Preliminary Master Thesis Report
at
BI Norwegian Business School

White-collar crime and cybersecurity: the potential of gamification approach in anticipating white-collar crime challenge

Thesis supervisor:

Petter Gottschalk

Hand-in date:

15.01.2018

Campus:

BI Oslo

Examination code and name:

GRA 19502 Preliminary Master Thesis Report

Programme:

Master of Science in Leadership and Organizational Psychology

Table of Content

Summary

The first objective of the thesis is to provide a comprehensive taxonomy of both white-collar offenses and offenders, based on integrated findings of previous research on this field, combining several perspectives and allowing for further implementation in a practical setting, which comprises the second objective of the thesis - gamification of employee training against white collar crime.

Gamification, commonly defined as "the use of game design elements in non-game contexts", has great potential in creating engaging and productive learning environments, in both education and business contexts. Therefore, the in second part of the thesis will be provide theoretical arguments in favor of gamification. We adopt an attacker centricity approach in the training, based on the taxonomy of white-collar offenders created in the first part of the thesis.

In order to achieve the stated objectives, we will employ a qualitative research approach to assess whether gamification can be used in security awareness and training programs in order to improve learning outcomes. Qualitative data will be collected through interviewing several experts in fields of cybercrime, white-collar crime and gamification.

Finally, in order to gain an understanding of the possibilities and limitations of the proposed concept, we will create a prototype of a gamified application.

1.0.Introduction to the topic of white-collar crime

White-collar crime is a broad concept, emerged in 1940 after Sutherland's introduction of white-collar criminals as opposite to "traditional" perpetrators from lower classes and street criminals. The main idea was that even wealthy and respectful persons from privileged society are able to commit profit-driven crime. White-collar crime covers all illegal behavior that takes advantage of positions of professional authority due to person's access to opportunities for personal or corporate gain. In general, white-collar crime is financial crime committed by trusted and potentially reliable persons in important business positions (Gottschalk, 2013). According to Gottschalk (2016)'s research, a white-collar criminal is typically a member of the privileged socioeconomic class in society, who commits non-violent financial crime in a professional setting. The criminal has power and influence, enjoys trust from others in privileged networks, does not consider own actions as crime and has no guilt feeling (Gottschalk, 2016).

The organizational context of this type of crimes is particularly important in distinguishing white-collar crime from other incidents. As Gottschalk (2017) highlights, such illegal actions as abusing social security benefits, committing tax evasion or committing Internet fraud on a personal level are not considered white-collar crime, because the latter are assumed to be committed only in a professional capability and in an organizational context.

Although motivation for committing such a crime seems to be simple financial gain, the reasons behind the desire for financial gain are one of the most discussed topics in this field. Gottschalk (2017) considers two general but opposite points of view. On the one hand, since white-collar crime has been mostly studied in USA, researchers apply there the concept of the American dream, which implies the everyone's possibility of becoming monetary successful and has a deep root in American mentality. A high white-collar crime rate can be explained by the person's commitment to the material success as experienced in the American dream (Gottschalk, 2017). When such overemphasis on value of success is present, the end justifies the means, i.e., committing non-violent crime does not provoke a feeling of being criminal. On the other hand, the fear of falling theory suggests that people in high-level positions are afraid of consequences from failure and therefore try to survive in their positions (Piquero, 2012). As Gottschalk (2017) explains this idea, white-collar managers and top executives are afraid of losing their wealth and status, working hard to remain successful and solve their problems by any means. Thus, financial gain becomes not only a matter of making even more money: “It is an issue of survival, and it may be about rescuing a sinking ship” (Gottschalk, 2017, p. 2).

In conformity with the managerial perspective, that highlights the role of managers as agents for deciding and leading enterprise strategies and operations, implementing corporate priorities, managers’ perceptions and interpretations determine their commitment to certain goals over other ones and may lead to implementation of legal and illegal strategies (Gottschalk, 2016).

The theory of profit-driven crime suggests that financial crimes are opportunity driven and should be understood mainly in economic rather than criminological terms. Naylor (2003) proposed a typology that shifts the focus from actors to actions by distinguishing between market crime, predatory crime and commercial crime. Agency theory has broadened the risk-sharing perspective and describes the relationship between the two parties (typically senior and middle management) as being engaged in an agency relationship, defined as a contract, where the decision-making authority is delegated to the agent (Michel, 2008; Gottschalk, 2016). However, corporate crime is not limited to such relationship. Whilst senior management may be responsible for the tone and culture they set within the corporation, middle management feel pressured into criminal practices without the explicit direction of their seniors (Punch, 2000).

Therefore, according to Gottschalk (2017), white-collar crime may be a response to possibilities and strengths as well as to threats and weaknesses. This leads us to consider the existing classification of white-collar crime.

