Economics, Management, and Financial Markets
Volume 6(2), 2011, pp. 373–380, ISSN 1842-3191

FRAUD, CORRUPTION AND CYBER CRIME IN A GLOBAL DIGITAL NETWORK

LUMINIȚA IONESCU
luminitaionescu2003@yahoo.com
Spiru Haret University, Bucharest
VIORICA MIREA
viobraga@yahoo.com
Spiru Haret University, Bucharest
ADRIAN BLĂJAN
blajan@contemporaryscienceassociation.net
Institute of Interdisciplinary Studies in
Humanities and Social Sciences, New York

ABSTRACT. Fraud cannot be eradicated, but fraud and corruption risks can be managed like any other risks. The economic crunch created the premises for a substantial increase of the computer crime and fraud. Computer crime or cyber crime refers to any crime that involves a computer and a network, where the computers may or may not have played an instrumental part in the commission of the crime. The global total of criminal gain from cyber fraud is impossible to estimate precisely, but has increased exponentially in the past 4 years. However, in the last few years, the computer specialist and internal controllers understood the fraud schemes and their characteristics and they know how to act to prevent them.

Keywords: fraud, corruption, cyber fraud, digital network

1. Introduction

Bishop and Hydoski show how in today's highly leveraged global economy, major fraud or corruption can set off a chain reaction resulting in serious corporate harm or failure. According to Bishop and Hydoski since the "Crash of 2008" led to economic conditions softening dramatically around the globe, fraud risks for businesses appear to be on the rise.

Their research show how a slowing economy may increase pressure on corporate executives to meet performance goals set in rosier times, or to demonstrate that the current executive team should be retained by shareholders. Individual managers may feel a much greater risk of job loss than usual, potentially making them eager to avoid having to report a performance shortfall in their operating unit.

From all the potential loss, fraud is the most complex and difficult to detect. Fraud represents intentional actions of the part of the client or its personnel to the client's financial statements, assets or both. Fraud is an act of making money by making people to believe something which is not true. Fraud is a deliberate deception perpetrated for unlawful or unfair gain. Fraud is not an unintentional mistake, such as incorrect accounting estimate, the application of a cost to an incorrect account or a lost inventory tag during a physical count. Between fraud and corruption is a strong connection. Most of the fraudsters and scammers are connected to the company or bank, where the fraud is developed. Inside thefts are very difficult to detect, some of them could be part of the management team. Detecting fraud is the purpose of financial control and internal audit for any kind of organization. In the last years, fraud, corruption and computer crime have increased significantly.

2. Cyber Fraud and Solving

Bryan et al. explained about the financial cyber fraud and its development. "Online financial cyber crime has increased exponentially in the past 4 years, forming the foundation of a trend that shows no signs of abating. What began with simple 419 scams and rudimentary phishing has grown into a highly complex underground economy generating professional-quality software tools, legitimate businesses that provide protection to cyber criminals, sophisticated stock-manipulation schemes, and, most tellingly, a sense of community among the criminals".[1]

There are some specific causes that determine the exponentially increasing of the cyber fraud. There are many complexities involved in making sure participants perceive the system as convenient to all involved. Bryan notes that as the total population of Internet users continues to swell, the cyber fraud underground accumulates incentives for its participants to diversify their activities, forming a market with a functional division of labor. This specialization, in turn, allows experts to evolve and to pass their products or knowledge on to others, decreasing the learning time of new entrants.

Bishop and Hydoski claim that as many companies expand around the world to source supplies from other countries, or to expand their sales in emerging markets, they may encounter complex risks for which they may not be prepared. “These risks range from bribery and corruption, to compliance with export controls and anti-money-laundering statutes, to product quality risks that can endanger customers. […] Globalization, in other words, increases the fraud risk management pressures on multinational companies. Each market relationship poses distinct risks that must be taken into account when developing risk strategies.”[2]

Bishop and Hydoski say that it is important to understand personal financial pressures and the personal needs. “Downturns in the economy, such as the global recession that followed the crash of 2008 can make it more difficult for executives and managers to achieve planned results. It also puts more employees under personal financial pressure. Fraud specialists suggest that economic pressures increase the likelihood and the number of individuals resorting to fraud to achieve corporate objectives or to meet personal needs. Financial losses due to fraud are additional costs that companies will have a hard time absorbing, especially in down points in the economic cycle.”[3]

Cyber fraud is strongly connected to corruption and lack of information. Olsen notes that there is no perfect system to prevent the cyber crime. Thus, corruption has a corrosive impact on both overseas market opportunities and the broader business climate. It also deters foreign investment, stifles economic growth and sustainable development, distorts prices, and undermines legal and judicial systems. Olsen notes that corruption is a problem in international business transactions, economic development projects, and government procurement activities.

