PREVENTION AND DETECTION FOR RISK AND FRAUD IN THE DIGITAL AGE – THE CURRENT SITUATION

HANNA DONNING, MATHIAS ERIKSSON[1]
MINNA MARTIKAINEN[1] AND OTHMAR M LEHNER[2] (EDITORS)

[1] Hanken School of Economics, Helsinki
[2] University of Applied Sciences Upper Austria and Hanken School of Economics, Helsinki

***Abstract**: "Fraud", "corporate crime" and "white collar crime" are all terms used when referring to economical- and operational crimes, where fraudulent activities has occurred. Illegal acts such as asset misappropriation, business misconduct fraud, money laundering, cybercrime, tax fraud and accounting fraud are major concern, and where an increased threat has been identified.*

This paper explores the possibilities new technology used in fraud detection and prevention mechanisms could provide. Furthermore, we connect the new technology mechanisms with the aspect of organizational culture, that has been proved significant in fraud risk. The contribution is twofold. First, we provide an assessment of modern approaches for fraud detection and prevention, second the insights given by the case study and previous research add encouragement and potential directions for both future research and business practice implications.

***Keywords**: Fraud; Internal fraud; Advanced technology; Organization culture; Case Study*

Introduction

"Fraud", "corporate crime" and "white collar crime" are all terms used when referring to economic crimes, where fraudulent activities has occurred. From an overhead perspective, economic crimes are committed illegal acts, executed by either an individual or a group of individuals to attain financial or professional advantage (O'Brien, 2019). Illegal acts, such as asset misappropriation, business misconduct fraud, money laundering, cybercrime, tax fraud and accounting fraud are looked upon as a major concern, and where an increased threat has been identified (O'Brien, 2019; PWC, 2019).

It is not only the fraudulent activities that have increased in recent years, recent development also includes regulations, technology, extended knowledge and stakeholder expectation, where transparency is the key word in the debate regarding fraudulent activities. High pressure is put on organizations to manage a good corporate governance function alongside meeting the demand from market expectations, and therefore the organization culture also plays an important role in reducing the internal fraud risk. (Healy and Whalen, 1999; West & Bhattacharya 2014).

The research area is complex and detail oriented, all focusing on different aspects and including different variables in their research scopes. To highlight some, Sima and Satyanarayan (2016) researched the auditors view of how internal fraud is conducted in the present, and Abassi, Albrecht, Vance and Hansen (2012) researched how meta-learning frameworks would help to detect financial fraud. We will focus our research to analyzing previous literature on the internal perspective of fraudulent activities, including

intentional misstatements such as material omissions or disclosures (ISA, 240, 2009 p. 167). Furthermore, we present the Volkswagen Dieselgate Scandal of 2015 as a case study, with the aim to gain an understanding of another aspect of internal fraud and technological advancement, yet with an emphasis on the organizational culture and exemplify a case of a non-functional corporate governance instrument. An analysis of previous research will be conducted, this to examine the development for methods and systems that are able to detect risks and prevent fraud, and also find positive and negative aspects with these systems. The aim is to connect the technological advancements with the aspects of organizational culture, to provide further insight in an area of research not yet discovered as much.

The article will provide value to practitioners and academics likewise, where a thorough background presentation is provided on the subject of internal fraud, new technologies and a future outlook with the aspect of past outcomings, that will gain new perspectives and aggregated knowledge. The remainder of this article is organized as follows: next section provides a background presentation and literature review regarding economic crime in general and internal fraud more specifically. Section three, presents the current development of methods and systems to detect risks and fraud. In section four the Dieselgate case is examined and conclusions from the case follows. Section five provides relevant research on organizational culture and modern approaches versus traditional ones in fraud detection, then follows a review of setbacks in regards of technological advancement. The final section concludes the main findings and propose some thoughts on future research.

Theoretical frames

For detecting risks and fraud, a lot of data must be analyzed and for detecting upcoming risks and fraud, even more data must be evaluated to learn patterns to which firms and individuals tend to act in. Because of the size of big data, traditional methods for fraud detection can also be considered impractical (West & Bhattacharya 2014).

Developing fraud detection systems is not an easy process and can affect the organizations reputation when done wrong. In the Global Economic Crime and Fraud Survey by PWC from 2018, about 34 percent of the respondents said that financial crime technologies produced too many false positives (PWC 2018). The progress in fraud detection systems and technologies are still evolving, and with time financial institutions will have more accurate and efficient mechanisms for attacking fraud and financial crimes (SAS 2018).

