly SE 2.0 issues.

7.4.2. Wombat Security Technology

Wombat[77], with the recent acquisition of ThreatSim, is offering an advanced tool [236] for both vulnerability assessment and security awareness based on the following modules:

- **Assess** to create custom knowledge assessments and use mock attacks to diagnose organizations' vulnerabilities.
- **Educate** with a broad set of focused interactive training modules.
- **Reinforce** to inform employees about best practices by bringing messaging into the workplace and providing methods for them to report suspicious activity, providing positive feedback for each reporting instance.
- **Measure** using data and analysis to drive strategies.

The Educate module is based on traditional Computer Based Training sessions supported by mock attacks tools.

[75] AlienVault, Inc. (2015) Unified security management (USM) platform. Available at: https://www.alienvault.com/products
[76] A free trial download is available on the Alien Vault web site.
[77] https://www.wombatsecurity.com

7.4.3. BT

BT[78] has recently launched a service designed to test the exposure of organisations to cyber-attacks. This service is aimed at assessing IT systems vulnerability and human failures.
To test the IT systems vulnerability the service mimics malicious attackers to provide tests targeted at the different entry points to an organisation (see for example the proposed approach for banking in Figure 39).

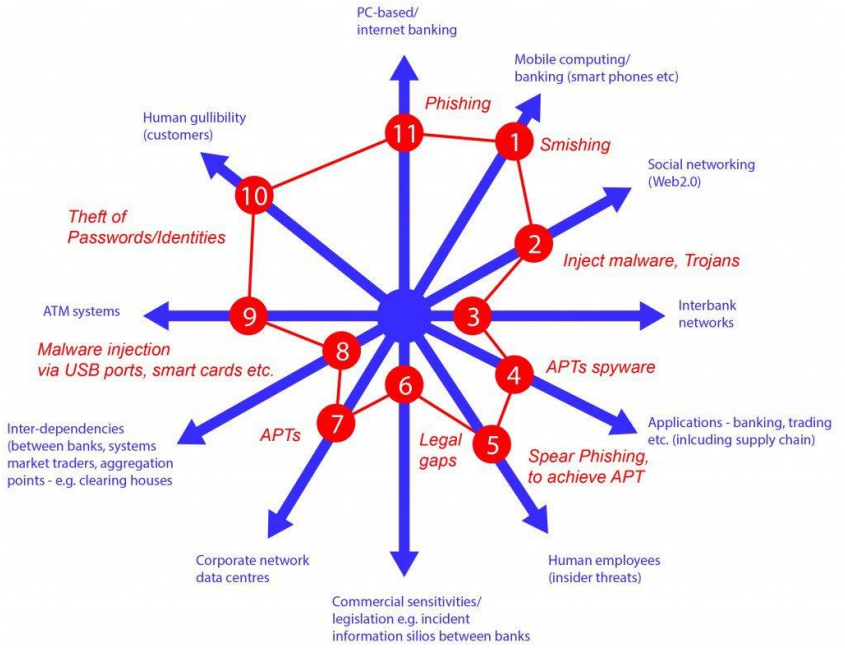


Figure 39 - Banking vulnerabilities (Source BT)

To test human failures, BT [225] has developed a standardized methodology for carrying out Social Engineering Ethical Hacking vulnerability assessments. The proposed methodology is based on checklists, client requirement documents, best practices and other well-known references in publicly available resources, such as, forums, hacker communities, internet, etc. The Social Engineering Ethical Hacking vulnerability assessment may include different types of attacks:

- gaining unauthorised access to building and/or secured area's when disguised as a service engineer or cleaner;
- creating a phishing website and sending to employees personnel E-mail about registering their computer assets;
- reading (and cloning) RFID tags of personnel while in a visitor's area near by the entrance gates;
- calling employees to reveal their password;
- sending E-mail to employees to reveal sensitive information;
- react on a job opening, after receiving the invitation for a job interview, and use the opportunity to get access to restricted areas while in the building;
- try to borrow access cards from employees;

[78] http://www.globalservices.bt.com

- look for sensitive information at waste bins, copiers, printers, scanners or any multifunctional devices;
- contacting the helpdesk to reveal a password of a user account already known (as seen on a locked screen while being in your building).

The result of the assessment is presented in the form of a detailed description of the tests that have been carried out, a list of all identified vulnerabilities and a set of mitigation actions.

7.4.4. Allianz

Allianz[79] is one of the largest insurance companies in the world. Amongst its insurance services, Allianz offer the Allianz Cyber Protect product, a cyber-insurance covering, with a limit of indemnity of up to €100 million for the most sophisticated clients, the following aspects

- Data breach liability - for personal & corporate data
- Data breach costs - including notification costs & IT forensic costs
- Network security liability - for hacked or compromised systems including denial of service attacks
- Media liability - for digital publications
- Business interruption - caused by a cyber incident
- Restoration costs for data & programs - resulting from a cyber business interruption event
- Crisis communication - to mitigate reputational damage
- Hacker theft cover - based upon theft of funds
- E-payment liability - PCI fines and penalties covered

Allianz, in its white paper [226], fully recognizes the human factor as one of the major weaknesses of an organisation and awareness as one of the main countermeasures: *"… Employees can cause large IT security or loss of privacy events, either inadvertently or deliberately. … Employees can easily create outages (intended or unintended) or cause data leakages. Improving employee awareness of the risks involved is crucial …"*.

7.4.5. Digital Shadows SearchLight

Digital Shadows[80] SearchLight™ is a data analysis platform aimed at generating a view of the digital footprint and the profile of attackers of an organisation using the approach described in Figure 40.

[79] http://www.agcs.allianz.com
[80] https://www.digitalshadows.com

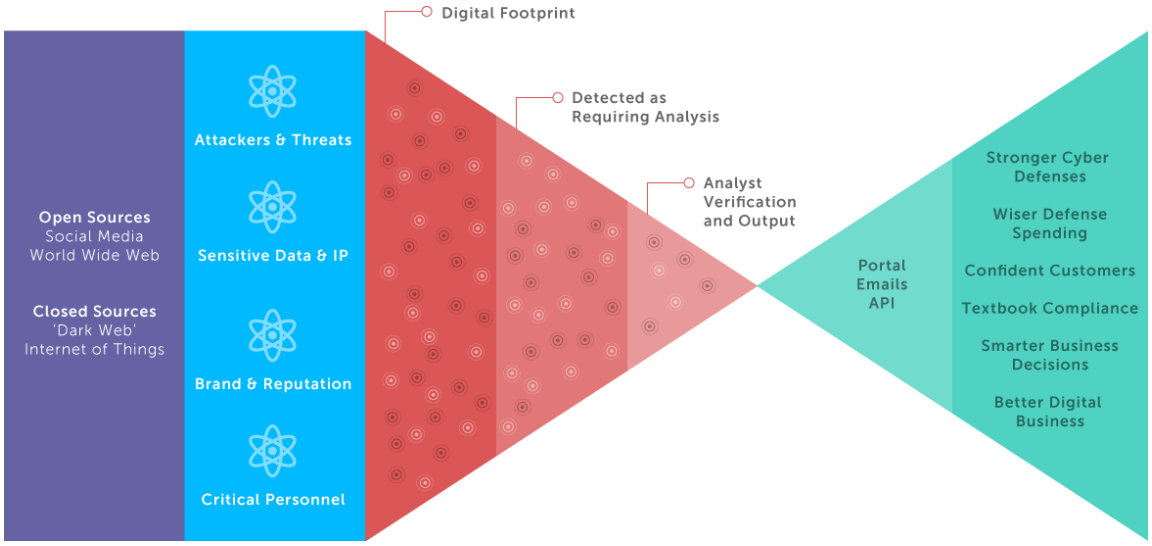


Figure 40 - Digital Shadow Search Light™ approach (Source Digital Shadow)

The approach is based on the digital shadow concept. Digital shadow [229] is defined as "*A digital shadow, a subset of a digital footprint, consists of exposed personal, technical or organizational information that is often highly confidential, sensitive or proprietary. As well as damaging the brand, a digital shadow can leave your organization vulnerable to corporate espionage and competitive intelligence. Worse still, criminals and hostile groups can exploit a digital shadow to find your organization's vulnerabilities and launch targeted cyber-attacks against them*".

SearchLight™ integrates:

- a threat intelligence tool;
- a Dark Web search tool covering Tor, I2P and criminal sites, as well as IRC conversations, including full page content and screen shots;
- real-time alerts and reporting;
- identification of data loss;
- assessment of malicious actors with the level of threat each actor poses and its geographical map view.

SearchLight™ continuously monitors the organization's digital shadow, identifying incidents as they occur, delivering only relevant alerts and regular reports by email, through the client portal and/or through API as required.
Also in this case the accent is on the IT part of an organization and not on the human factor.

7.5. Security metrics

7.5.1. The Dagstuhl Seminar framework

While many different metrics have been defined to estimate vulnerabilities in information systems [218], metrics necessary to estimate SE 2.0 security risks and the costs and effectiveness of countermeasures are not yet mature. An interesting approach to be considered for the DOGANA foundations has been reported as outcome of the Dagstuhl

Seminar [224]. The report tries to set a framework by identifying the properties of interest, the corresponding measures and by indicating possible actions based on measures.
In trying to define the measures of interest, the seminar has proposed a first subdivision of metrics into two different types depending on the inclusion or exclusion of real-life threats[81]: Type I and Type II (see Figure 41). For Type II metrics it is also necessary to have metrics on the threat environment: they can be either probabilistic (based on known average frequencies or Bayesian) or strategic (game-theoretic) to represent non-adaptive and adaptive attackers, respectively.

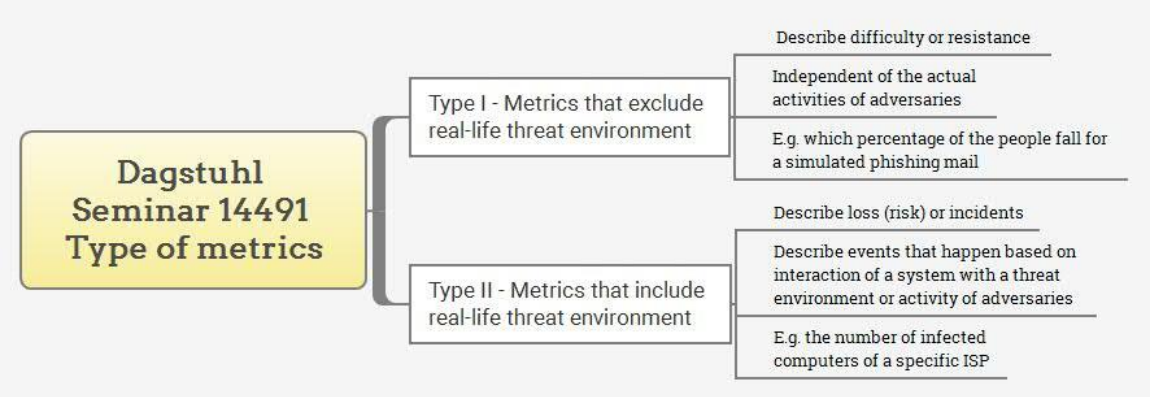


Figure 41 - The Dagstuhl Seminar types of metrics

The next step has been to identify the proposed socio-technical measurement methods, ranging from qualitative to quantitative indicators, from subjective to empirical methods, etc. A non-comprehensive list of such methods is described in the following Figure 42. An area that still requires research is the combination of methods to improve measurements quality.

[81] A simple example [224] justifies the need of the proposed subdivision: "*In system A, a locked door protects € 1,000. In system B, an identical locked door protects € 1,000,000. Which system is more secure? Or, alternatively, which door is more secure? One might say that system A is more secure, as it is less likely to be attacked (assuming the attacker knows the system). On the other hand, one might say that the doors are equally secure, as it is equally difficult to break the lock. The former argument is based on including an evaluation of the threat environment, the latter on excluding it.*"

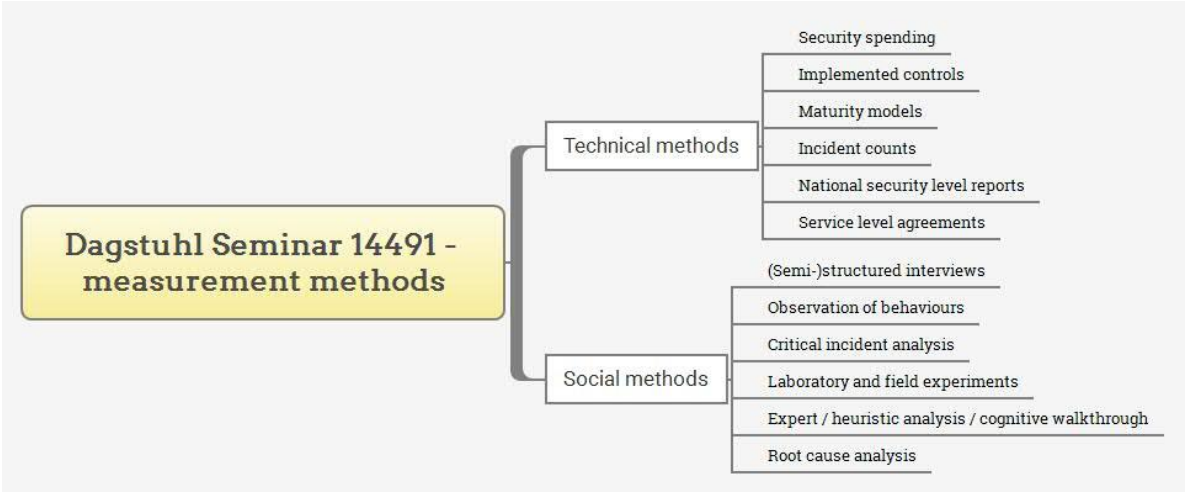


Figure 42 - The Dagstuhl Seminar measurement methods for metrics

The seminar has then addressed the possible usage of metrics for either knowledge or design assessment. The summary of the findings is described in Figure 43.

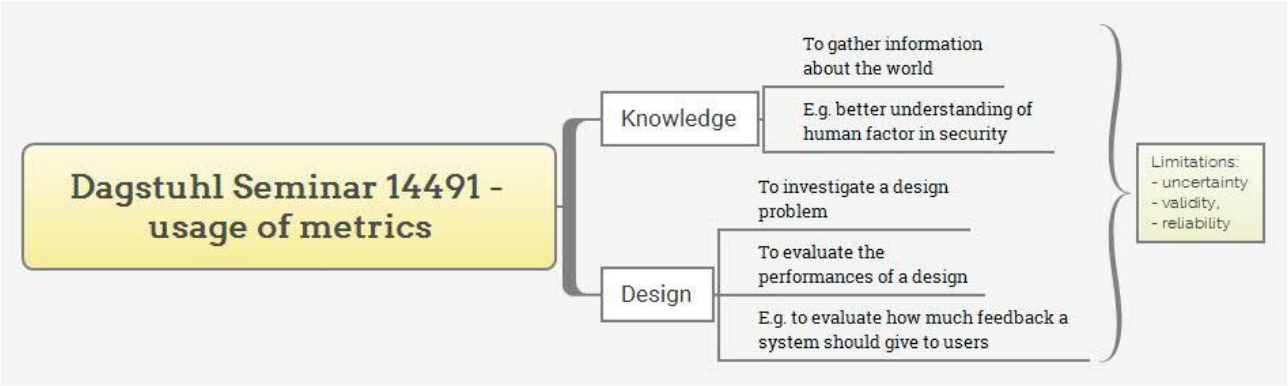


Figure 43 - Dagstuhl Seminar 14491 - usage of metrics

An interesting conclusion of the Dagstuhl Seminar to be considered in the DOGANA project relates to the possible stakeholders' strategic behaviour based on their knowledge of the metrics: the so called "gaming the metrics". If stakeholders' performances are rewarded on the metrics output (the higher the better), they may put effort in improving the metrics output and not the real actual security.

7.5.2. The SANS Institute Security Metrics

The SANS Institute[82] has identified different options for measuring security awareness programs. It includes metrics for both measuring impact (change in behaviour) and for tracking compliance. They are reported in Table 3 and Table 4.

