Essay

Masters Candidate: Veronica La Regina - Matr. Nr. 0210622

Supervisor: Prof. Roberto Setola

Security Awareness & the Systems Engineering Approach

THE METRICS: FROM THEORY TO PRACTICE

V. La Regina | Università Tor Vergata, Roma – Italia | 20 aprile 2015

To my foolishness

To the concept of meta-model

To 

To my family for always making problems and demanding solutions.
This places systems engineering in the service of everyday happiness.

Acknowledgments

Although only my name appears on the cover of this essay, a great many people have contributed to its production.

I wish to express my special thanks to prof. Roberto Setola from Campus Bio-Medico University in Rome. He is the supervisor of this work. I greatly appreciated his availability even outside official working hours. Above all, his insights and constructive advising supported the substantial thoughts behind this essay.

I am also grateful to all faculty and practitioners providing lectures during the Master Program. The Master matched my expectations also thanks to my classmates, Eng. Massimiliano Filippi of SELEX SI and Eng. Pierfelice Ciancia now of ASTER. I am extremely thankful and indebted to all of these people for sharing their expertise, and for the sincere and valuable guidance and encouragement extended to me.

In addition, I acknowledge Raffaele and Daniele for the idea of performing a survey.

I also thank all people usually labelled '~~cacacazzi~~' for bringing forward many problems –they are providing the opportunity to develop new solutions. Without venturing into this Master, I would never have seen the positive side of these people.

I also place on record my sense of gratitude to all who, directly or indirectly, have lent me their hand in taking on this challenge.

Disclaimer: The views and comments expressed in this essay belong solely to the author.

Table of Contents

Acknowledgments 2
Introduction 4
Definition of security awareness 7
Security Awareness Program 9
On-line survey: methodology and analysis 10
Survey format 11
Respondents 11
Limitations 12
Analysis 12
Main findings 13
The metrics: definition and systems engineering approach 14
Metrics for measuring the deployment of security awareness 15
Metrics for measuring the impacts of security awareness policies 23
Discussion 31
Conclusions 31
References 32

Introduction

The latest cyber-attacks experienced by Sony[1] and CENTCOM[2] definitely show the need to prioritize security awareness, not only for businesses or political concerns but also for individuals. Security attacks are becoming more and more sophisticated, and the traditional defence mechanisms are becoming more and more obsolete.

With Information Technology (IT) resources moving outside of the firewall and enterprises distributing their applications and data across multiple devices, it is now clear that simply protecting an organization's perimeter is not enough. These sophisticated attacks—, which include advanced persistent threats (APTs)—are bypassing traditional defences. Major security incidents can affect a company's data, networks and corporate brand, and sophisticated attacks, designed to gain continuous access to critical information or to cause damage to critical infrastructure, are becoming more severe, more frequent and more cost inducing.

There are at least three trends, e.g. convergence, networks' inter-dependences and Internet of Things, from which the border between physical and virtual attacks is a doubt. The first is ***convergence*** as a human behaviour and as a technological challenge. Convergence can be classified into four categories: convergence of services, convergence of transmission lines, convergence of terminals and convergence of providers. The driver of this phenomenon is user mobility and the increasing desire to know where the user is, where other users are and what is available in the vicinity. This situation arises from the desire for a continuous "local awareness" amongst people who travel and move around very often. The condition of mobility further demands access to user-friendly and convenient technology in terms of fast connectivity, deployment and hand-usage. Thus, great efforts have been made in the development of broadband and large-capacity info-communications network technology and the improvement of mobile communications technology, resulting in the explosive growth of the Internet in terms of "infrastructure" and the number of users.

This phenomenon has been accompanied by a growing ***dependence*** of the main infrastructures on communications systems. Communications systems are the backbone for much of the critical infrastructure within a community, and many of the other infrastructure components are completely dependent on communications systems to perform their missions. The communications sector provides the basis for information exchange for all other sectors including voice, data, video, and Internet connectivity. As such, communications systems sit on the level of other key national security and emergency preparedness resources, and are an important component of the overall critical infrastructure. It can also be said that Global Navigation Satellite Systems (GNSS), providing Positioning/Navigation and Timing services are becoming the *king master infrastructure*, e.g. US GPS, etc. Figure 1 below shows the master role of communications infrastructures in interconnections between critical services.

---

[1] Ira Winkler and Araceli Treu Gomes, Time to reprioritize security awareness efforts, February 2015, retrievable from http://www.csoonline.com/article/2879660/security-awareness/time-to-reprioritize-security-awareness-efforts.html (16 April 2015); Tim Hornyak, Hack to cost Sony $35 million in IT repairs, February 2015, retrievable form http://www.csoonline.com/article/2879444/data-breach/hack-to-cost-sony-35-million-in-it-repairs.html (16 April 2015)

[2] Steve Ragan, U.S. CENTCOM Twitter feed compromised by 'Cyber Jihadists', January 2015 retrievable from http://www.csoonline.com/article/2867561/disaster-recovery/u-s-centcom-twitter-feed-compromised-by-cyber-jihadists.html (16 April 2015)

The US National Association of Regulatory Utility Commissioners (NARUC)[3] has published a set of Critical Infrastructure Technical Briefs that "(...) identify key strategies for our consideration as we meet ongoing challenges within each of the electricity, natural gas, water, and telecommunications sectors". The following diagram - Figure 1 - from the NARUC "Issue Paper on Critical Infrastructure Protection" shows many of the interdependencies for the utility "sector", partially illustrating the extent of the interdependencies between utilities (electric power, oil and gas, water), and other sectors including communications, transportation, banking and finance, emergency services, transportation, and government services.

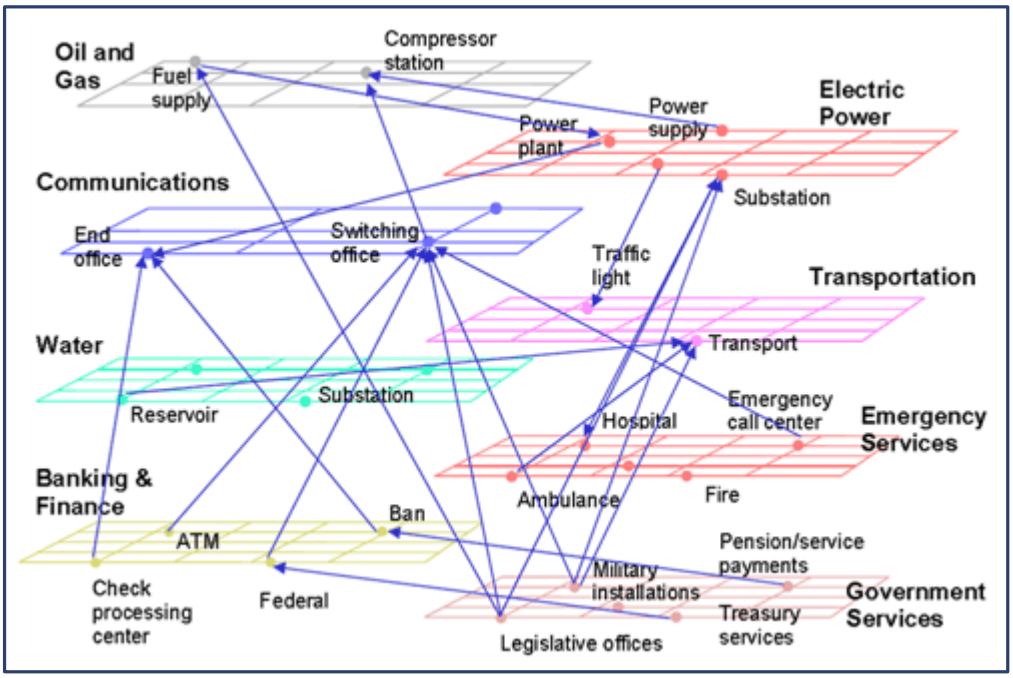

Figure 1: Interdependencies between utilities – Source: NARUC, 2005

On the other side the US Department of Homeland Security (DHS) is advancing beyond a simple assessment of the risks that GPS disruptions pose to critical infrastructure and is considering the development of new technology to mitigate jamming and spoofing while working with vendors to integrate that technology into receivers. The DHS's appraisal of the extent of GPS dependencies can be seen in Figure 2. GPS is the primary timing mechanism for communications, and loss of the signal would affect equipment ranging from SONET/SDH, SynchE, and clock nodes to mobile and landline switching centres and transceivers for cellular and micro-cell networks.