However, according to the PWC survey organizations today have access to a wealth of innovative and sophisticated technologies which they can use to defend themselves against fraud. These technologies help with monitoring, analyzing, learning and predicting human behavior and includes machine predictive analytics, machine learning and other artificial intelligence techniques (PWC 2018).

Internal fraud

From the organizations' perspective, internal fraud is fraud committed within the organizations or by the organizations. The risk of fraud internally could be explained by the triangle of fraud firstly developed by Cressy (1953). Incentive and pressure together with rationalization and opportunity are all components in fraudulent activities, and the triangle of fraud could be used for internal fraud risk assessment (Murphy and Free, 2016). Pressures are seen as the situational events in forms of personal satisfaction, fear of failures or money.

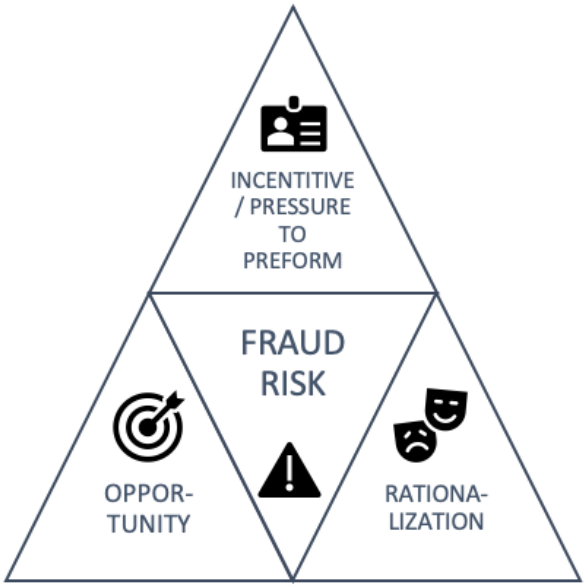

Figure 1 Triangle of fraud (Source: Authors)

Opportunities are the opening of situations where fraudulent activities are possible, for example weaknesses in internal controls within organizations could be one such opportunity event. The rationalization is the typical personal feature, which includes the willingness for intentional dishonesty and therefore the last component in the triangle of fraud that needs to be present for potentially fraudulent activities to occur (Waymond et al., 2015; Coleman and Cressey, 1980).

A common type of internal fraud is when management uses its own interpretation in financial reports (PWC 2018). This to either mislead stakeholders regarding the company's underlying financial situation, meeting the capital market's estimates and expectations or in contract negotiations benefit by reporting a more lucrative financial result. This can also be called earning management (Healy and Wahlen 1999). Safitiri, Kustono and Miqdad (2018) found that information asymmetry between the company in question and external parts can create an agency problem where the agent has more information than the principals. An agency problem could lead to an opportunistic behavior, where the agent also maximizes his private benefits or the utility, instead of prioritizing the principals' interest.

Among the different types of internal frauds, another common type is consumer fraud. Consumer fraud is business practices that cause the consumer to suffer, financially or by other losses. Fraud against consumers are often related to marketing, or other promises the firms ensures the consumer with, which later will appear to be inaccurate claims (Winston & Strawn 2019). Furthermore, money laundering and employees stealing from firms are crimes frequently occurring.

Prevention of fraud

The process of preventing fraudsters are costly and time-consuming, but fighting fraudsters is important to ensure a well-functioning society. Good corporate governance can make sure that the firm´s top management don't misappropriate assets and manage results in an unethical manner, while internal processes can help preventing employees stealing from the firm (Murphy and Free, 2016).

Fraud risk has been discussed as long as companies have existed and will probably exist as long as firms and people face benefits through committing frauds. Since frauds are becoming more sophisticated, devastating and thorough, more advanced and modern techniques are always needed to fight and predict fraudsters. We will in the next chapter look at the current development of modern techniques for fraud detection.

Current development

Organizations nowadays invest more in technology to prevent fraud, since fraud can be a business problem which could affect growth and reputation negatively. Therefore, use of artificial intelligence and machine learning is now a worldwide phenomenon and companies in developing territories are investing in these technologies more compared to companies in developed territories (PWC, 2018). The technology is still expensive to buy and to adopt across large organizations as well as for smaller organizations. So, the decision when to invest in more innovative technologies regarding fraud detection is a question organizations' must ask themselves (PWC 2018; Simha and Satyanarayan, 2016).

