Kuzmenko O.A. –
associate professor of economics, Tyumen State University

Dyachkova-Politi A.M. –
BBA in accounting CUNY Baruch College

SOCIAL ENGINEERING AS PART OF THE INTERNAL AUDIT PROGRAM

Introduction

In modern days protection of the financial and corporate information became an every day problem for a lot of companies. Very often loss of the information through leakage of the internal information happens through the employees of the company. In this case, every department becomes responsible for the part of the informational flow and reporting documentation it requires. Development of the documentation of this sort can become a problem due to the invisible at the first sight connections and informational flows between departments and employees of the various positions. Monitoring of the connections and informational flows are often guided by social engineering and managed by the security department or internal audit professionals. This work is considering the methodology and development of the documentation that is targeting developing the records showing accountability and assurance of the social engineering connections. It is meaningful to notice that lately the term social engineering have appeared in a few patents and became one of the discussed at various meetings.

MAIN CONTENT

Social engineering is a new definition widely used in audit and consulting. More often this term is used when we discuss the informational technology testing program for a newly developed software before it goes into production as a part of the quality and anti-hacking observation. We should emphasize that in consulting social engineering has a slightly different direction and includes in addition human resources, information, documentation, psychological maneuvers between humans and some retrospective fact. We can consider fact as an action in the past that has it result in the future. Social engineer usually perceived as a representative of the hackers, however, it could be an employee of the company's internal audit group. As opposite reflection just with the different task that could be described as the development of the internal control structure, forming protective sanctions over the access and spreading the valuable information.

Social environment of the organization has been put into the center of the internal audit group attention. There are various organizations which are ready to participate in formation of the methodology and to educate about the organization of the work with the social engineers. Some of them The Association of Certified Fraud Examiners, the Institute of Internal Auditors, The Association of Certified

Public Accountants are arrange some type of a framework. At the same time there are more and more written publications covering this question have been issued abroad. Most of these studies have been written by the representatives of academia in the areas of the sociology, psychology, and mostly are concentrated on forming a stable organizational structure based on the total or almost total control of the human behavior towards building highly secured informational environment. One of the biggest risk factors is human reaction. It is obvious that there is no way to completely escape the effect of the human activity, reactions, and actions however, it will help to mitigate to minimum, prevent and monitor this part of the organizational informational system. In practice it will bring to a strong control system and supporting procedures.

The international standards give us recommendations and some guidance over the development of the documentation. Some recently published articles have been covering records development and assurance of the effective interaction between the internal audit group and the management of the organization. The most important task for the company is to keep the informational flows, transactions between the subjects of the corporate structure with the lowest/minimal loses. The professionals of the internal audit group with the knowledge of the psychology have an important part in formation of the stable corporate system and conduct the compliance audit targeting to fight with the external representatives of the social engineering.

Forming and conducting the inspection at the organization often arranged by the representatives from the federal governmental representatives from the department of taxation or some consulting companies such as PriceWaterhouseCooper, Ernst and Young and so on. Inspections compare to the mare monitoring include interviewing of the employees, filling out the questionnaires, observation of the transactions performed, testing of the selected transactions, testing of the simulated transactions, description of the control and procedures based on findings.

The employees of the records management department can be helpful in developing the control function. The internal audit department developing detailed documentation beginning from the map of responsibilities to the employees instructions and finishing with the transactions established by the policy for records management. Here we can observe the difference among responsibilities of both departments: the internal audit department responsible for the effective implementation of the policies and the records department is responsible for the quality of the records supporting the corporate governance.

When we talk about social engineering from the practical stand point we have to remind that sometime it is used with the intentional distortion, concealment and omission of the facts with the intent to deceit or to manipulate. Some of such actions lead to damage of the person or a corporation in total. The result of the manipulation can bring to the situation when the crime could be committed in variation of the

degree from leak of the information to corporate espionage when information either sold to the competitors or destroyed completely. The plan of internal control can be developed to mitigate possible situation.