For this purpose GNSS infrastructures are becoming the most critical. At present, concern about this is being also raised by other nations or regions, such as Europe with the coming Galileo constellation, China with Beidou and Russia with GLONASS. In addition, sustainable systems are emerging in other regions such as the Quasi Zenith Satellite System (QZSS) from the Government of Japan. Within this context, some proposals favour a single encompassing system, and from a security awareness

[3] "NARUC is an association representing the State public service commissioners who regulate essential utility services, such as electricity, gas, telecommunications, water, and transportation, throughout the country. As regulators, our members are charged with protecting the public and ensuring that rates charged by regulated utilities are fair, just, and reasonable." The NARUC web site is at http://www.naruc.org/

perspective this opens the door to a weighty discussion about how firewall measures would then be established.

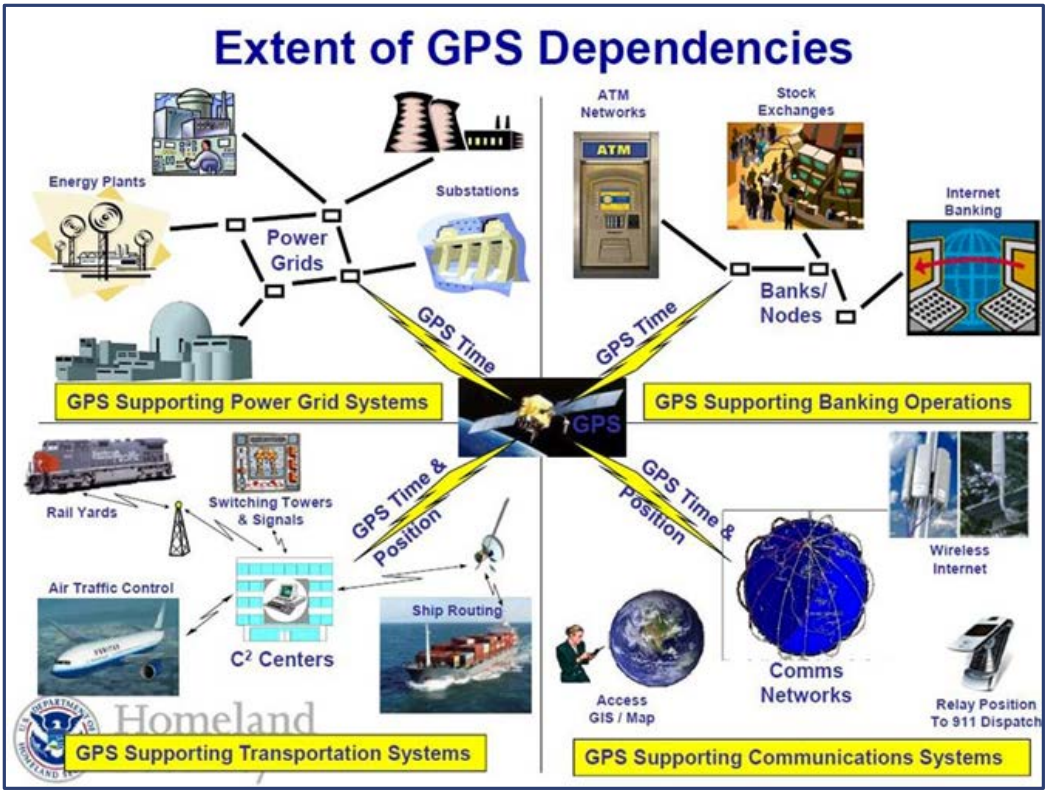

Figure 2: Extent of GPS Dependencies – Source: US Department of Homeland Security, 2014

In addition, growing local awareness creates needs for generating, storing and transmitting data. Thus, **smart devices** are becoming **intelligent** with a number of sophisticated sensors, **interconnected** to other data hubs (physically or virtually located) for storage or to other networks for transmission and **instrumented** with enormous computational power. Taking a broader view, the smart device enables a larger concept of smart homes, smart buildings and smart cities where the challenge is on the level of improving the living conditions of humankind.

All of these reported phenomena present at least two dimensions: a technological profile (hardware and software components) and a human behavioural profile. Thus, any attacks for whatever purpose shall have at least or technical side and/or a human behavioural one. There is now an emerging interest in security awareness, and the human behavioural aspect is becoming increasingly of interest in order to improve the security plans implemented within an entity (*e.g.* public institution, corporation, etc.). Increased security awareness helps to reduce risks. Every stakeholder should cooperate, and this cooperation requires motivation, stimulus and anticipation of benefit. Thus, a good security awareness policy should encompass also psychological elements to drive appropriate manners and behaviours.

Security awareness implies continued operational status and it requires an augmented knowledge of the nature of attacks, weaknesses of the target entity and new trends in the utilised technologies. In order to consider these incremental concerns of security, this work shall adopt a systems engineering (SE) approach to identify potential options for security awareness metrics, mainly applying by analogy the SE stakeholders' analysis and system requirements. For the purposes of this work, the definitions, theories and approaches of SE shall be applied to the target of this study: the metrics concerned with security awareness.

Definition of security awareness

In order to define the scope of this work it is of primary importance to find an answer to "what is security awareness?". The immediate response is "security awareness is awareness of security".; a correct answer as far as it goes but one that gives the opportunity to think more deeply in order to understand if the concept is still in its infancy or if there are already different perspectives and murky definitions developing around it. There are two main types of definitions of security awareness, one mainly related to ***business perspectives*** where threats, risks and potential damages raise concerns about security and thus security awareness is a form of prevention and precaution. The second type is mainly related to the ***safety of individuals*** as members of a community, organization, corporation, entity or other group. Here, security awareness is a state of wakefulness on the part of each single person to take care of herself and of the physical or virtual groups with which she is involved.

Merging these perspectives, Security Awareness (SA) is a state of consciousness about the value of data and related information, and it is an aim to be achieved through training and informative actions to build capacity and capability[4] about security concerns. For this purpose, security awareness is commonly used in government and industry. It is essential *security education* for members of employee populations that has immediate or practical application to the workplace and beyond. It suggests an awareness of possible risk, danger, or real threats to life, safety, or valued assets that will be translated into action or behaviours that address those risks and threats. Another dimension of security education is professional-level training for employees who perform specific security functions (full- or part-time) as members of a security workforce. Everyone needs security awareness as well, delivered as a dose of how-to training tailored to incorporate sound security practices into their specific job; the distinction between awareness and training therefore blurs.

Numerous drivers (other than common sense and statistics) make pursuing security awareness highly worthwhile. These include a number of international standards, although there is no single specific public standard published at present that defines security awareness practice. In this regard, the ***Information Security Forum (ISF)***[5] ***Standard of Good Practice*** defines security awareness as "the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual security responsibilities". This seems like a reasonable definition but note that there is no behavioural component; people can and do continue with unsafe behaviour despite having knowledge of the risks.

COBIT (the Control Objectives for IT) from ***ISACA (Information Systems Audit and Control Association)***[6] have made awareness one of the six main guidelines of their control framework. According to the COBIT approach, security awareness is the tool that ensures the confidentiality and integrity of information exchanged among people, while simultaneously providing availability to those who have business reasons to use it. Here, a trade-off is pointed out between the effort put into protection of available information and prompt access to the safe information.

Part Three of ***ISO/IEC TR 13335***, a standard often referred to as ***Guidance for the Management of IT Security (GMITS)***, contains excellent guidance on a number of information security practices, including awareness. In this context, "security awareness is an essential element for effective security. The lack of security awareness and poor security practices by personnel within an organization can significantly reduce the effectiveness of safeguards". Here, the concept *de quo* is a part of the implementation phase for overall security management.

---

[4] Capability is the measure of performance; capacity is the ability to effectively meet a target.
[5] ISF is a member-based organization that draws membership from large organizations across the world. Most of its work and output is retained for member use only, but it has decided to publish the Standard of Good Practice (SOGP), a thorough set of control statements for information security.
[6] COBIT is a professional body that represents (for the most part) IT Auditors.

BS 7799, the most widely used information security standard, says in Section 8.2.2: "Information security awareness, education and training. All employees and the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant to their job function". The standard also states that such initiatives should be ongoing and suitable to the roles and responsibilities of the people concerned. Within this framework, security awareness is diversified for each role and responsibility taken on by individuals.

The **Organization for Economic Co-operation and Developmen**t's ***(OECD) Guidelines for the Security of Information Systems and Networks – Towards a culture of security*** published in 2002 outline a series of nine principles. Awareness is the first of the nine, which states: *"1. Awareness - Participants should be aware of the need for security of information systems and networks and what they can do to enhance security. Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Participants should be aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants".* This statement operates as a soft rule non-binding value, as it stands as a recommendation and is not mandatory. It opens the door to a broader approach of security awareness including also interconnected and interdependent systems. This document marks a "new international understanding of the need to safeguard the information systems on which we increasingly depend for our life" ("OECD publishes," 2002). The guidelines "Towards a Culture of Security" specify that IT users have "to be aware of the need for security of information systems and networks". After releasing the initial document, the OECD Working Party on Information Security and Privacy (WPISP) promoted implementation plans, revised plans, and monitored the efforts to promote a "Culture of Security" among all participants who develop, own, provide, manage, and use information systems and networks.

