Does the government do enough to punish cyber-attacks and criminals?

Government

1. 0 Introduction

Cyber-attacks have become a significant problem for information systems (IS) worldwide. When referring to information systems, the term cyber-attack is used for denoting a malicious action that aims to result to specific benefit, usually financial, and which is developed through online routes as available in the Internet (Vacca, 2009). In the UK, the expansion of cyber-crime has been quite rapid the last few years leading to severe financial losses for the victims, individuals and businesses (Cabinet Office, 2011). The graph in Figure 1 shows the cost of the various types of cyber – crime to the UK economy. This paper explores the effectiveness of measures taken by the UK government in regard to the punishment of cyber-crime, aiming to show whether the current initiatives for the UK government for punishing the cyber-crime are sufficient or not. The paper also explains the key characteristics and the value of information systems (IS) security so that the potential of the UK government to secure safety from cyber-crimes is evaluated. I will argue that the UK government does not enough to punish cyber-attacks and criminals. Moreover, the introduction by the government of stricter punishment for cyber-attacks has not resulted to the limitation of this type of crime, as explained below.

Figure 1 – Cost of different types of cyber – crime to the UK economy (Cabinet Office, 2011, p. 2)

2. 0 Security of IS – characteristics and importance

Security, as a term, can be related to different fields. In the context of informationtechnology, the term security is used for describing ‘ a power system’s degree of risk in its ability to survive imminent disturbances without interruption of customer service’ (Cuzzocrea et al., 2013, p. 244). As for the term ‘ IT security’, this term refers to three values/ characteristics of an IT system, such as: ‘ confidentiality, integrity and availability’ (Katsikas, 2016, p. 28). According to Mehdi (2014), the term IS security denotes ‘ the protection of IS against unauthorized access’ (p. 4310). It is explained that a secure IS can ensure that its data will not be modified or lost (Mehdi, 2014). Also, such system is able to detect early any security threat activating appropriate protection mechanisms (Merkow, 2010). At organizational level, IS security is ensured by using an IS security policy, i. e. a set of rules referring to the security standards that would apply in all IS of the organisation involved (Kim and Solomon, 2016). However, the demands of such policy can be many, a fact which is justified if considering the several types of IS threats (Cabinet Office, 2011; Figure 1). Organisations often need to hire an Information System Security Officer (ISSO) for ensuring IS security (Kovachich, 2016).

3. 0 The punishment of cyber-attacks and criminals – government initiatives and effects

3. 1 Laws and policies focusing on IS security

In the UK, the first law addressing cyber – crimes appeared in 1990 and aimed to cover the gaps of existing legislation in regard to the protection of IT systems from cyber-attacks (Emm, 2009). This was the 1990 Computer Misuse Act. The introduction in the UK of a legislative text focusing on cyber-attacks has been highly related to a cyber-attack incident: the unauthorized access, by two cyber-attackers, to BT’s Prestel service in1984(Emm, 2009). When dealing with the above case, the court used the 1981 Forgery and Counterfeiting Act, due to the lack of a legislative text focusing on computer-related crimes (Emm, 2009). In May of 2015, the Serious Crime Act 2015 came into action (Eversheds-Sutherland, 2015). The articles 41 up to 44 of the above law introduced stricter punishment for cyber-crimes. More specifically, in the context of the 1990 Computer Misuse Act the imprisonment for serious cyber-crimes could not exceed the 10 years. With the 2015 Act, the imprisonment for cyber-crimes has been significantly increased, reaching the 14 years and even, the life sentence in cases of cyber-crimes threatening national security (Eversheds-Sutherland, 2015). This, stricter, punishment for cyber-crimes could discourage cyber-criminals but only if the enforcement of the law was appropriately supported, so that all cases of cyber-crimes are brought before the courts (White, 2016).