Development of methods and systems to detect risks and fraud

There are several different statistical and computational techniques for financial fraud detection. West and Bhattacharya (2015) presented data mining as a method for fraud detection. Data mining is the process of sorting through large data sets, with the purpose to identify patterns and establish relationships to solve problems. With the help from the information of data-mining, it is then easier to predict future outcomes. One method of data mining is artificial immune systems (West and Bhattacharya 2015).

Artificial immune systems imitate the behavior of biological immune systems to detect antigens, creating detector cells and their ability to detect foreign bodies. As mentioned, it functions in the same way as the human immune system, by cells fighting antigens and by that the cells will later be better suited for detecting antigens. This method is suitable for classifying problems with imbalanced data, such as fraud detection (West and Bhattacharya 2015).

Machine learning is also a commonly used method for fraud detection and prevention. Machine learning algorithms discovers patterns in big data and the process is much more efficient compared to humans doing the same task. With the information acquired throughout the process, it is easier to predict and prevent frauds. Machine learning can be divided into supervised and un-supervised machine learning. Supervised machine learning is the more commonly used by these two. What differs these two machine learning methods, is that in supervised machine learning guidelines and what conclusions it should come up with are given to the algorithms, this requires that possible outputs are already known. Unsupervised machine learning is instead identifying complex processes and patterns without any guidelines and human intervention, which can help with solving problems that humans normally couldn't do (DataScience 2017).

Another method is meta-learning. Meta-learning is a form of machine learning which uses information acquired through data mining or machine-learning with the purpose to increase the

quality of results obtained in future applications, also called learning-to-learn. It differs from machine-learning, since meta-learning provides a way to learn about the process itself and by that, also providing knowledge about which features and algorithms that can be most efficiently applied (Abbasi, Albrecht, Vance & Hansen 2012).

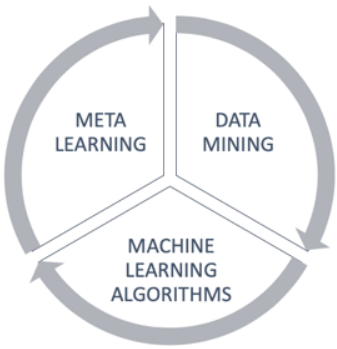

Figure 2 - Three techniques used when developing system and methods to detect risks and frauds (Source: Authors)

The current development of machine learning and artificial intelligence for risk and fraud detection is that firms do invest more in these technologies and that they are more efficient, but they are also costlier. Advantages with more innovative technologies is that it helps financial institutions to earlier detect risks and fraud. This with help from more innovative approaches for fraud detection (SAS 2018).

"Dieselgate" – Volkswagen Group

To further understand how the organizational culture of an organization, corporation, firm or company can change the prosperity for technological advancement in fraud prevention and detection, the Volkswagen Dieselgate scandal is one example that we believe could provide a thorough picture of how organizational culture mixed with tech improvements impacts reality.

Background to the case: Volkswagen anti-pollution system

Volkswagen amongst other automobile companies were all developing a cleaner line of diesel engines in the years prior to 2008, when the first defeat device was installed. The EA 189, was the new diesel engine line of Volkswagen, and one of the most important engines for the Volkswagen brand. The EA 189 came both as 1.6- and 2.0-liter versions and were planned to be used in vehicles of other brands included in Volkswagen group, such brands were Audi, Skoda and Seat. Moreover, the new engines were also scheduled to be included in Golf, Passat, Beetle and Jetta cars sold in the United States as a concept of "clean diesel" and make American drivers responsible for their environmental surroundings. Pressure put on the engineers employed by Volkswagen was high, and the developed EA 189 engines proved to be a disappointment, not able to meet the standards of emission regulations, in not only United States, but also in the European Union. The setback of canceling the production, was found to be too costly, therefore Volkswagen decided that an easier way out was to install a developed manipulation software, which later came to be called the Defeat Device (Eiwing, 2015).