1.1.The first objective and research question

First of all, one should acknowledge the ambidextrous nature of white-collar crime, since it can be defined in terms of the offense, the offender or both. In terms of the offense white-collar crime means a crime against property for personal or organizational gain. It is a property crime committed by non-physical means and by concealment or deception (Benson and Simpson, 2009, cited in Gottschalk, 2017). In terms of the offender, white-collar crime entails crimes committed by higher class members of society for personal or organizational gain, which posses a set of specific, related to their social status characteristics. They are individuals who are wealthy, highly educated, and socially connected, and they are typically employed by and in legitimate organizations (Hansen, 2009, cited in Gottschalk, 2017).

The first objective of this thesis is to *provide a simplified yet comprehensive taxonomy of both white-collar offenses (crimes) and offenders (criminals), based on integrated findings of previous research on this field*. This encompasses the first research question of that paper:

What are the main characteristics of white-collar crime as a multidimensional phenomenon?

Although there are several approaches to white-collar crime as a phenomenon (see, e.g., Sutherland (1940, 1949); Geis & Jesilow (1982); Shapiro (1990); Nelken (1994); Brightman (2011); Gottschalk (2013, 2016); etc.), in boundaries of this work we are not able to perform a wholly comprehensive meta-analysis of almost 80 years of existing research on white-collar crime. Instead, we aim to focus on the vital attributes any white-collar crime classification possesses and thereby offer an optimal taxonomy, combining several perspectives and allowing for further implementation in practical settings (which will be discussed when describing second objective of this thesis). Therefore, we will assume brief but clear model for assessing white-collar crime concept along three dimensions: offenses, offenders, victims (targets).

1.2. Dimensions for assessing white-collar crime concept

Since financial gain as a motive for white-collar crime may either benefit the person or the organization (Gottschalk, 2017), the first assessed dimension (offense) can be presented as distinction between occupational or corporate crime. Occupational crime occurs when an individual’s occupation enables him/her to commit white-collar crime in order to get personal benefits. The motives for illegal financial gain can vary: it can be increased personal wealth and providing relatives and friends, avoidance of personal bankruptcy/falling from a high status position in society, or even compensating for lack of popularity by buying friends (Gottschalk, 2017).

Corporate crime occurs when financial gain benefits not the individual but the organization (often through founders’ illegal actions). For instance, it could be motivated by a company’s need in achieving a new contract and establishing a subsidiary in a corrupt country, or by avoidance of bankruptcy of the business (e.g., through tax evasion and bank fraud) (Gottschalk, 2017).

Williams (2006) suggests a third type of crime as criminal activity disguised as legitimate business and groups some of the common white-collar criminal activities into one of these three categories. However, since the crime as an organized business is beyond the scope of our work, we will consider only two crime types in our taxonomy.

Thus, both occupational and corporate crimes can take any of these four broadly acknowledged forms of white-collar crime: fraud, theft, manipulation, corruption. *Fraud*, according to Henning (2009)'s definition, is an intentional perversion of truth for the purpose of inducing another in reliance upon it to part with some valuable thing belonging to him or to deprive a victim of a legal right, where a perpetrator tries to keep the property from the victim. On average, as Gottschalk (2013)'s analysis shows, most convicted criminals are involved in fraud crime cases, typically bank fraud. *Theft* can be defined as the illegal taking of another person's, group's or organization's property without victim's consent (Hill, 2008, cited in Gottschalk, 2013). Identity theft is one of the most common forms of this crime. *Manipulation*, in accordance with Malkawi and Haloush (2008) entails gaining illegal control or influence over others' activities, means and results. Tax evasion as a manipulation crime most prevalent in many countries is the result of the failure to comply with national income tax laws (Gottschalk, 2013). Finally, *corruption* is the giving or receiving of an improper advantage, linked to a person's position, office or assignment (Kayrak, 2008). "Corruption is to destroy or pervert the integrity or fidelity of a person in his discharge of duty, to induce to act dishonestly or unfaithfully, to make venal, and to bribe" (Gottschalk, 2013, p. 21).

Offender's perspective is the second dimension to consider in our overview. Although research identifies several common characteristics of white-collar criminals as their personal psychological and social attributes (e.g., wealthy, highly educated, employed in organization and committing crime in a professional settings, fearing to lose their status or striving for monetary success (Gottschalk, 2016); showing greater score in psychopathic traits (Ragatz et al., 2012); narcissistic (McKay et al., 2010; Ouimet, 2009; 2010); irresponsible, low in social conscientiousness and therefore behaving in antisocial way (Collins & Schmidt, 1993)), we suggest further offender differentiation based on their official role in relation to the organization.

There are several categorizations varying within the same field due to context used. Still, we integrate the findings from these two papers: White-collar Criminals in Modern Management (Gottschalk, 2013) and Principals, Agents and Entrepreneurs in White-Collar Crime: An Empirical Typology of White-Collar Criminals in a National Sample (Ketil Arnulf & Gottschalk, 2012). The first research, based on a sample of 305 convicted white-collar criminals in Norway, offers four groups of offenders: criminal entrepreneurs, corporate criminals, criminal followers, and female criminals. The second paper on the basis of agency theory and a sample of 222 convicted Norwegian offenders provides a framework of six roles of white-collar criminals: principal, agent, entrepreneur, servant, public official and robber criminal. With respect to all discussed types, we distinguish offenders not by their gender (males and females criminals) neither by the main motive behind illegal financial gain (corporate and occupational criminals), but by the frequency they hold the concrete position. Thus, the most frequent roles of white-collar crimes are principal, agent and entrepreneur criminals, while less frequent are servants, followers, public officials, and robber criminals.