All of these extracts from various standards make a clear point that security awareness is a fundamental requirement if one is to even contemplate meeting best practice. Given that many industries (financial services for example[7]) are driven by regulation, and that this regulation strongly recommends adherence to standards, in many circumstances security awareness is a prescribed requirement. Empirical evidence from outside of information security tells us that just knowing about a risk isn't enough. Consider smokers and people who drive without using a seat belt.; they are surely all "aware" of the risks but somehow their behaviour continues. Some people need to know the facts, others need something more in order to adopt safe behaviour. The OECD document, in contrast to the others, emphasizes ***a culture of security*** in all aspects of information systems, from designing and planning through to everyday use, and among all participants, from government down through business to consumers.

A real achievement in defining security awareness shall be made if cultural and behavioural elements are included, because these imply group norms which can encourage secure behaviour and good choices for secure technical systems (network and automation rules). It is important to play within an ecosystem where players are deeply conscious of their behaviours allowing the release and the acquisition of information and related commands (choices) without unwanted and harmful consequences. Certainly, attacks can be mounted through automation tools within networks or can be leveraged on people behaviours manipulated for adversary purposes. Thus***, a comprehensive security awareness's definition shall encompass elements not only of how people shall play but***

[7] The Financial Services Authority (FSA) in the UK has strongly suggested that certification to BS 7799 is seen as meeting many of their regulatory requirements that relate to information security.

also of how systems, e.g. IT management, shall allow people to play. The ways that a system works also reveal the security awareness culture backing the system itself.

SECURITY AWARENESS PROGRAM

Awareness is just what is stated, a knowledge of conditions and their impact on a well-protected environment. Employees, no matter how conscientious, will not behave in a prudent manner with regard to information assets just because you want them to; they must be told the "what and why" of the protective scheme [2]. This gives rise to a concern about the necessary features of a security awareness programme.

Educating on awareness methods is not just training. Information security and privacy awareness activities promote ongoing compliance; likewise, ongoing compliance helps with ongoing awareness. As business models change, so do compliance needs and awareness activities. Awareness is typically the "what" component of the education strategy; training is typically the "how" component. To make awareness activities effective, you must know your audience. Awareness audiences are very broad; they include everyone within the organization and all third parties who perform work for, or on behalf of, the organization. The awareness audience has diverse experiences, backgrounds, and job responsibilities. The awareness goal at the decision-making level is to convince the audience that information security and privacy risk reduction is achievable. Awareness goals at the end-user level are generally to help them understand information security and privacy risks and the actions to reduce them, thus creating a demand for risk reduction. Awareness programmes also must avoid being boring. The following is a list of 15 ways to make awareness interesting [3]:

1. Use analogies;
2. Use recent, significant, real-world examples and news events;
3. Explain the importance of your message;
4. Use scenarios and multifaceted situations (e.g., what would you do if …?);
5. Use graphics;
6. Use photos and videos;
7. Make it interactive;
8. Make it memorable … use humour, shock, and wit;
9. Make it personal … show how it relates to your audience, especially to their personal lives, such as preventing identity theft;
10. Make it fresh … tie it to something current;
11. Provide practical, "job-ready" information;
12. Use known people in examples … celebrities, sports figures, etc.;
13. Use animation;
14. Recognize employees who have done an outstanding job;
15. Use games and challenges.

Awareness activities are different from training activities. The objectives for delivering information security and privacy awareness are similar to training options. However, there are some very important differences between training and awareness activities. The options and methods for awareness activities are typically very different from the more formal and structured training. Awareness activities should:

- Occur on an ongoing basis;
- Use a wide range of delivery methods;
- Catch the attention of the target audience;
- Be less formal than training;
- Take less time than training;
- Be even more creative, memorable, and fun than how you may have your training sessions planned;
- Reinforce the lessons learned during formal training;

- Be the foundation for preparing for the first level of training for various target topics.

An awareness program must remain current. Personnel must be notified as information security and privacy regulations change and, subsequently, information security, security, privacy policies, and procedures are updated. Establish a method to deliver immediate information and updates when necessary. Perhaps new information is sent as the first alert item personnel see when logging into the network for the day. The awareness messages and methods must also be simple. The purpose is to get messages and ideas out to personnel quickly and easily. They must not be confused or convoluted, which will dissuade personnel from reading them, and eventually they will not pay any attention at all to the messages. Make it easy for personnel to get information security, security, and privacy information, and make the information easy to understand. Think of positive, fun, exciting, and motivating methods that will give employees the message and keep the information security and privacy issues in their mind as they perform their daily job responsibilities. The success of an awareness program is measured by its ability to reach all personnel using a variety of techniques.

One of the main factors pertaining to the creation of a successful culture of security awareness is the ability of an organization to remain dynamic in the face of changing industries and technologies. The different areas in which security awareness is an absolute necessity are shown in Figure 3. Because every organization is a unique entity, however, it would be an impossible task to provide an all-inclusive list of the areas of concern for each specific company. Providing effective information security and privacy training and awareness is one of the most cost-effective and results-effective practices that businesses can do to keep their information assets safe. Nevertheless, the main security attacks mainly take effect through one or more aspects of the 9 realms here reported in Figure 3. Real world awareness also includes elements of social engineering, email security, backups and business continuity.

A new, comprehensive security awareness program shall also propose topics related to the creation of automated rules, as freely decided by owners, to protect from unwilled induced behaviours. The option shall not be that the first suggestion on how to create security culture is “compulsory attendance at security awareness training”.

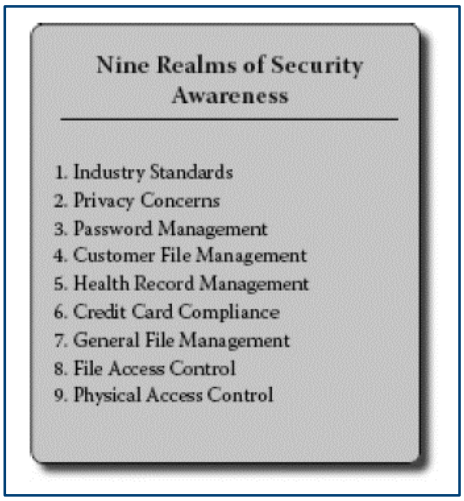

Figure 3: Security Awareness Realms – Source: Tyler Justin Speed, 2011

On-line survey: methodology and analysis

The objective of the online survey was to gauge interest in security awareness, understand the difference between awareness and training, understand the role of social engineering, gauge

management buy-in, gauge the the role of metrics, understand the decision to buy solutions versus building in-house, and to gain a broader vision of the topic.

SURVEY FORMAT

The survey was implemented using a free online tool (www.freeonlinesurveys.com), which provided all of the necessary tools for an anonymous survey, including tracking and analysis. The key questions were:

A. Introduction of "your-self": security manager, security professional or user;
B. What is security awareness in your opinion?
C. Why are social engineering and other non-technical attacks so successful?
D. How do you get management buy-in for a program?
E. What are the biggest challenges to build security awareness for organizations? Is budget an issue?
F. What were the political obstacles that needed to be overcome?
G. What metrics are useful for measuring the success of the security awareness?
H. What failures and pitfall did you encounter in building security awareness?
I. What is the best training cycle for raising security awareness?
J. What learning and teaching styles work the best?
K. What is your advice for others building security awareness?
L. What is the advantage of building internal security awareness over buying a prebuilt program from a vendor?
M. Is there anything we have not covered that you would like to add?

All questions offered a free text field. To provide for maximum freedom in response, the survey was conducted anonymously. There was, however, an incentive provided for respondents to indicate their participation via an email, as this would entitle them to a digital copy of the final report and enter them into a draw for a smartphone app with a price under 3.00 €. While it is possible that this supported the high participation rate, it is worth noting that not all participants entered their name into the raffle and none of the winners of the raffle claimed their prize. This would indicate that the survey subject itself provided a sufficiently large incentive to participate.

The questions as a whole helped the author to gather consistent insights of the main issues of the overall subject, the security awareness. The outcomes of the survey are here exploited for the identification of the metrics. The survey supported the systems engineering approach in order to identify the main issues, the related owners and from here to depict the stakeholders' ecosystem.

RESPONDENTS

The survey was sent to 120 contacts gathered from the main vendors of security awareness training. The contacts cannot be revealed because the author signed a non-disclosure agreement with them. The survey was on line from 14 November 2014 (Tokyo time 17.00 pm) to 25 January 2015 (Tokyo time 17.00 pm). The collected responses numbered 30, of which 3 were not fully completed forms, out of 120. This equates to a response rate of 25%[8], a surprisingly high participation rate in this timeframe given the unknown identity of the authors in this sector.