Olsen identified how computer-related crimes can be grouped into three categories that parallel the three stages of data processing: input tampering, throughput tampering, and output tampering. Input crimes involve the entry of false or fraudulent data into a computer, that is, data that have been altered, forged, or counterfeited – raised, lowered, destroyed, intentionally omitted, or fabricated. Input scams are probably the most common computer-related crimes, yet perhaps the easiest kind to prevent with effective supervision and controls (such as separation of duties and proper audit trails). “Throughput crimes require a knowledge of programming. The publicly reported cases of these crimes are far fewer than input crimes. Output crimes, such as theft of computer-generated reports and information files (customer mailing lists, research-and-development results, long-range plans, employee lists, secret formulas, etc.)

seem to be increasing in this era of intense competition, particularly among high-technology manufacturers."[4]

Olsen explains the value of stored data and the significant benefit for the companies. In the global digital network, a new form of asset has been created: the data held in the computer. Olsen says how intellectual property maintained in computers can be extremely valuable to foreign governments and foreign competition. Other, more intangible assets include valued or confidential programs, scientific data files, confidential financial information, personnel records, client lists, acquisition lists and so on. Olsen writes that companies will greatly benefit from strong adherence to retention policies, and the governance of such policies, for documents and information in hard or electronic formats.

In some research fields it can be hard to find a person who is qualified to analyze the data, and to secure the information. Olsen notes that for information that is extremely confidential or classified, a division of responsibilities will reduce the risk that an entire process, procedure, or strategy will be misappropriated or otherwise accessed in an unauthorized manner. This will also ensure that no one person will possess all the information or knowledge, thus reducing the risk of loss. Information security control officers or custodians can be identified within the organization to ensure that access is limited to those who need access to the information.[5]

There is no perfect system for preventing cyber crime or fraud. Sometimes hackers attack financial institutions or their clientele with email worm. Nemati notes how email worm spreads through infected email messages. It is well known how the worm may be carried by attachment, or the email may contain links to an infected website. Inevitably, when the user opens the attachment, or clicks the link, the host gets infected immediately. "The worm exploits the vulnerable email software in the host machine to send infected emails to addresses stored in address book. Thus, new machines get infected. Worms bring damage to computer and people in various ways. They may clog the network traffic, cause damage to the system and make the system unstable or even unusable."[6] Nemati explains the traditional way of worm detection is signature based. A signature is a unique pattern in the worm body that can identify it as a particular type of worm. However, a worm can be detected from its signature. But the problem with this approach is that it involves significant amount of human intervention and may take long time (from days to weeks) to discover the signature. Thus, this approach is not useful against "zero-day" attacks of computer worm. Besides that, signature matching is not effective against polymorphism.

Masera makes recommendations to ensure the integrity of stored data: (1) The assurance of the information infrastructure upon which modern societies rely is recognized as being of growing importance for citizens, businesses and governments. (2) The social and economic fabric of these societies vitally depends upon the secure and reliable flow, storage and access to information managed through electronic means. A key question that has to be solved is about the challenges that may hinder that assurance.[7] Masera notes that security is the quality or state of a system that keeps anyone person or technical component) from carrying out unauthorized actions that might cause unwanted incidents with potential risky consequences. The unauthorized actions can occur within, with or from the system, and the consequences can be related to assets internal or external to the system. Masera writes that the damage caused by a security breach can derive from unsafe conditions, from the unavailability of services, or from the violation of the confidentiality or the integrity of the data managed by the system. All the cyber crimes could be prevented by increasing security for data and developing the internal control.

Cyber Fraud Model

Bryan et al. observe that the carding underground consists of some resource input (here, account credentials) that is extracted and processed by suppliers (usually scammers), brought to market and retailed by middlemen (carding forum leaders), and finally purchased and consumed by the demand pool (end-user carders). They presented a cyber fraud model that is use more and more often in global digital network. The model explains the process by which criminals involved in such activity first steal account credentials and then refine and market the raw data into readily usable packages of information that “end-user carders” finally purchase before cashing out the accounts or buying high-value goods. It is the most common cyber fraud model with negative consequences in the global digital network.

According to Bryan, within the cyber fraud model several elements could be identified:

1. Phishers, scammers, malicious insiders, and database hackers attack financial institutions or their clientele to obtain account credentials.
2. The acquirer then engages a carding market.
3. Carders in the market sell refined credentials to “account consumers” who may need additional help from a reshipper, money mule, or cash-out provider to turn the account information into actual value.

4. In doing so, the consumer or the agents he or she employs use the credentials to obtain merchandise or currency in the legitimate economy.

This model could be developing according to the market and country where the scammers and database hackers attack financial institutions or their clientele.

The process of creating cyber fraud model is iterative and typically consists of four stages: research and collecting data (R & C) to identify possible scheme; promoters are scammers and middlemen, agents, others, etc. (example: employees); developing fraud model (DFM) – it is a potential of source of profit, develop a pattern that can be implemented and coded; using innocent people who get involved in this fraud model with no intention (IP); collecting funds and goods from victims (FG). The most common fraud is cyber fraud from financial institutions.