The scandal erupted in September of 2015, after an illegal manipulation software (also named the "defeat device") was discovered by EPA (Environmental Protection Agency) on the basis of tests conducted by ICCT (International Council on Clean Transportation), who found significant differences between lab tests and road tests, where in the testing of the later one higher doses of pollutants such as nitrogen oxides (NOx) where reported. Volkswagen admitted

to have had installed the so-called defeat device in approximately 500 000 cars sold in the United States (Tovey, 2015). The defeat device was found to enable the Volkswagen cars to detect when they were being tested, and therefore the engines of the cars emitted less CO_2 and NOx than they would under normal circumstances emit (Siano et al., 2017). The instant negative impact on both Volkswagen and various stakeholder groups involved followed, and a public outrage made the shares of Volkswagen to drop with more than 20 % in one day on the Frankfurt Stock Exchange (Siano et al., (2017). Both internal and external investigations begun not only in the United States, also Germany, France and several other states decided to investigate potential fraud further, where Volkswagen was the main suspect.

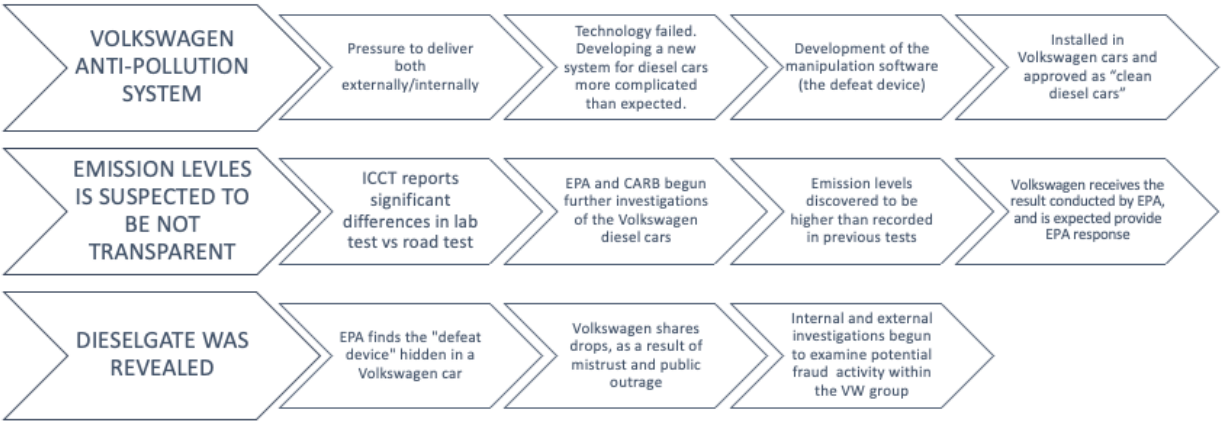

Figure 3 Sequence of events the years prior to the reveal of Dieselgate (Source: Authors)

The internal organization culture and management response

Siano et al., (2017) performed a content analysis on the revelations and findings from Dieselgate reported in media, and the reported content from Volkswagens personal statements and sustainability communication to their share- and stakeholders. The result proves that Volkswagen in fact did not report a true and fair view, instead they presented an inconsistent picture of what the reality looked like. Looking to the sustainability communication, Volkswagen did communicate more ambitious statements compared to other automobile companies, where they specifically highlighted the reduction of emissions such as CO_2 and NOx. *"Due to climate change issues and ever scarcer resources, we reduce the CO_2 emissions of our vehicles on an ongoing basis"; "Reduce global facility CO_2 emissions per vehicle by 30 percent by 2025 compared to a 2010 baseline"* (Siano et al., 2017, p. 31) are two examples found in the annual statements of Volkswagen group.

When seeking parallels in prior fraud cases, Enron and Worldcom are two cases that has similar characteristics to Dieselgate. When following the individual investigations of each fraud case, all related suspected data led to senior managements fraudulent acts, in order to camouflage the businesses financial situations or operational failures (Crete, 2016). After its first internal investigation Volkswagen found that a handful of software engineers within the management, were the ones responsible, and the CEO of Volkswagen group in the United States claimed to the Congressional Subcommittee that no allegations towards the organizational management were in line (Crete, 2016; Boston, 2015). The CEO was not able to convince neither the Subcommittee, external investigators nor the public and suspicions were drawn to the management of the corporate governance function within the Volkswagen group.

In December of 2015, the senior management of Volkswagen Group released the preliminary results of the more in-depth internal investigation. They found following

observations: (1) misconduct and shortcoming were compelled by individual employees, (2) Volkswagen did have some weaknesses in certain internal control processes, and (3) the mindset within some divisions of Volkswagen were wrong, and lacked ethical behavior where breaches of rules were tolerated.