[82] http://www.securingthehuman.org/resources/metrics

Table 3 - SANS Metrics for measuring impact

Metric Name	What Is Measured	How It Is Measured	When Is It Measured	Who Measures?	Details
Phishing Awareness	Number of people who fall victim to a phishing attack.	Phishing assessment.	Monthly	Security team	These attacks replicate the very same ones cyber attackers are using. The goal is to measure who falls victim to such attacks. This number should decrease over time as behaviours change.
Phishing Detection	Number of people who detect and report a phishing attack.	Phishing assessment.	Monthly	Security team	Uses the above methodology, but instead of tracking who falls victim it tracks who identifies the attacks and reports them. This number should increase over time.
Infected Computers	Number of infected computers.	Help desk or centralized AV management software.	Monthly	Help desk or security team	Most infected computers are a result of human behaviour (infected attachments, malicious links, etc.). This number should go down over time as employees are trained.
Awareness Survey	Number of employees who understand and are following security policies, processes and standards.	Online survey.	Bi-annually	Security team or HR	Employees take a survey consisting of 25-50 questions that determine their understanding and following of policy. Questions can cover if people share passwords, know how to contact security and if they have been hacked.
Updated Devices	Percentage of devices that are updated and current.	When employees connect to an internal server or use an external service such as browsercheck.qualys.com.	Monthly	Security or technology team	Measure whether people are keeping their devices updated and current, especially when concerning BYOD (Bring Your Own Device).
Lost / Stolen Devices	Number of devices (laptops, smartphones, tablets) that were lost or stolen. What percentage of those devices were encrypted.	Reports to security team or by physical asset audits.	Monthly	Security team or asset management	Employees should be trained in maintaining physical security of their devices. In addition, if your organization has policies on the use of encryption for devices, this measures if employees are following them.
Secure Desktop	Number of employees who are securing their desk environment before leaving, as per organizational policy.	Nightly walkthrough.	Monthly or weekly	Information security or physical security team	Security team does a walkthrough of organizational facilities, checking each desktop or separate work environment and looking to ensure that individuals are following organizational desktop policy.

Metric Name	What Is Measured	How It Is Measured	When Is It Measured	Who Measures?	Details
Passwords	Number of employees using strong passwords.	Password brute forcing.	Monthly or quarterly	Security team	Security gains authorized access to system password database (such on AD or Unix server) and attempts to brute force or crack password hashes.
Social Engineering	Number of employees who can identify, stop and report a social engineering attack.	Phone call assessments.	Monthly	Security team	Security team calls random employees, attacking them as real cyber attacker would by attempting to social engineer the victim. An example could be pretending to be Microsoft support and having victim download infected anti-virus.
Sensitive Data	Number of employees posting sensitive organizational information on social networking sites.	Online searches for key terms.	Monthly	Security team (or outsource)	Do extensive searches on sites such as Facebook and LinkedIn to ensure employees are not posting sensitive organizational information.
Data Wiping or Destruction	Number of employees who are properly following data destruction processes.	Check digital devices that are disposed of for proper wiping. Check dumpsters for sensitive documents.	Random	Information security or physical security	Any digital devices that are disposed of (donated, thrown out, resold) may contain sensitive data. Check to ensure proper wiping procedures. Check any rubbish bins or dumpsters for any sensitive documents that were not shredded.
Device Physical Security	Number of employees who left their devices unsecured in their cars in the organization's parking lot.	Do a physical walkthrough of the parking lot and identify any cars that have devices that are visible on a car seat.	Monthly	Information security or physical security	While your organization's parking lot may be a secured environment, this measures employee behaviours. If they are leaving unsecured or visible devices in their car at work, they are most likely doing it when they are off facilities, as well.
Facility Physical Security	Number of employees who understand, follow and enforce your policies for restricted or protected access to facilities.	Test how many employees are wearing their badges or stopping those who are not.	Monthly or weekly	Information security or physical security	For many organizations, physical security is a major control in reducing risk, especially when dealing with secured facilities. This metric will test and measure people's understanding and enforcement of this control.

Table 4 - SANS metrics for tracking compliance

Metric Name	What Is Measured	How It is Measured	When Is It Measured	Who Measures?	Details
Training Completion	Who has or has not completed annual security awareness training.	Reports from LMS or sign-in sheets for onsite workshops.	Annually	Whoever is responsible for primary training.	Primary training is when people are taught all awareness material for the first time or in a single sitting, usually online computer based training (CBT) or onsite workshops.
Communication Methods	Types of reinforcement training, who it is being communicated to, and how often.	Track and document when and how materials distributed to communicate program.	Monthly	Security awareness team.	For a security awareness program to have an impact it must communicated to people on a regular basis. This metric measures other communications methods that repeat and reinforce lesson objectives from annual training. Examples of such metrics can include: • Monthly hits to internal security blog or website. • Distribution of newsletters, posters or screensavers • Tip of the day questions • Number of attendees for Lunch-n-learns • Number of attendees for Podcasts / Webcasts • Number of mousepad, Sticky notes or other materials distributed • Number of security awareness emails sent
Policy Sign-off	Ensuring employees have completed training, acknowledge they understand the training and will adhere to the policies.	Signature or sign-off.	Part of annual review.	Supervisor and/or human resources.	From a compliance perspective you may be required to document that employees not only received training, but acknowledge they understand and will follow the training.

7.5.3. Human Aspects of Information Security Questionnaire (HAIS-Q)

The use of the Human Aspects of Information Security Questionnaire (HAIS-Q) to measure the human vulnerability to SE attacks using a self-report measure has been presented in [265]. The HAIS-Q is aimed at estimating "*the relationship between knowledge of policy and procedures, attitude towards policy and procedures and behaviour when using a work computer*" and is focused on 7 focus areas: internet use, email use, social networking site use, password management (including locking workstations), incident reporting, information handling and mobile computing.

The HAIS-Q is addressing 3 different types of behaviours - Good behaviours (Deliberate) Neutral behaviours (Accidental) Bad behaviours (Deliberate) – and considers the human aspects of information security shown in Figure 44.

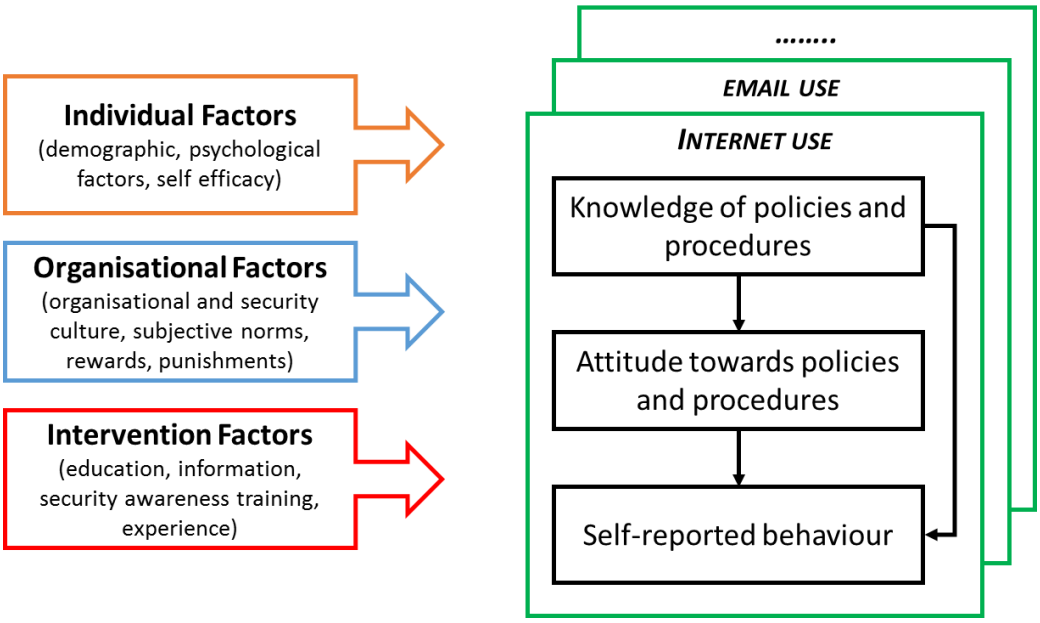


Figure 44 - The HAIS-Q model

7.5.4. Common Misuse Scoring System (CMSS)

Other alternatives for measuring the risks inducted by SE is through metrics that, despite not being specifically meant to include SE attacks, are generic enough to consider this threat as a special case. Among the most interesting is the **Common Misuse Scoring System (CMSS)** [263], which is a set of measures of the severity of software feature misuse vulnerabilities. CMSS is the third of the vulnerability measurement and scoring specifications, the former two are the Common Vulnerability Scoring System (CVSS) and the Common Configuration Scoring System (CCSS) [264]. CMSS fits better because it is open by nature: the vulnerabilities addressed by CVSS and CCSS are concrete (known software flaws and security configuration settings), yet a dictionary of software feature misuse vulnerabilities does not exist.

The description of the metric reports: "*A software feature is a functional capability provided by software. A software feature misuse vulnerability is a vulnerability in which the feature also provides an avenue to compromise the security of a system. Such vulnerabilities are present when the trust assumptions made when designing software features can be abused in ways that violate security. Misuse vulnerabilities allow attackers to use for malicious purposes the functionality that was intended to be beneficial.*"

SE is included as a special external case of misuse of the software systems. This is a rough approximation of which types of threats SE exploits, but for the scope of software security, in most situations, the approach works well-enough. An example is reported in the document

[263], section "User Follows Link to Spoofed Web Site": "in case of phishing the hyperlink capability is misused because takes the user to a malicious site". SE is clearly considered to indirectly abuse a software functionality rather than the human.

7.6. Current trends in legislation and policies for fighting SE

7.6.1. EU policies

The EU's Digital Agenda [231] forms one of the seven pillars of the Europe 2020 Strategy which sets objectives for the growth of the European Union (EU) by 2020. The Agenda proposes actions covering the following aspects: achieving the digital single market, enhancing interoperability and standards, strengthening online trust and security, promoting fast and ultra-fast Internet access for all, investing in research and innovation, promoting digital literacy, skills and inclusion and ICT-enabled benefits for EU society.
For DOGANA the obvious field of interest lies in the III Pillar related to strengthening online trust and security, where 14 actions have been identified. Amongst these it is worth highlighting the following initiatives:

- Action 29: "Combat cyber-attacks against information systems" under which the "Directive on attacks against Information Systems"[83] was adopted by the European Council on 22 July 2013 and EC is ensuring implementation of the Directive by September 2015 and continuing to monitor cyber-threats.
- Action 33: "Support EU-wide cyber-security preparedness". Under Action 33 ENISA is planning the "Cyber Europe 2016"[84] a pan-European set of exercises to enhance trust and confidence in online services across Europe.
- Action 123 "Proposal for Directive on network and information security". The Directive[85] has been adopted in 2014 and Member States have 18 months to reach agreement on it. Its adoption could improve the exploitation potential of DOGANA approach.
- Action 124: "EU Cyber-security strategy" aimed at enhancing cyber resilience of information systems, reducing cybercrime and strengthening EU international cyber-security policy and cyber defence. Under the framework of Action 124, EU has published the "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"

[83] European Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA 2013

[84] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", Brussels, 7.2.2013, JOIN(2013) 1 final

[85] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union 2013, c. 2013/0027 (COD). Available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1666

7.6.2. Legal implications in fighting SE

Because social engineering involves a human element, preventing these attacks can be very complicated for companies. The essential aim of a SE attack is to trick the employee and force him7her to violate a policy. By doing this, cybercriminals do not have scruples, using whatever information they can retrieve.
Even if SDVA has the same purpose, companies must observe severe moral and legal limitations. From a moral perspective, the assessment should be executed guaranteeing the respect of the relationship between employer and employee, avoiding invading the personal sphere.
Moreover, it is necessary to consider the labour legislation regarding the privacy of employees that particularly in Europe protects employees from any interference of the employer.

Article 8 of the European Convention on Human Rights grants everyone "the right to respect for his private or family life, his home and his correspondence". However, in Niemietz v. Germany[86], the European Court of Human Rights extended this fundamental right to privacy to activities of a "professional or business nature", and it has been used ever since as a legal basis for privacy protection in the workplace. Per this ruling, there is no distinction between private or professional correspondence and therefore every European has the right to respect for his business relations, e-mails, and electronic correspondence.
Now, the main European Union document partly regulating the relationship between the employer and the employee in the matter of controlling electronic workplace is the European Parliament and Council **Directive on the protection of personal data and on the free movement of such data (95/46/EC).** This Directive lays down the general principles under which data controllers must process personal data (including employers handling employees' personal data). Even though this Directive is not directly addressing the issue of employer's surveillance, it inserts privacy principles already argued in employer/employee disputes regarding surveillance in the workplace.
Another EU Directive dealing with privacy and e-communications is **EU Directive 2002/58/EC**. As a general principle, Directive 2002/58 prohibits interception of private communications over networks; this includes e-mails, instant messengers, and phone calls. However, the Directive specifically addresses public networks and public employees; thus, surveillance of private employee's communications under internal-private networks is not protected by this Directive.
It is also important to mention that **Article 29 Working Party** (formed according to EU General Data Protection Directive 95/46/EC, Article 2910 consisting of various national data protection authorities) has adopted Opinion 8/2001 on the processing of personal data in the employment context. The Opinion established a set of fundamental data protection principles that employers should comply with when processing personal data of individuals, setting a framework scene on how Directive must be interpreted regarding more specific employee data protection issues. Another relevant Working Party document is the Working Document

[86] Niemietz v. Germany (1993) 16 EHRR 97

on the surveillance of electronic communications in the workplace (29 May 2002)[87]. This document is designed to offer guidance and concrete examples about what constitutes legitimate monitoring activities and the acceptable limits of workers' surveillance by the employer.

As the Directive doesn't have direct applicability in the Members States, the impact of this Directive has been paramount, causing a dynamic of amending/modifying Member States' data protection laws among the lines of its general rules and principles. Therefore, the issue of workers' data protection needs to be assessed considering the Member States' legal framework, including social policy and labour laws, principles and traditions, which differ from state to state.
In general, all Member States of EU protect the right to privacy and is self-evidently influenced by the respective national legal and political traditions. There is a strong interaction of privacy and labour laws, implying that the application of the general data protection principles (as laid down in Directive 95/46) to the employment context, needs to consider the Member States' labour laws.

With the rise of the internet, technology evolved rapidly and the ways in which personal data could be used by businesses expanded. The explosive growth of social networking and big data analytics (among other things) made it increasingly clear that a new approach to data protection was required. Therefore, from 2012 The European Commission planned to unify data protection within the European Union with a single law, the **General Data Protection Regulation (GDPR),** which is expected to come into force by 2018. The Regulation is designed to further harmonise national data protection laws across the EU while, at the same time, addressing new technological developments. The Regulation will be directly applicable across the EU, without the need for national implementation. Businesses are likely to face fewer national variations in their data protection compliance obligations. However, so far it seems areas in which differences from one Member State to another will remain, including the employment one, as the Member States may adopt their own rules regarding the processing of personal data in an employment context (art.82).
Therefore, the main challenge in understanding if and how a company can perform a SDVA keeping into account the labour laws applicable in a certain country and the way these laws interact with and implement the privacy and data protection principles.