Considering the fact that social engineering is a type of the psychological hacking, we should pay attention to the methodology. One of the most important parts of this particular type of audit concentration of the attestation on minor evidence of the deviation from the corporate standards. This deviations could be summed further and initiate a trend which should be accounted for. When we use general methodology such as interviewing of the newly coming stuff and revealing of the intentions, interests and motivation of the employees. We also, conduct observations of the employees reactions when imitating the similar to reality situations that are either admissible in the corporate culture or could be simulated to defeat the threat. Methodology can vary depending on the technological aspect of the tested function and on non-technological complexity of the function belonging to the survey of the particular employee. At the basis for the testing we are developing maps of the directions and connections for each employee and according connections with the departments of the firm, connections with the other employees, revealing spots that are the most sensitive for the threats. After the connections and informational flows are established we can develop a plan of the functional audit. Quite often victims of the social engineering could be both: management from the employee and vice versa. Employees of the lower positions are susceptible to the social engineering from the management. It depends on the corporate structure and tone at the top. Tone at the top brings together both requirements to the audit and the corporate culture. Both of them define what psychological type of personality can become a perfect fit for current position. Psychology of the employment effects the social side based on the ability to carry the fiduciary duty to the company. In the basis of the tax law lays a doctrine of the burden of proof when tax payer is the one liable to proof his/her innocence. Here it is important to notice the fact of the witness position who see or experience the event, action, goes through some internal cycles. The auditor of the social business processes represents an expert witness and is in a position of trust and neutrality to the company in general and especially when it is a legal matter.

For example, standards of the Institute of the internal audit are naming a few stages for the company's security: management, risk management and system of internal audit. They are usually called three lines of defense. Each line of defense functioning represented and regulated internally by instructions, procedures and rules, which assure their effectiveness. Most part of the documentation is developed based on the amount of risk that company has. The riskiest attributes are tested for leakage and disbursement of the information among employees and departments of the company. The testing is conducted based on the currently enacted regulations. Crucial point at this stage is to involve representative of the participating in testing departments in to brainstorming. The result of such brainstorming could be a put into the base of the testing process together with the internal standards, policies and

the comments from the corporate attorney. After the risks have been identified and all preliminary work for gathering of the information was done, implementation of the first stage procedures can be prepared and executed. The Deming cycle suggests PDCA: plan, do, control/check, act.

After all the work have been accomplished and the procedures have been identified, we can start working with existing differences, intersections between procedures and organization of the procedures into the straight forward areas of managements responsibility and strengthening the controls over the procedures. According to the practice, when analysis of the tested material is finished we can identify new trends and newly formed traits of the risky situation. In this case the frequency of the monitoring and development of the new processes will be considered according necessity. There is a pivotal step in developing business processes to develop graphs, charts, diagrams, schedules and reports which will include dates, areas of testing, results inquired during the monitoring and recommendations how to improve them must be assumed by the management and the board of directors. The graph of the internal audit program standardized for each particular organization separately is forming the controlling environment. Such graph contain of the table with the name of the document, function, responsible for control group or department. Each control group is numerated and this numeration is progressing and graded to the more detailed function: for example 3rd is Human resources department; 3.1 - Hiring, 3.2 - Diagnostics of the newly hires employees, 3.3 Training etc. (see pic.1) . This document allows actively manage informational flow in the company. It can be as detailed as possible or can be presented in the short form. The details that can be added to the schedule is the name of the department, responsible person, date of the development and date or the period when it was renewed. The program of the internal audit should be developed individually for each organization and the alterations should be made according to the necessity of the changes in the function itself and in the level of risk.

Department	Function	Risk level	Responsible position	Type of the work paper
1	2	3	4	5
Human resources department	Hiring Diagnostics of the newly hires employees Training	H-high M-medium L - Low N/A- Not applicable	Name of the position of the internal audit group	Questionnaire identifying the current functions situation, lead testing schedule, schedule of the testing dates, table of the findings and recommendations

Pic. 1 Program of the internal audit, example.