The National Cyber Security Strategy (CSS) of 2011 has been an effort of the British government to control cyber-crime (Shefford, 2015). The Computer Emergency Response Team (CERT) is a national team that was established in 2014 for helping towards the achievement of the objectives of CSS (Cabinet Office, 2014, p. 13). The CERT team provides to organisations in the private and the public sector critical information for the protection from cyber-attacks (Cabinet Office, 2014). Additionally, in the context of CSS, educational initiatives focusing on cyber security are developed by institutions across the UK; these initiatives are funded by the government and aim to achieve two targets: First, to increase the awareness of the public in regard to cyber security. Second, to help individuals to acquire skills which are necessary for supporting cyber security and for facing cyber-attacks (Cabinet Office, 2014; Figure 2). The Cyber Security Challenge (CSC) is a programme developed by the UK government for helping young people to understand the risks from using their cyber skills in the wrong way; the programme includes competitions and other schemes that can motivate young people to use their cyber skills in a proactive way and not for the commitment of cyber – crimes (National Crime Agency, 2017).

Figure 1 – Initiatives/ measures of the National CSS for facing cyber-crime (Cabinet Office, 2014, p. 22)

3. 2Cyber-attack incidents in governmental and non-governmental organisations

The number of cyber-attacks against governmental and non-governmental organisations in the UK is continuously increased (White, 2016). From January to October of 2016, 75 cyber-attacks have been reported against banks in the UK, while in 2014 these attacks were just five (White, 2016). In 2013, three individuals in Britain were convicted to jail, from 6 months up to 22 months, for unauthorised access of sensitive private data stored in ' PayPal, Visa and Mastercard' (McTague, 2014). The above punishment was considered as too soft compared to the seriousness of the crime. In 2014, the government decided to initiate the modification of existing punishment for cyber-crimes, so that future perpetrators are discouraged from committing a cyber-crime (McTague, 2014). Pultarova (2016) argued that banks in the UK face cyber-attacks quite regularly but they avoid reporting the specific incidents trying to protect their market image. In November of 2016, Chancellor P. Hammond noted that critical infrastructure units of the

UK, such as airports and gas facilities, are threatened by ‘ cyber-attacking techniques developed by other countries’ (BBC News, 2016). It was noted that the protection from such attacks would be a priority for the UK in order for the country’s security, at national level, to be ensured (BBC News, 2016). In 2011 the general police officer in the e-crime department of Scotland-Yard argued that the punishment of cyber – crimes in the UK is too soft if considering the actual damage that these crimes cause (BBC News, 2011). It was explained that the annual damage on the UK economy from cyber-crimes reaches the ? 27bn (BBC News, 2011). In 2016, the National Crime Agency of the UK published a report for showing the status of cyber-crimes, in terms of occurrence/ rate of appearance. According to the above report, the cyber – crime represents a major part of criminal activity in the UK, reaching the 36% among all crimes developed in the UK. At the same time, the crimes related to computer misuse reached the 17% among the country’s total crimes (National Crime Agency, 2016). The above figures and facts indicate the inability of the UK government to control cyber-crime. The introduction in 2015 of stricter punishment for cyber-crimes has been an important initiative by the UK government for controlling cyber-crime. However, this initiative should be combined with other measures, at national and at community level.

In a speech in mid-February of 2017, Chancellor P. Hammond noted that in the previous three months a total of 188 severe cyber-attacks had been reported; these attacks aimed to cause severe damage to governmental services, infrastructure and businesses (Cole, 2017). A similar issue has been raised by Lord West of Spithead who noted in 2010 that in 2009 the UK had to face ‘ 300 significant attacks’ on the IS of the government (Doward, 2010). According to Lord West, this problem had become quite serious, denoting that the UK had been targeted by cyber criminals worldwide, as these attacks seemed to be supported by foreign governments, as Lord West noted (Doward, 2010). The above arguments verify the existence of gaps in the existing national framework for the protection from cyber-attacks, as this framework constitutes the national legislation and national policy for the control of cyber – crime. The facts presented above further verify the inability of the UK’s policy to reduce the occurrence of cyber-crime.

Guitton (2012) developed an experiment, using data related to cyber-attacks that occurred between 2003 and 2010 in businesses located in three European countries: Germany, UK and France. It was revealed that the relationship between attribution and deterrence is strong only in cases of individuals of individuals who are aware of the existing legislation for cyber-crime and who can realise the actual effects of their actions. These individuals represented the 1/3 of the cases reviewed by Guitton (2012). In opposition, it was found that most individuals involved in cyber-crimes are not fully aware of the relevant legislation and they tend to ignore the effects of their actions. For these individuals, the control theory which emphasises on the power of attribution, as held by the state, to ensure deterrence is not applied, as Guitton (2012) argued. In the context of the above study, the potential of the British government to control cyber-crime is limited. This fact, even it would be accepted, could not affect the view on the government’s efforts to confront cyber-crime. The update of the terms of punishment of cyber-crimes just in 2015 and the lack of effective control mechanisms for identifying and reporting cyber – attacks verify thefailureof the government to ensure the punishment of cyber-attacks and criminals.