Conclusions from Dieselgate

The Dieselgate scandal was the result of ambitious production and market targets, for specifically the United States market, with strict time and budget limits. Furthermore, this led to encouragement of the employees to make unethical decisions in order to meet the operational goals and achieve the objectives of Volkswagen group's business model. The internal control mechanisms did not work, and therefore the misconducts within the organization could not be discovered. Issues has been found especially within the compliance system, which were there to ensure that the respect of legal requirements were met (Eiwing, 2015). Among other circumstances that led up the outcome of Dieselgate, poor corporate governance managed by senior management is the main one. The external investigations did see a centralization of decision-making to the senior management, and where the organization culture of Volkswagen made the internal communication between mid-level management to senior management, not functional. Passing on "bad news" were discouraged, and pressure to deliver was high (Crete, 2017; Ewing, 2015).

Research

This section provide a presentation of what previous research found about the relationship between organizational culture, artificial intelligence, machine learning and fraud detection. Also, to further investigate whether more modern approaches to detect frauds are in favor of traditional ones.

Organizational culture

Decision making within organizations are dependent on both individual and organizational factors, and where the organizational ethical culture will influence the ethical behavior (Douglas, Davidson and Schwartz, 2001). Fraudulent activities could be looked upon as intentional dishonesty, and could derive from either perceived pressures, perceived opportunities or rationalization (Waymond, Söderbom and Guiral, 2015; Cressy, 1953). As mentioned in section two, the three components (pressure, opportunity and rationalization) put into the fraud triangle are also the three requirements for fraud to potentially occur (Cressy, 1953). Previous research has clearly seen a connection between the triangle of fraud and employees within organizations who commit fraud. This could also be explained by the upper echelon's theory (Hambrik and Mason, 1984), which suggest that senior management are a reflection on the organizational culture within the organization. Therefore, the praxis for fraudulent activities and the questions of whose responsible in prior fraud investigations has also changed its direction to some extent. For example, the guidelines of the Principles of Federal Prosecutions of Business Organizations, issued by the U.S. Department of Justice still emphasis the further investigation of individual wrongdoers in fraud cases, but recent development has also started to seek explanations for fraud in the organizational environment (Crete, 2016).

Modern approaches for fraud detection versus traditional ones

Abbasi, Albrecht, Vance and Hansen (2012) conducted a research paper about how a meta-learning framework will help to detect financial fraud. To evaluate the proposed framework, thousands of legitimate and fraudulent firms were investigated (Abbasi et al., 2012).

Prior studies suggest that data based on financial statements does not have a high fraud detection rate and because of that the use of ratios and financial statements are incapable of accurately identifying financial fraud or at least, that it has a limited capability (Kaminski 2004). So, the question to ask is if meta-learning do increase the fraud detection rate.

By comparing meta-learning processes with traditional approaches for detecting risks and fraud, Abbasi et al., (2012) found that the Meta-Fraud framework was remarkably effective. The framework was found to improve the performance and the results, therefore using meta-learning methods where confirmed to be more effective compared to traditional approaches, such as studying financial ratios (Abbasi et al., 2012).

Soviany (2018) studied how artificial intelligence can come to help with detecting online payment frauds and transactions in real time. The design focus is on a supervised learning engine to support high-performance fraud detection of the data, as well as improving the predictive value. With this AI method, the design exploits the discriminant properties of customer data and by that, finding hidden patterns. Soviany (2018) found that artificial intelligence was superior compared to the static rule-based methods. This due to that the method is considered more effective and can manage a greater data set with less human intervention. Soviany (2018) claims that in many legacy-rules based fraud detection systems, the target performance achieves a lot of false positive results, while artificial intelligence has a faster adoption process and can therefore find more detailed data as well as hidden patterns. Furthermore, statistics provided in the study found an increase from 85 to 90 percent, comparing the methods with detection of fraudulent transactions (Soviany 2018).

The complexity of using artificial intelligence in fraud detection

Baldwin, Brown and Trinkle (2016) reviewed the relationship between auditing and accounting problems and artificial intelligence. The paper examines the problem between two totally different professions. Accounting and auditing are in its nature a specialized domain requiring significant education as well as expertise and experience, which can result in a low number of persons. Because of that, research on accounting is also done most successfully by accountants. The significant differences and the expertise required for both artificial intelligence and auditing, is that auditing and artificial intelligence researchers must bridge the gap and improve collaboration to improve fraud detection using artificial intelligence. Baldwin, Brown and Trinkle (2006) do say that artificial intelligence researchers hold the key to solve issues regarding auditing and assurance through techniques as fuzzy logic, neutral networks and other areas of artificial intelligence. Because of that, collaboration and further investigation into the topic is a requirement for the future in fraud detection (Baldwin, Brown & Trinkle 2016).