The main target of the thorough documentation is to provide smooth transfer from one stage of management to the next one without severe damage of the documentation flow. At the same time we have to understand that there is a time-value and cost constrains for development of the records control system in the organization and beyond its boards.

We need to underline, how important it is to perform internal monitoring to collect data about employees, their behavior, their sustainability to various difficult decision driven situations. Planned internal audit can also be supplemented with sudden visits deployed to check separate transactions. This method aiming to identify financial shenanigans and other types of arrangements made within the organization that is draining its financial resources out. the quality of the records of transactions and procedures of the records handling can be create a shield for the company from litigation, threats of the potential charges and even criminal actions.

Internal audits usually conducted in two directions. First as part of the constant monitoring program, second are inspections that are conducted after the fact of financial theft, after the financial crime have been committed or as scheduled preventive sanctions.

Monitoring represents the biggest part of the internal audit that challenging all the aspects of the corporate management. It is important to notice that monitoring is a part of the COSO framework protecting management from the risk factors. There is a definition abbreviation widely used CRIME: C-Controlled activities, R risk assessment, I Information and communication, M – monitoring, E - Control environment. This framework is beneficial and used as recommendations and guidance to prevent fraud.

Records with all the necessary attributes to them are representing the quality of the information and shows the legal protection of the company from spreading it secret technologies and internal matters from inner and outer risks. Monitoring function is a constant process that starts with the planning development of the key points that require immediate attention, stages of the information gathering, handling, and writing of the final report. The information gathering stage is the most crucial and requires precise attention. The quality of monitoring function depends fully on the amount of the gathered information, its fullness and define the stability of the processes taken into action.

There was an emphasis in the most recent publications on internal auditors being responsible for the errors, omissions, minor mistakes in the documentation, use of the wrong information. The result of the limited and wrongful information can lead to the gaps in the corporate standards that could potentially bring the company into the situation of the deception. The internal auditors poses a set of tools and skills to conduct the audits and monitoring of the social security in the organization. These type of the audit is testing social side of the business and use wide variety of testing tool as duplicating of the realistic situations close to the real conditions. Security of the information and its parts also includes knowledge about those who

we trust. Such knowledge are forming during the sociological audit. We have to be ready to diagnose various stories about the same situation based on the sociological interview. It allows to estimate the current situation and the result it have entailed. There is a need for a widely arranged testing and constant monitoring when security and protection from the potential risks are the first questions on agenda of the Board meetings. The inspection quite often organized after some illegal acts or in a result of the upcoming legal battle. In this case, scenario documentation and records are two of the most intensive sources of the qualified information for resolution of the situation. When we are discussing a control function, we speak about the systematic process, not just a separate testing of the procedures. For this purpose, it will be beneficial to separate the difference between documented information and operational information. Documented information represents only a part of the informational based on testing of the effectiveness of management. As the result of the inspection, we have an oral story made out of the few stories from the employees and documentation supporting it. It will bring us to the final stage of the clearance of the given situation.

The first pointed task for the internal auditors is to train the employees on how the social engineering can be used to benefit the company, on the other side protect, and secure the company and its financial information. In this case, the employees of the internal audit group can call corporate psychologists. As widely known, people are socialize and trust others to build their relationship, sometimes creating some type of the hold on the future developments by not releasing enough trust. Professional who possess skill of social engineering can otherwise prevent wrongful or intentional situation of the informational leakage without any technical breaking in just based on their skills and knowledge. Organized corporate training and training can prepare employees how to respond to such attacks and stay on top of the human hacking. Such trainings are especially popular in the financial and governmental organizations.