[8] The author was assisted in reaching these contacts by the staff of DEKRA Italia. She negotiated with them the release of the full identification data of the interviewed persons. The contact list most probably consists of people interested in security awareness for professional reasons.

LIMITATIONS

The most notable limitation is the selection of the survey recipients, which was dictated by availability and access. No inferences can be made about the influence that existing interests and concerns about security awareness might have on prospective users in their investment in these topics.

While limited in scope and number of participants, there is strong indication that the survey format and content appealed to a specific group of concerned persons, namely those that have an explicit interest in the security field. Given the emergence of substantial concerns regarding security, the survey result data is expected to be realistic and relevant for this selected group of respondents.

ANALYSIS

Analysis of the survey result was centred on the understanding of security awareness and the identification of related metrics. The hypothesis was that respondent interest in security awareness would be very high given the emerging concerns about cyber-attacks and the rising awareness of data value. Mention of recent cyber-attacks was expected, at least as a driver of debates over security. If harmful activity takes place often, then prevention and/or protection are more likely to be undertaken. The response rate was surprisingly high at 25% of all recipients, and hence it is assumed that the results are representative of the completely recipient population. To the extent that the survey recipients are representative of the population of general users who are very interested in security awareness (which can be assumed as likely, but not proven), the results can yield insights into the more general population of persons interested in these topics.

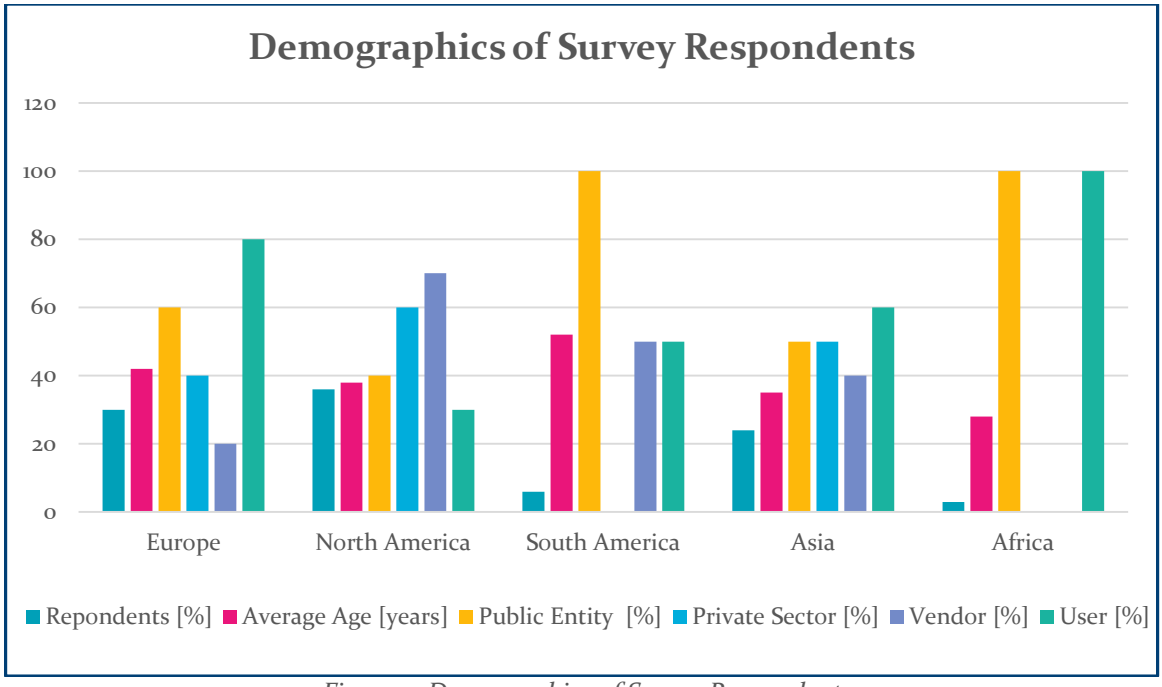

Figure 4: Demographics of Survey Respondents

Very limited demographic information about the respondents was available, so no detailed demographic analysis could be performed. The highest percentage of respondents were from North America (36%), led by the USA, followed by 30% from Europe, 24% from Asia, 6% from South America and 3% from Africa. In terms of age, concern with security awareness engages older persons in South America, with an average age of 52, followed by average ages of 42 in Europe, 38 in North America, 35 in Asia and 28 in Africa. In the old Continent, security awareness is mainly found among the new generation familiar with IT facilities and their uses.

MAIN FINDINGS

The main findings can be stated as follow ones:

A. Public entities in Europe, South America and Africa are mainly handling security awareness. The vendors of security awareness programs are mainly from the North America. There are vendors even vested in public entities, representing a form of revenue generation in order to help pay for the initial investments to be made for the benefit of the overall national community.
B. Security awareness is an on-going dynamic that encompasses two components: the existing deployment level of measures protecting assets and the flow of the information; and the attempts to improve conscious knowledge of emerging threats and the related risks and harms.
C. Social engineering and other non-technical attacks are becoming more and more successful. To break a system there are both physical and behavioural barriers. Breaking down behavioural barriers can enable an attacker to activate commands to break down physical ones. Thus psychological manipulation targeting a number of users' systems can increase the probability of success in breaking down protections.
D. Management buy-in is a crucial element for building effective security awareness within an organization. Top-level management is very sensitive to financial parameters, s quantitative metrics showing future cost-savings arising from present investment always helps to increase management sensitivities to these topics.
E. The biggest challenges to build security awareness for organizations are not only budget related. The main challenge is to bring the concern closer to the daily life of everyone, to overcome the typical attitude of "I do not believe these threats reach me, thus I do not worry about them".
F. Political obstacles that need to be overcome are mainly related to the contents to be delivered in training sessions. Security awareness courses report on the main cyber-war attacks and techniques, and this information can be misused not to prevent but to provoke an attack.
G. Metrics are useful for measuring the success of security awareness measures; a deep analysis of metrics can be found in the following sections of this essay.
H. The principal failures and pitfalls encountered in building security awareness are found during the initial steps, in particular due to a lack of consistency, metrics, follow-through procedures, clear policies, enforcement, and/or importance placed upon the initiative. This typically comes about where some actions are done merely for compliance with certain requests and without substantial interest amongst the target audience; "We had to do because it was requested ..."
I. The best training cycle for raising security awareness is to raise self-interest in these topics. The dynamics change a lot and people should be self-motivated to review their behaviours. The key-message is to avoid the cooperation of the victim when an attack takes place.
J. The most effective learning and teaching styles are therefore those that provide useful tips for the daily life of people.
K. The main advice for others building security awareness varies a lot depending on whether the question is addressed to a security analyst, to a user or to a vendor of training courses. The analyst looks at the optimal time to build a culture of security awareness as a key asset of the organization. The user is often mostly concerned with cost, and the vendor provides a more comprehensive overview taking into account costs and benefits and also follow-up measures for future updating.
L. The advantage of building internal security awareness over buying a prebuilt program from a vendor is to make people constantly concerned about security threats and to stimulate ongoing security-conscious behaviours. If there is no one internal with the necessary

expertise, then it is preferable to choose an external expert for the initial activity. The most balanced option is to create a dedicated responsible unit within the organisation.

M. The additional advice expressed is to concentrate more on people rather than on technical measures, e.g. IDS/IPS, firewalls, etc.

The metrics: definition and systems engineering approach

Metrics represents a key element enabling a successful policy of security awareness within an organization. For the purpose of this essay security awareness is a *status* of knowledge, belonging to people working toward delivering the same mission (corporation, public entity, etc.), to prevent damage coming from security threats. The threats are addressed to physical or virtual assets involving the human behaviour of people who are regularly allowed to use them. There are basic concepts and measures to prevent these attacks but there are always new emerging types of attacks, therefore the knowledge can often become obsolete in need of augmentation in terms of content and the people who need to be engaged. Metrics assess the knowledge behind human behaviours and the adopted IT management rules of the systems. For instance, it is relevant to assess how many times users change their passwords, and to assess the system's automatic detection of how many times users are changing their passwords. There exists one aspect of security awareness in which human beings are the target of observation and another aspect in which the primary targets are the systems. In conclusion, every system is backed by human choices, and, in addition, users often play within systems where they do not have the right or the means to establish the rules of the game.