According to agency theory, owners of a company (principals) hire managers (agents) to perform on their behalf and for maximizing the company’s value (Engelmann-Zach, 2014). In this light, high incentives are the way to align the interests of agents with the interests of principals, while relating compensation to the achievement of performance goals can have motivational effects on employees, improving firm performance (Engelmann-Zach, 2014). However, Ketil Arnulf and Gottschalk (2012) state that since principals always suspect agents of making decisions that benefit themselves, CEOs may always be suspected of cheating the owners and appropriate measures of checks are needed. Thus, one of the prevalent offender’s type is agent criminal, represented by CEOs or similar top executive positions. Nevertheless, principals (in terms of chairmen and members of board) may also commit white-collar crime. However, as Arnulf and Gottschalk (2012) recognize, when there is a mix of roles, the principal-agent distinction is not always applicable in practice. They label those offenders who are themselves sole owners and CEOs of a company that partly or entirely engage in unlawful activities to make revenues, often using creative methods in novel ways instead of more established ways of organizing similar work, as entrepreneur criminals, highlighting the “entrepreneurship” as the nature of such crimes (Ketil Arnulf & Gottschalk, 2012). Although the CEOs are twice as likely to engage in crimes as their principals, the most typical role of a white-collar criminal is the entrepreneur one. It is also worthy to note that in the sample of Ketil Arnulf and Gottschalk (2012)’s research, a large share of the entrepreneurial criminals have established or used their companies to cover up crimes of others, making their role of leader of crime questionable. Besides, when comparing to others, this type of offenders makes the biggest profits. When board members and top managers are making themselves criminal for profits that are only fractions of their wealth, entrepreneurs engage in crime striving for exceeding their recorded assets much more (Ketil Arnulf & Gottschalk, 2012).

The less frequent types of offenders in terms of their occupied position are servants (accomplices to entrepreneurs or CEOs due to their specific knowledge or access); followers (non-assertive persons, convinced by cause of the crime or charisma of their leaders or just following the orders expecting returns for their obedience); public officials (third party regulators as police or municipalities with their own interests); robber criminals (private persons acting without any business relation to the victim for individual purpose).

Paying attention to specific characteristics of offenders in relation to their position (abilities, access to confidential data and leadership level) may enrich the existing research, focusing on both personality and formal role of white-collar criminals.

The third dimension of white-collar taxonomy worth to mention is the victim perspective. The criminals differ in terms of the targets for their illegal activities. Again, an integrated view will be presented below.

In general, white-collar criminals cause financial damage to four categories of victims: business owners (in terms of investors, shareholders or any employers involved), customers, society and government (in terms of tax authorities and nation prosperity), and innocents (bystander persons). According to Gottschalk (2013)’s research, based on the national sample, employers represent the largest group of victims, while banks are the second largest group of victims with the most severe jail sentence for white-collar criminals in this category. As research states, all white-collar criminals are about equally likely to engage in crime against government (in form of tax frauds); every third white-collar criminal (in particular CEOs and board members) is convicted of cheating investors; entrepreneur criminals are also cheating investors but more inclined to cheat customers through maximizing their returns by reducing the value created for their customers (Ketil Arnulf & Gottschalk, 2012).

The crime strategy is likely to vary depending on the victim specificity, therefore, if we aim to anticipate and prevent white-collar crime, the understanding of interrelatedness of all these dimensions taken together - offense, offender and victim - can influence the effectiveness of preventing program.

2.0.Introduction to the topic of cybercrime

Fraud, theft, manipulation and corruption are well-known, common traditional white-collar crimes in the field of deviant behavior. However, due to rapid growth and increased availability of new technologies, which enable electronic commerce, negotiation and banking through computer-related media and Internet, traditional form of crime is actively replacing by its cyber form. In general, cybercrime (or computer crime) may be divided in two big categories: crime where a computer serves as a means or as an end.

Similarly, Kirwan & Power (2013) divide cybercrimes into internet-enabled and internet-specific. Internet-enabled crimes can also exist offline, but the presence of internet-enabled devices allows for easier and faster execution of such offences. Internet- specific crimes are those cybercrimes that do not exist without a computer-enabled environment.

In case of white-collar crime, the first category is prevalent. Thus, for instance, traditional fraud and theft committed by white-collar criminals become online fraud and online identity theft (in most cases), while manipulation and corruption incidents are also facilitated by computer technologies. Although there is no specific statistical data available on the amount of white-collar crime committed through computer-related media, the general tendency allows for speculations about the constant growth of this form of crime as a function of a total amount of cybercrime.

