Identifying risk

06 May 2015Censeo

article written by Servaas du Plessis, chief executive officer of Censeo Pty Ltd

Are there any alternative technologies available for the use of employers, financial institutions, economically active entities and government to identify risk?

Layer voice technology, a product of Nemesysco, is the technology of choice used by Censeo to great benefit of both the organisation as well as their clients. Not only has it improved operational efficiencies, it also enhanced customer experience results in the process of proactive risk identification.

When looking at risk, one of the most common factors relates to deceptive behaviour between parties, regardless of the relationship or engagement. Guy van Damme, senior advisor to Nemesysco Ltd, gives us an understandable overview of facts relating to the detection of deception. Servaas du Plessis, chief executive officer of Censeo Pty Ltd, a company specialising in the verification of information supplied by, amongst others, job applicants and insurance claimants, explains how the use of technology enhanced efficiencies and client experience relating to service since introducing the technology in the pre-verification process.

Detection of deception, most commonly known as “lie detection”, is a topic regarded by most people as both intriguing and repulsive. The subject is indeed fascinating. Imagine having the ability to see through others’ lies, undeniably a secret skill which would be highly desired by most of us.

On the other hand, just thinking about the possibility that someone else might be able to peep into our most secret and intimate thoughts, is repulsive. The telling of a lie is, in many instances, a form of ultimate defence or escapism. The well known neurologist Sigmund Freud (1856 – 1939) even measured that a piece of escapist fantasy might indeed be essential for us. All of us have that little secret corner in our minds where very intimate memories and thoughts are kept and exposing those would be a horrifying thought indeed.

So, does lie detection really exist and, most importantly, if it exists, does it really work?

The fact is that all living beings are continuously busy with a form of deception, and/or the detection thereof. Both the practice of deception as well as the attempt to see through the deception of others are routines, which we are not aware of anymore.
Just think about the use of camouflage in nature, or the habitual white lie we all do tell. In the strictest of senses, putting on makeup or applying after shave in the morning, is a form of deception.
The problem is that we are neither really good at lying, nor are we good at lie detection – we have never been and probably never will be.

What about the technologies and techniques we always hear of, you may ask?

Most experts in the field, such as Judee Burgoon, Bella DePaulo, Paul Ekman, Mark Frank, Joe Navarro, Maureen O'Sullivan and Aldert Vrij, agree to the fact that the detection of lies is very difficult and that there simply is no indicator of deception. The technologies (“machines”, instruments, software) such as the polygraph, do not detect lies but identify some or other physiological change(s), resulting from a cue given by the interviewer.
This same principle applies to the techniques, such as the reading and interpretation of body language and calligraphy (hand writing analysis). It must be said however that both the technologies and the techniques have shown themselves better than chance and have thus indeed been (and are) a huge help in many situations.

From emotional profile to risk assessment

Professionals in the field of investigation know that there is no such a thing as a real “Lie-Detector”, and that most risk assessment-systems are based on the identification of abnormalities in the tested party’s behaviour over time. The demand on Nemesysco was to develop a new, superior technology. After much research by an international team of professionals, a unique idea came into fruition. As previously stated, humans are indeed not really good at the detection of lies but neither are they in hiding their emotions. The voice, often referred to as the mirror of the soul, is a dead giveaway when analysed by a set of sophisticated software tools.

Ongoing research resulted in the establishment of a proprietary set of vocal parameters to correlate with key human emotions. In various combinations, they allow us to identify deceptive intentions in “real life” scenarios. These vocal parameters were identified from a bank of audio files recorded in different languages and in numerous environments, including police interrogations, call centres and controlled experiments.

Many of the parameters Nemesysco’s technologies use are new to the world of phonetics and focus on the uncontrolled and yet phonetically unexplained properties of the human voice. The reading and classification of emotions revealed in the voice is where Nemesysco has concentrated its efforts on.

Nemesysco’s Emotional Diamond™ (illustration depicted below) represents in different modes both the subject’s steady state (Homeostasis) as well as its current state and real-time reactions. When relevant, Nemesysco’s “Risk Level” is calculated based on multiple emotion deviations of the current state from the steady state, taking into account the circumstances and environmental influence.