7.7. The role of Social Driven Vulnerability Assessment

In general, traditional approaches to IT security and risk management tend to underestimate (or even ignore) the human factor in the assessment models, tools, processes and legal structure. This happens because the focus is still on technological part of the IT infrastructure, through setup and configuration of appliances and systems and traditional vulnerability assessment. Despite it still being the basis to guarantee a correct security posture inside companies, those security measures are no longer enough because cyber-attacks increasingly

[87] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec16

rely on human vulnerabilities. Cybercriminals understood they might leverage on social engineering techniques to manipulate their victims and obtain sensitive information, simply convincing them to perform certain operations, thus increasing the success rate of attacks.
Social Engineering attacks may put company information at risk, therefore, nowadays it is necessary to extend IT security governance to include also the human factor into corporate risk analysis and assessment. In this context, the role of so-called Social Driven Vulnerability Assessment (SDVA) is therefore very important: this kind of assessments allow better understanding the current extent of the threat, measuring the actual risk and potentially finding effective and tailored countermeasures to mitigate it.
Involving employees in an assessment is a relatively innovative approach and it is considered risky; planning the assessment in a proper way assumes an important role. First, IT and security departments are not the sole actors to define the assessment, because people are the target. Therefore, it is necessary to involve all the relevant stakeholders, such as human resources (HR), legal and communications departments, to explain the threats, share the objectives, define the scope of the assessment and obtain commitment. Moreover, several ethical concerns and requirements need to be considered when performing an assessment on the human factor [241].
Social engineering attacks mean that an employee is deceived into violating a policy. Even though unscrupulous cybercriminals will make these attempts, enterprises must observe serious ethical and legal limitations guaranteeing the respect of the trust relationship between employer and employee and avoiding invasion of an employee's personal sphere. Furthermore, it is necessary to consider the labour legal frameworks, which are radically different between countries in Europe. Despite the limitations and the presence of some legal and ethical risk, the topic must be considered.
In recent years, there are examples of research and study on the topic [240] and of attempt to create dedicate frameworks aimed at measuring the risk [230]. For example, the main part of a SDVA could be aimed at measuring how personnel react during a phishing simulation attack, thus exposed to drive-by-infection and/or drive-by-download attack schemas. The results is the actual measure of the inclination of employees to fall victim to such an attack, and it is possible to estimate the level of exposure of the enterprise to technological follow-up attacks from the simulated phishing campaign (e.g., identifying unpatched services that can be exploited through a system fingerprinting).
The results of Social Driven Vulnerability Assessments may be useful both to raise awareness within the employees and to obtain commitment from senior management to implement mitigation actions.

8. Foreseen Evolutions

In this chapter we discuss the current, prevalent view on the future of cyber related Social Engineering. In her talk on the future of social engineering at the international NCSC conference in 2013 S. Conheady [266][279] summarizes her presentation with the following thoughts on the future of Social Engineering:

1. Same tricks, new technology
2. More sophisticated and targeted Social Engineering attacks
3. Social networking as an enabler to SE
4. More technology to improve / automate SE Attacks
5. Social Engineering as a service

This is an interesting view into what an expert expects to see in SE in the future. There will be a more critical look at this list later in the chapter with attention to the first item: "Same tricks, new technology".

As anticipated in chapter 3 Social Engineering is fuelled (both at the attacker and at the victim's level) by human nature. Conheady [286][294] makes the case that the fundamental "human nature" (psychological, sociological, cognitive) aspects of social engineering are the same today as they were centuries ago. What has changed is the arena in which SE operates. She then naturally concludes that there is no reason to suppose that the fundamental tricks will be any different in the future. What is expected to change and evolve soon is the technological scenario in which the social engineer will operate. Thus, both the tools of the social engineer as well as the details of the "sting" may be dramatically different than in the past. In any case, the basic weak points of human nature that facilitate the abuse will **remain the same.**
We thus begin this chapter on the future of SE by describing some of the expected changes in the technological arena as they relate to the expected evolution of Social Engineering [278][279][280].

8.1. Technological Trends

The clear majority of technological trends that are expected to affect SE in the near future have already begun. Many of these trends will provide a new arena for the social engineer whereas others will assist the social engineer in carrying out his scheme. On the other hand, it is already predictable that new appearing technologies will assist developers, users and the public to protect themselves from social engineers in ways that are, today, not feasible (e.g., behavioural security above all).

One of the best ways to look into the future is to see what has happened in the recent past. Modern Social Engineering (what we call Social Engineering 2.0, as defined in chapter 1) is enabled by two main technological trends:

- The huge proliferation of computing devices (computer, laptops, smartphones & tablets) – used by nearly everyone
- The extremely high level of interconnectivity between these devices both at the hardware level and at the user level in which social networks and cloud computing have provided a very profitable scenario for social engineers.

A first look at the future of social engineering leads us to a parallel list of trends. Social Engineering of the future will likely be enabled by:

- The huge proliferation of smart devices of all kinds – devices that interact with the world around them and are meant to provide a service to their user.
- The extremely high level of interconnectivity between these web-enabled devices (e.g. Internet of Things).

8.1.1. Internet of Things (IoT)

It can be argued, convincingly, that the Internet of Things is already here. Web connected devices are everywhere and their prominence is increasing at a very high speed. Figure 45 below is taken from [267] and is indicative of the high rate of expected growth of connected devices in the next few years. This phenomenal growth is expected to have significant consequences for social engineering [283][284][285].

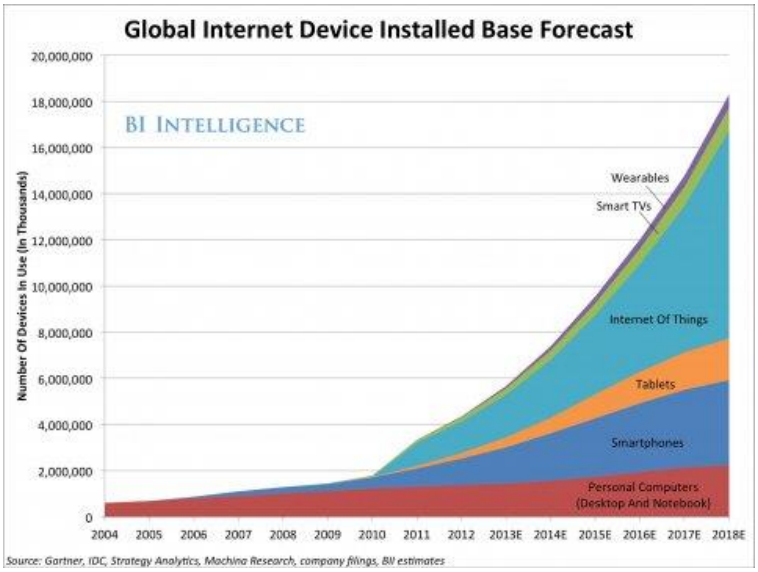


Figure 45. Global Internet Device Installed Base Forecast [267]

It is clear that if a cybercriminal can gain control of a multitude of such devices he/she can wreak havoc and cause significant damage [273][274][275][276].

Personal Data Collection in IoT

The most dramatic effect of the Internet of Things (IoT) on SE (especially on SE 2.0) is the ability to collect a huge amount of personal data that can subsequently be used to perform a targeted and/or a personalized SE attack. The more data are available to a SE attacker the better he/she can personalize the attack. Currently, in the context of ubiquitous devices, personal information is mostly obtained from smart phones and tablets. However, the multitude of IoT objects is extremely vulnerable to release a huge amount of information, also due to weak nature of common protections used to date[88]. All this information can be used to improve for

[88] For example refer to the following link "Millions of IoT devices using same hard-coded CRYPTO keys," [Online]. Available: http://thehackernews.com/2015/11/iot-device-crypto-keys.html. Accessed: Feb. 1, 2016.

example the level of contextualization of the attacks, which is a natural consequence of the improved knowledge of the attacked humans (see also the discussion in Section 2.4).

Some examples of the kind of information that could be available:

- Medical/fitness information: Pulse & heart rate at various times of day, exercise times and locations, diseases, blood sugar level – all in real time and with capabilities for obtaining a history of these parameters.
- Home habits ranging from times when meals are served, the family menu, sleep times, air conditioning/heating habits, etc.
- Hobbies
- Driving habits: Although this information is available today to Google and several other companies we can expect its availability to be much more widespread as "connected cars" become more prominent.
- Increased information regarding "real-life friends" (as opposed to social network friends) through increased ability to correlate locations of different people
- Increased use of Fitbit, Google Glasses, etc. expose a huge amount of personal information such as: geo-location, heart rate, sleep, activities.
- ….

It should be understood by now how the Social Engineer uses this information. When he directs, for example, a spear phishing attack he uses the information to personalize his message and convince the target that he is a legitimate party to a future mutual interaction. There are many other ways that this personal information could be used. A simple example is password recovery using one or more personal questions. The more personal information we have the easier it is to respond to these questions (e.g., it is reported that often people choose easy questions and give truthful answers to these questions[89]).
There are several ways for social engineers to get this information. They could either remotely hack the online devices (Most IoT devices are lacking in proper security features and, due to the cost constraints, this situation is not expected to change significantly soon). They could hack the access points (such as router or cellular entry point) or they could also hack the service provider (where the data is stored or at least through whom the data passes). A potential social engineer could provide an app that monitors IoT devices and then use the data for SE attacks. The potential supply chain for IoT products also provides a possible concern and, finally, it is highly likely that the cybercriminal of the future will be sufficiently innovative to find a way to obtain the information that he needs [291][292][293].

Payments with IoT

Another aspect of SE that will increase with the proliferation of IoT is the mass of people to make payments through their devices with weak passwords and/or other credentials – all in the name of user convenience. We see this phenomenon today with (for example)

[89] For example refer to the following link "Top 10, 000 passwords are used by 98.8% of all users," [Online]. Available: https://uwnthesis.wordpress.com/2012/08/30/top-10000-passwords-are-used-by-98-8-of-all-users/. Accessed: Feb. 1, 2016.

smartphone payments that do not require the user to enter any credentials. Google payment for apps or in-app payments are probably the most well-known example. A huge number of people have their smartphones set up for payment with no password required. This is a kind of situation Social Engineers could profit. The situation is expected to get worse (better for the social engineer,) in the future as IoT proliferates. Many IoT devices will be set up for direct payment. The low cost of these devices will limit their ability to perform proper authentication. Even if they do, their expected weak security profile may allow relatively easy bypass of the security features.
Thus, (IoT) payment technologies will offer more ways to pay but with less security. The model of "un-passworded" payments from smartphones will pass on to IOT "carryable" devices. People likely will be socially engineered on mass to make payments in the easiest possible way.

Blackmail
More information yields more opportunities for blackmail, which is a lucrative form of crime. Blackmail is, of course, even today a lucrative form of cybercrime. However, the huge amount of possibly unprotected data obtainable from IoT will increase this phenomenon significantly. A good example of this are the images from cameras on smart TVs that, if compromised, could readily be used for blackmail. This information could be correlated with the victim's "ability to pay" which would also be more easily obtained via the proliferation of IoT sensors.

New, creative SE ideas
When your light bulb (used here as an example of a hitherto benign and minor part of one's home) becomes part of the attack surface, there is room for new and innovative SE attacks. Turning all the lights off in a home, for example, (or, for that matter, creating any other significant discomfort) makes most people much more vulnerable to manipulation. This same scenario applies to all the smart environments, which usually include offices, cars and vessels.

Looking for High Value Targets and Information
IoT and new gathering technologies will allow cyber criminals to look for the most valuable victims "high value targets" as well as the most valuable information such as financial, social, criminal etc. The proliferation of sensors and immense connectivity will create a revolution in Open Source Intelligence (OSINT) using "Big Data" (i.e., developments in data analytics) to make the extraction of this information from the data much more reliable.

Advertising
IoT provides a new fertile ground for what is probably the oldest form of social engineering – advertising[90]. There are two prominent aspects to advertising in the IoT world:

[90] Malerstising involves SE because it required to attract the victim to click on a fake advertisement which was properly created. See for example "Realtor.com the latest victim of malvertising plague,". Available: http://goo.gl/7PSW4P and "Blue Coat Systems 2014 Mobile Malware Report,". Available: http://goo.gl/VUhwVV. Accessed: Feb. 1, 2016

1. Personal information is the fuel that drives directed advertising. In today's world, personalized advertising is far from perfect. This is due partly to the lack of sufficiently detailed information. The proliferation of IoT information together with developments in data analytics is expected to improve personalized advertising dramatically[91].
2. Companies do and will continue to advertise via IoT devices. When a refrigerator for example is low on milk, you will receive a notice, either via a "talking refrigerator" or on the smartphone with an ad for milk. If the baby monitor senses that the baby is crying at night, it may suggest a product to help alleviate the problem. Even children's toys will not be immune: not only they will advertise related products (hopefully subject to applicable laws), but they may remotely "share" information among users directly via the toy; thus, porting the Facebook model to IoT devices usable even by small children. (Legislation will need to keep up with these developments.)

Quantified Self / Augmented Human

The "Internet of Things" is a catchall phrase whose boundaries are ill defined (or, at least, there is significant disagreement on the boundaries). The term "Internet of Everything" is often used to include all connected devices [283][284][285]. There are several sub trends in the world of IoT applications. We now discuss briefly the SE aspects of one of the most notable such trends: Quantified Self (with the related trend referred to as the Augmented Human) [281][295].

A "Quantified Self" would be a person who has a variety of sensors on and around his/her person with the purpose of measuring whatever possible about his/her daily life. Some people may only use a single sensor, for example an asthmatic may purchase a wireless inhaler with a GPS that measure the precise location of each time the inhaler is used. This one, combined with the sensors on the user's smartphone, enables the user to obtain a profile of his/her disease and thus help to control it. Of course, adding a heart rate and breathing monitor as well as body temperature sensor will increase the value of the data to the user. This way, user may opt for these extra sensors[92].

The one above is a simple example. Many people have decided to measure everything they can about themselves including sleeping data, physiological data, location, moods, speech information, environment etc. Such devices could allow advertisers or cyber criminals to exploit cognitive biases that may be obtained automatically. This would then allow them to attack automatically when a target's vulnerabilities are heightened (i.e. when their guard is down). This is a modern version of the old SE trick used in selling expensive funeral arrangements to bereaved families based on, for example, newspaper obituaries.

It is advertised in the specific sector studies[93] that sensors will be everywhere, implanted in nearly everything imaginable, networked and connected. A related trend adds active components to devices that people carry around with them. This version of IoT can trick a

[91] See for example the following source from realtor.com "latest Victim of Malvertising Plague", September 2015, http://goo.gl/7PSW4P

[92] Beside this trend exposes the users to **cyber-murder** scenarios such as "Hacked Medical Devices May Be The Biggest Cyber Security Threat In 2016", Popular Science, http://mcaf.ee/b6pqut

[93] For example "22% Of Tech Leaders Say Wearable Computing Is The Next Big Thing In Mobile", *Business Insider India*, http://mcaf.ee/qbizmr

person into harming herself or others. In other words, if (when) a vulnerability is found in such a system, the devices themselves (directed by an attacker) can become the social engineer encouraging you to run and not drink enough, take medicines inappropriately, take money out of the bank etc. This could lead to a Pretexting or Reverse Social Engineering scenario (see section 4.4.4) useful for reaching the Social Engineer goal.

Driverless Cars, Airplanes, and Unmanned Services in General

Car manufacturers are working intensively on development of the "driverless car". We are told that the world of unmanned aircraft will eventually evolve towards unmanned commercial flights. We are surrounded by services that, in the past, required people to operate but today operate autonomously. The best-known examples are cash machines, banking in general, check-in kiosks at airports though the list is nearly endless. It is widely appreciated that all these automated devices must be secured against cyber-attacks (though implementation of this security is extremely slow). However even if (ideally) these devices could be properly secured, they provide a fertile platform for a variety of social engineering attacks.

Not only SE can be used to attack these devices, creating losses, damage and general havoc but these devices can be used to extract information for use in an SE attack and as a platform for "communicating" with a victim. One of the oldest examples of that is the use of fake bank machine facades to obtain bankcard information. With all the new platforms becoming available, the opportunities are endless for a social engineer.

Other Aspects of SE in the Future IoT Environment

- An attack on IoT systems can trick a user by feeding him/her with misinformation to execute complex commands as to the cyber criminal's wish.
- A coordinated attack on many IoT systems simultaneously has the potential to create havoc. The social engineer can then utilize this havoc to manipulate victims in a variety of (yet unknown) creative ways.
- Attacks, for example, on a corporation will be harder to stop when a cybercriminal can study the Vice President's voice, habits and preferences without being detected.
- Successful SE attacks via IoT can give people the perception that they are surrounded by hostile devices. This could retard the development and public acceptance of IoT devices. Thus, the consequences of SE on IoT may be very significant.
- As IoT devices become more prevalent and cyber-attacks on these systems become more damaging, new technologies for authentication and encryption of low-resource "Things" will be developed. These developments have already begun (e.g. multiparty authentication) but there is a long way to go!