4. 0 Conclusion and Recommendations

It is concluded that the UK government does not make enough to punish cyber-attacks and criminals. First, a significant delay has been identified in the introduction of appropriate/ fair penalties. Indeed, the introduction of strict punishment for cyber-crimes took place just in 2015, as explained above. The facts and views presented in this paper lead to the assumption that for many years, the government has avoided confronting cyber-attacks as a criminal activity, a fact that led to the radical increase of cyber-attacks against IS systems in governmental services and in financial institutions. At the same time, IS security has several aspects, meaning that eliminating cyber – crime is rather impossible. The soft punishment framework for cyber-crimes, as used in the past, has led to the severe deterioration of the problem across the UK. The increase of effectiveness of current legislation, as from May 2015, on cyber-attacks could be achieved through certain practices, such as: First, events and seminars would be organized at community level for informing individuals on the characteristics of cyber-attacks and the available measures for protection; these seminars would also provide guidelines to entrepreneurs in regard to the value of IS security policy, as part of business strategy. Second, incentives would be provided to entrepreneurs for pursuing the certification of their business according to the information security management standards, such as the ISO/IEC 27000 standards. Third, an independent authority would be established for controlling the performance of governmental and non-governmental organisations in regard to IS safety. Finally, the investment on IS security in governmental and non-governmental organisations would be increased. Security frameworks, such as the ‘ Intrusion Detection System’ (IDS), could be employed in these organisations for ensuring IS security in IS systems that manage and store high volume of private data (Stair and Reynolds, 2015, p. 460).

5. 0 Personal reflections

This project has been related to a critical issue: the findings in regard to the study’s subject have been contradictory. More specifically, the UK government has tried to confront cyber-attacks through legislation and relevant policies but the punishment for these crimes has been characterised as soft, at least up to 2015, while the number of cyber-attacks in the UK is continuously increased. Under these terms, I had to face a dilemma: how should the performance of the UK government in facing cyber-crime would be evaluatedBy referring to the initiatives taken or by emphasising on the actual results of these initiativesReflection has helped me to face the above problem. Indeed, reflection can help the researcher to have ‘ an objective sense of things’ (Gillett et al., 2013, 85). Moreover, using reflection I tried to estimate the balance between the positive and negative aspects of government’s efforts to punish cyber-crime and to understand which aspect of the government’s strategy against cyber-crime is more related to the research question: this paper aims to explain whether the government has done enough on the punishment of cyber-crime. Through reflection, I understood that the occurrence of cyber-attacks in the UK should be preferred as the criterion for answering the research question. Ventola and Mauranen (1996) explained that reflection can help the researcher to identify the research findings that are closer to the research question, a fact that allows the researcher to use the right material for answering the research question. Additionally, I used reflection during the development of the study for managing time and for tracking research gaps, which have been covered after the completion of the project. The above tasks have been supported by a research diary (Day, 2013), in the form of notes, where daily progress in regard to research and writing was reported. Thus, the use of reflection while developing this project helped me to control risks, in regard to the project’s structure and content, and to manage time more effectively, covering all aspects of the research question.

6. 0 References

BBC News (2016) UK must retaliate against cyber-attacks says chancellor. Available from: http://www. bbc. com/news/technology-37821867 [Accessed 15 March 2017].

BBC News (2011) Cyber criminals ‘ should get tough sentences’ say police. Available from: http://www. bbc. com/news/uk-15680466 [Accessed 15 March 2017].

Cabinet Office (2011) The cost of cabinet crime. Available from: https://www. gov.

uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report. pdf [Accessed 15 March 2017].

Cabinet Office (2014) The UK Cyber Security Strategy. Report on Progress and Forward Plans. Available from: https://www. gov. uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___. pdf [Accessed 15 March 2017].

