ESCOLA NAVAL TÉCNICO LISBOA FACULDADE DE DIREITO UNIVERSIDADE DE LISBOA

The Human Factor for the information security in organizations

Master Degree’s dissertation in Information Security and Cyberspace Right

Author: **Telma Kidy da Conceição Tavares**[1]

[1] Instituto Superior Técnico, Technical University of Lisbon, Portugal.
proftelma2010@gmail.com

Abstract

One of the biggest threats to information security in the recent years is the Social Engineering (SE) which has been put many organizations in risk. As per the statistical data , more than half of breaches to data occurred last year were due to internal threats, using or not technological means in the attack.

This dissertation aims to analyse the influence of human factor for the information security of an organization and the consequences of inappropriate behaviour of employees , based on the principle that in the security mechanism the human being is the only factor that has the option to breach the rules.

Taking into account the non territoriality of cyber crimes, nothing and no one anywhere in the world can be considered safe. The focus of this research is to address the importance of the behavioural factor for the information protection in an public service company of an African country with a growing economy , emphasizing the relevance of the study in the international scene.

The obtained results will be used to find out vulnerabilities in the information security of this organization and to suggest solutions in order to remove and/or mitigate them.

Key words: information security, behavioural component, Social Engineering and training and education.

1. Introduction

The human factor has been seen by many organizations as one of the biggest challenges of information security since users allow or authorise third parties to access the data, places or devices and allowing non authorised persons access to important information of the organization and thus jeopardizing its security.

The importance of this study for the international scene is the basis of our choice to focus this research on a company that has made significant investments on equipment and human capital , although located in the African continent where issues associated with security of computer systems have not been fully developed yet due to technical and professional shortcomings that most of African countries face as a result of weak technological development of the continent.

The most used technique to influence users to allow or authorise third parties to access privileged information is social engineering, which will be at the centre of the development of this dissertation, taking into account the importance that it may play in changing an organization's employees behaviours and resulting in significant improvement or even down play the role of other implemented security measures , no matter well developed and updated they are.

1.1 Issue

It has been proven by many professionals, even the most expensive and advanced information security systems can be compromised in an unexpected manner granting access to ackers the information stored in them.

This ascertainment has called our attention to find out how the human factor is seen in one of Angolan private sector company that recently has made the highest investment in human resources, equipment and technology, taking into account that even the most expensive and advanced information security systems can be compromised in an unexpected manner granting access to ackers the information stored in them.

We aim to analyse the influence that the human behaviour can have in the information security of an organization. Thus, we wish to develop a proposal that, through the evidence of various types of psychological principles used to manipulate the users of systems, makes more clear the attacks to Social Engineering for the organization and provide better defensive measures.

Specific Objectives

1. Identify the level of awareness of the employees of the company about the main issues linked with the information security, in particular with Social Engineering as well as the more frequent ways of attack.
2. Verify whether there are policies, standards and procedures of information security adopted by the company. And whether they in line with the academic education of the employees.
3. Propose best practices that helps to reduce the identified weaknesses

The quantitative research method has been adopted based on a exploratory study and the following techniques were used:

- Documentary analysis/ Literature review (books, articles, publications and dissertations
- Direct observation of employees in the working place
- Questionnaires

To this aim, specific questions were raised while interacting with the employees in order to find out their behavioural weaknesses when dealing with emotional issues (behaviioral influenced factors) and technical (hardware and software). The information collected at the company was used in a qualitative fashion as a way of strengthening the research which allowed an approach through a mixed research method (literature review and case study).. (Hill & Hill, 1998).

1.2 Statistical data

The Verizon's research report on data breach indicates that in 2016 more than 100.000 incidents reported and 2.260 confirmed data breaches (Verizon, 2016).

According to the same source, cybercriminals continue to exploit the human nature as they depend on the standards of the attacks which play with psychology, as it is the case of ransomware attacks which increased by 16% comparing to 2015, where the data is accounted and a ransom is required.

Comentado [AV1]: Versao em Portugues pouca clara

Internal attacks represent 77% of the incidents, being 26% errors in sending sensitive information to unauthorised third parties and the remaining 51% inadequate disposal of information, improper set up of systems and stolen or lost laptop/smartphone. The privileged user abuse is most used method of invasion as the user just need to make use of the tools made available by the company (data access). (Verizon, 2016).