Overall, computer-enabled crime causes unique problems due to the truly global nature of the Internet. The speed at which new technologies are developed requires a choreographed nimbleness that legislative deliberation may not be able to deliver on a global scale: national laws may utilize different standards for conviction and impose different punishment; computer crime in more industrialized nation will have greater ramification than in a less industrialized nation; laws amendments done by developing countries may still lack the clarity that the industrialized nations desire. Moreover, in confronting the rising phenomenon of computer crime, strategies that focus solely on increasing the effectiveness of prosecution will inevitably fail (Lewis, 2004).

From organizational perspective, investments in IT and digitalization are expected to boost profits. Indeed, a number of studies on a company-by-company basis, have found that companies that use more IT are more efficient and productive than their competitors (Tarafdar et al., 2015).

On the other hand, according to the recent research drawn on 14 studies that were published from 2007 to 2014 and involved 3,100 organizational employees and IT users of 28 organizations in the United States, from sectors such as health care, industrial sales, manufacturing, higher education and government services - rapidly emerging “dark side” of IT hurts employees and their organizations and robs companies of some of the productivity gains they expect from their IT investments (Tarafdar et al., 2015). According to this study, one of the key negative effects of IT use in the workplace includes employee misuse of IT. While firewalls and other network defenses can potentially stop attacks from the outside, without a robust “human firewall” in place, a technical one becomes virtually useless (Sloman, 2016). Since, no security technology can stop an employee with an authorized access to a computer system. Reportedly, attacks stemming from internal sources are greater in scope and can result in about 10 times as many compromised records as those from external sources (Tarafdar et al., 2015).

From the global perspective, according to Ginni Rometty, IBM’s chairman, cybercrime is the greatest threat to every company in the world (Forbes, 2015), while Warren Buffet says that cyber-attacks are even worse than nuclear weapons and become the number one problem with mankind (Business Insider, 2017). As CSO’s report states, the cybersecurity community and major media predict that cybercrime damages will cost up to $6 trillion annually by 2021, representing the greatest transfer of economic wealth and exceeding the global trade of all illegal drugs combined (CSO, 2017).

Cyber security is not an IT problem or just the matter of IT specialists; it concerns all humans in the organization connected through computer-mediated technologies. In practice, surprisingly many employees, business partners and third-party suppliers are unaware of cyber security issues, and are not consistently following recommended practices. By connecting personal devices to company networks, using weak passwords and allowing poor coding practices, organizations become predisposed to e.g. phishing attacks, which may result in loss of profit and other negative consequences such as costly investigations, lawsuits, loss of reputation or loss of license to operate (Sloman, 2016).

Thus, there is an evidence that organizations strive to reduce the risk and the cost of cybercrimes through implementation of cyber security policies and programs. As Hendrix et al. (2016) state, one of the main ways to achieve this is to educate employees and make sure they are aware of the latest prevention measures and have access to the latest tools. Human errors, lack of awareness and technology misuse may lead to unpredicted results. According to Lewis (2004), Tarafdar et al. (2015), Sloman (2016) and Bounfour (2016), it is important not only to have traditionally taken primarily technical approach, consisting of largely routine, mostly one-time and one-size-fits-all technical training activities where employees go through material on how and when they can use features of particular systems, but to recognize that awareness does not equal lasting behavior change. It is important to include non-technical actions, such the concept of "digital mindfulness" for educating employees about responsible IT use, making them aware about potential dark side effects, and providing resources and support for dealing with cyber security related issues.

Cyber security as an area for response to cyber threats includes different aspects from digital software, technical firewalls to human psychology, typically divided in two sub-categories: security of IT infrastructure and security on the user side. The latter is an area of our interest, because it entails secure user behavior and people recognizing of any web-related attacks (Hendrix et al., 2016).

3.0. Security awareness training

Security is typically one of such things, that does not lead to tangible outcomes. If everything is done right, nothing happens. In organizational setting, it is only a mistake that eradicates reactions, usually negative and costly. Simultaneously, good security behavior does not make people better or more efficient, sometimes it is actually the opposite. Consequently, security training on the employee side can become a struggle for security management.

While it is unlikely, that cybercrime can ever be eradicated, it is possible to prevent some crimes by accentuating on the importance of construction security competence by taking various approaches in order to change behavior or reinforce good security practices. For instance, Kirwan & Power (2013) suggest that providing a more complete profile of the various types of cybercriminal aids in preventing criminal behavior by intervening with at-risk groups. Other approaches suggest prevention strategies and the potential aid of psychologists in identifying methods of encouraging users to engage in safer online behaviors, and implementing tools able to improve the engagement of learners (Zyngier, 2008; Dabbagh & Kitsantas, 2012; Pesare et al., 2016).