Extension of security to the physical world: safety

IoT devices operate both in a virtual and in a physical world, and the environment is consequently characterized by the convergence of Information Technology (IT) and Operational Technology (OT) [268]. Traditional security issues must be addressed also in the IoT scenario (IT). As far as the operational capabilities of IoT devices are concerned (OT), also safety issues must be considered. In fact, the power of the attacker is not limited to the cyber-

space, but is extended to the physical space of the victim, and the IoT devices could, in general, have been designed to perform dangerous operations.

Social Engineering is often defined as the act of influencing a person to make him taking an action that is not in his interest. In this new scenario, the attacker can provide false information to convince his victim to execute complex sequences of operations in the physical world. The attacker can gain power on the physical environment of his victim, or persuade him to modify it in such a way that it can be successively maliciously exploited. Thus, IoT drastically enlarges the space in which improper actions can take place, with the possible consequence of making the common user feel the IoT as a dangerous technology. One fact is to be afraid that a malicious agent hidden in a computer will steal us information, another one is to be afraid that a device will physically hurt us. This can have the undesired effect of slowing down or even stopping the effective deployment of such promising technology.

Types of possible attacks are presented below to figure out how a social engineer can operate, both in the victim's physical and virtual space:

1. attacks that are completely performed in the cyber-space (traditional social engineering), e.g., ask to set the credit card code as a default configuration of an IoT device, with the excuse that this would improve the user experience;
2. attacks that originate in the cyber-space but have effects in the physical one. For instance, the attacker can fake the data collected by a medical instrument (e.g., very high blood pressure) to convince the victim to perform improper actions that have dangerous effects on his health (e.g., use of a medicine).

How SE can affect the business revolution of IoT

IoT is expected to revolutionize the way many services are currently offered, and it consequently has a promising business impact. The collection of very personalized data, as well as the ability of things to operate in the physical world, enable the development of high-level and specifically-tailored services for the users (e.g., medical-related services). However, such strong points are also the factors that most improve the capabilities of social engineers, and can make the IoT be perceived as a weak and dangerous technology. To allow this revolution, the academy and the industry must look for solutions which are cheaper than the current ones (to facilitate the deployment of devices) and that drastically reduce the freedom of movement of social engineers. Otherwise IoT will destroy instead of creating value. We now present the main aspects that it is necessary to focus on: development of well-defined security standards, and implementation of light but still effective security processes [269][272].

Now, there is not a widely-adopted security standard in the IoT world (such as the ISO 27000 for the traditional IT network). Without a coherent regulation, IoT networks become even more complex than what they already are. Thus, each network requires an individual and unique security investment/assessment [271]. The heterogeneity of IoT networks at all the layers (from the physical to the application one) make the malicious actions of a social engineer easier. Very heterogeneous systems should not lead users to properly know their

devices and how they work. The social engineer can exploit this weakness, since he can more easily persuade the victim that a dangerous operation is a good one.
As far as security processes are concerned, being IoT devices resource-constrained, traditional authentication/encryption procedures are hardly applicable. The development of more suitable security technologies will be a beneficial remedy also against social engineering attacks, since the easier is to send and display fraudulent messages via IoT devices, the easier social engineering will become [270].

8.1.2. New and Evolving Software Tools

There are varieties of software tools that have been developed supporting the work of the Social Engineer. As discussed above it is difficult to predict what new methods (in this case software) will be available but we can predict with relative certainty that the software tools that are in their infancy today as SE tools will either develop into more sophisticated and aggressive tools or they will be replaced by other tools with greatly enhanced abilities.
A partial list of software available today and whose utility is expected to evolve in a significant manner, see section 5.6 Attack tools. This software are made for the white-hat penetration testers or those who want to measure their digital footprints to perform SE-like OSINT tests (and actually are part of the KALI distribution). Being open-source these tools could anyway be used more and more as social engineers in an entangled co-evolutive loop.

8.1.3. Developments in Data Analytics

Data Analytics (or, simply, “Big Data”) is one of the most active areas of research in cyber technology in general and in cyber security. Data Analytics is a rapidly developing field that is expected to improve in leaps and bound in the next few decades.
Interestingly, Data Analytics provides an excellent opportunity, not only for the defender but also for the attacker. We have discussed, at length, earlier in this chapter the huge amount of new data that will certainly be available in the future (even relative to the large amount available today). For a SE attackers to be able to make full use of this data in an automated way they must use the evolving techniques of Big Data. This will allow more automation in the attackers search for information and especially as it relates to finding the most valuable target to attack. Data Analytics could be used, for example, to find bank managers who post enough personal details on their Facebook pages (for example) to allow the attacker to access the bank's database, possibly via a compound attack of SE, with personal contact and malware.

8.1.4. Developments in non-SE Cyber Security

The enormous effort that is now going into cyber security is constantly producing new and better protection systems. Techniques are being developed for speeding up antivirus and firewall software, new techniques for discovering zero day attacks are being developed, microprocessor manufacturers are developing hardened integrated circuits, Big Data analytics is being developed for detecting distributed attacks etc. At the same time, relatively little research is being done into the mitigation of social engineering attacks.

As technological methods for preventing cyber-attacks improve, attackers will opt even more than today for social engineering as a major component in their attack strategy. Increase in non-SE security means more social engineering attacks.
People are the weakest link. Even biometrics is not fool proof. We may also see more compound attacks that use SE followed by malware injection and even SE followed by malware injection and then followed again by SE. In addition, we can expect to see a great deal of new innovative attacks.
This same trend will likely be seen for IoT devices. We shall inevitably see increased security on IoT devices (despite the cost-size challenges). This will then lead hackers to use social engineering as an integral part of their toolset.

8.1.5. SEO Poisoning

SEO (Search Engine Optimization) poisoning is as old as search engines themselves and, although both technically and practically a hacking activity, it is practiced not only by stereotypical hackers but by a very large number of (otherwise) legitimate companies. The idea is to engineer certain parameters on your own website so that your links come up first (or close to first) on a search engine's results.
Malicious hackers make use of SEO to inject viruses or Trojans to a victim's computer by using the well-established fact that people tend to trust and thus blindly click on nearly any link that makes it onto the first page of a search engine. Most unsophisticated users are unaware of this vulnerability which is a very basic form of Social Engineering. Google and other search engines have developed algorithms to prevent SEO however, this has developed into a cat and mouse game.
One of the most recent trends in SEO poisoning (which we expect to see much more of in the future) is that instead of a site putting a virus or Trojan directly onto your computer the site may start to form a relationship with the victim for a future SE or reverse SE attack. (A reverse SE attack is one in which the victim is enticed to initiate the relationship with the attacker thus making the attacker seem more trustworthy) [282].
Several possible future trends have been identified in SEO poisoning:

- Attacks will get more sophisticated and thus more effective
- Victims may become more sophisticated and learn to put less trust in search results
- The major search engines may develop technologies (such as link scanners) to either warn or filter more of these malicious search results – more quickly.

8.1.6. Other Technological Developments

There are many technologies being developed that may affect the future Social Engineering in the Cyber domain. We shall briefly discuss two of such technologies.

- Future advances in the analysis of physical movement (Gait Analysis): In our discussion of Quantified Self, we dealt with the trend of people who implement a multitude of sensors to measure everything possible about themselves. This is an ideal situation for analysing a person's movement i.e. Gait Analysis. However, what interests a social engineer most (this is also of great interest to security personnel) is the relationship

between a person's gain and his mood and intentions. A social engineer could use these results to find a victim and to properly time his attack.

- Future developments in semantic analysis. For our purposes, semantic analysis is the process of analysing a sentence or expression by breaking it down into its phrases and words and then extracting some useful meaning from the sentence. The relevance to Social Engineering is clear. One of the main sensors, which already exists in our environment and will continue to increase in its presence, is the microphone. It is technically possible for our smartphone to listen to every word that we say without us being aware. This capability will increase in the IoT world. Improvements in semantic analysis will allow an attacker to learn more useful information about our environment, our habits and us in an automated way. This would then improve significantly his ability to carry out automated (or nearly automated) social engineering attacks.

8.2. Expected Trends in the Mitigation of SE Attacks

This section discusses some of the expected developing concepts for the mitigation of SE attacks. One might wonder why discussing this in a document on the role of SE in cyber-attacks. The reason is that mitigation techniques will greatly affect the evolution of social engineering. By reviewing what is expected to develop in mitigation techniques we can begin to prepare for the counterattack by the social engineer. This section briefly discusses some of the trends in SE attack mitigation that are expected to be implemented soon [286].

- Moving away from "front door" protection to "data protection": The idea is that a social engineer can often enter right through the front door and bypass all possible protections. He can do this in many ways but the simplest is by managing to acquire a user's credentials. In cases where the dominant threat is the stealing of data from an organization a possible solution is to keep track of all critical data including its access history. This has been described as “checking the living room wall to see if your painting is still there” as opposed to just guarding the doors and windows to see if it is being stolen. This does not protect against the full variety of SE attacks but is a promising direction for an important protection layer.
- De-linking users (i.e. users' actions) from authentication: The current authentication paradigm of “Something I know + something I have” does not deal properly with the SE an alternative paradigm may be “Something that's me”. Biometric authentication is one example of this trend. In fact, it is reasonable to demand 3-factor authentication (for example: password, one time password (OTP), fingerprint) in critical areas such as banks, security systems, medical records etc. This would mitigate the SE attack based on obtaining a victim’s username and password (possibly including an OTP).
- It has been suggested that data analytics could be used to analyse a user's behaviour to see if the authentication used is reasonable or possibly anomalous.
- Developments in standoff lie detection technologies could detect phishing and other frauds without direct contact. An example of this would be semantic analysis of a received email and correlation with other data regarding the email.

- A shared opinion is that education and awareness are the key to mitigating social engineering attacks.
- It has been suggested that Social Engineering could be used as a mitigation tool. Society can use SE techniques to provide better programmers, better system administrators and better (more security savvy) user.

8.3. Other Trends

The Digital Revolution has led to significant social changes [277]. The most notable of these are social networks. Facebook was the main innovator in this area and still "leads the pack" but there are many other very significant interconnected social networks. Social networks have provided and continue to provide a ripe pasture for a large variety of social engineering activities. There have been several developments in social networks that will, in the future, affect how social engineering is done. Below are some notable examples:

- Social network phishing: We have all become accustomed to phishing spread via emails. In the past few years, phishing attacks via social networks have begun to appear. It is expected that this trend will grow at an alarming rate. Instead of receiving an email from Nigeria one might receive and email from one of your friends on Facebook (or another social network).
- Demographic trends in social networks: There has been a growing trend for young people to abandon Facebook for other social networks and for middle aged and older people to be more connected with Facebook. Typically, “older” people have more financial means. Thus, SE attacks on Facebook (as well as other networks frequented by those with a strong financial base) will become more lucrative and thus more prominent. At the same time, we may see re-worked attacks on social networks frequented by young people (possibly including children).
- There seem to be changing trends in the targets of social engineering attacks. There seems to be a move from the financial sector to gaming, healthcare (for obtaining medical data), politicians (for power brokering or possibly blackmail), war and terrorism (c.f. extensive use of social networks by ISIS).
- We may see changes to the Dark Web in the future. Several possible suggestions have been made in this regard:
    - The Dark Web highly in the focus of law enforcement worldwide and thus new monitoring technology may be developed causing the Dark Web to become "brighter".
    - On the other hand, we may see increased use of the Dark Web with more sophisticated techniques for hiding, sharing etc.

The Dark Web provides valuable resources for social engineers. The simplest example of this is that a successful SE attack often involves making use of a person with specific traits: language, accent, profile (probably fake), etc. It is common to see requests on the dark web for someone to help with certain kinds of phishing or vishing (voice phishing – using a telephone, for example) attacks.

- Non-connection is becoming counterculture. Being disconnected from the "digital tether" even for a short period can lead to social consequences. A social engineer can use "denial of service" i.e. arrange separation from the digital tether to create the kind of stress needed to manipulate the individual. The term "iPhone separation" has been coined to describe the reduced cognitive ability discovered in studies on some people's psychological reliance on their connected devices (e.g., [252]).
- Social-bots are becoming more prevalent. A social-bot is a software program that simulates human behaviour in automated interactions on social network sites such as Facebook and Twitter. “Automated bots can not only evade detection but also gather followers and become influential among various social groups”. Social-bots are a dream tool for social engineers allowing them to find gullible friends easily and to convince them that the social-bot is their friend, thus tricking them into performing actions that they would not normally do.
- As utility systems and other Industrial Control Systems are becoming more connected and, as cyber-security for these systems is improved, we can expect to see more SE attacks on these systems.
- Reverse Social Engineering as a new form of SE Reverse SE occurs when the attacker manipulates the target into initiating the contact himself. Since it is the target that initiates the contact, the attacker is typically more trusted. It is thus easier for the attacker to perform the attack. In many cases, an attacker will make himself a point of help for the victim [56].
- Another form of reverse SE is when the attacker becomes the victim. This typically occurs when police or military are the intended victims. Once they realize that they are attacked they can turn the tables and use social engineering or other tools to hit back at the attacker.
- Society's perception of privacy has changed dramatically in the past decade and we expect more changes in this direction in the future. If, in the past, we were educated not to give out sensitive information such as address and place of work to stranger, in the future, if we wish to by cyber-safe we will need to give out no information at all. Every bit of information can be used to build a profile that can later be used for social engineering. No information is inconsequential. This observation is in direct contrast with the current trend which is, in fact, the opposite. The current trend is to make all information available as demanded by the many social (and other) applications that we use in our daily lives.
- Another fascinating trend is the providing of Social Engineering as a service. This may include professional callers according to a needed profile such as language and/or accent spoken. Other services may include caller ID spoofing and the availability during business hours throughout the world. The possible availability of SE services at a low cost, together with attack automation technologies, would dramatically increase the number and types of SE attacks.

8.4. Legal and Ethical Trends

The proliferation of interconnected computing devices poses new legal and ethical challenges that societies have only begun to deal with [287][288][289][290]. The novelty of this interconnected technology has allowed the lines between ethical and unethical behaviour to be blurred due, partly, to the lack of clear legislation. An example is between marketing and rogue marketing (e.g. viral marketing or even phishing-like practices): as long, a business stays in the grey area, where it is not illegal, as easily it is adopted as a normal ethical practice. This phenomenon will likely occur largely in the future as new technologies and business practices related to these technologies are introduced.

Privacy

Privacy in the cyber environment has been a growing concern since the dawn of the internet era (and possibly even earlier). The emergence of cloud computing and cloud storage as a major trend has created an even more urgent concern over privacy. It seems that cloud service providers believe that it is their inherent right to either ownership or at least full right of use of their clients' data. In a recent Guardian article on the new EU privacy legislation the author writes “Companies including Amazon and IBM have warned that it (new EU legislation on privacy in cloud computing) could kill off Europe’s cloud computing industry”[94] .

Smartphone App Permissions

A particularly disturbing development in cyber data collection is in the area of Smartphone App Permissions. When downloading an app onto our smartphones or tablets we are asked to approve an often-long list of permissions (such as access to camera, microphone, phone book etc.). Refusal to agree to all the requested permissions nearly always means that the application will not install on your device. There are two main issues here:

- Many apps ask for permissions that they do not need. The likely purpose of this is to access your data and use it for a variety of purposes including advertising, sale of data, company valuation etc.
- Even if an app does need a given permission there is no guarantee that it will only use this permission for its intended purpose. Thus, if a phone app needs access to your contact list to find a phone number and you allow such access, the access is typically carte blanche so that the app can "legally" download all your contacts and use them for their own purposes.

In some sense smartphone app permissions, can be viewed as the ultimate in social engineering; given how ubiquitous and widespread it has become. The clear majority of people grudgingly (but without much thought) agree to these permissions because many of these apps have become an essential part of their lives. The number of socially defined "essential" apps is large and growing.