The Symantec report on the threats to the Internet security in 2016 recorded more than one million of daily attacks against users in which the cyber criminals took advantage of the weaknesses of the websites. The same source reported the quantity of daily zero vulnerability doubled in comparison to the previous year, exposing/leaking about 429 million of identities (Symantec, 2017a).

2. Information Security

Information Security is the process of protecting information from various types of internal and external threats that put at risk the continuity of the business and the return of investments (Harvey & Evans, 2016).

According to Beal (2005, p. 71), Information Security is "the process of information protection from threats in order to ensure its integrity, availability and confidentiality". In another words, information security ensures that the information in any forma is protected against any access by unauthorised (confidentiality), always available when needed (availability) , trustful (integrity) and authentic (authenticity). (Beal, 2005).

The adoption and implementation of an security system is an option of each organization and, in general, it is influenced by factors such as business needs and objectives, necessary security requirements, invested capital, size and structure of the organization.

3. Social Engineering

In the first pages of "Engenharia Social: A Arte do Hacking Humano", Chritopher Hadnagy states that "social engineering is the act of nagging a person in order to take an action that may or not be in the best interest of the target".

Hadnagy adds stating that social engineering techniques are frequently used in our day to day life by people from all works of life. For example, it is used by doctors to influence patients behaviour in order to improve their health and by parents to influence their children behaviour in order to behave themselves (Hadnagy, 2010).

Mouton and Huber argue that:
"Social Engineering refers to the various techniques used to obtain information, in order to circumvent security systems, by exploiting the human weaknesses."

In Mouton at al, (2010)

"Social Engineering is the art of exploiting the weakest element of the information security system: the people who use them."

In Huber (2009)

Examining the above mentioned opinions, it is obvious that the primary and unique target of a social engineering attack is the human being which is considered the weakest element of the information security system.

Another important inference from the above quotations is the absence of a computer device during the attack which makes possible the use of social engineering within an organization which manages its information on paperwork.

In this scenario, the most used attack technique is the nagging or influence which is very subtle and difficult to detect as it involves more and limitless complex scenarios linked to the day to day interactions among the human beings (Winnefeld at al, 20105).

The complexities are exploited due to innate features of the human beings which tend to trustful, willing to be useful and be seen as “good persons”. (Peltier, 2006). That being said, Kevin Mitnick (2002) justifies the social engineering in 6 human basic trends.

- Friendship and fondness
- Consistency and commitment
- Scarcity
- Reciprocity
- Natural tendency to be useful (Social Approval)
- Authority

Below are listed some of the methods of attacks associated with social engineering:

- Information Gathering (pretexting)
- Use of Google Hacking
- Use of social network
- Telephone Call
- Personal Approach
- Analysis of Garbage
- Inverse Social Engineering

As far as the tools used for the attack, we highlight the followings:

- Use of SET to capture confidential information such as the target credentials.
- Use of fraudulent websites to collect credentials through fraudulent websites that tend to appear as legitimate.
- Use of Maltego tool to consult various source of public data and graphically describe the relationship among entities, persons, companies, websites and documents.
- Use of FOCA to carry out the analysis of metadata in any document available in a website.

Generally the following with email attacks:

- Worms as they spread quite quickly. In this case the attacker generally uses a text to attract the interest of the target such as sales, news about famous people, as well as the personal life of the target.
- Spyware to spy and collect information about the target by monitoring its behaviour and preferences while surfing the internet
- Phishings to fool the target. These email messages generally contain attachments or links that direct the target to a situation desired by the attacker
- Baiting to attract the target with an asset or item (virtual or physical) as a bait
- Ransonware to infect the target´s computer with a virus that cryptograph the files until the victim pays a ransom.

In summary, the fact that the person can be nagged, fooled or forced to breach the security policies to grant access or privileges to someone else, makes them the biggest issue when addressing the security. Therefore the biggest protection against social engineering still is the education and awareness. (JONES, 2004). Training the staff on how to act and report strange or abnormal actions are the more effective measures against social engineering. However, this is only possible if everyone in the organization are aware that they can be target of this evil.