Cole, H. (2017) UK Government and businesses are hit by two ‘ serious’ cyber-attacks a day. The Sun. Available from: https://www. thesun. co. uk/news/2857508/uk-government-and-businesses-are-hit-by-two-serious-cyber-attacks-a-day/ [Accessed 15 March 2017].

Cuzzocrea, A., Kittl, C., Simos, D., Weippl, E. and Xu, L. (2013) Availability, Reliability, and Security in Information Systems and HCI: IFIP WG 8. 4, 8. 9, TC 5 International Cross-Domain Conference, CD-ARES 2013, Regensburg, Germany, September 2-6, 2013, Proceedings. New York: Springer.

Day, T. (2013) Success inAcademicWriting. Oxford: Palgrave Macmillan

Doward, J. (2010) Britain fends off flood of foreign cyber-attacks. The Guardian. Available from: https://www. theguardian. com/technology/2010/mar/07/britain-fends-off-cyber-attacks [Accessed 15 March 2017].

Emm, D. (2009) Cybercrime and the law: a review of UK computer crime legislation. SecureList. Available from: https://securelist.

com/analysis/publications/36253/cybercrime-and-the-law-a-review-of-uk-computer-crime-legislation/ [Accessed 15 March 2017].

Eversheds-Sutherland (2015) Will the Serious Crime Act 2015 toughen the UK’s cybercrime regimeAvailable from: http://www. eversheds-sutherland. com/global/en/what/articles/index. page? ArticleID= en/tmt/Serious_Crime_Act_2015_May2015 [Accessed 15 March 2017].

Gillett, A., Hammond, A. and Martala, M. (2013) Inside Track to Successful Academic Writing. Essex: PearsonEducation.

Guitton, C. (2012) Criminals and Cyber Attacks: The Missing Link between Attribution and Deterrence. International Journal of Cyber Criminology, 6(2), pp. 1030-1043.

Katsikas, S. (2016) Information Systems Security: Facing the information society of the 21st century. New York: Springer.

Kim, D. and Solomon, M. (2016) Fundamentals of Information Systems Security. Sudbury: Jones & Bartlett Publishers.

Kovachich, G. (2016) The Information Systems Security Officer’s Guide: Establishing and Managing a Cyber Security Program. Oxford: Butterworth-Heinemann.

McTague, T. (2014) Computer hackers face life in prison under new Government crackdown on cyberterrorism. Mail Online. Available from: http://www. dailymail. co. uk/news/article-2649452/Computer-hackers-face-life-prison-new-Government-crackdown-cyber-terrorism. html [Accessed 15 March 2017].

Mehdi, K. (2014) Encyclopedia of InformationScience and Technology. Hershey: IGI Global.

Merkow, M. (2010) Security Policies and Implementation Issues. Sudbury: Jones & Bartlett Publishers.

National Crime Agency (2017) Cyber – crime: preventing young people from being involved. Available from: http://www. nationalcrimeagency. gov. uk/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved [Accessed 15 March 2017].

National Crime Agency (2016) Cyber – Crime Assessment 2016. Available from: http://www. nationalcrimeagency. gov. uk/publications/709-cyber-crime-assessment-2016/file [Accessed 15 March 2017].

Pultarova, T. (2016) UK banks under constant cyber-attack but don’t report incidents. Engineering & Technology. Available from: https://eandt. theiet. org/content/articles/2016/10/uk-banks-under-constant-cyber-attack-but-dont-report-incidents/ [Accessed 15 March 2017].

Shefford, M. (2015) What is the UK government doing about cybersecurityDatonomy. Available from: http://datonomy. eu/2015/04/01/what-is-the-uk-government-doing-about-cybersecurity/ [Accessed 15 March 2017].

Stair, R. and Reynolds, G. (2015) Fundamentals of Information Systems. 8th ed. Belmont: Cengage Learning.

Vacca, J. (2009) Computer and Information Security Handbook. Burlington: Morgan Kaufmann.

Ventola, E. and Mauranen, A. (1996) Academic Writing: Intercultural and textual issues. John Benjamins Publishing.

White, L. (2016) British banks keep cyber-attacks under wraps to protect image. Reuters. Available from: http://uk. reuters. com/article/us-britain-banks-cyber-idUKKBN12E0NQ [Accessed 15 March 2017].