COVID-19 and fraud: a perfect storm?

Prof. Dr. Sylvie C. Bleker-van Eyk, Program director VU postgraduate education Compliance & Integrity Management, senior director PwC CyberFraud&Privacy

COVID-19 holds the world hostage. All our efforts globally are focused on three main areas: keeping hospitals up and running, providing some kind of relief to home-schooling and preventing the economy from going belly-up. We need to survive now but we must also be smart in how we tackle our problems now. The solutions we choose now will determine the fitness of our position at a later stage when we will have tamed the Corona shrew. The question is whether the backlog of work we stalled for after the crisis will be our main problem in the future?

COVID-19 brings out the best in people! Solidarity is thriving. Nurses and police are revered as heroes, and rightly so. However, COVID-19 also brings out the worse in people that have a tendency towards frauding. Working from home inspires crooks to develop phishing-mails and similar fraudulent behavior. Crooks will be crooks and we need to deal with them no matter what crisis our society faces. The fact is that COVID-19 offers not only an opportunity for those who have a fraudulent inclination but will also induce others to commit fraud. Billions – in the US even trillions – of Euro's and dollars are being released to ease the burdens on business and families.

Another problem we encounter is that working from home has an impact on the usual internal controls we are using. For instance, a control such as the segregation of duties may become less efficient. Setting up a virtual reality may make some controls less effective and the eagerness to keep the business up and running may result in employees skipping controls to assure business as usual. Not all organization's internal controls may be cyber savvy as we would imagine.

What makes fraudsters tick may be analyzed with the use of the Fraud Triangle. The concept of the Fraud Triangle was first launched by Cressey. According to Cressey, "trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, are aware that this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions as users of the entrusted funds or property." The Fraud Triangle focuses on fraud opportunities within the organization. In fact, according to the Fraud Triangle the perceived opportunity to defraud increases when the potential fraudulent individual feels pressure to commit fraud (pressure from inside or outside the organization) and will rationalize the seizing of the perceived opportunity through arguments (often fueled by perceived culture) on why he/she should seize the opportunity. Behavior is influenced by three main factors: opportunity, pressure and rationalization. In times of crisis business may seriously slow down and may have ramifications for our workforce such as dismissals or de decrease of bonusses. The latter can increase the pressure felt by employees and increase their willingness to seize any business opportunity with lesser or sometimes no regard for internal controls. For instance, extensive screening of customers may reduce. Fraud deterrence should aim at disenabling the Fraud Triangle by removing causal and enabling factors. The concept of the Fraud Triangle still is regarded as a valid model to analyze abusive behavior.

The most daunting aspect of fraud prevention is the rationalization. COVID-19 taps in to man's most primal instinct: fear! Fear of loosing employment, of loosing benefits, of being cut off from perceived 'necessities' (hoarding). Fear will lead good men from the righteous path and open the window to temptation and solidarity vanishes into thin air.

We also need to understand that there will be a surge in fraud due to the opportunities given by enormous financial relief packages and the urgency with which this relief is offered to all those who need it. As stated above, rationalization will lead to more people acting upon the possibilities for help offered even though that help is not meant for them. They act as a precaution against harsh times. However, there may also be a group with rationalizations that go towards 'entitlement'. In the Netherlands a large sum is made available for relief. The rationalization can be: "that's tax money. That's my money because I paid my taxes and now I'm entitled to my portion". Our taxes are not a piggybank and relief is meant fore those who are in dire straits.

COVID-19 will increase fraudulent activity of the usual suspects and by those that you would less expect to act in such a way. The most important question is: how can we deal with this? Let's discuss the different approaches necessary to tackle the problem of fraud.

Digital fraud

Yesterday a new COVID-19 joke on internet best summarizes the current position of organizations. The question was: "Who led the digital transformation of your company"? The answers were: CEO, CTO or COVID-19? Except for those parts of the economy which are vital to our health and safety, all organizations are all of a sudden becoming digital organizations. Licenses are rapidly bought to organize the digitalization of our workforce. At the VU University I see that many different licenses are set in place to replace face-to-face lectures by digital lectures. At PwC we are used to work at the client or at the office, but at the same time at PwC the digital workplace was already well-established to support working remotely and digitally. However, other organizations might struggle to get this right.

Digital fraudsters thrive on the innocence of the workforce and know that the employee will press any button that promises enhancement of the working environment. Phishing mails not only take your money, but they will also take your intellectual property! Ransomware and other detrimental methods are flooding our corporate and private digital workspace. Firing up a digital workspace must be synchronized with enhancing cybersecurity. Now is the time for penetration tests, for setting up cyber security and enhancing identity management. Overdue maintenance of your cyberspace now requires that the protection of our cybersecurity should be the first priority of any organization. If not, the aftermath of the COVID-19 crisis will be daunting for your organization. Do not give cybercriminals access to your funds or to your IP. Recently, PwC disclosed how foreign actors are targeting valuable IP of organizations worldwide, including universities in the Netherlands. Do not give your IP away!

Defrauding governmental and organizational funding

The massive relief packages need to be distributed quickly, the government realizes that there is no time to set up extensive measures to protect the wrong allocation of funds. Herewith, the government realizes that the funds may go to people and companies that do not need it. The idea will be that after the crisis a retrospect research will be done as to who defrauded the government funds. With the help of Artificial Intelligence, it is possible to start prevention of fraud at the very beginning of the process to release the relief funds. For instance, the same company may use different addresses or even company names to apply for relief funding. AI can detect this with for instance KvK registration and VAT numbers of different companies. Two registration numbers may occur, but multiple VAT numbers often will not. This is but a very simple example. Forensic analytics and visualization tooling offer tremendous possibilities to prevent fraud. Prevention is always to be preferred. With the help of AI the government can get a better grip on the applicants and prevent fraud. Retrospective fraud detection will be far more costly, and the funds may no longer be recoverable.

The reduced effectiveness of the internal controls and the pressure to seize opportunities are mounting and organizations which are in dire straits may have difficulties to deal with this. Within the external supply chain pressure will be mounted upon invoicing. Due to the current crisis situation, opportunities will increase to defraud organizations and the primal survival instinct may lead to an adversative rationalization.

Conclusion

COVID-19 is an immediate threat to our individual health, our community in general and our (non) governmental organizations. We all have to step up. Resurging from this crisis we will have learned the hard way that we weren't ready for the digitalization of our lives. Most of us have left the 'front door' open to those who defraud and/or disrupt our families and organizations. However, it's not too late; we can still close the door albeit not as secure as we would want to, but this is the time to realize that crises bring out the best and the worse in mankind and protective measures are called for. We need not just to board up the windows but we can reinforce or even build the levees from scratch where we forsake to build them in good times. Stay safe!