App developers fall into roughly two categories. There are those who consider themselves ethical and only do what is legal and what they believe is ethical with the public's data and

[94] “EU privacy reform: who pays when the rules are broken?”, Reuters - http://mcaf.ee/u0gbme

those who are purposely deceitful. Flashlight apps have been notorious for being "fronts" for data mining (i.e. spying).
The only way to deal with this problem is through legislation. We can expect that legislation will provide some limits to the private collection of data via app permissions. Future legislation may restrict the "export" of information from a user's device and allow the user to choose more privacy without having to give up the use of the app.

New EU Legislation
One of the major changes that should affect the future of cyber-crime in general and social engineering is the new European laws that will govern data privacy. As discussed above in the section on smartphones, laws do not stop criminals. Thus, a true cyber-criminal is certainly not expected to obey the law.
Details of the new legislative proposals can be found on the EU website. A good summary of some of the main features of the new legislation are described in an article in Computer World UK. The highlights are:

- Harmonizing legislation at the EU level so that organizations will no longer be able to register their activity in the EU country with the weakest legislation.
- Under the new regulations any company or individual that processes your data will be held responsible for its protection including third parties such as cloud providers.
- The new regulations affect every global organization that may have data on EU citizens and residents not only those whose place of business is in the EU.
- Users will be able make compensation claims
- There are tighter rules on transferring data on EU citizens outside the EU
- Harmonized rules as to user requests for information regarding data stored about them.
- New erasure rights
- Responsibility of those who hold or use the data to inform users of their rights
- Tougher sanctions for violation of the law

We have seen throughout this chapter that one of the most reliable predictions about the future of social engineering is the availability of a huge amount of hitherto unattainable data about most individuals and companies. New legislation protecting data privacy and security will provide new controls on how the major corporations as well as the providers of legitimate applications handle this data. At the same time, such legislation has the potential of changing both corporate and individual attitudes towards private data. Corporations may need to be somewhat more ethical in order to maintain their public image whereas individuals may learn to be more careful with their own treatment of their private data.
The social engineers of the future must cope with the consequences of this new legislation and adapt their techniques to this new reality.

9. Conclusions

This document presented the reference model for DOGANA of the multi-faceted world of the modern Social Engineering. D2.1 reports which is the view of DOGANA of the SE and its evolution.

Being SE the "queen" of the attacks' strategies today, it evolved since the "old-school days", to a very complex phenomenon. SE is not anymore, "The art of Deception", like the title of the famous book of D. Mitnick states. SE is rather a complex science that inherits from other human sciences a lot of best-practices and concepts. It's also an invaluable instrument for OCG to make moneys.

The document presented an overall model of modern SE, describing how much important it is in modern cybercrime. Then, across the different chapters D2.1 detailed the importance of the human element for security, the impact of the social networks and the typical attack workflow. Being the objective of DOGANA that of building a tool for testing the human element, understanding the attack workflow is fundamental. The DOGANA workflow must emulate, as much as possible, the attack strategies used in the wild by OCGs.

All the human sciences contribute to understand how we, the humans, behave, which are our habits and desires. The same level of understand is nowadays actively exploited by SE-experts of the OCGs, to create more economically remunerative attacks. OCG well understood this lesson and today almost 95% of the attacks starts with an SE phase, without which the infection would not proceed[95].

The results of this document will be useful during in different phases of the project, as a reference model for the development of the toolchain, the awareness strategies and the legal and ethical framework.

[95] For example, look at the "Phishing activity trends report unifying the global response to Cybercrime," AntiPhishing Working Group (APWG), Oct. 3, 2016. [Online]. Available: http://docs.apwg.org/reports/apwg_trends_report_q2_2016.pdf

10. References

[1] D. Gragg, "A multi-level defense against social engineering," in *Sans Institute InfoSec*, 2002. [Online]. Available: https://www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-920. Accessed on: Dec. 1, 2015.

[2] K. D. Mitnick, W. L. Simon, and S. Wozniak, *The art of deception: Controlling the human element of security*. Indianapolis, IN: John Wiley & Sons, 2001.

[3] K. D. Mitnick and W. L. Simon, *The art of intrusion: The real stories behind the exploits of hackers, intruders & Deceivers*. New York: John Wiley & Sons, 2005.

[4] lvxferis, "Hacking the mind for fun and profit," in *Phrack Magazine*, 2010. [Online]. Available: http://phrack.org/issues/67/15.html. Accessed on: Dec. 1, 2015.

[5] S. Granger, "Social Engineering Fundamentals, Part I: Hacker Tactics," in Symantec, 2001. [Online]. Available: http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics. Accessed on: Dec. 1, 2015.

[6] J. D. Meier, A. Mackman, M. Dunner, S. Vasireddy, R. Escamilla, and A. Murukan, Improving web application security: Threats and countermeasures. United States: Microsoft Press,U.S., 2003, ch. 3 Threat Modeling. [Online]. Available: https://msdn.microsoft.com/en-us/library/ff649874.aspx.

[7] C. Castelfranchi, R. Falcone, and R. F.., *Trust theory: A Socio-Cognitive and computational model (Wiley Series in agent technology)*. United States: John Wiley & Sons, 2010, ch. 1, 2, 3. [Online]. Available: http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470028750.html.

[8] R. Samani and C. McFarland, "Hacking the human operating system," in *McAfee*, 2015. [Online]. Available: http://www.mcafee.com/de/resources/reports/rp-hacking-human-os.pdf. Accessed on: Dec. 1, 2015.

[9] Z. Zorz, "Carbanak cyber gang stole hundreds of millions from banks," in *HelpNet Security*, 2015. [Online]. Available: http://www.net-security.org/secworld.php?id=17956. Accessed on: Dec. 1, 2015.

[10] G. Mann, "Forget the horse, this is the year of the F[ph]ish and the RAT," in *The Future of Cybersecurity*, London, 2014.

[11] T. Dimkov, W. Pieters, and P. Hartel, 'Two methodologies for physical penetration testing using social engineering', *Proceedings of the 26th Annual Computer Security Applications Conference on - ACSAC '10*, 2010.

[12] A. Prakash, "White paper: 1H 2015 advanced Endpoint threat report," in *Invincea*, 2015. [Online]. Available: https://www.invincea.com/2015/08/white-paper-1h-2015-advanced-endpoint-threat-report/. Accessed on: Dec. 1, 2015.

[13] S. Bratus, C. Masone, and S. W. Smith, "Why Do Street-Smart People Do Stupid Things Online?", *IEEE Security & Privacy Magazine*, vol. 6, no. 3, pp. 71–74, May 2008.

[14] U. Rivner, "Anatomy of an attack - speaking of security - the RSA Blog and Podcast," in *RSA FraudAction Research*, 2011. [Online]. Available: http://blogs.rsa.com/anatomy-of-an-attack/. Accessed on: Dec. 1, 2015.

[15] T. Reeve and S. Reporter, "Hacking team hacker identity linked to gamma international attack," SC Magazine UK, 2015. [Online]. Available: http://www.scmagazineuk.com/hacking-team-hacker-identity-linked-to-gamma-international-attack/article/424978/. Accessed on: Dec. 1, 2015.

[16]L. A. Times and T. Hsu, "Target CEO resigns as fallout from data breach continues," *LA Times*, 2014. [Online]. Available: http://www.latimes.com/business/la-fi-target-ceo-20140506-story.html. Accessed on: May 28, 2015.
[17]D. Yadron, "Symantec Develops New Attack on Cyberhacking," WSJ, 2014. [Online]. Available: http://www.wsj.com/articles/SB10001424052702303417104579542140235850578. Accessed on: May 28, 2015.
[18]T. Qin and J. K. Burgoon, "An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering," *2007 IEEE Intelligence and Security Informatics*, 2007.
[19]R. Heartfield and G. Loukas, "On the Feasibility of Automated Semantic Attacks in the Cloud," *Computer and Information Sciences III*, pp. 343–351, Jan. 2013.
[20]Cisco, "Cisco Annual Security Report," 2014. [Online]. Available: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf. Accessed on: May 28, 2015.
[21]C. McDaid, "The WhatsApp of wall street," in HelpNet Security, 2015. [Online]. Available: http://www.net-security.org/article.php?id=2371. Accessed on: Dec. 1, 2015.
[22]B. Prince, "Social Engineering: Attackers' Reliable Weapon," in Security Week, 2015. [Online]. Available: http://www.securityweek.com/social-engineering-attackers-reliable-weapon. Accessed on: Dec. 1, 2015.
[23]J. Henderson, "Is cybersecurity awareness a waste of time?," *New Zealand Reseller News*, 2015. [Online]. Available: http://www.reseller.co.nz/article/576316/cybersecurity-awareness-waste-time/. Accessed on: Dec. 1, 2015.
[24]I. Kirlappos and M. A. Sasse, "Security education against Phishing: A modest proposal for a major rethink," *IEEE Security & Privacy Magazine*, vol. 10, no. 2, pp. 24–32, Mar. 2012.
[25]T. Fox-Brewster, "Netflix is dumping anti-virus, presages death of an industry," in Forbes, Forbes, 2015. [Online]. Available: http://www.forbes.com/sites/thomasbrewster/2015/08/26/netflix-and-death-of-anti-virus/. Accessed on: Dec. 1, 2015.
[26]T. Berners-Lee, "The next web," TED Talks, 2009. [Online]. Available: http://www.ted.com/talks/tim_berners_lee_on_the_next_web?nolanguage=us. Accessed on: Dec. 1, 2015.
[27]S. J. Blackmore, *The meme machine*. United Kingdom: Oxford University Press, 1999.
[28]R. Brodie, *Virus of the mind: The new science of the meme*. United States: Integral Press, 2004.
[29]I. Mann, *Hacking the human: Social engineering techniques and security countermeasures*. Aldershot, Hants, England: Ashgate Publishing, 2009.
[30]I. Mann, *Hacking the human 2*. United States: Consilience Media, 2013.
[31]E. Frumento, C. Lucchiari, G. Pravettoni, and M. A. Valori, "Cognitive approach for social engineering," in *DeepSec*, Wien, 2010. [Online]. Available: https://deepsec.net/docs/Slides/2010/DeepSec_2010_Cognitive_approach_for_Social_Engineering.pdf. Accessed on: Dec. 1, 2015.
[32]A. Algarni, Y. Xu, T. Chan, and Y.-C. Tian, "Social engineering in social networking sites: Affect-based model," *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, pp. 508–515, Dec. 2013.

[33]G. M. Weiksner, B. J. Fogg, and X. Liu, "Six patterns for persuasion in online social networks," *Lecture Notes in Computer Science*, pp. 151–163, 2008.
[34]G. Farrell, K. Clark, D. Ellingworth, and K. Pease, "Of Targets and Supertargets: A routine activity theory of high crime rates," *Internet Journal of Criminology (IJC)*, Mar. 2005. [Online]. Available: http://www.internetjournalofcriminology.com/Farrell,%20Clark,%20Ellingworth%20&%20Pease%20-%20Supertargets.pdf. Accessed on: Dec. 2, 2015.
[35]H. Jahankhani and A. Al-Nemrat, "Cybercrime profiling and trend analysis," *Advanced Information and Knowledge Processing*, pp. 181–197, 2011.
[36]R. Aunger, Ed., *Darwinizing culture: The status of memetics as a science*. New York: Oxford University Press, USA, 2001.
[37]A. Bermingham, M. Conway, L. McInerney, N. O'Hare, and A. F. Smeaton, "Combining social network analysis and sentiment analysis to explore the potential for online Radicalisation," *International Conference on Advances in Social Network Analysis and Mining*, Jul. 2009.
[38]C. Dwyer, S. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," in *Americas Conference on Information Systems (AMCIS)*, Keystone, Colorado, USA, 2007.
[39]M. Huber, S. Kowalski, M. Nohlberg, and S. Tjoa, "Towards automating social engineering using social networking sites," *International Conference on Computational Science and Engineering*, 2009.
[40]K. Thomas, "Framing Dependencies Introduced by Underground Commoditization," in ', *Workshop on the Economics of Information Security (WEIS)*, Delft, Netherlands, University of Delft, 2015. [Online]. Available: http://www.inwyrd.com/blog/wp-content/uploads/2010/03/weis2015_blackmarket.pdf. Accessed on: Dec. 2, 2015.
[41]S. Pontiroli, "Social Engineering, Hacking The Human OS," in *Kaspersky Blog*, 2013. [Online]. Available: https://blog.kaspersky.com/social-engineering-hacking-the-human-os. Accessed on: Dec. 2, 2015.
[42]C. Nachreiner, "Signature antivirus' dirty little secret," in *HelpNet Security*, 2015. [Online]. Available: http://www.net-security.org/article.php?id=2239&p=2. Accessed on: Dec. 2, 2015.
[43]H.-P. Bauer, "Strategy Cloud and Security as a Service," in McAfee, 2010. [Online]. Available: http://www.slideshare.net/Aberla/strategy-cloud-and-security-as-a-service. Accessed on: Dec. 2, 2015.
[44]T. L. Thomas, "Cyberskepticism: the Mind's Firewall," in *I Sphere*, 2008. [Online]. Available: http://fmso.leavenworth.army.mil/documents/cyberskepticism.pdf. Accessed on: Dec. 2, 2015.
[45]E. Willems, "2009 Kl Cybercrime Kaspersky," in *Kaspersky Labs*, 2010. [Online]. Available: http://www.slideshare.net/ICTloket/2009-kl-cybercrime-kaspersky. Accessed on: Dec. 2, 2015.
[46]D. Harley, "AV is dead. Again. Apparently," *Anti-Malware Testing*, 2012. [Online]. Available: https://antimalwaretesting.wordpress.com/2012/04/18/av-is-dead-again-apparently/. Accessed on: Dec. 2, 2015.
[47]"Understanding the power of OSINT," BrightPlanet, 2015. [Online]. Available: https://www.brightplanet.com/2015/11/white-paper-understanding-the-power-of-osint/. Accessed on: Dec. 2, 2015.
[48]J. Long, *Google hacking for penetration testers*. United States: Syngress Publishing, 2014.

[49]E. Frumento and R. Puricelli, "An innovative and comprehensive framework for Social Vulnerability Assessment," presented at the DeepSec 2014, Wien, Nov. 19, 2014, Proceedings: Magdeburger Journal zur Sicherheitsforschung, 2014. [Online]. Available: http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_033_Frumento_Assessment.pdf. Accessed on: Dec. 2, 2015.

[50]S. Lee and S. Lebowitz, "20 cognitive biases that screw up your decisions," in Business Insider, 2015. [Online]. Available: http://uk.businessinsider.com/cognitive-biases-that-affect-decisions-2015-8?r=US&IR=T. Accessed on: Dec. 2, 2015.

[51]S. Martijn and Van Den Broek Egon L, "Physiological signals: The next generation authentication and identification methods!?," pp. 159–162, Aug. 2014. [Online]. Available: http://dx.doi.org/10.1109/EISIC.2013.35. Accessed on: Dec. 2, 2015.

[52]J. Turow, *Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth*. Yale University Press, 2013.

[53]D. Boyd, *It's complicated. The Social Lives of Networked Teens*. http://www.danah.org/itscomplicated/: Yale University Press, 2014.

[54]A. VV, *The Future of Identity Personal information space – The future of identities in a networked world,* 1st ed. http://goo.gl/G9UncA: Giesecke & Devrient, 2013.

[55]D. Harley and R. Abrams, "Whatever Happened to the Unlikely Lads? A Hoaxing Metamorphosis," *Virus Bulletin Conference*, Sep. 2009.

[56]D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C. Pu, "Reverse social engineering attacks in online social networks," *Detection of Intrusions and Malware, and Vulnerability Assessment*, pp. 55–74, 2011.

[57]M. Nohlberg and S. Kowalski, "The Cycle of Deception-A Model of Social Engineering Attacks, Defences and Victims," in *Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008)*, 2008. [Online]. Available: https://www.cscan.org/openaccess/?id=50.

[58]"The best defense against spear Phishing attacks," FireEye. [Online]. Available: https://www.fireeye.com/current-threats/best-defense-against-spear-phishing-attacks.html. Accessed on: Dec. 2, 2015.