Unfortunately, despite a substantial amount of research, dedicated to the relations between security awareness, training and psychology; and multiple suggestions and recommendations on how to account for various aspects of awareness and policy compliance, while building Security Awareness and Training (SAT) Programs, recent PwC's Global Economic Crime Survey (2016) reveals that most of the studied companies are still not adequately prepared for cybercrime or even underestimate the risks faced. Moreover, only 37% of organisations have a cyber incident response plan and less than half of board members request information about their organisation's state of cyber-readiness (PwC, 2016). Furthermore, traditional training programs may be outdated or inconvenient for implementation in cyber settings. As Nagarajan et al. (2012) claim, disadvantages of most of the current forms of cyber skills training are that they are disengaging, they do not require participants to apply security concepts in real time, happen once a year, presented by security professionals who are bad communicators. Although theoretical knowledge of security concepts is important, defending against cyber-attacks in real time is highly stressful and, therefore, a prior hands-on experience (learned and continuously practiced competence to make right decisions in short time guided by automatic "rules of thumb" rather than by time consuming thorough analysis of situation) is needed. Thus, given the digital nature of cyber-crime and cyber security, the latter appears to be a topic that is especially well-suited to training by applying an agile, engaging learning approach and newest digital tools.

For instance, a flexible, scalable and highly interactive video game could help simulate an environment for the trainees, appropriate to training goal (Nagarajan et al., 2012).

To conclude, in a world where competition is global, and technology has lowered entry barriers, organizations whose employees, communities and customers are deeply engaged will outperform those that cannot engender authentic motivation. Engagement is a competitive advantage and game-design simulation techniques of training programs are not only providing the means to achieve it, but pointing towards a radical transformation in business conduct (Werbach & Hunter, 2012).

4.0. Introduction to the topic of gamification as a training approach

First, we discuss the principles of gamification and game design. This will provide us with theoretical foundation and understanding of how the obtained background can be leveraged to apply gamification with regards to the main research question.

Games have been a fundamental part of human civilization for thousands of years. Games are popular in every demographic, gender and age group, but they are especially pervasive among the generation now moving into the workforce (Werbach & Hunter, 2012).

McGonigal (2011) suggests that all games share four defining traits: a goal (gives a sense of purpose), rules (foster strategic thinking and endorse creativity), a feedback system (provides motivation and indication of how much time does it take to achieving the goal), and a voluntary participation (makes the experience safe and pleasurable). To sum up, playing a game is the voluntary attempt to overcome unnecessary obstacles (Suits, 2005 cited in McGonical, 2011).

Gamification as a phenomenon is a trend in both human-computer interaction and game studies research and practice. The most widely accepted definition of gamification is the use of game elements and game-design techniques in non-game contexts (Deterding et al., 2011; Werbach & Hunter, 2012). Kapp (2012) extends their definition of gamification as the use of game-based mechanics, aesthetics and game thinking to engage people, motivate action, promote learning, and solve problems. As Landers and Armstrong (2017) note, gamification has become a popular technique to enhance instructional outcomes in both education and organizational learning.

The purpose of gamification is to emphasize the attitudes of voluntariness, learning, problem-solving and exploration. Gamification is not about turning all business into a game or rewarding people with trinkets and tokens, but it is about enriching activities with “gameful” aspects and using it as a powerful toolkit to apply existing business challenges, regardless the nature of the firm. The essence of gamification of certain activities is not entertainment, but a fusion of human nature and skillful design (Dal Sasso et al., 2017).

According to Werbach and Hunter (2012), gamification approach prominently works in internal, external and behavior change settings. *Internal gamification* or enterprise gamification is used by the companies to improve productivity and foster innovation. *External gamification* involves external stakeholders and is usually driven by marketing objectives. It provides with a toolkit for better understanding and stimulating customer motivation and loyalty; additionally, it produces increased identification with the product, and ultimately higher revenues. *Behavior-change gamification* aims at forming beneficial new habits and can produce not only desirable societal outcomes, but also private benefits.

The positive effects of a well-designed gamification system include the following three elements: 1) Inherent relatedness (being part of something bigger than ourselves); 2) Reward and motivation; 3) Behavior change (e.g. changing the habits, doing something previously unknown).

Hamari et al. (2014) assessed the effects of gamification by conducting a review of 24 empirical studies. As a result of this analysis, gamification has shown positive effects in improving learning outcomes on multiple occasions. According to Hendrix et al. (2016) research, serious games (games with a purpose other than pure entertainment) may be a cost-effective solution to educate people and reduce cybercrimes. Although this field is still developing, other researchers also confirm the potential of gamified approach in education and training (Deterding et al., 2011; Le Compte et al., 2015; Rieb et al., 2017; Landers & Callan, 2011; Landers, 2014; Nagarajan et al., 2012; Adams & Makramalla, 2015; Dal Sasso et al., 2017; Pesare et al., 2016).

Games provide an engaging interface that enhances training, draws more trainees and simulates a variety of scenarios, yielding positive results in supporting health, education, management and other sectors (Nagarajan et al., 2012). Therefore, one may assume that application of gaming concepts to training in cybersecurity and defense can also be equally fruitful: research is advancing in modeling and simulation that seem potentially applicable to cybersecurity and defense gaming (Nagarajan et al., 2012, p.256). Hendrix et al. (2016) suggest that in order to increase the training effectiveness, organizations and researchers should focus more on the type of scenario-based training that is already common in the security field and often includes gaming elements. Games may represent specific case studies and facilitate a case-based learning approach (Hendrix et al., 2016).