So, how is this technology used to improve the customer experience?

The operational strategy of Censeo soon made them realise that a definitive edge will separate the mice from the men in a highly regulated and very competitive industry. Prior to introducing the technology, Censeo would react to matters based on assumed and perceived risk as established by the client. This resulted in very high and unacceptable levels of false-positive referrals in terms of client perceived risk.

A quick 4 – 7 minute telephone conversation via use of the technology was introduced as an "in-between" step in Censeo's forensic process resulting in the reduction of the false-positive ratio by more than 95%. These clients would have been subjected to the entire forensic process previously, but are now being dealt with in several fast-track or immediate resolution channels without delay or further hassles.

After processing well in excess of 30,000 high-risk insurance claim referrals (roughly about 2.5% of total claims submitted to insurance companies serviced) we can report that less than 35% of the 30,000 referred, were in fact confirmed higher risk requiring further scrutiny and verification. The significant resultant benefit of this further segmentation turned into hassle free, fast and efficient finalisation of almost 20,000 claims of customers no longer having to endure a full verification process.

It further improved operational and employee efficiencies

It is common fact that technology enables most modern day businesses. It is also common knowledge that not all companies have the capital required to invest in the newest technology with several huge corporates still limited to the abilities of legacy infrastructure.

On top of an aged infrastructure challenge limiting real scalability and improved efficiencies, we live in an era where we need to adapt to the ever-changing employment environment. Human resources management and departments face many challenges, very topical in South Africa currently, applicants using false credentials to secure lucrative positions in organisations. The roles of human resource managers are certainly no longer limited to the hiring of new employees and the monitoring of regulatory compliance with labour laws.

New age human resource managers and departments had to adapt to ensure that they attract the best credible talent available, and more importantly, to retain this credible and talented workforce. There are several pre-employment vetting processes and although the use of the Nemesysco pre-employment screening programme is not intended to replace any of the existing protocols, it most certainly helps to identify those areas requiring further vetting much earlier in the recruitment process.

We found that around 23% of all applicants lie on their resumes, more specifically in terms of qualifications and experience. An even higher percentage of applicants (25%) are involved in ongoing criminal activities like theft, fraud or the use of illegal narcotics and related offences. More concerning however, is the fact that almost the same ratios noted here, apply to employees in organisations – these are employees either stealing from their employers, soliciting cash or favours from providers, or using illegal narcotics in the workplace.

What do the trends tell us?