[59]R. Kraut, T. Mukhopadhyay, Janusz, S. Kiesler, and B. Scherlis, "Information and communication: Alternative uses of the Internet in households," in Information Systems Research, 1999, vol. 10, no. 4, pp. 287–303. [Online]. Available: https://www.cs.cmu.edu/~kiesler/publications/PDFs/1999Kraut-InfoCommunication.pdf. Accessed on: Dec. 15, 2015.

[60]S. Greenspan, Annals of gullibility: Why we get duped and how to avoid it. Praeger, 2008.

[61]N. D. Weinstein, "Unrealistic optimism about future life events," Journal of Personality and Social Psychology, vol. 39, no. 5, pp. 806–820, 1980.

[62]R. E. Guadagno and R. Cialdini, "Online Persuasion and Compliance: Social Influence on the Internet and beyond,". [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.2.6571. Accessed on: Dec. 15, 2015.

[63]J. A. Bargh and K. Y. A. McKenna, "Plan 9 from Cyberspace: The implications of the Internet for personality and social psychology," Personality and Social Psychology Review, vol. 4, no.

1, pp. 57–75, Feb. 2000. [Online]. Available: http://psr.sagepub.com/content/4/1/57.abstract. Accessed on: Dec. 15, 2015.

[64]K. Matheson and M. P. Zanna, "The impact of computer-mediated communication on self-awareness," Computers in Human Behavior, vol. 4, no. 3, pp. 221–233, 1988. [Online]. Available: http://www.sciencedirect.com/science/article/pii/0747563288900155. Accessed on: Dec. 15, 2015.

[65]J. Siegel, V. Dubrovsky, S. Kiesler, and T. W. McGuire, "Group processes in computer-mediated communication," Organizational Behavior and Human Decision Processes, vol. 37, no. 2, pp. 157–187, Apr. 1986. [Online]. Available: http://www.sciencedirect.com/science/article/pii/0749597886900506. Accessed on: Dec. 15, 2015.

[66]B. Bett, "The psychology of sharing: why do people share online?," 2011. [Online]. Available: http://www.iab.net/media/file/POSWhitePaper.pdf. Accessed on: Dec. 17, 2015.

[67]Steinmetz, K. (2015) 'Help! My Parents are Millennials', Time (November), pp. 35–43. Available at: https://d.maxfile.ro/hxfupsxbjy.pdf (Accessed: October 2015).

[68]Bratus, S., Masone, C. and Smith, S. W. (2008) 'Why Do Street-Smart People Do Stupid Things Online?', IEEE Security & Privacy Magazine, 6(3), pp. 71–74.

[69]Barn, B. S., Barn, R. and Tan, J.-P. (2014) 'Young People and Smart Phones: An Empirical Study on Information Security', 2014 47th Hawaii International Conference on System Sciences.

[70]VV, A. (2013) The Future of Identity Personal information space – The future of identities in a networked world. 1st edn. Available at: http://goo.gl/ZklqPm (Accessed: October 2015)

[71]Algarni, A., Xu, Y., Chan, T. and Tian, Y.-C. (2013) 'Social Engineering in Social Networking Sites: Affect-Based Model', The 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013): . pp. 508–514.

[72]Boyd, D. (2014) It's complicated. The Social Lives of Networked Teens. http://www.danah.org/itscomplicated/: Yale University Press.

[73]K. D. Mitnick and W. L. Simon, The art of deception: Controlling the human element of security: Wiley, 2001.

[74] C. Hadnagy, Social engineering: The art of human hacking: Wiley, 2010.

[75] D. P. Twitchell, "Social engineering in information assurance curricula," in Proceedings of the 3rd Annual Conference on Information Security Curriculum Development, 2006, pp. 191-193.

[76] B. Blunden, "Manufactured Consent and Cyberwar," in LockDown Conference Proceedings, 2010.

[77] S. T. Thompson, "Helping the hacker? Library information, security, and social engineering," Information Technology and Libraries, vol. 25, pp. 222-225, 2013.

[78] R. G. Brody, "Flying under the radar: Social engineering,"International Journal of Accounting and Information Management,vol. 20, pp. 335-347, 2012.

[79] S. Abu-Nimeh, T. Chen, and O. Alzubi, "Malicious and spam posts in online social networks," Computer, vol. 44, pp. 23-28, 2011.

[80] T. Thornburgh, "Social engineering: The dark art," in Proceedingsof the 1st Annual Conference on Information Security CurriculumDevelopment, 2004, pp. 133-135.

[81] Sven, U. and Susanne, Q. (2018) 'The social engineering personality framework', pp. 24–30. doi: 10.1109/STAST.2014.12

[82] W. Luo, J. Liu, J. Liu, and C. Fan, "An analysis of security in social networks," pp. 648-651, 2009.

[83] T. S. N. Mohd, M. S. Noorsuriani, and G. N, 'The use of online social networking and quality of life', pp. 131–135, Jun. 2026.
[84] USA 2008 briefings speaker list', 2008. [Online]. Available: http://www.blackhat.com/html/bh-usa-08/bh-usa-08-archive.html.
[85] Stringhini, G., Kruegel, C. and Vigna, G. (2010) 'Detecting spammers on social networks', Proceedings of the 26th Annual Computer Security Applications Conference on - ACSAC '10, https://cs.ucsb.edu/~vigna/publications/2010_stringhini_kruegel_vigna_socialspam.pdf
[86] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts are belong to us: Automated identity theft attacks on social networks. In World Wide Web Conference, 2009
[87] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne, 'The psychology of security for the home computer user', 2012 IEEE Symposium on Security and Privacy, May 2012.
[88]Prensky, M., "Digital Natives, Digital Immigrants Part 2: Do They Really Think Differently?", On the horizon, 9(6), 2001, pp.1--6.
[89]Canina, M. (2015) IndossaME. Il design e le tecnologie indossabili.
[90] String battery (2012) Available at: http://www.talk2myshirt.com/blog/
[91] http://www.crunchwear.com/
[92] Willemsen, M. (2013) Control your mobile phone or tablet directly from your brain | next nature network. Available at: http://www.nextnature.net/2013/05/control-your-tablet-directly-from-your-brain/
[93] Cooney, M. (2012) Gartner: 10 critical IT trends for the next five years. Available at: http://www.networkworld.com/news/2012/102212-gartner-trends-263594.htm
[94] Soegaard, M., Dam, R. F., Whitworth, B., Ahmad, A., Kumar, J. M., Herger, M., Schmidt, A. and Cheverst, K. (2003) Context-aware computing. Available at: http://www.interaction-design.org/encyclopedia/context-aware_computing.htm
[95] Security, H. N. (2015) How the threat landscape will change by 2020. Available at: http://www.net-security.org/secworld.php?id=19092
[96] Chang, L. (2015) Report: Teens now spend more hours consuming media than sleeping. Available at: http://www.digitaltrends.com/mobile/teenagers-spend-9-hours-per-day-consuming-media/
[97] Turkle, S. (2000) Life on the screen: Identity in the age of the Internet. Available at: http://goo.gl/55sWPV
[98] Benini, M. Flavio (2015) It's complicated: La vita sociale degli adolescenti sul web. Danah boyd. Available at: http://goo.gl/pLa3LQ
[99] Dwyer, C., Pace and Passerini, K. (2007) 'Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace'
[100]Perché coloriamo la foto di Facebook? (2015) Available at: http://www.ilpost.it/2015/11/16/attentati-parigi-prayforparis-facebook
[101] Kochetkova, K. (2015) Why it's unsafe to take phones in bed and into the bathroom. Available at: https://blog.kaspersky.com/smartphones-in-bathrooms/10521/
[102] Amoroso, E. G. (2013) 'From the enterprise perimeter to a mobility-enabled secure cloud', IEEE Security & Privacy, 11(1), pp. 23–31. doi: 10.1109/msp.2013.8.

[103] L. Kirill and et. al., "Click Trajectories: End-to-end analysis of the Spam value chain," pp. 431–446, May 2025.
[104] B. Krebs, Spam nation: The inside story of organized Cybercrime from global epidemic to your front door. United States: Brilliance Audio, 2014.
[105] W. Pedrycz and S.-M. Chen, Social networks: A framework of computational intelligence. Springer International Publishing, 2015.
[106] D. D. Caputo, | Mitre, S. L. Pfleeger, J. D. Freeman, and E. M. Johnson, "Going spear Phishing: Exploring embedded training and awareness," 2014.
[107] R. Dhamija, J. D. Tygar, and M. Hearst, "Why Phishing works," 2006.
[108] J. S. Downs, M. B. Holbrook, and L. F. Cranor, "Decision strategies and susceptibility to Phishing," 2006.
[109] G. Goth, "Phishing attacks rising, but dollar losses down," in IEEE Security and Privacy, IEEE Educational Activities Department, 2005, p. 8.
[110] J. Hong, "The state of Phishing attacks," Communications of ACM 55, 1, 74-81, 2012.
[111] T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer, "Social Phishing," 2005. [Online]. Available: http://markus-jakobsson.com/papers/jakobsson-commacm07.pdf.
[112] M. Khonji, Y. Iraqi, and A. Jones, "Phishing detection: A literature survey," IEEE Communications Surveys & Tutorials, vol. PP, no. 99, pp. 1–31, Apr. 2013. [Online]. Available: https://goo.gl/mASvUm. Accessed on: Dec. 11, 2015.
[113] L. D. Paulson, "Spike in phishing and malware a danger to IT," in IT Professional, IEEE, 2005, p. 5.
[114] T. Kurt et al., "Framing Dependencies Introduced by Underground Commoditization," in Workshop on the Economics of Information Security. [Online]. Available: https://cseweb.ucsd.edu/~savage/papers/WEIS15.pdf. Accessed on: Dec. 13, 2015.
[115] C. McFarland, F. Paget, and R. Samani, "The Hidden Data Economy - The Marketplace for Stolen Digital Information," Intel Security, Oct. 15, 2015. [Online]. Available: http://www.mcafee.com/us/resources/reports/rp-hidden-data-economy.pdf.
[116] R. Samani and F. Paget, "Cybercrime Exposed - Cybercrime as a Service," McAfee, 2014. [Online]. Available: http://www.mcafee.com/it/resources/white-papers/wp-cybercrime-exposed.pdf.
[117] R. Stoyanov, "Russian Financial Cybercrime: How it Works," Kaspersky Lab, 2015.
[118] F. L. Greitzer, J. R. Strozer, S. Cohen, A. P. Moore, D. Mundie, and J. Cowley, "Analysis of unintentional insider threats deriving from social engineering exploits," in 2014 IEEE Security and Privacy Workshops, Institute of Electrical & Electronics Engineers (IEEE), 2014.
[119] W. Zhou, Y. Zhou, X. Jiang, and P. Ning, "Detecting repackaged smartphone applications in third-party android marketplaces," ACM, 2012, pp. 317–326. [Online]. Available: http://dx.doi.org/10.1145/2133601.2133640. Accessed on: Dec. 14, 2015.
[120] M. Goncharov, "Russian Underground 2.0," 2015. [Online]. Available: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/wp-russian-underground-2.0.pdf. Accessed on: Dec. 14, 2015.
[121] I. Kirlappos and M. A. Sasse, "Security education against Phishing: A modest proposal for a major rethink," in Security & Privacy, IEEE, vol. 10, IEEE, 2012, pp. 24–32.
[122] A. Ammar and et. al., "A survey of Phishing Email filtering techniques," in Communications Surveys & Tutorials, IEEE, vol. 15, IEEE, 2013, pp. 2070–2090.

[123] D. Irani and et. al., "Evolutionary study of Phishing", in eCrime Researchers Summit, pp. 1-10, 15-16 Oct. 2008.
[124] Symantec, "Internet Security Threat Report 2015,". [Online]. Available: https://goo.gl/RkY2MI. Accessed on: Dec. 14, 2015.
[125] Cisco, "Email Attacks: This Time It's Personal," 2011. [Online]. Available: http://www.cisco.com/c/dam/en/us/products/collateral/security/email-security-appliance/targeted_attacks.pdf. Accessed on: Dec. 14, 2015.
[126] C. Yue and et. al., "BogusBiter: A transparent protection against Phishing attacks 6: 2," in ACM Transactions on Internet Technology, vol. 10, 2010.
[127] T. Peltier, "Social engineering: Concepts and solutions," Information Systems Security, vol. 15, no. 5, pp. 13–21, Nov. 2006.
[128] The CERT Insider Threat Team, "Unintentional insider threats: A Foundational study," 2013. [Online]. Available: http://www.sei.cmu.edu/reports/13tn022.pdf. Accessed on: Dec. 14, 2015.
[129] M. Motoyama, K. Levchenko, C. Kanich, D. McCoy, G. M. Voelker, and S. Savage, "Re: CAPTCHAs: Understanding CAPTCHA-solving services in an economic context," USENIX Association, 2010, p. 28. [Online]. Available: http://dl.acm.org/citation.cfm?id=1929820.1929858. Accessed on: Dec. 13, 2015.
[130] Z. Haijun, L. Gang, C. T. W. S, and L. Wenyin, "Textual and visual content-based Anti-Phishing: A Bayesian approach," in Neural Networks, IEEE Transactions on, IEEE, 2011, vol. 22, no. 10, pp. 1532–1546. [Online]. Available: http://dx.doi.org/10.1109/TNN.2011.2161999. Accessed on: Dec. 14, 2015.
[131] W. Jingguo, H. Tejaswini, C. Rui, V. Arun, and R. H. Raghav, "Phishing susceptibility: An investigation into the processing of a targeted spear Phishing Email," in Professional Communication, IEEE Transactions on, IEEE, 2012, vol. 55, no. 4, pp. 345–362.
[132] K. Nirmal, B. Janet, and R. Kumar, "Phishing - the threat that still exists," IEEE, pp. 139–143.
[133] J. Epstein, "Phishing our employees," Security & Privacy, IEEE, vol. 12, no. 3, pp. 3–4, June 2014.
[134] N. Agarwal, S. Renfro, and A. Bejar, "Phishing forbidden," Queue, vol. 5, no. 5, pp. 28–32, January 2007.

[135] A. A. M. Sasse, "Users are not the Enemy: Why users compromise computer security mechanisms and how to take remedial measures," Communication Transaction of ACM, vol. 42, 1999.
[136] K. D. Mitnick and W. L. Simon, The art of deception: Controlling the human element of security. John Wiley & Sons, 2001.
[137] M. Nohlberg and S. Kowalski, The Cycle of Deception, 3rd ed. Buckingham [UK] ; Philadelphia: Open University Press, 2001.
[138] C. P. Pfleeger, Security in computing, 3rd ed. London: Prentice-Hall International, 1989.
[139] P. R. B. Cialdini, Influence: The psychology of persuasion, 2nd ed. Australia: The Business Library, 1983.