However, Kohn (1999) raises concerns about e.g. the use of reward systems and virtual economies used in game-based learning, since rewarding a certain behavior educates the users towards obtaining the specific reward and hides the actual goal of the task. He also acknowledges that the users might perceive the rewards as a controlling mechanism, thus generating rejection instead of engagement. Moreover, Dal Sasso et al. (2017) discuss legal and moral perils that endanger the process of gamification process constitute a new area of law, further complicated by its borderless nature. These include privacy issues (gamified systems and contexts can be misused to collect a vast amount of information about the players); property and ownership (players spend time and effort in building their avatars and they might consider "owning" them); threat of deceptive marketing.

Overall, gamification is a rising phenomenon. Despite its double-edged nature, well designed gamification learning has a vast potential in enhancing training, by helping and stimulating experts and by fostering employee motivation over a longer period of time.

4.1. The second objective and research question

Since 1) white-collar criminals, discussed in previous chapter of this paper, are currently adopting the form of cybercrime, and 2) one of the ways of prevention cybercrime is an adequate and effective training, preferably in the digital form, we suggest the second (and the main) research question of this paper as the following:

How can the use of gamification methods enable organizational leaders to anticipate vulnerability towards cyber-attacks and, eventually, prevent white-collar criminals' intervention?

In particular, on the basis of integrated white-collar crime taxonomy and a gamified approach to training on cyber security, we expect to contribute to research on both fields by introducing a pilot model of gamified training on recognizing, responding and dealing with white-collar criminals within an organization. Thus, *the second objective of this paper is to present a theoretical foundation for creation a gamified approach to white-collar crime prevention.*

Once an integrated taxonomy of white-collar crime is provided and taken into consideration for creation of different training scenarios, representing specific case studies, we adopt the attacker perspective as the principal one in our training.

Attacker centricity or attacker centric approach entails using known characteristics of cyber-attackers in order to train employees in anticipating an attacker's motivation, behavior, used strategy and potential weaknesses in carrying out certain attacks (Adams & Makramalla, 2015). As Rieb et al. (2017) note, offender-oriented analysis of cybercrime can help to develop strategies for intervention and prevention. For example, they continue, analysis of techniques of neutralization which criminals are used to apply in order to psychologically enable themselves to commit crimes may contribute to overall understanding of offenders' cognitive processes and consequent behavior. According to the theory of neutralization, proposed by Sykes and Matza (1957), there are five techniques that allow people to justify breaking existing social norms and laws and rationalize deviant behavior: denial of responsibility, denial of injury, denial of victim, condemnation of the condemners, appeal to higher loyalties. If we adopt attacker centricity as a principal perspective in cybercrime training, we may achieve a better understanding of attacker's desires and actions and thereby develop a better defensive strategy against their attacks. Therefore, a serious game first played as by the attackers and then played as by managers/other victims/ enhances the creation and application of both offensive and defensive strategies against cyber-attacks (Adams & Makramallla, 2015).

Thus, we hypothesize that by adoption of attacker centricity approach in gamified training program (i.e., through playing the roles of white-collar attackers differentiated according to the type of crime committed, criminal's position in the company and chosen target) the use of gamification methods may increase the effectiveness of cyber security training and therefore enable proactive rather than reactive response of organizational leaders to this threat.

5.0.Methodology

The chosen research design includes qualitative methods for data collection. We are going to assess the current state of white-collar crime prevention training through the review of available literature on this topic, interviewing several experts in field of cybercrime, white-collar crime and gamification. Moreover, we will present theoretical arguments in favor of or against the above-mentioned hypothesis. Next, we aim to create, in collaboration with practitioners, a pilot model of white-collar crime training, where we briefly describe training scenarios (various combinations of attacker's type, crime specificity and victims acting in selected settings) and practical implications of this training program. Finally, limitations will be discussed as well as potential for further research and development in this field.

In general, preliminary literature analysis allows us to claim that there is dramatically little training on prevention of white-collar crime. There are some training programs dedicated to white-collar crime, but some of them are offline courses provided by university (e.g., BPP University, U.K.), some of them are online, yet short-term oriented and not contingent (e.g., 2-hours online introduction to the topic of white-collar crime provided by National White-Collar Crime Center and Bureau of Justice Assistance, U.S.). Moreover, many of these trainings are organized by governmental structures and therefore not available for companies or individuals without agency identification/accreditation. After a brief review we could not find any related gamified approach to this topic. Such trainings are either not available for general public or do not exist at all, and the degree of their gamification is unclear. Therefore, our thesis aims to contribute to existing research through filling this gap in crossover study of white-collar crime, cybersecurity and training gamification in both theoretical and practical dimensions.

6.0.Conclusion

According to the security reports, the human factor constitutes a vulnerability and possess threat in the information security domain. Existing cyber security training programs fail to create the behavior and competence needed for employees to anticipate and prevent security breaches.