4. Methodological approach

To respond to the predefined objective and question, we carried out a survey through questionnaires in a medium size Angolan road transportation company with subsidiary in all provinces. We decided to collect data only in the head office located in the capital city as due time constraints, technical and financial limitations we could not visit the provinces. The head office of the company has 810 employees, 105 of them are technicians and administrative workers with access to a computer or data digital system.

The questions were designed specifically to find out:

1. The level of knowledge on information security, social engineering and the most used techniques.
2. Availability of security policy and incidents response plans.
3. Availability training programs on information security
4. The employees´ commitment towards the protection of information system

4.1 Case Study “Matox Transportes”

For security reasons, we will use the fictitious name MATOX-Transportes in order to not identify the researched company as the information provided is consider confidential. This company was selected due to the fact that it is the biggest road transportation service provider in the country and it has a considerable financial, material and human capital. The company operational fleet comprises 350 buses and has a daily capacity to transport 30 thousand passengers within the capital urban services and 1,500 passengers in the interprovincial trips. For this purpose, the company employs throughout the country 765 direct employees.

Recently the company invested several million US Dollars on bus terminals, real state and movable assets despite the huge investment on IT. These can be determinant factors for the company to become target of the kind of attacks object of this study as these are usually driven by financial and competitive factors (Puricelli, 2015).

4.2 Implementation of the Questionnaire to the employees of the Company

The characterisation of the study population revelled that about 69% of the employees have the educational level below the college. These information requires a special attention should be given to adequate the policies, standards and procedures of the company security.

We found out the 28% of the employees responded to have read the information security policy at the time of signature of the employment contract and 9% stated that from time to time have access to it.

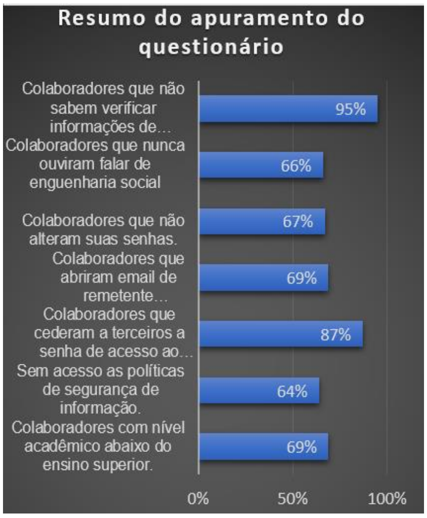
According to the Information technology department of the company, the security policies are not made known to the employees given that the security restrictions are directly to the system and thus preventing that non work related actions can be undertaken. This has been confirmed by the 64% of employees that confirmed not having knowledge of the policy , as otherwise it would be desirable.

The opinion of the surveyed population about the most vulnerable point of the information system was 75% to the software /hardware, leaving the human factor to the secondary stage. We can consider that the lack of real knowledge of the importance of human factor to the security system has led to this margin of responses.

About 56% of the employees have confirmed giving their passwords to a co-worker, team leader or technical assistant. 44% has confirmed to have connected third parties pen drives or other USB devices to the company computer and 69% have acknowledge to have opened files from unknown sources. As far as passwords change is concerned, 67% stated that has never changed their passwords to access the system.

In relation to Social Engineering and its techniques, the study revealed that 66% has never heard about it and 94% is not aware of preventative measures against these kind of attacks (Graph 1).

We have seen that the majority of the surveyed population, including those working for the IT department shown scant knowledge about the issue.



Graph 1- Summary of the questionnaire results

Based on these results, we managed to develop a list of weaknesses that we will use as a starting point to propose a set of best practices which includes the development of adequate policies as well program of permanent training and education of employees, incidents response plan and use of punitive measures.

5. Results analysis and discussion

Aiming to address the identified weakness in the previous chapter, we propose the adoption of the following countermeasures:

- ➔ Divulge the security policy taking into account the educational, cultural and social level of the company´s employees
- ➔ Develop a security education, training and awareness program capable of making users aware of the important role they play in the security information of the company
- ➔ Adopt and implement solutions that create logic barriers against attacks from electronic devices
- ➔ Set up a security incidents response plan that quickly identifies and react to an attack or attempt of attack, establishing punitive measures to discourage employees to practice or take part in such offenses.