Critical voices expressed by society

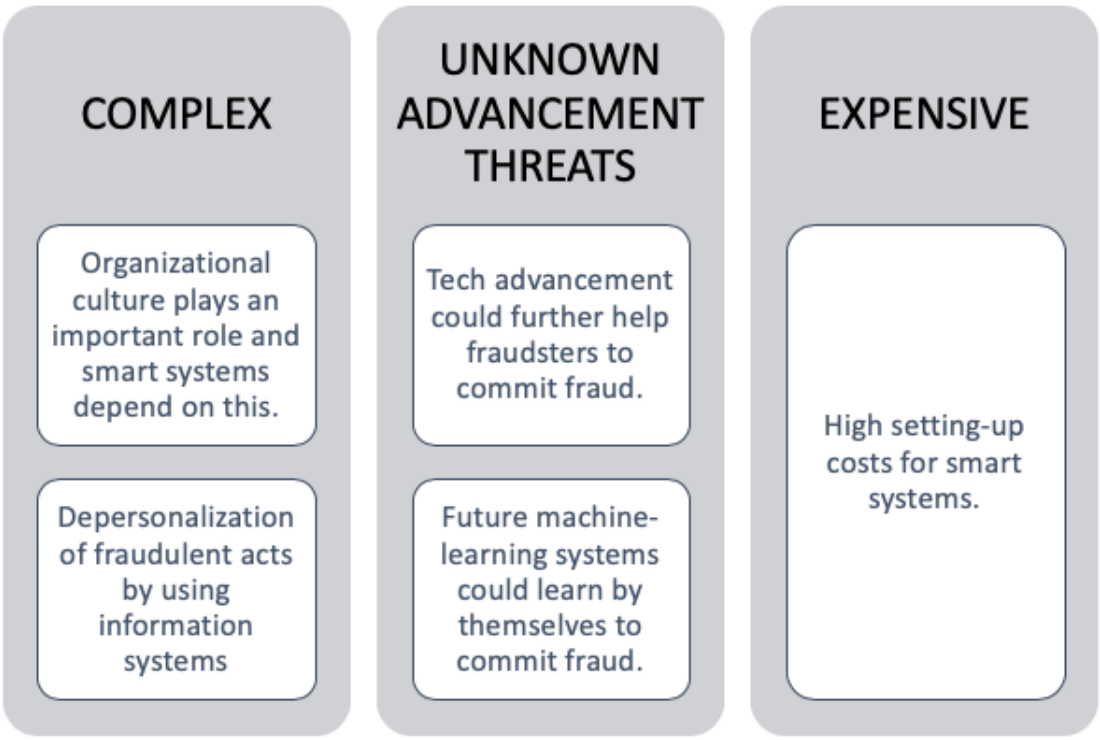

Figure 5 The main arguments in negative response (Source: Authors)

The link between technology and fraud is not only identified as a helpful tool used to detect and prevent fraud. As previously mentioned, the organizational environment and its culture do play a significant role in detection and prevention of fraud of the internal control methods. Therefore, critics has suggested that technology and advanced methods to detect fraud do not matter in an organizational culture of high pressure to meet targets, similar to the case of Volkswagen and Dieselgate (Donelson, Ege and McInnis, 2017; Ewing, 2015).

The presence of technology advancement seems to distance the employees from their responsibility towards dishonest actions, such as fraudulent actions. Prior research on the subject has found that information systems has a tendency to depersonalize fraudulent situations (Schwartz and Wallin, 2002), and therefore the opportunity to commit fraud seems to rise above the rationalization, where justifications of the dishonest actions could be that they are not the ones committing to anything, rather the system or software itself would be the ones accused. Technology loops are exploitable, where the advancement also could help the fraudsters to commit fraud. Moreover, future concerns regarding unsupervised machine learning indicating that systems could learn how to commit fraud on their own is a possibility has been expressed.

Furthermore, the discussion regarding whether to apply technological fraud prevention and control system or not, depends on the setting-up costs, Sima and Satyanarayan (2016) found that even though small organizations are affected tremendously by fraudulent activities, the cost of setting up a smart system is too costly to be handled by smaller organizations (SAS, 2018).