In these dynamics, metrics can help measure deployment and impact:

- Metrics that measure the deployment of awareness program – *Are you compliant?*
- Metrics that measure the impact of awareness program – *Are you changing behaviour?*

In these ways, the actions can be traceable to show progress and to measure impacts. In addition, they allow for the rapid and easy improvement of the plan in case of pitfalls or misleading advice. The recursive approach behind the systems engineering model presents a prompt analogy between the identification of the metrics for security awareness purposes and the features of requirements as an element of the problem and solution domains. The metrics can be classified in terms of goal, type, objective, description, purpose, data source, implementation evidence, formula, frequency and indicators in accordance with with the approach developed by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-55, Security Metrics Guide for Information Technology Systems. In addition, every single metric should be assessed for its value; a metric should measure a human risk or behaviour that you care about, and it should be actionable, low cost and potentially automated and repeatable. Taking this in mind the following section will report a list of metrics, coming from the aforementioned survey and tabulated to give an indication of the category (*Human behaviour* or *System*), the scope of the metrics (detection of security awareness level or impact of the security awareness policies), the content of the measure (*what is measured*), the data source (*how it is measured and who measures*), the frequency (*when it is measured*), and the rationale behind the metric.

The reported metrics focus on security awareness concerns within the Information Technology ecosystem. This focus emerges from current trends in which systems feature an increasing interrelation and dependence upon the Internet. There is now a strong belief that every security plan should begin with information security, because of the ripple effect on other dimensions of human security, as represented in the following Figure 5.

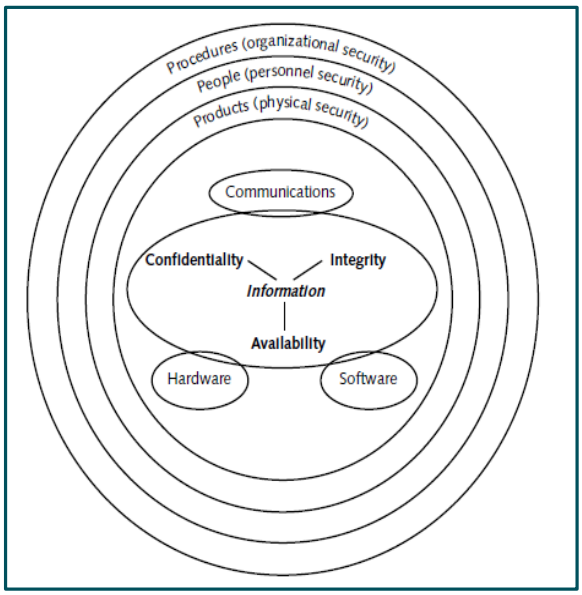

Figure 5: Information Security components – Source: M. Ciampa, 2010

METRICS FOR MEASURING THE DEPLOYMENT OF SECURITY AWARENESS

The clusters of metrics for measuring the deployment of security awareness include the following:

- Metrics to assess the *behaviours* of users of a system concerning their degree of SA;
- Metrics to assess the *system* in order to understand the degree of SA underlying the behaviour of system administrators. The owner of the system can be the developer and the manager of the system in some cases; in other cases, these three stakeholders can be three distinct persons and roles. For this reason, these metrics target the systems themselves instead of human behaviour.

These metrics mostly aim to show the status of the current degree of security awareness on the part of users and systems. The following table reports examples of metrics drawn directly from the surveys and/or indirectly induced during interviews. Aside from the two clusters defined above, the table displays *what* is measured, *how* and *when* it is measured and *who* measures. The rationales behind this list take into account the 9 realms of security awareness (Figure 3) as the critical targets of attacks. A qualitative evaluation of the effort required to use the metrics is also done in order to understand:

- If the metric is *actionable*, if it is able to be done or acted on, thus having practical value;
- If the introduction of the metric is *low cost*, i.e. relatively inexpensive; and
- If the metric is *repeatable*, if it is able to be reiterated even while subject to improvements and adjustments.

Each feature also receives an additional qualification as:

- ***Easy*** when it requires a low effort in terms of resources involved and when automation of procedures is relatively simple;
- ***Medium*** when it requires a medium effort in terms of resources involved; and
- ***Hard*** when it requires significant effort drawing on substantial resources and when automation of procedures is relatively difficult.

In this work, the list is a simple guide showing only qualitative assessments. A tailored adoption of the metrics could also choose in favour of quantitative ranges to move from *easy* to *medium* and to *hard*. For instance, each organization could use cost values, or time spent, or number of stakeholders, etc. for defining the borders of the *easy*, *medium* and *hard* ranges.

The purposes of these metrics are to detect and to regularly monitor the culture of the security awareness within an organization. There are three main stakeholders[9]:

- The ***users*** of the systems: a user[10] is someone in need of authentication to a system and granted authorization to access resources provided by or connected to that system;
- The ***security manager***: she is in charge of procedures like information classification, risk assessment, and risk analysis to identify threats, categorise assets, and rate system vulnerabilities so that she can implement effective controls[11];
- The ***network administrator***: she is responsible for joining up a computer network including the maintenance and monitoring of an active data network or converged infrastructure and related network equipment.

The last two stakeholders can have similar competence, but it is preferable to distinguish the two tasks because the security manager can help to guarantee improvement of the security awareness, implementation plan while avoiding any trade-off between speed of use and security protections, or between the cost of security investment and user-friendly access to the system.

The network administrator is often in a direct relation with users and her behaviour favours a reduction of the regularity of intervention and/or assistance. This induces the network administrator's behaviour to take care of speed of use while being more relaxed about a higher profile of system protection. The security manager is in charge of asset protection and she is most probably accountable for harmful consequences coming from attacks when precaution measures are not sufficient.

The users in themselves are often frustrated by security rules making their work tasks more cumbersome. This often creates a relaxed attitude on the part of the network administrator in order to smooth relations with them. This interplay is often critical because it reduces the potential effort for intrusion into the system from unauthorized persons. At the occurrence of the intrusion, the main target is to find out the identity of the unfair intruder. This identification capacity is linked with the registration phase - more items are required to open a user account and it is therefore more difficult to build up an imaginary identity. On the other hand, if the registration phase requires a lot of information then users are discouraged from joining.

[9] In some cases, the metrics are measured through the involvement of the Human Resources department or supervisors of the personnel; the reason for this is the identification of a more effective and less burdensome way of measuring.

[10] "One of the horrible words we use is 'users'. I am on a crusade to get rid of the word 'users'. I would prefer to call them 'people'" ["Don Norman at UX Week 2008 © Adaptive Path" retrievable from: https://www.youtube.com/watch?v=WgJcUHC3qJ8 (16 April 2015)]

[11] Dell.com, Manage IT Security Risk with a Human Element, 2011

N.	Category Metric	*What Is Measured?*	*How is It Measured?*	*When Is It Measured?*	*Who Measures?*	Rationale	Actionable	Low Cost	Repeatable
1	Human behaviour	Number of persons attended a SA training	Feedbacks from users' systems	Log-in, enrolment, registration to the system	Security manager *annually* reports	Securing a common degree of SA within the organization	***Easy***	***Easy***	***Easy***
2	System	Number of elements (PC, devices, etc.) equipped with tools to prevent unauthorized access	Feedback from users' elements	Enabled entry of elements within the system	Security manager *annually* reports	Maintaining a uniform degree of security within the system from the augmentation of the initial system	***Medium***	***Medium***	***Easy***
3	System	Number of nodes of interconnected networks equally protected from unauthorized access	Feedback from network's administrators	Request for the interconnection	Security manager *annually* reports	Securing a consistent degree of security of the system in order to prevent harmful behaviours from interconnected systems	***Medium***	***Medium***	***Medium***
4	System	Number of systems compliant with the basic security rules	Feedback from network administrators	Upon inquiry from security manager	Security manager *annually* reports	Assuring basic compliance with security regulation over time	***Easy***	***Medium***	***Easy***
5	Human behaviour	Number of qualified personnel for security awareness purposes	Human Resources inquire to personnel	Signature of job contract and contract reviews	Head of Human Resources	Assuring an uniform degree of SA among human resources	***Easy***	***Medium***	***Medium***
6	System	Number of identified suspicious emails during last year	Automatic identification and personnel flagging	Entry of emails in the system and/or opening of emails	Network administrators	Understanding how secure the system is in accordance with IT management choices	***Medium***	***Medium***	***Easy***