5.1 First stage – Development of the right security policy

Policies are a set of rules developed to guide the behaviour of the employees as they should protect the information systems and sensitive information. They should be based on standard of rules and procedures but also meet the real needs of each company (Barman, 2001). The development and deployment of a policy should be anticipated and carried out in conjunction with awareness and education campaigns about the security policy and procedures to follow while performing the working activities.

Taking into account the education and intellectual level of the majority of the company´s employees the developed policy must be easy to read, interpret and access. It must be avoid the use of complex words and ambiguities. The rules and processes must be well detailed and, when possible, depicted to avoid different readers to interpret differently (Blank & Gallagher, 2013). T his means that the policy must be read and understood by the employees from all tiers of the organization and not only by the administrative or the IT employees.

According to Griffin (2016) , Schwartz (2016) & Nicholson (2016), some of the suggestion are:

- ➔ Adopt a policy with “minimum privileges” to protect the users against attacks. It is important that employees are made aware of this in order to avoid dissatisfactions which may increase the risk of attacks from discontent employees.

- Adopt the use of scripts for each flow of information when the employees are communicating by the phone or email.
- Always use two factors authentication whenever possible in order to avoid that the theft of credentials do not cause much damages.
- Classify the information according to its decree of importance and the sensitive information must be subject to stronger security requirements.
- Appoint someone responsible to deal with the attempt of Social Engineering. This will make that the employees to take a proactive approach in the defence of the organization.

5.2 Second stage – employees' awareness and training

A defensive tactic often suggested against Social Engineering attacks is to ensure that all employees irrespective of their job receive instructions to recognise and handle this kind of attacks. Special attention should be given to social network (taking into account its relevance) as users are not able to perceive the amount of confidential information they publically share that identify them as employees of the company.

The training should be extensive to the entire company, including directors, managers, team leaders, technicians and other employees, all of them must be trained, Gavrilova (2014). The most common tactics used in the attacks and ways of prevention also must be communicated. The employees should be instructed that whenever they perceive an attack, they should notify other co-workers.

5.3 Third stage – Technical defences

It requires the use of technical solutions already available in the market in order to prevent the increase of attacks through technical means. For the security of emails there at least three technical solutions that may be adopted by the company to authenticate the email communication which are the following:

- The OpenPGP standard to cryptograph and sign messages. (Callas, 2007).
- The S / MIME protocol which is operationally similar to OpenPGP with a notable exception of the treatment public keys. (Ramsdell, 2010).
- The SPF / DKIM / DMARC protocols that supply a solution based on DNS. (kucherawy, 2015).

The **OpenPGP** is an encryption and desencryption of data end to end, using the cryptography of the public key which supply cryptographic authenticity and privacy to the email message communication.

The **S / MIME protocol** is a bit similar to OpenPGP standard in terms of desing and objective with the difference that it uses the same confidence model of certificates X.509, used in connection TLS.

The **SPF / DKIM / DMARC protocols** allows to guarantee the authentication of all users of a specific domain using the SNS protocol.

SPF defines a format of TXT records in DNS for the domain of the company and creates a list of IP addresses allowed to send emails to that domain name.

DKIM is an authentication protocol of the parties involved in a communication by inserting a header to each email message, containing a cryptographic signature of the e-mail content.

DMARC is a standardization protocol that ensures the authenticity of emails, it is based on SPF and DKIM, and adds a special function, which allows to monitor the e-mails behaviour. (Kucherawy, 2015), (Steve, 2016).

Anti-phishing technical solutions

In addition to the protocols pointed out above, many other technologies are available in the market capable of identifying phishing attempts and inform them to the users, as it is the case of the below options: (ARDI & HEIDEMANN, 2016)

- ➔ Carnegie Mellon Anti-Phishing is a network analysis tool (CANTINA). In this approach a combination of DOM analysis and the results of a search engine are used to detect potential phishing websites. This approach detects with success 95% of the phishing websites.
- ➔ CodeShield uses a Whitelist of a Customised Application (PAW) to automatically block any phishing site that is not in the list of permissions.
- ➔ Password Google alert is a browser extension that focuses on alert and mitigate instead of prevention, it senses when a user enters the credentials of Google account on another site and let him know to change the password immediately.
- ➔ AuntieTuna is a web browser plug-in that uses the personalization along with detection algorithms in order to decidie whether a page is a phishing attempt.