Conclusion and future outlook

Our paper intends to connect the aspect of technological advancement with organizational culture in order to reduce internal fraud. The paper highlights that frauds are committed in situations where benefits can be gained. From the company's perspective, frauds are committed by organizations through, for example, asset misappropriation, to gain private benefits as well as keeping the firm competitive.

It is important to consider that one of the peculiarities of internal fraud is that the person, or persons, that commit fraud often sees it as a victimless crime and can neither visualize any person who will be directly harmed (PWC, 2018; Shwartz and Wallin, 2001). This would also explain why the main perpetrators of economic crimes are internal actors, including human resources fraud (81%), insider trading (75%), asset misappropriation (75%), accounting fraud (74%) and also procurement fraud (73%) (PWC 2018).

Current development of innovative and modern fraud and risk detection methods includes machine learning algorithms, data mining and meta-learning. They are all useful means accessible in risk and fraud prevention and detection systems (West and Bhattacharya, 2015; Data Science, 2017 and Abbasi et al., 2012). With that said, these methods will not be utilized in an efficient manner, if the organizational culture emphasize dishonest actions from perceived pressures, opportunities or rationalization (Waymon et al., 2015). Therefore, as showcased in the case study (Dieselgate, a well-managed corporate governance function is essential in order to not create opportunities and prevent rationalization internally. PWC 2018, implies the same conclusions where they suggest that focus needs to be drawn to the environment that governs employee behavior. To assess the strengths and weaknesses of the culture, surveys and comprehensive interviews should be made as well as consistent training. If people clearly understand what's right and what's wrong, and why, the process of fighting fraudulent activities will also be easier (PWC 2018).

Furthermore, when connecting technological advancement with organizational culture, we find that future research should investigate this connection in more detail. For example, the aspects of the principal-agency theory could in future be applied to answer the questions regarding the possible situations of asymmetric information and conflicts of interest between management and stakeholders. Moreover, the practical business implications given from our findings, is that a combination of further development in organizational culture and more advanced technologies are the key to reduce the risk of fraud (see figure 4).

Figure 4 The combination of tech and a positive organizational culture in order to prevent and detect fraudulent activities internally (Source: Authors)

References

Abbasi, Albrecht, Vance and Hansen (2012). Metafraud: A meta-learning framework for detecting financial fraud. *MIS Quarterly*, 36(4), 1293-1327.

American Institute of Certified Public Accountants (AICPA) (2002, October), SAS No. 99: Considerations of Fraud in a Financial Statement Audit, AICPA, New York, NY.

Baldwin, Brown & Trinkle 2016. Opportunities for artificial intelligence development in the accounting domain: The case for auditing. *Intelligent systems in Accounting, Finance & Management*, 14(3), 77-86.

Beatty & Weber (2005). Accounting discretion in fair value estimates: An examination of SFAS142 goodwill impairments. *Journal of Accounting Research*, 44(2), 257-288.

Boston, W. (2015). Volkswagen Emissions Investigation Zeroes In on Two Engineers. The Wall Street Journal 5.10.2015. Availeble: https://www.wsj.com/articles/vw-emissions-probe-zeroes-in-on-two-engineers-1444011602. Retrieved: 3.3.2019.

Coleman, J. W., & Cressey, D. R. (1980). *Social problems*. New York: Prentice Hall.

Cressy, D. R. (1953). *Other people's money: The social psychology of embezzlement*. New York: The Free Press.

Crete, R. (2016) The Volkswagen Scandal from the Viewpoint of Corporate Governance. *European Journal of Risk Regulation*, 7(1), 25-31.

DataScience (2017). *Supervised vs. Unsupervised Machine Learning.* Available: https://www.datascience.com/blog/supervised-and-unsupervised-machine-learning-algorithms. Retrieved: 08.03.2019.

Dain C. Donelson, Matthew S. Ege, and John M. McInnis (*2017*) Internal Control Weaknesses and Financial Reporting Fraud. *A Journal of Practice & Theory*, 36,(3), 45-69.

Douglas, P.C., Davidson, A., and Schwartz, N. (2001). The Effect Of Organizational Culture and Ethical Orientation on Accountants' Ethical Judgements. *Journal of Business Ethics*, 34(2), 101-121.

Ewing, J. (2015). Volkswagen C.E.O Martin Winterkorn Resigns Amid Emissions Scandal. *The New York Times* 23.9.2015. Availeble: https://www.nytimes.com/2015/09/24/business/international/volkswagen-chief-martin-winterkorn-resigns-amid-emissions-scandal.html. Retrieved: 3.3.2019.