Most of the cyber frauds are developed with involvement of the malicious insiders. Insider threats are a real danger for any National Digital Information Infrastructure and Preservation Program. Bryan et al. observe that insider threats are the primary concern of most major organizations. Thus, standard malicious or greedy insiders are more likely to exist as persistent concerns to organizations. Ultimately, the relative frequency of insider and external attacks differs according to the type of attack. The chart shown in Figure 2, from the 2006 U.S. Secret Service/Computer Emergency Response Team (USSS/CERT) E-Crime Watch Survey, illustrates this distinction. In proportion to attacks committed by insiders, these attacks increased significantly in 2005 as compared to the previous year. [8]

We can observe that the theft of intellectual property is dramatically increased, from 16% in 2004 to 63% in 2005 for insider attack. In the same time the theft of intellectual property for outsider attack is increased from 33% in 2004 to 45% in 2005. We consider that insider attack is more dangerous that the outsider attack because could indicate the weakness of the system and could create premises for other future attacks.

Bryan et al. note that the attacks are mostly a matter of employees overstepping their authority and using company resources for nonfinancial gain. Attack means for information gain motives include accessing proprietary and trusted information on customers and other businesses for personal use or for other scammers use. Most of the controllers are concern because the information gain attacks go unnoticed due to lack of auditing capabilities on this type of data, as no direct financial loss occurs. However, companies are liable for information breaches under increasingly stringent laws and guidelines for the safeguarding of personal information.

Here are a few methods to help us to detect a fraud, no matter its size or type: watch the environment, watch the controls, watch employee lifestyles, be available. Corruption became more and more important to investigate nowadays. Globalization and global digital network make controllers job more and more difficult. Financial control and internal audit must to detect any small fraud before scammers will cover their steps. In order to detect frauds, the controllers could use mathematical intuition. Mathematical intuition can be replaced by conventions about the use of symbols and their application. [9]

3. Conclusion

Managing the risk of fraud and corruption requires an ongoing commitment to acquiring fresh knowledge and skills. Quite often this fresh knowledge must be obtained from outside the organization and requires training and involvement. In the global digital network, organized criminal groups constantly evolve new fraud schemes to part companies from their money. Scammers and database hackers develop new twists, taking advantage of new technologies. Bishop and Hydoski note that fraud and corruption risks can be better managed by the financial controllers and auditors, and the practical frameworks for managing fraud risks effectively already exist. However, managing the fraud, corruption and cyber crime requires involvement and help from all employees not matter occupied position in any organization. More then that, preventing and detecting a fraud is possible with involvement of stakeholders and all the partners of the organization. In a global digital network the cyber fraud attacks are dramatically increased based on economic vulnerability models that exist in the market today. This target of the cyber crime attack could be financial data, but also a particular software application, operating system, or piece of hardware. The target could also be the management, a specific corporate or government network. The connection between cyber crime and corruption is complex and is affecting the organization on long term. The resources used by management to prevent fraud include financial resources, human resources and time. In a growing global economy, preventing fraud will be one of the most important objective for governments and companies, as well.[10]

NOTE

This work was supported by the project "Post-Doctoral Studies in Economics: training program for elite researchers – SPODE," contract no. POSDRU/89/1.5/S/61755, funded from the European Social Fund through Human Resources Development Operational Program 2007–2013.

REFERENCES

[1.] Bryan, K. et al., *Cyber Fraud. Tactics, Techniques, and Procedures*, CRC Press, Taylor & Francis, 2009.

[2.] Bishop, T. and Hydoski, F., *Corporate Resiliency. Managing the Growing Risk of Fraud and Corruption*, John Wiley & Sons, Hoboken, NJ, 2009.

[3.] Ibidem, p. 13.

[4.] Olsen, W.P., *The Anti-Corruption Handbook. How to Protect Your Business in the Global Market Place*, John Wiley & Sons, Hoboken, NJ, 2010.

[5.] Ibidem, p. 90.

[6.] Nemati, H.R., "Techniques and Applications for Advanced Information Privacy and Security: Emerging Organizational, Ethical, and Human Issues", Information Science Reference (an imprint of IGI Global), 2009.

[7.] Masera, M., "Systemic Challenges for Critical Information Infrastructure Protection", *II. Mathematics, Physics and Chemistry, NATO Science Series* 196, 2004, p. 57.

[8.] Bryan, K. et al., *Cyber Fraud. Tactics, Techniques, and Procedures*, CRC Press, Taylor & Francis, 2009, p. 56.

[9.] Lazaroiu, G. et al., "Gödel on Conceptual Realism and Mathematical Intuition," *Recent Advances in Applied Mathematics*, University of Harvard, January 2010.

[10.] Bishop, T. and Hydoski, F., *Corporate Resiliency. Managing the Growing Risk of Fraud and Corruption*, John Wiley & Sons, Hoboken, NJ, 2009, p. 23.