N.	Category Metric	*What Is Measured?*	*How is It Measured?*	*When Is It Measured?*	*Who Measures?*	Rationale	Actionable	Low Cost	Repeatable
7	Human behaviour	Number of users using the same passwords	Automatic detection	Updating of database at login	Network administrators	Assure that intrusion is hard because each alpha-character series has low probability to be a password	*Easy*	*Easy*	*Easy*
8	Human behaviour	Number of users choosing the same password for several systems	Direct query to the user	Check-up	Security manger inquires every three months	Measuring the attitude of users to diversify risk of intrusion	*Hard*	*Medium*	*Hard*
9	Human behaviour	Number of passwords displayed on desktops or boards	Detection in offices (every 6 months)	Check-up or incentivise people to report (awarding)	Security manager	Reducing the risk of unwanted password dissemination to unknown persons	*Hard*	*Hard*	*Hard*
10	System	Number of seconds before warning of an attack	Automatic identification and personnel flagging	Upon occurrence of the attack	Security manager detects and reports	Test the response of the system to an attack as symptomatic of the degree of SA	*Medium*	*Medium*	*Easy*
11	System	Number of threats (virus and similar) automatically detected	Automatic identification	Check-up every three months performed by the network administrator	Security manger	Test the reliability of the systems as symptomatic of the degree of SA	*Easy*	*Easy*	*Easy*
12	System	Number of obsolete threats	Automatic identification and manual updating	Reports performed monthly by network administrator	Network administrator	Test the reliability of the systems as symptomatic of the degree of SA	*Easy*	*Easy*	*Easy*
13	System	Number of detectable threats	Automatic identification and manual updating	Reports performed monthly by network administrator	Network administrator	Test the reliability of the systems as symptomatic of the degree of SA	*Easy*	*Hard*	*Medium*

N.	Category Metric	*What Is Measured?*	*How is It Measured?*	*When Is It Measured?*	*Who Measures?*	Rationale	Actionable	Low Cost	Repeatable
14	Human behaviour	Number of users attending training on a voluntary basis outside the organization	Feedbacks from users' systems	Log-in, enrolment, registration and review of the data	Security manager	Assessment of the potential SA	***Easy***	***Easy***	***Easy***
15	Human behaviour	Number of days to review the password to log-in to the system	Automatic detection at log-in	Log-in or change of password	Security manager	Monitoring a constant level of SA	***Easy***	***Easy***	***Easy***
16	System	Number of information items required to register and their review	Automatic query form to register	Registration phase to become a user of the system	Network administrator	Assessment of the information related with users' profile	***Easy***	***Easy***	***Easy***
17	Human behaviour	Number of times noting password somewhere	Direct query to users	Check-up from security manager every 3 months	Security manger	Assessment of SA	***Hard***	***Hard***	***Hard***
18	Human behaviour	Number of times cancelling a password noted somewhere	Direct query to users	Check-up from security manager every 3 months	Security manger	Assessment of SA	***Hard***	***Hard***	***Hard***
19	Human behaviour	Number of times reporting password to someone (with and without third persons)	Direct query to users	Check-up from security manager every 3 months	Security manger	Assessment of SA	***Hard***	***Hard***	***Hard***
20	System	Number of suspicious files detected	Automatic detection and manual notifications	Count at occurrence	Security manger	Assessment of the reliability of the system	***Easy***	***Medium***	***Easy***

N.	Category Metric	*What Is Measured?*	*How is It Measured?*	*When Is It Measured?*	*Who Measures?*	Rationale	Actionable	Low Cost	Repeatable
21	Human behaviour	Number of suspicious files/emails opened by users	Direct query to users	Check-up	Security manger	Assessment of SA	*Hard*	*Medium*	*Hard*
22	System	Number of suspicious websites detected	Automatic detection and manual notifications	Count at occurrence	Security manger	Assessment of the reliability of the system	*Easy*	*Medium*	*Easy*
23	Human behaviour	Number of suspicious websites visited by users	Direct query to users	Check-up	Security manger	Assessment of SA	*Hard*	*Medium*	*Hard*
24	Human behaviour	Number of data back-ups done by users	Automatic operation day by day	User command	Security manager	Reduce concern about lost data	*Easy*	*Medium*	*Easy*
25	System	Number of data back-ups done	Automatic operation day by day	Automatic command (network administrator)	Network administrator	Reduce risks of lost data	*Easy*	*Medium*	*Easy*
26	Human behaviour	Number of times introducing credit card credentials (or similar data) into to the system	Automatic detection of credit cards credentials (with user approval)	Count at the time of data introduction	Security manager	Assessment of valuable data held within the system	*Easy*	*Medium*	*Easy*
27	System	Number of hours credit card credentials or similar data are stored in the system	Automatic detection of credit cards credentials (with users' approval)	Check by the network administrator	Security manager	Assessment of valuable data held within the system	*Easy*	*Medium*	*Easy*

N.	Category Metric	*What Is Measured?*	*How is It Measured?*	*When Is It Measured?*	*Who Measures?*	Rationale	Actionable	Low Cost	Repeatable
28	Human behaviour	Number of personnel/user have completed the security awareness training	Final attendance list	Human Resources and network administrator count attendees	Security manager	Assessment of SA	*Easy*	*Medium*	*Medium*
29	Human behaviour	Number of 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 reports	Security manger	Monitoring the improvement of SA	*Hard*	*Hard*	*Hard*
30	Human behaviour	Number of 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	Assessment of SA	*Easy*	*Medium*	*Medium*
31	Human behaviour	Number of visited webpages concerning security awareness	Automatic detection (daily)	Count at occurrence	Security manager	Assessment of how much SA is an element of a common culture	*Easy*	*Easy*	*Easy*
32	Human behaviour	Number of suspicious files/email not fully intentionally opened	Direct query to users	Check-up	Security manager	Assessment of effective SA	*Hard*	*Medium*	*Hard*
33	Human behaviour	Number of suspicious downloads not fully intentionally opened	Direct query to users	Check-up	Security manager	Assessment of effective SA	*Hard*	*Medium*	*Hard*
34	Human behaviour	Number of suspicious websites not fully intentionally opened	Direct query to users	Check-up	Security manager	Assessment of effective SA	*Hard*	*Medium*	*Hard*

N.	Category Metric	*What Is Measured?*	*How is It Measured?*	*When Is It Measured?*	*Who Measures?*	Rationale	Actionable	Low Cost	Repeatable
35	Human behaviour	Number of help-desk calls from users making suspicious requests (phone calls, questions from outsiders, emails, web-data mining)	Automatic detection of the email/command and/or initiative of the user	Reports every 6 months	Security manager	Assessment of SA	***Medium***	***Medium***	***Hard***
36	System	Number of protections adopted to phone networks, camera recorded data	Feedbacks from network's administrators	Reports every 6 months	Security manager	Monitoring the safeness of data acquisition	***Medium***	***Hard***	***Hard***
37	Human behaviour	Number of postings of "sensitive" data on social networks (Facebook, tweeter, etc.)	Direct query to users	Check-up every 3 months	Security manager	Assessment of SA	***Hard***	***Hard***	***Hard***
38	Human behaviour	Number of pictures/video taken within the office	Direct query to users	Check-up every 3 months	Security manager	Assessment of SA	***Hard***	***Medium***	***Hard***
39	System	Number of minutes waiting time for assistance upon call	Direct query to the users	Check-up every 3 months	Security manager	Assessment of the response of the systems to an attack	***Hard***	***Easy***	***Hard***
40	Human behaviour	Number of times per day users leave the system open to everyone	Direct query to the users	Check-up every 3 months	Security manager	Assessment of SA	***Hard***	***Easy***	***Hard***
43	System	Amount of data lost from servers, memory boxes and similar	Direct query to the users or upon user's notification	Check-up every 6 months	Security manager	Assessment of the reliability of the system	***Medium***	***Medium***	***Medium***

Table 1: List of metrics for measuring the deployment of security awareness

METRICS FOR MEASURING THE IMPACTS OF SECURITY AWARENESS POLICIES

The previous metrics represent the prevailing degree of security awareness within an organization. The following metrics aim to represent improvements arising from adopted security-related policies focusing on maintaining and/or increasing the awareness as previously defined. For this purpose, some metrics will be similar to the previous ones, because each organization has its current status from which it would improve upon by maintaining or building upon existing practices and policies. In addition, the first list intended to assess the security awareness of the overall system of which users are one element. The following metrics assess improvements mainly in user behaviour as the main contributor to awareness. Aside from this, the impact assessment also involves an understanding about the target system's resilience in the face of direct and indirect attacks.

The scope of these metrics makes them crucial for people involved in making relevant decisions, e.g. budget allocation for further security awareness training, for hiring employees already partially aware of security threats, etc. These decisions often involve economic and/or financial trade-offs to be advised to top-level management.

Two clusters of metrics are used to measure the improvement stemming from security awareness policies:

- Metrics to assess the improved watchfulness of the user consciously adopting *behaviour*s; and
- Metrics to assess the improved performance of the *system* in order to understand if the SA measures realised the systems administrators' aims towards a consistently safer and more secure environment - the rationale is the same as explained in the earlier section.