The first objective of the thesis is to provide a simplified yet comprehensive taxonomy of both white-collar offenses and offenders, based on integrated findings of previous research on this field. The aim is to focus on the vital attributes any white-collar crime classification possesses, and thereby offer an optimal taxonomy, combining several perspectives and allowing for further implementation in a practical setting, which comprises the second objective of the thesis - gamification of employee training against white collar crime.

Therefore, the in second part of our thesis we will provide theoretical arguments in favor of gamification, as a design technique used to increase user engagement and motivation. According to the literature, gamification of crime related training may become a revolutionary approach to training in organizations. We adopt an attacker centricity approach in the training, based on the taxonomy of white-collar offenders created in the first part of the thesis. Attacker centricity approach uses known characteristics of cyber-attackers to train participants in anticipating an attacker's motivation and behavior in carrying out certain attacks. This anticipation enhances the creation and application of both offensive and defensive strategies against cyber-attacks.

In order to achieve the stated objectives, we will employ a qualitative research approach to assess whether gamification can be used in security awareness and training programs in order to improve learning outcomes. Qualitative data will be collected through interviewing several experts in fields of cybercrime, white-collar crime and gamification.

In order to gain an understanding of the possibilities and limitations of the proposed concept, we will create a pilot model of white-collar crime training, where we briefly describe training scenarios (various combinations of attacker’s type, crime specificity and victims acting in selected settings) and practical implications of this training program.

Finally, limitations will be discussed as well as potential for further research and development in this field.

7.0. Plan for thesis progress

Activities	Timeline				
	January	February	March	April	May
Supervisor meeting*)		■			■
Timeplan for activities related to research	■				
Preliminary report	■				
Introduction	■				
Methodology	■	■			
Literature review on topics (WCC, cybercrime and gamification)		■			
Analysis of the literature review		■			
Preliminary evaluation by supervisor (1)		■			
Interviews*)		■	■		
Coding of interviews		■	■		
Creation of scenarios for pilot model of WCC training			■	■	
Preliminary evaluation by supervisor (2)				■	
Combining parts				■	
References/ appendix	■	■	■	■	
Abstract				■	■
Printing and binding				■	■
Submission of final thesis				■	■

*) To be decided later.

Holidays: week 8, 12 & 13.

8.0.List of references

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: an attacker-centric gamified approach. *Technology Innovation Management Review*, 5(1), 5.

Armstrong, M. B., & Landers, R. N. (2017). An Evaluation of Gamified Training: Using Narrative to Improve Reactions and Learning. *Simulation & Gaming*, 1046878117703749.

Bounfour, A. (2015). Digital Futures, Digital Transformation: From Lean Production to Acceluction (1st ed. 2016. ed., Progress in IS).

Brightman, H. J. (2011). Today's White Collar Crime: Legal, Investigative, and Theoretical Perspectives. *Routledge.*

Business Insider, (2017). Buffet: This is the number one problem with mankind. Retrieved from: http://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5

Coleman, J. W. (2005). The criminal elite: Understanding white-collar crime. *Macmillan.*

Collins, J. M., & Schmidt, F. L. (1993). Personality, integrity, and white collar crime: A construct validity study. *Personnel Psychology*, 46(2), 295-311.

Dabbagh, N., & Kitsantas, A. (2012). Personal Learning Environments, social media, and self-regulated learning: A natural formula for connecting formal and informal learning. *The Internet and higher education*, *15*(1), 3-8.

Dal Sasso, T., Mocci, A., Lanza, M., & Mastrodicasa, E. (2017, February). How to gamify software engineering. In *Software Analysis, Evolution and Reengineering (SANER), 2017 IEEE 24th International Conference on* (pp. 261-271). IEEE.

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011, September). From game design elements to gamefulness: defining gamification. *In Proceedings of the 15th international academic MindTrek conference: Envisioning future media environments* (pp. 9-15). ACM.

Deterding, S., Sicart, M., Nacke, L., O'Hara, K., & Dixon, D. (2011, May). Gamification. using game-design elements in non-gaming contexts. *In CHI'11 extended abstracts on human factors in computing systems* (pp. 2425-2428). ACM.

Engelmann-Zach, H. (2014). Executive Board Compensation of Publicly Traded Companies in Switzerland: The Influence of Compensation Gaps Between CEOs and Their Direct Reports on Firm Performance (Doctoral dissertation).

Forbes, (2015). IBM's CEO On Hackers: Cyber Crime Is The Greatest Threat To Every Company In The World. Retrieved from: http://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world

Geis, G. (1982). On white-collar crime (p. 53). P. Jesilow (Ed.). *Lexington Books*.

Gottschalk, P. (2013). Empirical differences in crime categories by white-collar criminals. *International Letters of Social and Humanistic Sciences*, 5, 17-26.

Gottschalk, P. (2013). White-Collar criminals in modern management. *Modern Management Science & Engineering*, 1(1), 1.