[140] M. Francois, M. M. M, L. Louise, and V. H.S, “Social engineering attack framework,” 2014, pp. 1–9.
[141] C. Castelfranchi, R. Falcone, and R.F., Trust theory: A Socio-Cognitive and computational model (Wiley Series in agent technology). United States: John Wiley & Sons, 2010.
[142] N. Huq, “Follow the data: Dissecting data breaches and debunking myths,” 2015. [Online]. Available: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-follow-the-data.pdf . [Accessed: 06-Dec-2015].
[143] “Anatomy of an Attack - Speaking of Security - The RSA Blog and Podcast.” [Online]. Available: https://blogs.rsa.com/anatomy-of-an-attack/ . [Accessed: 11-Nov-2015].
[144] E. Frumento and R. Puricelli, “An innovative and comprehensive framework for Social Vulnerability Assessment,” Magdebg. J. Zur Sicherheitsforschung Ausg. 8 Jahrg. 4 Band 2 2014.
[145] A. Algarni, Y. Xu, T. Chan, and Y.-C. Tian, “Social engineering in social networking sites: Affect-based model,” presented at the 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), Dec-2013.
[146] “Hackers Profiling.” [Online]. Available: http://goo.gl/WXhBvW. [Accessed: 14-Dec-2015].
[147] “Threat Report H2 2014.” [Online]. Available: https://www.f-secure.com/documents/996508/1030743/Threat_Report_H2_2014 .
[148] “Understanding Cyberthreat motivations to improve defense, in Intel Enterprise Security, 2015.” [Online]. Available: http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/understanding-cyberthreat-motivations-to-improve-defense-paper.pdf . [Accessed: 07-Dec-2015].
[149] V. Benjamin, W. Li, T. Holt, and H. Chen, “Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops,” presented at the 2015 IEEE International Conference on Intelligence and Security Informatics (ISI), May-2015.
[150] S. Curtis, “Unmasked: The six hacker ‘tribes’ you need to avoid," in The Telegraph, Telegraph.co.uk, 2015.” [Online]. Available: http://www.telegraph.co.uk/technology/internet-security/11568376/Unmasked-the-six-hacker-tribes-you-need-to-watch-out-for.html . [Accessed: 07-Dec-2015].
[151] B. Riley-Smith, “Cyber hackers ‘hired to attack governments and banks’," in The Telegraph, Telegraph.co.uk, 2013.” [Online]. Available: http://www.telegraph.co.uk/technology/news/10317634/Cyber-hackers-hired-to-attack-governments-and-banks.html . [Accessed: 07-Dec-2015].
[152] K. Thomas, “Framing Dependencies Introduced by Underground Commoditization," in ’, Workshop on the Economics of Information Security (WEIS), Delft, Netherlands, University of Delft, 2015.” [Online]. Available: http://www.inwyrd.com/blog/wp-content/uploads/2010/03/weis2015_blackmarket.pdf. [Accessed: 02-Dec-2015].
[153] D. Goodin, “Advanced spyware for Android now available to script kiddies everywhere," Ars Technica, 2015.” [Online]. Available: http://arstechnica.com/security/2015/07/advanced-spyware-for-android-now-available-to-script-kiddies-everywhere . [Accessed: 07-Dec-2015].
[154] “25 ways to become the ultimate script kiddie, in InfoSec Institute, InfoSec Resources, 2015.” [Online]. Available: http://resources.infosecinstitute.com/25-ways-to-become-the-ultimate-script-kiddie . [Accessed: 07-Dec-2015].

[155] J. Keane, “This ain’t CSI: How the FBI hunts down cyber criminals around the globe," Digital Trends, 2015.” [Online]. Available: http://www.digitaltrends.com/computing/how-the-fbi-hunts-down-cyber-criminals-around-the-globe. [Accessed: 07-Dec-2015].

[156] A. Bermingham, M. Conway, L. McInerney, N. O'Hare, A. Smeaton, “Combining social network analysis and sentiment analysis to explore the potential for online radicalisation”. *ASONAM 2009 - Advances in Social Networks Analysis and Mining*, 20-22 July, 2009

[157] P. Tagliapietra, “Il percorso d’acquisto tra FMOT, SMOT e ZMOT," in Comunicare stanca, pierotaglia, 2012.” [Online]. Available: . [Accessed: 07-Dec-2015].

[158] “The Bigger Picture, ‘Using social graphs to understand your network - part 1,’ YouTube, 2014.” [Online]. Available: https://www.youtube.com/watch?v=s6PIyHUl-U4 . [Accessed: 07-Dec-2015].

[159] “The Bigger Picture, ‘Using social graphs to understand your network - part 2,’ YouTube, 2014.” [Online]. Available: https://www.youtube.com/watch?v=vtTa5bPgfJs . [Accessed: 07-Dec-2015].

[160] M. Junger and C. Broekman, “Supertargets do exist in cyber space” [Online]. Available: http://mcaf.ee/j3nvh4. [Accessed: 07-Dec-2015].

[161] “General discussion - security through education," Security Through Education.” [Online]. Available: http://www.social-engineer.org/framework/general-discussion. [Accessed: 15-Dec-2015].

[162] M. Huber, S. Kowalski, M. Nohlberg, and S. Tjoa, “Towards automating social engineering using social networking sites,” in Computational Science and Engineering, 2009. CSE’09. International Conference on, 2009, vol. 3, pp. 117–124.

[163] T. Lauinger, V. Pankakoski, D. Balzarotti, and E. Kirda, “Honeybot, your man in the middle for automated social engineering,” in LEET’10, 3rd USENIX Workshop on Large-Scale Exploits and Emergent Threats, San Jose, 2010.

[164] “Attack vector definition,” TechTarget, SearchSecurity. [Online]. Available: http://searchsecurity.techtarget.com/definition/attack-vector .

[165] Henry Dalziel, “Categories of Social Engineering Attacks [Technical and Non-technical],” 2015. [Online]. Available: https://www.concise-courses.com/security/categories-of-social-engineering/ .

[166] Stephenson and Debbie, “Spear Phishing: Who’s Getting Caught?". Firmex. Retrieved July 27, 2014.” .

[167] C. Hadnagy, Social engineering: the art of human hacking. Indianapolis, IN: Wiley, 2011.

[168] “Guardline ® professional spy pen camera user’s manual,” 2014. [Online]. Available: http://ecx.images-amazon.com/images/I/91SCEYIriUS.pdf. Accessed: Feb. 1, 2016.

[169] “Amazon.com : ToughstyTM Mini Hidden Camera Button Camcorder Video Recorder Security DVR with Audio Function : Spy Cameras : Camera & Photo.” [Online]. Available: http://www.amazon.com/dp/B00GBTIS30?psc=1 . [Accessed: 10-Dec-2015].

[170] “Best Real Time GPS Tracking Equipment - Spy Associates.” [Online]. Available: http://www.spyassociates.com/real-time-gps-tracking-equipment-1/ . [Accessed: 10-Dec-2015].

[171] “Caller ID Spoofing w/ Asterisk.” [Online]. Available: http://allanfeid.com/content/caller-id-spoofing-w-asterisk . [Accessed: 10-Dec-2015].

[172] “Asterisk.org,” Asterisk.org. [Online]. Available: http://www.asterisk.org/ . [Accessed: 10-Dec-2015].

[173] "Paterva / Maltego." [Online]. Available: https://www.paterva.com/web6/products/maltego.php . [Accessed: 10-Dec-2015].
[174] "ALICE and AIML Software and Downloads - ALICE A. I. Foundation Natural Language Chat Robot (Chatterbot) Programming and Virtual Personality Development Tools." [Online]. Available: http://www.alicebot.org/downloads/programs.html . [Accessed: 10-Dec-2015].
[175] Honan, B., "Ubiquiti networks victim of $39 million social engineering attack," 2015. [Online]. Available: http://www.csoonline.com/article/2961066/supply-chain-security/ubiquiti-networks-victim-of-39-million-social-engineering-attack.html .
[176] "DHS: Spear Phishing Campaign Targeted 11 Energy Sector Firms | SecurityWeek.Com." [Online]. Available: http://www.securityweek.com/dhs-spear-phishing-campaign-targeted-11-energy-sector-firms . [Accessed: 09-Nov-2015].
[177] "Critical infrastructure," 2012. [Online]. Available: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm. Accessed on: Dec. 15, 2015.
[178] "My EUR-Lex," 2008. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114. Accessed on: Dec. 15, 2015.
[179] "European commission - PRESS RELEASES - press release - the European Programme for critical infrastructure protection (EPCIP)," 2006. [Online]. Available: http://europa.eu/rapid/press-release_MEMO-06-477_en.htm. Accessed on: Dec. 15, 2015.
[180] [Online]. Available: http://www.sersc.org/journals/IJCA/vol1_no1/papers/03.pdf. Accessed on: Dec. 15, 2015.
[181] K. Lauta, R. Cedervall , L. Hoffmann, L. Struwe, and Bangert, 2013. [Online]. Available: http://curis.ku.dk/ws/files/66128849/Cyberwarfare.pdf. Accessed on: Dec. 15, 2015.
[182] "Denial-of-service: The Estonian Cyberwar and its implications for U.S. National security," 2001. [Online]. Available: http://www.iar-gwu.org/node/65. Accessed on: Dec. 15, 2015.
[183] "Butterfly: Corporate spies out for financial gain Symantec security response," 2015. [Online]. Available: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/butterfly-corporate-spies-out-for-financial-gain.pdf. Accessed on: Dec. 15, 2015.
[184] R. M. Lee, M. J. Assante, and T. Conway, "German Steel mill Cyber attack," 2014. [Online]. Available: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf. Accessed on: Dec. 15, 2015.
[185] "The unlocked backdoor to healthcare data," in *HelpNet Security*, 2014. [Online]. Available: http://www.net-security.org/secworld.php?id=17062. Accessed on: Nov. 30, 2015.
[186] C. Kemp, "Ponemon report shows abysmal state of data security in the healthcare industry - web host industry review," in *Cloud Computing*, Web Host Industry Review, 2015. [Online]. Available: http://www.thewhir.com/web-hosting-news/ponemon-report-shows-abysmal-state-of-data-security-in-the-healthcare-industry. Accessed on: Nov. 30, 2015.
[187] "Healthcare industry sees 340% more security incidents than the average industry," in *HelpNet Security*, 2015. [Online]. Available: http://www.net-security.org/secworld.php?id=18889. Accessed on: Nov. 30, 2015.
[188] "Damage Control: The Cost of Security Breaches," in *Kaspersky Labs* (IT Security Risks Special Report Series), 2015. [Online]. Available: http://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf. Accessed on: Nov. 30, 2015.

[189] M. Hiltzik and L. A. Times, "Anthem is warning consumers about its huge data breach. Here's a translation," in *Los Angeles Times*, LA Times, 2015. [Online]. Available: http://www.latimes.com/business/hiltzik/la-fi-mh-anthem-is-warning-consumers-20150306-column.html. Accessed on: Nov. 30, 2015.

[190] "Anatomy of a healthcare data breach. Prevention and remediation strategies," in *ClearDATA*, 2015. [Online]. Available: http://net-security.tradepub.com/free/w_clec01/prgm.cgi?a=1. Accessed on: Nov. 30, 2015.

[191] G. L. Koroneos, "Enterprise tech spotlight: Wearable security, Phishing targets, healthcare data breaches," in *Verizon*, 2015. [Online]. Available: http://news.verizonenterprise.com/2015/06/wearable-security-phishing-healthcare-networkfleet/. Accessed on: Nov. 30, 2015.

[192] B. Barney, "Healthcare: Recognize social engineering techniques," in *Security Metrics Blog*, 2015. [Online]. Available: http://blog.securitymetrics.com/2015/08/healthcare-social-engineering.html. Accessed on: Nov. 30, 2015.

[193] C. Cook, "The rise of multifaceted social engineering attacks - social-engineer.Com - professional social engineering training and services," in *Social-Engineer.Com*, 2015. [Online]. Available: https://www.social-engineer.com/rise-multifaceted-social-engineering-attacks/. Accessed on: Nov. 30, 2015.

[194] A. Ossola, "Hacked medical devices may be the biggest Cyber security threat in 2016," in Popular Science, 2015. [Online]. Available: http://www.popsci.com/hackers-could-soon-hold-your-life-ransom-by-hijacking-your-medical-devices. Accessed on: Dec. 1, 2015.

[195] P. Peachey, "Cyber crime: First online murder will happen by end of year, warns US firm," in The Independent - News, 2014. [Online]. Available: http://www.independent.co.uk/life-style/gadgets-and-tech/news/first-online-murder-will-happen-by-end-of-year-warns-us-firm-9774955.html. Accessed on: Dec. 1, 2015.

[196] D. Emm, A. Nikishin, and A. Gostev, "Kaspersky security bulletin 2015. Top security stories," 2015. [Online]. Available: https://securelist.com/analysis/kaspersky-security-bulletin/72886/kaspersky-security-bulletin-2015-top-security-stories/. Accessed on: Dec. 15, 2015.

[197] "Future of critical infrastructure - Cyber security threat landscape,". [Online]. Available: http://mcaf.ee/ph0bge. Accessed on: Dec. 15, 2015.

[198] "Inside the aftermath of the Saudi Aramco breach," Dark Reading, 2015. [Online]. Available: http://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676. Accessed on: Dec. 15, 2015.

[199] "Target hackers broke in via HVAC company — Krebs on security," 2015. [Online]. Available: http://www.krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/. Accessed on: Dec. 15, 2015.

[200] W. Ho, C. Kozowyk, and R. Peak, "McAfee labs threats report," 2015. [Online]. Available: http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-aug-2015.pdf. Accessed on: Dec. 15, 2015.

[201] T. M. Incorporated, "Data Exfiltration: How do threat actors steal your data?," 2013. [Online]. Available: http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/how_do_threat_actors_steal_your_data.pdf. Accessed on: Dec. 15, 2015.

[202] B. Barth, "Analysis of background investigation incident," 2015. [Online]. Available: https://www.archives.gov/isoo/notices/notice-2015-04.pdf. Accessed on: Dec. 15, 2015.

[203] N. Vostrecova, 2015. [Online]. Available: https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf. Accessed on: Dec. 15, 2015.
[204] D. Kushner, "The real story of Stuxnet," 2013. [Online]. Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet. Accessed on: Dec. 15, 2015.
[205] "Active Ageing: A Policy Framework,". *WHO*, [Online]. Available: http://whqlibdoc.who.int/hq/2002/WHO_NMH_NPH_02.8.pdf. Accessed on: Dec. 15, 2015.
[206] J. Vincent, "More hospitals are trying apple HealthKit than Google fit," The Verge, 2015. [Online]. Available: http://www.theverge.com/2015/2/5/7983707/apple-healthkit-hospitals-google-samsung. Accessed on: Dec. 15, 2015.
[207] E. Woollacott, "Will Apple satisfy regulators over HealthKit data privacy?," in Forbes, Forbes, 2014. [Online]. Available: http://www.forbes.com/sites/emmawoollacott/2014/08/29/will-apple-satisfy-regulators-over-healthkit-data-privacy/. Accessed on: Dec. 15, 2015.
[208] "HealthKit di apple: La diffusione delle app mediche passa per l'adeguamento normativo," 2014. [Online]. Available: http://www.dimt.it/2014/09/18/healthkit-di-apple-la-diffusione-delle-app-mediche-passa-per-ladeguamento-normativo/. Accessed on: Dec. 15, 2015.
[209] A. Drozhzhin, "The Carbanak hacker group stole $1 billion USD," 2015. [Online]. Available: https://blog.kaspersky.com/billion-dollar-apt-carbanak/7519/. Accessed on: Dec. 15, 2015.
[210] [Online]. Available: http://www.ihs.com/pdfs/IHS-IOT-Evolution.pdf. Accessed on: Dec. 15, 2015.
[211] U.S. Department of Homeland Security, "Communications sector," 2015. [Online]. Available: http://www.dhs.gov/communications-sector . Accessed on: Dec. 15, 2015
[212] Electronic Communications Resilience & Response Group, "Telecommunications Networks - a vital part of the Critical National Infrastructure,". [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62279/telecommunications-sector-intro.pdf . Accessed on: Dec. 15, 2015.
[213] U.S. Department of Homeland Security and Office of Cybersecurity and Communications, "Communications sector-specific plan 2010," 2010. [Online]. Available: http://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2010-508.pdf . Accessed on: Dec. 15, 2015.
[214] Industrial Control Systems Cyber Emergency Response Team, 2013. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Apr-Jun2013.pdf . Accessed on: Dec. 15, 2015.

[215] Trend Micro Incorporated, "Report on Cybersecurity and critical infrastructure in the Americas," 2015. [Online]. Available: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf . Accessed on: Dec. 15, 2015.
[216] The Economist, "War in the fifth domain," The Economist, 2010. [Online]. Available: http://www.economist.com/node/16478792 . Accessed on: Dec. 15, 2015.