Ewing, J. (2015) Volkswagen Engine-Rigging Scheme Said to Have Begun in 2008. *The New York Times* 2.10.2015. Availeble: https://www.nytimes.com/2015/10/05/business/engine-shortfall-pushed-volkswagen-to-evade-emissions-testing.html. Retrieved: 3.3.2019.

Hambrick, D.C., and Mason, P. A. (1984). Upper echelons: The organization as a reflection of its top managers. *Academy of management review,* 9(2)**,** 193-206.

Healy & Wahlen (1999). A Review of The Earnings Management Literature and Its Implications for Standard Setting. *Working Paper*.

Kathleen, Sterling & Guan (2004). Can financial ratios detect fraudulent financial reporting?. *Managerial Auditing Journal*, Vol. 19(1), 15-28.

Kaspar, Jan; Fornasiero, Paolo; Hickey, Neal (2003). "Automotive Catalytic Converters: Current Status and Some Perspectives". *Catalysis Today*. **77**(4), 419–449.

Mock, Srivastava & Wright (2017). Fraud Risk Assessment Using the Fraud Risk Model as a Decision Aid. *Journal of emerging technologies in accounting*, 14(1), 37-56.

Morato, Berrueta, Magana & Izal (2018). Ransomware early detection by the analysis of file sharing traffic. *Journal of Network and Computer Applications*.

Murphy, P, R. and Free, C. (2016). Broadening the Fraud Triangle: Instrumental Climate and Fraud. Behavirourl research in accounting. 28(1), 41-56.

O'Brien (2019). Battling the rising threat of white collar crime. Chartered Accountants Ireland. Available: https://www.charteredaccountants.ie/News/battling-the-rising-threat-of-white-collar-crime. Retrieved: 26.2.2019.

PWC (2017). Top financial services issues of 2018. Available: https://www.pwc.com/us/en/industries/financial-services/research-institute/top-issues/artificial-intelligence.html. Retrieved: 24.02.2019.

PWC (2018). Pulling fraud out of the Shadows. Available: https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf. Retrieved: 20.02.2019.

Rodgers, W., Söderbom, A., and Gurial, A. (2015). Corporate Social Responsibility Enhanced Control Systems Reducing the Likelihood of Fraud. Journal of Business Ethics, 131(4), 871-882.

Ruddick, R. (2015). VW admits emissions scandal was caused by 'whole chain' of failures. *TheGuardian* 10.12.2015. Availeble: https://www.theguardian.com/business/2015/dec/10/volkswagen-emissions-scandal-systematic-failures-hans-dieter-potsch. Retrieved: 3.3.2019.

SAS 2019. *Fraud Management*. Available: https://www.sas.com/en_us/software/fraud-management.html. Retrieved: 20.02.2019.

Safitri, Kustono & Miqdad (2018). Audit Quality and Earnings Management: Review and Synthesis of Empirical Evidence. *International Journal of Management, Accounting and Economics.*

Schwartz, S.T. and Wallin, D.E. (2002), "Behavioral implications of information systems on disclosure fraud", *Behavioral Research in Accounting*, 14(1), 197-221.

Siano, A.,Vollero, A., Conte, F., and Amabile, S. (2017). "More than Words": Expanding the taxonomy of greenwashing after the Volkswagen scandal. *Journal of Business Research*, 71, 27-37.

Simha, A., and Satyanarayan, S. (2016). Straight from the Horse's mouth: Auditors's on Fraud Detection and Prevention, Roles of Technology, and White Collars Getting Splattered with Red!. Journal of Accounting and Finance, 16(1), 26-44.

Soviany (2018). The benefits of using artificial intelligence in payment fraud detection: A case study. *Working Paper*.

Tovey, A. (2015). Volkswagen's US boss knew about emissions problem in 2014. *The Telegraph* 8.10.2015. https://www.telegraph.co.uk/finance/newsbysector/industry/11918299/Volkswagens-US-boss-knew-about-emissions-problem-in-2014.html. Retrieved: 4.3.2019.

West and Bhattacharya (2015). Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, 57, 47-66.

Winston & Strawn (2019). What is the definition of consumer fraud. Available: https://www.winston.com/en/legal-glossary/consumer-fraud.html Retrieved: 23.02.2019.