Another measure to mitigate the threat of phishing is to use a "phishing simulation". The approach consists in carrying out a phishing attack in the direction of the target group in a controlled environment and provide feedback to the participants in accordance with the personal performance. In addition, it must be carried out regularly external auditing and penetration tests that includes vector tests of social engineering attacks.

5.4 Fourth stage – incidents Response plan

Even then all reasonable precautions are adopted, there is still the risk of a security incident occurs and for this reason the organization must have in place response mechanisms for this events. The speed of an organization in recognising, analysing and responding to an incident, can minimise damages and reduce losses.

The incident response plan is a document that describes the general guidelines and procedures to deal with the main security incidents that may occur in the organization and give to the helpdesk support team instructions on the measures to take in order to quickly sort out the issues. The way to handle the security incident varies according to its intensity and risk. The appropriate actions may involve the intervention of external entities (such as partners, service providers, etc) or even the law enforcement bodies.

Penalties for Social Engineering Crimes

It is never easy to penalise those responsible for social engineering attacks as many of the offenses that take place are criminalised under the legal regime of many countries, including in Angola.

We stress out the offenses resulting from the psychological nagging of the employees to gain access to classified information, overlook at information on top of workstations or monitors, search the trash of a company in a public place, and many other offenses that take place in accessing information that will be used to carry out the attack.

In the meantime, at the local level the company have to have in place penalties to discourage the employees´ participation or collusion in these practices, adopting measures from verbal warning and registered warning to dismissal of employees.

6. Conclusion

This study concludes that the majority of accidents and incidents related to the information security have the human intervention as the main factor and that the security has first of all to do with people and processes before being technology related. According to some information security subject matter experts quoted in this study, social engineering represents the major threat to the business continuity of our time and therefore it is not worthy investing millions in technology if the human factor is left at a secondary place.

Through the study carried out at the Company Matox-Transportes (with the use of questionnaire and the in-loco findings in the company) we have verified that 69% of employees have an education level below college education and this factor contributes to the weak awareness of security related issues and this is justified by the very short on knowledge about most of the issues addressed in the questionnaire as well as the lack of knowledge in relation to the techniques most used by social engineers to access information that endangers the information security of the company.

Comentado [AV2]: O nome usado acima é Matox-Transportes

This factor associated with the lack of a training plan and permanent awareness of employees defining clearly and concisely which security procedures to adopt in a work related activity, security standards and policies well publicized and known by everybody within the organization, and the incident response plans which details the guidelines and procedures that the helpdesk services should follow to rapidly tackle the security incidents that take place within the organization, were given a dominant attention in this study.

The awareness raising, training and education of employees are the most valuable weapon that should not be discarded even when it is assumed that everybody is aware of the danger and know the right way to act. The purpose of awareness and training of employees is not to make people paranoid but to pay attention to the requests they receive and are aware of the value of information they are responsible for. The best armed are the employees, the best secure will be the company.

The aim of this essay is that, having identified the issue in the information security system of the company, the hereby suggested adequate measures be taken so that the professionals of Social Engineering find it more difficult to gain access and disclose confidential information of the company.

References

Ardi C., Heidemann J.(2016). AuntieTuna-Personalized Content-based Phishing Detection, NDSS Usable Security Workshop 2016, disponível em: <https://www.isi.edu/~calvin/papers/Ardi16a.pdf> acedido aos: 12/02/17

Barman, S.(2001). “Writting Information Security Policies”.1st Ed. Indianapolis, New Riders.

Blank, R. & Gallagher, P. (2013). Security and Privacy Controls for Federal Information Systems and Organizations. nvlpubs.nist.gov. U.S. Department of Commerce. National Institute of Standards and Technology. Disponível em: < nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf> acedido aos: 24/03/17

Beal, A. (2005). Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo. Atlas.