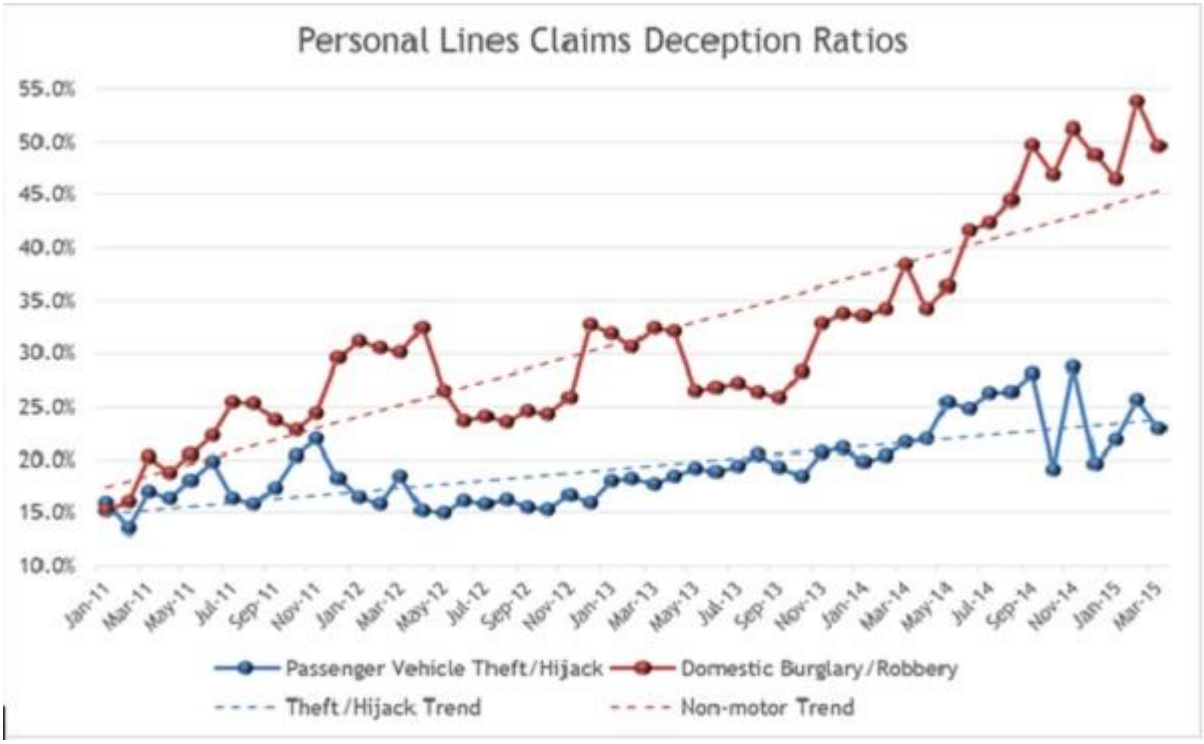
1. Insurance claims

It is suffice to say that the use of technology in the various segments/applications of risk segmentation should only be used within the scope and ambit of the relevant South African laws and regulations applicable to the different industries and/or for the purposes it is used for.

To illustrate the levels of deception in terms of terms of insurance claims (deception in terms of losses as a result of two specific loss types) in the personal lines property insurance segments – motor theft/hijacking and household goods robbery/burglary claims. The claimed amounts identified and confirmed unduly claimed for are expressed as percentages of the total amounts claimed relating to the claims flagged for further scrutiny through use of the technology.

Quite evident in the graph, the following:

- Seasonal peaks are evident over the summer periods between October and March of 2011/2012, 2012/2013 as well as 2013/2014.
- The segmentation process via use of the technology was implemented mid-May 2014 on all risk categories and perils referred – the spike since May especially in the household property segment is evident.
- There is a definite long-term increase in propensity of dishonesty in short-term property and motor claims, but the application of new-age technologies establishes more accurate and efficient risk segmentation.



2. Applicants/Employee integrity

To illustrate the level of risk in the pool of pre-employment candidates and pool of staff already employed, I used the information of employees vetted for, as well as in the employ of several small to medium sized companies. The two graphs depict the following information:

- Overall employee integrity:
  - More than 80% of the total number of employees vetted are generally honest and credible;

- 31% of employees are questionable on certain of the integrity subjects tested, and
- Shockingly, almost 20% of employees are generally dishonest and/or not credible.

- Crime in the workplace relating to theft and corruption:
  - Almost 55% of staff are not involved, and not generally susceptible to become involved in theft of bribery;
  - 30.4% are generally susceptible to, and know of fellow employees involved in theft from the employer of accepting bribes from providers, and
  - Almost 15% of all employees tested are either stealing from their employer, and/or solicit bribes from providers of the employer.

The bottom line - risk can only be managed effectively in collaboration

In closing, the information contained in this article relates to experience in South Africa. Just by following the news headlines in terms of high profile individuals involved in falsifying their credentials and qualifications, as well as regular news in terms of several types of insurance fraud schemes, the information should come as no surprise.

The good news however, is that there are new generation tools and specialist organisations available in the market to reduce the propensity of risk in almost every sector of your business. There are also several collaborative industry initiatives via bodies such as the Association of Certified Fraud Examiners (ACFESA), the South African Insurance Crime Bureau (SAICB), the Association for Savings and Investment South Africa (ASISA), and the South African Banking Risk Information Centre (SABRIC) to name but a few.

http://www.fanews.co.za/article/risk-management/32/general/1218/identifying-risk/17881