93 – November 2007

Intelligence of Fraud

In Criminal Law, fraud is a crime or offence of deliberately deceiving others with the intention of injuring them, usually to obtain belongings or services unjustly. Fraud can also be practised with the assistance of fraudulent objects, by using different means and targeting distinct aims; all of the mentioned categories allowing this type of crime to be classified as scientific fraud, artistic, archaeological, financial, intellectual, electoral, accounting and journalistic, among others.

According to a source specialised in fraud, recent studies have found, for example, that the ancient Egyptians, around 500 B.C., would trick the rich and nobles by selling false cats and other sacred animals embalmed for their funeral ceremonies. By the same token, in Greek and Roman mythology, Hermes, considered the god of thieves and fraudsters, would con other gods and this is why he was always in trouble with Zeus. These and other historical facts prove that the problem of fraud is quite ancient. Obviously, with technological progress, these systems have also evolved. The fraudsters are normally creative, well-informed, flexible and adaptable to new situations, and that is why there are always new types of well-adjusted fraud used at every new opportunity. In the universe of electronic fraud, what we have seen is a considerable amount of professionalism in cons, as well as an increase in the extension of damage caused by this modality. This is especially due to the growth of interactivity between the Real and Virtual environments and to the extent to which cons can reach nowadays. The world is globalised and so are the con artists and we read news about the same con done in North and South America being applied in another continent with subtle adjustments. Whatever the con is, we are always a potential victim. Thus, the best way to avoid the traps and reduce the probability of falling into them is to be well informed. Identifying the intention of the fraudster in advance makes all the difference and studying the intelligence system of the fraud will make you better prepared, and in theory, a less interesting target. In general, the frauds exist due to the coexistence of three basic factors:

- The existence of motivated fraudsters.
- The availability of adequate and vulnerable victims.
- The absence of effective fraud controls.

Explaining the motivation of fraudsters is relatively easy. It may happen because of the deficiency in the prison system, the inefficiency of laws, the lack of regulation, the lack of inspection, the amount of vulnerable victims, the ease of performing frauds, the reduction of fraud costs, and impunity, among others.

Moreover, the existence of fragile and vulnerable victims is due to a series of factors having to do with human behaviour, even though some of the differences are noticeable in different cultures. However, in general, the individuals become vulnerable victims due to the lack of information, ingenuity, not being prepared to deal with the new electronic

environment, the habit of disrespecting laws, greed, trustfulness and ignorance, among others.

The absence of effective controls represents the third factor for the existence of fraud and is mainly due to the lack of preparation of authorities, the legislation, the powers that should be integrated and learn about fraudster's intelligence and foster knowledge of counter-intelligence to act preventively. If we take, for example, electronic fraud done by e-mail, we see fraudsters beginning to exploit the user's lack of technological knowledge, command and make operational errors that would benefit the fraudsters themselves or at least that would open the path for the next stages of the con. However, as the culture of information technology has become more popular, the ratio of effective technological fraud was reduced, which made fraudsters to increase the level of intelligence of their cons. This movement of transition can be clearly observed by the new methods based on personal information or company information and people closely related to the victim, making the con seem as realistic and plausible as possible. It is true that the efficiency of a fraud is directly related to the victim's decision of going ahead, accepting the invitation, believing in the discourse, and thus, acting according to what the fraudster expects. It is also feasible that there are cons so well designed that it would be difficult not to be a victim, but these are a minority. Unfortunately, the human being is vulnerable by nature and their exposure is even greater when other leverage factors are added to the fraud, which are well exploited by the fraudsters. The main one is greediness to obtain more money and other advantages without running the corresponding risks or making the efforts. If you do not fit this profile and you do not want to become the next victim, follow the ten basic tips in case you are facing a doubtful approach:

1. Don't believe everything you hear, see or read;
2. Everything has its price. Always doubt if something is evidently easy;
3. Resist what seems irresistible, until you have made a detailed assessment;
4. Before going ahead, assess the potential impacts and their tolerance to the worst case;
5. Collect as most pieces of information as possible to support your judgement;
6. Use and abuse the Internet to seek information from different sources;
7. Don't lose time with basic cons by learning a bit more about technology;
8. Don't act on impulse or by the pressure of the approach;
9. If it is too late, act immediately and focus on restraining the fraud; and
10. Acquire a preventive conduct by studying the anatomy of fraud.

The theme is interesting and extensive, and for this reason, I will leave the techniques and psychological factors for Christmas time, when the fraudsters put on a white beard and the victims fill their hearts with kindness, which seems perfect for Christmas fraud.
Source: www.fraudes.org

Marcos Sêmola *is Director of Risk Information Operations at Atos Origin, in London, CISM, BS7799 Lead Auditor, PCI Qualified Security Assessor; Member and founder of the Institute of Information Security Professionals of London. MBA in Applied Technology, Professor at FGV with specialisation in Negotiation and Strategy by London School, Bachelor in Computer Science, author of books on information security*

management, governance and competitive intelligence. Visit www.semola.com.br or contact marcos@semola.com.br

N.B.: This article expresses exclusively the personal opinion of the author, and does not represent necessarily the opinion of the company mentioned.