Callas J., Donnerhacke.(2007). OpenPGP Message Format, RFC 4880, IETF, disponível em: < https://tools.ietf.org/html/rfc4880 > acedido aos: 05/05/17

Gavrilova, M. (2014). Biometric-Based Authentication for Cyberworld Security: Challenges and Opportunities. Computer Science, University of Calgary. Disponível em: < http://docplayer.net/1130729-Biometric-based-authentication-for-cyberworld-security-challenges-and-opportunities-by-m-l-gavrilova.html> acedido aos 30/08/17

Griffin, P. (2016). Biometric-Based Cybersecurity Techniques- In book: Advances in Human Factors in Cybersecurity. Disponível em: < https://www.researchgate.net/publication/305082243_Biometric-Based_Cybersecurity_Techniques> acedido aos 30/08/17

Hadnagy, C. (2010).Social Engineering: The Art of Human Hacking. Indianapolis. Whiley.

Harvey, S. & Evans, D. (2016). Defending Against Cyber Espionage: The US Office of Personnel Management Hack as a Case Study in Information Assurance. Proceedings of the National Conference On Undergraduate Research (NCUR) . University of North Carolina Asheville. Disponível em< http://ncurproceedings.org/ojs/index.php/NCUR2016/article/view/1764/982>acedido aos 09/09/17

Hill, M. & Hill, A. (1998). A construção de um questionário. Disponível em: < https://repositorio.iscte-iul.pt/bitstream/10071/469/4/DINAMIA_WP_1998-11.pdf> acedido aos 21/07/17

Huber, M. et al.(2009). "Towards Automating Social Engineering Using Social Networking Sites".in International Conference on Computational Science and Engineerin. vol. 3, pp. 117–124.Jones C. (2004). Social Engineering: Understanding and Auditing. GSEC. SANS Institute.

Kucherawy M.(2015). Domain-based Message Authentication, Reporting, and Conformance (DMARC), RFC 7489, IETF, disponível em: <https://tools.ietf.org/html/rfc7489. > acedido aos: 05/01/17

Mitnick K., Simon W. (2002). The art of deception: Controlling the human element of security. New York. John Wiley & Sons.

Mouton, et al, (2010). "Social engineering attack detection model. SEADM" in Information Security for South Africa, pp. 1–8.

Nicholson, D. (2016). Advances in Human Factors in Cybersecurity. Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity. Walt Disney World®. Florida. USA. Disponível em: < http://www.springer.com/gp/book/9783319419312> acedido aos 30/08/17

Peltier T.(2006). Social Engineering:Concepts and Solutions. Information Systems Security, disponível em: <https://www.researchgate.net/publication/220450160_Social_Engineering_Concepts_and_Solutions> acedido aos: 08//02/17

Puricelli, R. (2015). The Underestimated Social Engineering Threat in IT Security Governance and Management. ISACA Journal. CISM. Disponível em: < https://www.isaca.org/Journal/archives/2015/Volume-3/Pages/the-underestimated-social-engineering-threat-portuguese.aspx> acedido aos 03/04/17

Ramsdell B.(2010). Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, RFC 5751, IETF, January 2010, disponível em: < https://tools.ietf. org/html/rfc5751> acedido aos: 03//12/16

Steve L.(2016). Domain-Based Message Authentication Reporting and Conformance, InfoSec Institute, disponível em: <http://resources.infosecinstitute.com/domain-basedmessage-authentication-reporting-and-conformance/.> acedido aos: 23//03/76

Symantec.(2016). Relatório de Ameaças à Segurança na Internet; disponível em: <https://www.symantec.com/pt/br/security-center/threat-report, acedido aos: 22//04/17

Verizon.(2016). Data Breach Investigations Report finds cybercriminals are exploiting human nature; disponível em:< http://www.verizon.com/about/news/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human-0> acedido aos: 10//11/16

Stroz, E. et al (2016). Psychology Is the Key to Detecting Internal Cyberthreats. Disponível em: <https://hbr.org/2016/09/psychology-is-the-key-to-detecting-internal-cyberthreats> acedido aos 30/08/17

Schwartz, J. (2016). Machine Learning Is No Longer Just for Experts. Analytics. Disponível em: < https://hbr.org/2016/10/machine-learning-is-no-longer-just-for-experts?referral=03759&cm_vc=rr_item_page.bottom> acedido aos 30/08/17

Winnefeld, J. et al (2015). Cybersecurity's Human Factor: Lessons from the Pentagon. SECURITY & PRIVACY. Disponível em: < https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon> acedido aos 21/07/17.