[217] Eastman, R., Versace, M. and Webber, A. (2015) Big Data and Predictive Analytics: On the Cybersecurity Front Line. Available at:

http://www.sas.com/content/dam/SAS/en_us/doc/whitepaper2/idc-cybersecurity-front-line-107673.pdf
[218] Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S. and Frye, J. (2012) Cyber Threat Metrics. Available at: http://prod.sandia.gov/techlib/access-control.cgi/2012/122427.pdf
[219] Schneier, B. (2000) Crypto-Gram: May 15, 2000 - Schneier on security. Available at: https://www.schneier.com/crypto-gram/archives/2000/0515.html
[220] Wood, P. (2013) How to tackle big data from a security point of view. Available at: http://www.computerweekly.com/feature/How-to-tackle-big-data-from-a-security-point-of-view
[221] Shackleford, D., (2015) 2015 Analytics and Intelligence Survey. Available at: https://www.sans.org/reading-room/whitepapers/analyst/2015-analytics-intelligence-survey-36432
[222] Predictive Analytics: What it is and why it matters (2015) Available at: http://www.sas.com/en_us/insights/analytics/predictive-analytics.html
[223] Price Waterhouse Coopers (2004) The Use of Spreadsheets: Considerations for Section 404 of the Sarbanes-Oxley Act Available at: http://www.spreadsheetdetective.com/main/PwC-SpreadsheetsSoX.pdf
[224] Herley, C., Sasse, M. A., Gollmann, D., Pieters, W. and Koenig, V. (2015) 'Socio-Technical security metrics (Dagstuhl seminar 14491)', Dagstuhl Reports, 4(12), p. 28. doi: 10.4230/DagRep.4.12.1.
[225] BT British Telecommunication (2015) Penetration testing - BT Assure Ethical Hacking. Available at: http://www.globalservices.bt.com/uk/en/products/ethical_hacking_services
[226] Allianz Global Corporate & Specialty (2015) A Guide to Cyber Risk - Managing the Impact of Increasing Interconnectivity. Available at: http://www.agcs.allianz.com/insights/white-papers-and-case-studies/cyber-risk-guide/
[227] Smith, A., Papadaki, M. and Furnell, S. M. (2013) 'Improving awareness of social engineering attacks', Information Assurance and Security Education and Training, , pp. 249–256. doi: 10.1007/978-3-642-39377-8_29.
[228] Robinson, A. (2013) 'Using Influence Strategies to Improve Security Awareness Programs', SANS Institute InfoSec Reading Room.
[229] Digital Shadow Ltd. (2015) Cyber Situational Awareness - Gain an 'Attacker's Eye View' of your Organization. Available at: http://info.digitalshadows.com/CyberSituationalAwareness-Website.html
[230] Frumento, E. and Puricelli, R. (2014) 'An innovative and comprehensive framework for Social Driven Vulnerability Assessment', Magdeburger Journal zur Sicherheitsforschung, 2, pp. 493–505.
[231] European Digital Agenda, https://ec.europa.eu/digital-agenda/en/cybersecurity
[232] Cyber Europe — ENISA (2015) Available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe
[233] SANS Securing the Human (2015) 2015 Security Awareness Report. Available at: http://www.securingthehuman.org/media/resources/STH-SecurityAwarenessReport-2015.pdf

[234] Sedova, M. (2105) Security awareness Blog | Gamification at Salesforce - #SecAwarenessSummit. Available at: https://www.securingthehuman.org/blog/2015/07/08/gamification-at-salesforce-secawarenesssummit

[235] Kirlappos, I. and Sasse, M. A. (2012) 'Security education against Phishing: A modest proposal for a major rethink', IEEE Security & Privacy Magazine, 10(2), pp. 24–32. doi: 10.1109/msp.2011.179.

[236] Wombat Security Technologies (2015) Deploying Continuous and Measurable Security Education for Employees.

[237] Help Net Security (2015) Instilling a culture of cyber security. Available at: http://www.net-security.org/article.php?id=2304

[238] Resellernews (2015) Is cybersecurity awareness a waste of time? Available at: http://www.reseller.co.nz/article/576316/cybersecurity-awareness-waste-time/

[239] Winnefeld Jr., J. A., Kirchhoff, C. and Upton, D. M. (2015) 'Cybersecurity's human factor: Lessons from the pentagon', Harvard Business Review (September)

[240] "The Human Factor 2015," in Proofpoint, 2015. [Online]. Available: https://www.proofpoint.com/sites/default/files/documents/bnt_download/pp-human-factor-2015_0.pdf. Accessed on: Dec. 12, 2015.

[241] F. Mouton, M. M. Malan, and H. S. Venter, "Social engineering from a normative ethics perspective," 2013 Information Security for South Africa, Aug. 2013.

[242] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An Integrative Model of Organizational Trust," Academy of Management Review, vol. 20, no. 3, pp. 709–734, Jul. 1995.

[243] C. I. Hovland, I. L. Janis, and H. H. Kelley, Communication and persuasion. London: Yale University Press, 1953.

[244] J. Cook and T. Wall, "New work attitude measures of trust, organizational commitment and personal need non-fulfilment," Journal of Occupational Psychology, vol. 53, no. 1, pp. 39–52, Mar. 1980.

[245] C. Hadnagy, Unmasking the social engineer: The human element of security, P. K. F, Ed. United States: Wiley, 2014

[246] M. Gilbert-Lurie, "Are You In A Codependent Relationship With Your Phone? Science Says The Struggle Is Definitely Real," in Bustle, https://www.facebook.com/bustledotcom . [Online]. Available: http://www.bustle.com/articles/82494-are-you-in-a-codependent-relationship-with-your-phone-science-says-the-struggle-is-definitely-real. Accessed on: Dec. 14, 2015.

[247] L. Chang, "FOMO is a real thing, and it's adversely affecting teens on social media," in Social Media, Digital Trends, 2015. [Online]. Available: http://www.digitaltrends.com/social-media/social-media-overuse-teen-anxiety/ . Accessed on: Dec. 14, 2015.

[248] A. Dachis, "How to plant ideas in someone's mind," in LifeHacker, 2014. [Online]. Available: http://lifehacker.com/5715912/how-to-plant-ideas-in-someones-mind. Accessed on: Dec. 14, 2015.

[249] N. Luhmann, Familiarity, confidence, trust: Problems and alternatives. D. G. Gambetta (Ed.), 1988, pp. 94–107.

[250] "The Human Factor 2015," in Proofpoint, 2015. [Online]. Available: https://www.proofpoint.com/sites/default/files/documents/bnt_download/pp-human-factor-2015_0.pdf Accessed on: Dec. 12, 2015.

[251] E. Frumento, C. Lucchiari, A. Valori, and G. Pravettoni, "Cognitive approach for social engineering," in DeepSec, Web, 2010. [Online]. Available: https://deepsec.net/docs/Slides/2010/DeepSec_2010_Cognitive_approach_for_Social_Engineering.pdf. Accessed on: Dec. 14, 2015.

[252] R. B. Clayton, G. Leshner, and A. Almond, "The extended iSelf: The impact of iPhone separation on Cognition, emotion, and physiology," Journal of Computer-Mediated Communication, vol. 20, no. 2, pp. 119–135, Jan. 2015.

[253] B. S. Barn, R. Barn, and J.-P. Tan, "Young people and smart phones: An empirical study on information security," 2014 47th Hawaii International Conference on System Sciences, Jan. 2014.

[254] D. Harley, E. Willems, and J. Harley, "Teach Your Children Well. ICT Security and the Young Generation," in Virus Bulletin Conference, Proceedings, 2005.

[255] R. Abrams and D. Harley, "People Patching is user education of any use at all?," 2009. [Online]. Available: http://www.welivesecurity.com/media_files/white-papers/People_Patching.pdf. Accessed on: Dec. 14, 2015.

[256] D. Harley and A. Lee, "Phish Phodder: is User Education Helping or Hindering?," 2007. [Online]. Available: http://www.welivesecurity.com/wp-content/uploads/2012/11/PhishPhodder.pdf. Accessed on: Dec. 14, 2015.

[257] M. Wilson and J. Hash, "Building an information technology security awareness and training program," Oct. 2003. [Online]. Available: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=151287 .

[258] I. Kirlappos and M. A. Sasse, "Security education against Phishing: A modest proposal for a major rethink," IEEE Security & Privacy Magazine, vol. 10, no. 2, pp. 24–32, Mar. 2012.

[259] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, "Going spear Phishing: Exploring embedded training and awareness," IEEE Security & Privacy, vol. 12, no. 1, pp. 28–38, Jan. 2014.

[260] T. Qin and J. K. Burgoon, "An investigation of Heuristics of human judgment in detecting deception and potential implications in countering social engineering," 2007 IEEE Intelligence and Security Informatics, May 2007.

[261] A. Neupane, M. L. Rahman, N. Saxena, and L. Hirshfield, "A multi-modal Neuro-Physiological study of Phishing detection and Malware warnings," Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15, 2015.

[262] L. J. Janczewski and L. Fu, "Social engineering-based attacks: model and New Zealand perspective," in International Multiconference on Computer Science and Information Technology, Proceedings: IEEE, 2010, pp. 847–853.

[263] E. LeMay, K. Scarfone, and P. Mell, "The common misuse scoring system (CMSS): Metrics for software feature misuse vulnerabilities," Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, no. NIST Interagency Report 7864, Jul. 2012.

[264] E. LeMay, K. Scarfone, and P. Mell, "The common misuse scoring system (CMSS): Metrics for software feature misuse vulnerabilities," no. NIST IR 7502, Jul. 2012.

[265] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014) 'Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)', Computers & Security, 42, pp. 165–176. doi: 10.1016/j.cose.2013.12.003.

[266] S. Conheady, "Future of Social Engineering" NCSC conference 2013. [Online]. Available: https://www.ncsc.nl/binaries/content/documents/ncsc-en/conference/conference-2013/speakers/sharon-conheady/1/Sharon%2BConheady.pdf . Accessed on Dec. 3, 2015

[267] E. Adler, "Here's Why 'The Internet Of Things' Will Be Huge, And Drive Tremendous Value For People And Businesses" Business Insider 2013. [Online]. Available: http://www.businessinsider.com/growth-in-the-internet-of-things-2013-10/ . Accessed on Dec. 3, 2015

[268] Cloud Security Alliance T. M, "Security Guidance for early adopters of the internet of things" [Online]. Available:

[269] https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf . Accessed on Dec 5, 2015

[270] T. Macaulay, "Multi-party authentication and cryptography in the IoT" [Online]. Available: https://blogs.mcafee.com/business/multi-party-authentication-cryptography-iot/ Accessed on Dec 5, 2015

[271] T. Macaulay, "Social Engineering in the Internet of Things (IoT)" [Online]. Available: https://blogs.mcafee.com/executive-perspectives/social-engineering-internet-things-iot/. Accessed on Dec 5, 2015

[272] T. Macaulay, "International Security Standards and the Internet of Things" [Online]. Available: https://blogs.mcafee.com/executive-perspectives/international-security-standards-internet-things/ . Accessed on Dec 5, 2015

[273] N. Dhanjani, Abusing the Internet of things: Blackouts, Freakouts, and Stakeouts. 'O'Reilly Media, Inc.', 2015.

[274] R. Van Kranenburg, A. Bassi, S. Dodson, and M. Ratto, "The Internet of things," vol. 4, 2008. http://www.researchgate.net/profile/Matt_Ratto/publication/228360933_The_Internet_of_Things/links/0912f513755ebd1e87000000.pdf . Accessed on: Dec. 16, 2015.

[275] https://scholar.google.co.il/scholar?q=%22Internet+of+things%22+%22social+engineering%22+%22cyber+security%22&btnG=&hl=en&as_sdt=0%2C5 . Accessed on: Dec. 16, 2015.

[276] "The future of security and social engineering - security through education," in Podcast, AC, 2015. [Online]. Available: http://www.social-engineer.org/podcast/ep-065-2015-future-security-social-engineering/#Download . Accessed on: Dec. 16, 2015.

[277] T. Thomas, "Social engineering gets more um, social: Facebook security & link scanners," Top Ten Reviews, 2010. [Online]. Available: http://internet-security-suite-review.toptenreviews.com/social-engineering-facebook-security-and-link-scanners.html . Accessed on: Dec. 16, 2015.

[278] S. Johnson, "Social engineering attacks: Is security focused on the wrong problem?," SearchSecurity, 2014. [Online]. Available: http://searchsecurity.techtarget.com/feature/Social-engineering-attacks-Is-security-focused-on-the-wrong-problem . Accessed on: Dec. 16, 2015.

[279] "Security summit: Italian security summit: The future of social engineering - keynote speaker: Sharon Conheady,". [Online]. Available: https://www.securitysummit.it/archivio/2010/milano/eventi/view/54.html . Accessed on: Dec. 16, 2015.

[280] P. Baofu, The future of post-human engineering: A preface to a new theory of technology. Cambridge Scholars Publishing, 2009.

[281] E. Selinger and B. Frischmann, "Will the internet of things result in predictable people?," in The Guardian, The Guardian, 2015. [Online]. Available: http://www.theguardian.com/technology/2015/aug/10/internet-of-things-predictable-people . Accessed on: Dec. 16, 2015.

[282] "What is reverse social engineering?," 2015. [Online]. Available: http://security.stackexchange.com/questions/18723/what-is-reverse-social-engineering . Accessed on: Dec. 16, 2015.

[283] C. Kerley, "From Smartphones to smart everything: Welcome to the 'smart' revolution (part 1 of 2)," 2014. [Online]. Available: http://allthingsck.com/wp-content/uploads/CK-From-smartphones-to-smart-everything.pdf . Accessed on: Dec. 16, 2015.

[284] R. Miller, "Cheaper sensors will fuel the age of smart everything," TechCrunch, 2015. [Online]. Available: http://techcrunch.com/2015/03/10/cheaper-sensors-will-fuel-the-age-of-smart-everything/#.oeoofin:otGd . Accessed on: Dec. 16, 2015.

[285] "Smart everything," 2002. [Online]. Available: http://www.shapingtomorrow.com/home/alert/625628-Smart-Everything . Accessed on: Dec. 16, 2015.

[286] S. L. Pfleeger and D. D. Caputo, "Leveraging behavioral science to mitigate Cyber security risk," 2012. [Online]. Available: https://www.mitre.org/sites/default/files/pdf/12_0499.pdf . Accessed on: Dec. 16, 2015.

[287] "Protection of personal data - European commission," 2011. [Online]. Available: http://ec.europa.eu/justice/data-protection/ . Accessed on: Dec. 16, 2015.

[288] "Essential guide: EU data protection regulation,". [Online]. Available: http://www.computerweekly.com/guides/Essential-guide-What-the-EU-Data-Protection-Regulation-changes-mean-to-you . Accessed on: Dec. 16, 2015.

[289] S. Gibbs, "EU states agree framework for pan-european data privacy rules," in The Guardian, The Guardian, 2015. [Online]. Available: http://www.theguardian.com/technology/2015/jun/15/eu-privacy-laws-data-regulations . Accessed on: Dec. 16, 2015.

[290] "A guide for in-house lawyers," 2015. [Online]. Available: https://www.huntonregulationtracker.com/files/Uploads/Documents/EU%20Data%20Protection%20Reg%20Tracker/Hunton_Guide_to_the_EU_General_Data_Protection_Regulation.pdf. Accessed on: Dec. 16, 2015.

[291] S. Isaacs, "Why the 'Internet of things' is a ticking bomb," VentureBeat, 2014. [Online]. Available: http://venturebeat.com/2014/08/18/why-the-internet-of-things-is-a-ticking-bomb/ . Accessed on: Dec. 16, 2015.

[292] T. Macaulay, "Social Engineering in the Internet of Things,". [Online]. Available: https://blogs.mcafee.com/executive-perspectives/social-engineering-internet-things-iot/ . Accessed on: Dec. 16, 2015.

[293] B. Contos, "Security and the Internet of things – are we repeating history?," CSO Online, 2015. [Online]. Available: http://www.csoonline.com/article/2947477/network-security/security-and-the-internet-of-things-are-we-repeating-history.html . Accessed on: Dec. 16, 2015.

[294] A. Henry, "Why social engineering should be your biggest security concern," Lifehacker. [Online]. Available: http://lifehacker.com/why-social-engineering-should-be-your-biggest-security-1630321227 . Accessed on: Dec. 16, 2015.

[295] S. Heisig, G. Cecchi, and I. Rish, "Augmented Human: Human OS for Improved Mental Function,". [Online]. Available: https://www.aaai.org/ocs/index.php/WS/AAAIW14/paper/download/8838/8361 . Accessed on: Dec. 16, 2015.