These metrics consider the impact coming from human behaviour and the impact in terms of costs or time spent to achieve a target. They are more demanding in terms of effort and the stakeholders' involvement in related procedures. The following Table 2 reports examples of metrics taken directly from the surveys and/or indirectly induced during interviews. Aside from the two clusters defined above, the table displays the category (*human behaviour* or *systems*), *what* is measured, *how* and *when* it is measured and *who* measures. The rationales behind this list take into account the 9 realms of security awareness (Figure 3) as the critical targets of attacks and the content of information that will be displayed to a diversified set of concerned peoples, from top-level management to personnel, customers and users. In addition, as in the previous section, a qualitative evaluation of the effort required to use the metrics is done in order to understand:

- If the metric is *actionable*, if it is able to be done or acted on, thus having practical value;
- If the introduction of the metrics is *low cost*, i.e. relatively inexpensive; and
- If the metric is *repeatable*, if it can be reiterated even while subject to improvements, adjustments or *ad hoc* investment.

Each feature also receives an additional qualification as:

- ***Easy*** when it requires a low effort in terms of resources involved and when automation of procedures is relatively simple;
- ***Medium*** when it requires a medium effort in terms of resources involved and;
- ***Hard*** when it requires significant effort drawing on substantial resources and when automation of procedures is relatively difficult.

In this work, the list is a simple guide showing only qualitative assessments. A tailored adoption of the metrics could also choose in favour of quantitative ranges to move from *easy* to *medium* and to *hard*. For instance, each organization could use cost values, or time spent or number of stakeholders, etc. for defining the borders of the *easy*, *medium* and *hard* ranges.

The purposes of these metrics are to detect and to regularly monitor the going on implementation of the security awareness within an organization. There are three main stakeholders[12]:

- The ***users*** of the systems: a user[13] is someone in need of authentication to a system and a granted authorization to access resources provided by or connected to that system;
- The ***security manager***: she is in charge of procedures as information classification, risk assessment, and risk analysis to identify threats, categorise assets, and rate system vulnerabilities so that she can implement effective controls[14];
- The ***network administrator***: she is responsible for joining up a computer network including the maintenance and monitoring of an active data network or converged infrastructure and related network equipment.

Because the efforts in establishing these metrics are more comprehensive, their implementation often requires also involvement of the Chief Financial Officer (CFO), or a similar role who has responsibility for investment concerns, and the head of Human Resources for personnel issues. For this reason, the frequency of measurement is not as high as the previous cases and the qualification as *easy*, *medium* and *hard* of the three features – *actionable*, *low cost* and *repeatable* - may not be directly comparable for quantitative meaning with the previous metrics.

[12] In some cases the metrics are measured through the involvement of the Human resources' department or supervisors of the personnel. The reason is the identification of an effective and burden less way of measuring.

[13]. "One of the horrible words we use is 'users'. I am on a crusade to get rid of the word 'users'. I would prefer to call them 'people'" ["Don Norman at UX Week 2008 © Adaptive Path" retrievable from: https://www.youtube.com/watch?v=WgJcUHC3qJ8 (16 April 2015)]

[14] Dell.com, Manage IT Security Risk with a Human Element, 2011

N.	Category Metric	*What Is Measured?*	*How is It Measured?*	*When Is It Measured?*	*Who Measures?*	Rationale	Actionable	Low Cost	Repeatable
1	System	Lags between scheduled and actual maintenance operations of the systems for security purposes	Automation of the calendar in terms of plan and operation (network administrator)	Counting of the operations every 6 months	Security manager	Assure an updated secure system due to the awareness of the network administrator and security manager	***Easy***	***Easy***	***Easy***
2	System	Lags between emergency change and actual implementation of the change within the systems for security purposes	Automation of the calendar	Counting of the operations every 6 months	Security manager	Assure an updated secure system due to the awareness of the network administrator and security manager	***Easy***	***Easy***	***Easy***
3	System	Cost estimation of unauthorized access for each different profile affecting business functions	Study report between human resource, business functions and network administration	Cost estimation to be reported bi-annually	Security manger	Assessing if the security awareness policies are reducing the impact on business functions	***Hard***	***Hard***	***Medium***
4	System	Cost estimation of the value of each single system in relation with the main business functions of the organization	Study report between human resource, business functions and network administration	Cost estimation to be reported bi-annually	Security manger	Assessing if modular security awareness policies are reducing the impact on business functions	***Hard***	***Hard***	***Medium***
5	System	Cost estimation of the marginal value of new emerging threats and related business functions	Study report between human resource, business functions and network administration	Cost estimation to be reported bi-annually	Security manger	Assessing if new threats are relevant to be considered in a potential SA training	***Hard***	***Hard***	***Medium***
6	System	Dependence of the internal systems on the main infrastructural systems (electricity, transportations, utilities)	Study report between production process, business functions and network administration	Assessment performed bi-annually	Security manger	Assessment if the SA training is reducing the affect factor of the systems among themselves	***Hard***	***Hard***	***Medium***

N.	Category Metric	*What Is Measured?*	*How is It Measured?*	*When Is It Measured?*	*Who Measures?*	Rationale	Actionable	Low Cost	Repeatable
7	System	Number of autonomous sub-systems as back-ups of the system	Study report between production process, business functions, purchasing and financial units and network administration	Assessment performed bi-annually	Security manger	Assessment if the system has redundancy measures	*Hard*	*Hard*	*Medium*
8	Human behaviour	(Δ) Number of users detecting new threats (external or internal, natural or man-made)	Direct query to users	Check-up every 6 months	Security manger	Assessment if the SA policies are improving human behaviours	*Medium*	*Medium*	*Medium*
9	System	Lag between the identification of new threats and the implementation of new related policy	Planning of the network administrator	Check-up every 6 months	Security manger	Assessment of response time of the system	*Medium*	*Medium*	*Medium*
10	System	Number of fake warnings	Review of the network administrator	Check-up every 6 months	Security manager	Assessment of reliability of the systems	*Medium*	*Medium*	*Medium*
11	Human behaviour	Number of people making others aware of security threats	Direct query to people	Survey every year	Security manager	Assessment of the improvement from SA policies	*Easy*	*Easy*	*Medium*
12	Human behaviour	Number of people with advanced security awareness training	Request for the course from personnel	Survey every year	Security manager	Assessment of the improvement from SA policies	*Easy*	*Easy*	*Easy*
13	Human behaviour	Number of people obtaining advanced security awareness qualifications	Reporting to human resources	Survey every year	Security manager	Assessment of the improvement from SA policies	*Easy*	*Easy*	*Easy*
14	Human behaviour	Number of people reporting behavioural changes in relation to security awareness	Direct query to people	Survey every 6 months	Security manager	Assessment of the improvement from SA policies	*Medium*	*Medium*	*Easy*

N.	Category Metric	*What Is Measured?*	*How is It Measured?*	*When Is It Measured?*	*Who Measures?*	Rationale	Actionable	Low Cost	Repeatable
15	Human behaviour	Number of behavioural changes by users for reducing the interdependence of a system in relation to another one	Direct query to users	Survey every year	Security manager	Assessment of firewall behaviour adopted by users	*Medium*	*Medium*	*Easy*
16	Human behaviour	Number of persons always changing to a new, challenging password	Automated detection of new password at log-in	Detection monthly	Network administrator	Assessment of improvement of security awareness	*Easy*	*Medium*	*Easy*
17	Human behaviour	Number of people who fall victim to a phishing attack	Upon phishing assessment	Counting occurrence monthly	Security manager	Assessment of the ability to resist attack	*Hard*	*Easy*	*Hard*
18	Human behaviour	Number of people who detect and report a phishing attack	Upon phishing assessment	Counting occurrence monthly	Security manager	Assessment of environment's SA	*Hard*	*Medium*	*Hard*
19	System	(Δ) Number of infected computers	Help desk or centralized AV management software	Reporting of the information monthly	Security manager	Assessment of the effectiveness of SA training	*Medium*	*Medium*	*Medium*
20	Human behaviour	Number of employees who understand and are following security policies, processes and standards	Online survey	Report bi-annually	Security manager	Assessment of the effectiveness of SA policies	*Hard*	*Hard*	*Hard*
21	System	Percentage of devices that are updated and currently compliant with basic security requirements	When employees connect to an internal server or use an external service	Report monthly	Security manager	Assuring a uniform SA	*Medium*	*Hard*	*Medium*