Gottschalk, P. (2016). Investigating fraud and corruption: Characteristics of white-collar criminals. *Journal of Forensic Sciences & Criminal Investigation* ;Volume 1.(2) p. 1-7

Gottschalk, P. (2016). Investigation and prevention of financial crime: Knowledge management, intelligence strategy and executive leadership. *CRC Press.*

Gottschalk, P. (2017). White-Collar Crime Triangle: Finance, Organization and Behavior. *Journal of Forensic Sciences & Criminal Investigation*;Volume 4.(1) p. 1-7

Hamari, J., Koivisto, J., & Sarsa, H. (2014, January). Does gamification work?--a literature review of empirical studies on gamification. In *System Sciences (HICSS), 2014 47th Hawaii International Conference on* (pp. 3025-3034). IEEE.

Hendrix, M., Al-Sherbaz, A., & Victoria, B. (2016). Game based cyber security training: are serious games suitable for cyber security training? *International Journal of Serious Games*, 3(1), 53-61.

CSO, (2017). Top 5 cybersecurity facts, figures and statistics for 2017. Retrieved from: https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

PwC, (2016). Global Economic Crime Survey 2016. Retrieved from: https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf

Punch, M. (2000). Suite violence: Why managers murder and corporations kill. *Crime, law and social change*, *33*(3), 243-280.

Ketil Arnulf, J., & Gottschalk, P. (2012). Principals, Agents and Entrepreneurs in White-Collar Crime: An Empirical Typology of White-Collar Criminals in a National Sample. *Journal of Strategic Management Education*, 8(3).

Kirwan, G., & Power, A. (2013). Cybercrime: The psychology of online offenders. *Cambridge University Press.*

Kohn, A. (1999). *Punished by rewards: The trouble with gold stars, incentive plans, A's, praise, and other bribes*. Houghton Mifflin Harcourt.

Landers, R. N., & Callan, R. C. (2011). Casual social games as serious games: The psychology of gamification in undergraduate education and employee training. In *Serious games and edutainment applications* (pp. 399-423). Springer London.

Le Compte, A., Elizondo, D., & Watson, T. (2015, May). A renewed approach to serious games for cyber security. In *Cyber conflict: Architectures in cyberspace* (CyCon), 2015 7th international conference on (pp. 203-216). IEEE.

Lewis, B. C. (2004). Prevention of computer crime amidst international anarchy. *Am. Crim. L. Rev.*, 41, 1353.

McGonigal, J. (2011). *Reality is broken: Why games make us better and how they can change the world*. Penguin.

McKay R, Stevens C, Fratzi J (2010) A 12-step process of white-collar crime. *International Journal of Business Governance and Ethics* 5(1): 14-25.

Michel, P. (2008). Financial crimes: the constant challenge of seeking effective prevention solutions. *Journal of Financial Crime*, *15*(4), 383-397.

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012, May). Exploring game design for cybersecurity training. In *Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012 IEEE International Conference on* (pp. 256-262). IEEE.

Nelken, D. (Ed.). (1994). White-collar crime (pp. 355-392). Aldershot,, England: Dartmouth.

Ouimet, G. (2009) Psychology of white-collar criminal: In search of personality. *Psychologie Du Travail Et Des Organisations* 15(3): 297- 320.

Ouimet, G. (2010) Dynamics of narcissistic leadership in organizations. *Journal of Managerial Psychology* 25(7): 713-726.

Pesare, E., Roselli, T., Corriero, N., & Rossano, V. (2016). Game-based learning and Gamification to promote engagement and motivation in medical learning contexts. *Smart Learning Environments, 3*(1), 5.

Piquero, N.L. (2012). The only thing we have to fear is fear itself: Investigating the relationship between fear of falling and white collar crime. *Crime and Delinquency* 58 (3): 362-379.

Ragatz, LL.; Fremouw W.; Baker, E. (2012) The Psychological Profile of White-Collar Offenders: Demographics, Criminal Thinking, Psychopathic Traits, and Psychopathology. *Criminal Justice and Behavior* 39 (7): 978-997.

Rieb, A., Gurschler, T., & Lechner, U. (2017). A Gamified Approach to Explore Techniques of Neutralization of Threat Actors in Cybercrime. In *Annual Privacy Forum* (pp. 87-103). Springer, Cham.

Shapiro, S. P. (1990). Collaring the crime, not the criminal: Reconsidering the concept of white-collar crime. *American Sociological Review*, 346-365.

Sloman, C. (2016). What impact does human behavior have on cyber security? *Accenture.*

Sutherland, Edwin H. (1940). The White-collar criminal. *American Sociological Review* 5:1–12.

Sutherland, Edwin H. (1949). *White collar crime.* New York: Dryden.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American sociological review*, 22(6), 664-670.

Tarafdar, M., DArcy, J., Turel, O., & Gupta, A. (2015). The dark side of information technology. *MIT Sloan Management Review*, 56(2), 61.

Werbach, K., & Hunter, D. (2012). *For the win: How game thinking can revolutionize your business*. Wharton Digital Press.

Williams, H. E. (2006). Investigating white-collar crime: embezzlement and financial fraud. Charles C Thomas Publisher.

Zyngier, D. (2008). (Re) conceptualising student engagement: Doing education not doing time. *Teaching and Teacher Education*, *24*(7), 1765-1776.