N.	Category Metric	*What Is Measured?*	*How is It Measured?*	*When Is It Measured?*	*Who Measures?*	Rationale	Actionable	Low Cost	Repeatable
22	Human behaviour	Number of devices (laptops, smartphones, tablets) that were lost or stolen, and what percentage of those devices were encrypted	Reports to security manager or through physical asset audits	Report monthly	Security manger	Assessment of degree of SA	***Hard***	***Easy***	***Hard***
23	Human behaviour	Number of employees who are securing their desk environment before leaving, as per organizational policy	Nightly walkthrough	Monthly or weekly	Security manager	Testing level of security care amongst personnel	***Hard***	***Medium***	***Hard***
24	Human behaviour	(Δ) Number of employees using strong passwords	Password brute forcing	Report monthly or quarterly	Security manager	Assessment of impact from SA policies	***Easy***	***Easy***	***Easy***
25	Human behaviour	(Δ) Number of employees who can identify, stop and report a social engineering attack	Phone call assessments	Report monthly	Security manager	Assessment of impact from SA policies	***Hard***	***Hard***	***Hard***
26	Human behaviour	Number of employees posting sensitive organizational information on social networking sites	Online searches for key terms	Report monthly	Security manager	Assessment of impact from SA policies	***Hard***	***Easy***	***Hard***
27	Human behaviour	Number of employees who are properly following data destruction processes	Check digital devices that are disposed of for proper wiping, and check dumpsters for sensitive documents.	Random check-up	Security manager	Assessment of the improvement from SA training	***Hard***	***Easy***	***Hard***

N.	Category Metric	*What Is Measured?*	*How is It Measured?*	*When Is It Measured?*	*Who Measures?*	Rationale	Actionable	Low Cost	Repeatable
28	Human behaviour	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	Check monthly	Security manager	Assessment of risk exposure from human behaviour	***Hard***	***Medium***	***Hard***
29	Human behaviour	Number of employees who understand, follow and enforce policies for restricted or protected access to facilities	Test how many employees are wearing their badges or stopping those who are not	Check monthly or weekly	Security manager	Assessment of conscious behaviour for critical facilities	***Hard***	***Medium***	***Hard***
30	System	Number of incidents due to failed safeguards	Assessment done by security manager	Check every 6 months	Security manager	Assessment of the effective safeness of the system after SA policies	***Hard***	***Medium***	***Easy***
31	System	Number of incidents due to non-existence of safeguards	Assessment done by security manager	Check every 6 months	Security manager	Assessment of the risk exposure of the system due administration choices	***Hard***	***Medium***	***Medium***
32	System	Number of alternative measures of the key-functions	Assessment of the network administrators	Report performed bi-yearly	Security manager and network administrators	Assessment of the redundancy of the systems	***Hard***	***Medium***	***Medium***
33	Human behaviour	Number of claims about others' poor behaviour in relation to security awareness	Automated reporting system and manual notification	Check monthly	Security manager	Assessment of self-enforcement measure within the organization	***Medium***	***Easy***	***Medium***
34	System	Return from Investment of security awareness expenditures	Assessment of this ratio from accounting data and business functions	Study report bi-annually	Security manager and CFO	Assessment of the financial impact of SA measures	***Hard***	***Medium***	***Medium***

N.	Category Metric	*What Is Measured?*	*How is It Measured?*	*When Is It Measured?*	*Who Measures?*	Rationale	Actionable	Low Cost	Repeatable
35	Human behaviour	Number of new initiatives of SA	Proposal of new initiatives	Reporting monthly	Security manger	Assuring an augmented degree of SA	*Medium*	*Medium*	*Easy*
36	System	Number of devices and/or equipment shared between professional and private purposes	Inquiry to users and automation detections	Report annually	Security manger	Assuring a constant and uniform degree of SA	*Medium*	*Medium*	*Easy*
37	System	Reduction in suspicious files/emails delivered to the users	Automated assessment	Reporting monthly	Security manager	Detecting the trend of improvement	*Easy*	*Easy*	*Easy*
38	Human behaviour	Reduction in suspicious files/emails opened partially intentionally by the users	Automated assessment and direct inquiry to users	Reporting monthly	Security manager	Enhancing more conscious behaviours	*Easy*	*Easy*	*Easy*
39	System	Number of induced simulated attacks	Automated assessment	Reporting every 3 months	Security manager	Assuring constant training	*Easy*	*Medium*	*Easy*
40	Human behaviour	Number of time security awareness is a topic of discussion among people	Direct query to users	Reporting every year	Security manager	Assessing a culture of SA	*Hard*	*Medium*	*Hard*
41	Human behaviour	Number of new books, magazine and reviews about security awareness	Assessment from formal request and purchasing evidence	Reporting every year	Security manager	Supporting the development of a culture of SA	*Hard*	*Medium*	*Hard*
42	Human behaviour	Reduction in posted sensitive data on social networks	Direct query to users or commitment to intelligence company	Reporting every year	Security manager	Evaluating the impact from SA	*Hard*	*Medium*	*Hard*
43	System	Reduction in loss of data stored on servers, memory boxes and similar	Assessment made by the security manager	Every 6 months	Security manager	Assessment of the improved reliability of the systems	*Medium*	*Medium*	*Medium*

Table 2: List of metrics for measuring the impacts of security awareness policies

These metrics allow stakeholders to monitor the on-going impact of security awareness. Some metrics are similar to the previous group, but there is a difference in that here we are interested in catching a trend or a dynamic, thus the measure refers to reduced counts instead of absolute indicators; *e.g.* reduction in loss of data is an impact assessment and amount of data loss is a deployment assessment.

Furthermore, these metrics have the key role of providing evidence that SA is valuable and needs resources made available from the decisions of top-level management. The impact of SA comes from human behaviour being more conscious of their actions, and refers to the system being reliable (low level of attacks, redundant, resilient to threats, etc.) and encouraging users to behave in a sound and conscious manner.

Discussion

The information gathered from the metrics should be carefully edited in order to deliver understandable messages and to enhance the engagement of the people concerned.

Discernment between metrics referring to human behaviour and metrics referring to the system is essentially borderless. If the focus is on human behaviour, then the required actions are broader and shall encompass all users involved. If the target is the system, then the actions shall be undertaken by a network administrator under the approval and/or command of the security manager.

The implementation of the metrics' plan, independently if it is for monitoring of improving the compliance of peoples' behaviour to SA, shall take in count that different stakes are in the trilateral game among the user, the network administrator and the security manager. The user wishes to have an easy interaction with the network, the network administrator with the wish to easily satisfy users' requests – and the security manager which wish is to preserve the security and safety of the network. Thus, the metric shall be built as a cooperative game with a win-win-win pay-off.

Conclusions

In conclusion, this work exploits the potential of a systems engineering approach, commencing with problem and solution domains and supporting the analysis of stakeholders about their needs in the face of user requirements. The satisfaction of user demands then guide the designation of system requirements. The requirements shall be, *inter alia*, clear, traceable, and precisely matching their targets. These features are by analogy the attributes of the metrics included here as to be identified and analysed for the purposes of Security Awareness.

The outcomes of this project can also be used in order to identify the main requirements of a potential successful security awareness policy and related training program. Further research should be done to outline the plan of a Security Awareness program and related policies.

In conclusion, the systems engineering approach can play two roles, simulating research from a critical point of view and guiding the identification of solutions. The attitude of the systems engineer is result-oriented and cooperative; the attitude of the researcher is questioning and challenging. Where the systems engineer will promote the use of a proposed method or technique, the researcher needs to question its validity. Experts in systems engineering are typically educated in the technical domain. However, the effectiveness of systems engineering depends largely on human aspects, such as the competence and behaviour of individual stakeholders, social interaction between stakeholders, political circumstances, organization and governance, and many more. Research in systems engineering has to build on available scientific methods, both technical and from the social sciences.

The dimension of interdisciplinary is theoretically highlighted in the field of systems engineering and at present, it is still partially missing from practical deployments. An emerging mind-set shared among

technical experts and social scientists ought to be built up and exploited for the mutual benefit of effectively managing complexity.

References

[1] Ciampa Mark, *Security Awareness: Applying Practical Security in Your World*, 3rd Edition, Course Technology, Cengage Learning, 2010

[2] Desman Mark B., *Building an information security awareness program*, CRC Press LLC, Auerbach, 2002

[3] Herold Rebecca, *Managing an information security and privacy awareness and training program*, Ed. Taylor & Francis Group, LLC, Auerbach, 2005

[4] Jajodia Sushil, Liu Peng, Swarup Vipin, Wang Cliff, *Cyber Situational Awareness - Issues and Research*, Springer Science & Business Media, LLC 2010

[5] Kott Alexander, Wang Cliff, Erbacher Robert F., *Cyber Defense and Situational Awareness*, Springer International Publishing Switzerland 2014

[6] Langford Gary O., *Engineering Systems integration - Theory, Metrics, and Methods*, Taylor & Francis Group, LLC, 2010

[7] McIlwraith Angus, *Information security and employee behavior: how to reduce risk through employee education, training and awareness*; Ed. Angus McIlwraith 2006

[8] Roper Carl, Grau Joseph, Fischer Lynn, *Security education, awareness, and training: from theory to practice*, Elsevier Inc., 2006

[9] Speed Tyler Justin, *Asset Protection through Security Awareness*, Taylor & Francis Group, LLC, 2011