Human is the weakest part of the informational security system because he can become a part of the communication process or a separate scenario. Testing of the behavioral aspect during the audit or lead to the recreation of the truthful story as to what happened. Social engineers or just regular manipulators create a conflict situation when someone is the victim and is madly overlooking the potential outcomes. Thus, some type of the chaos created and the potential victim is losing its trust to others. The manipulator is coming as a hero who helps to resolve the situation that tangled in a realm of problems at the first sight. This hero can even threaten the victim that in case of the violation of the typically oral agreement the fault will draw to the innocent professional. For example, there is a patented program developed by the professionals from the USA that creates some type of the simulations to test the potential outcomes for social engineering networks. As result of such simulations, data obtained may show connections between employees inside and outside the company. For example, based on the level of trust other than owner of the e-mail can have access the classified information or account of the social network. Group of internal auditors should carefully consider obtained this way during the planning

stage of the audit information and account the testing procedures accordingly to minimize this type of the opportunity.

As it was pointed out before, social engineer incorporates malicious information that can be so small lead to the success of the initial deceptive idea. Thus, when we plan and develop the organizational structure we have to consider how it can be protected from such malicious attacks. The more we know about the employee the more protected the firm is from each side. The human resources department can conduct the behavioral testing as one of the functions and use the outcome of the responses for the internal audit tastings. The leakage of the information resulted from the social engineering brings to the wanted outcomes when the employments instructions are either not followed or when the professional subordination is intersecting among the few professionals. Records can be falsified, altered, changed, through away, or even not used in a specific event. On the other hand human factor is considered even when KYC – "know your customer" concept integrated into the management system. Quite often words, format, and quantity of the documentation in transactions allow to establish control after the behavioral aspect as well. There are have been a few scandals in financial world Enron, WorldCom, Medoff that clearly have shown that social engineering sometimes result from network developed and based on the clients commonly known wish to be as much beneficial as possible from the investments made into the company. It have brought legislative bodies to enact the laws and regulations of various levels that have established more clear relationship between supervising employees, management and staff. At this point most of the responsibilities have been targeting the error and omissions that documentation may contain. Another note regarding the practice is that even American internal revenue services have legally require managers and supervisors to take responsibility for preparation quality and even inputting the data into the electronic tax preparation system. Another important for formation of the control environment regulation is the Sarbanes-Oxley Act which not only made management (CEO's, CFO's и COO's) responsible for the effectiveness of the controls but made it also a part of the annual auditors report. Another foreign practice includes use of the general liability and directors and officers insurance policies covering decision making with a due care to the company. However, it is not always guarantee the full coverage of the litigated amount if the litigation was filed against the company.

As the CEO of the International association of the internal auditors has mentioned in his book "Trusted adviser" is not the one who flows the flow but the one who has the power to be ethical to follows the organizational rules. Our human nature sometimes lead us to conduct some actions that open the door to the thieves. There are a lot of the factors and feelings such as kindness that could lead to the ethical dilemma. Mr. Chambers in his book has given a definition to the solution of the such dilemma: "Courage: it is a type of the behavior when person is ready to speak up his opinion and give an advise even if the ideas look not as popular".

References:

1. http://www.intuit.ru/studies/courses/102/102/lecture/2975?page=12
2. https://habrahabr.ru/post/83415/
3. Social engineering: the art of human hacking. Christopher Hadnagy –
4. Uncovering
1. Susan Burch. The three lines in harmony. – Internal auditor., April 2017, p. 51–55.
2. Richard F. Chambers. Trusted Advisors: Key attributes of outstanding internal auditors. – IIA Foundation, Fl., 2017.
3. Robert R. Moeller. Sarbanes-Oxley. Internal Controls. Effective Auditing with AS5, CobiT and ITIL. – Wiley, NY. – 2008.
4. Social engineering: The basics http://www.csoonline.com/article/2124681/social-engineering/security-awareness-social-engineering-the-basics.html George V. Hulme and Joan Goodchild
5. https://www.webroot.com/ie/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering
6. Derek Kortepeter JUNE 21, . http://techgenix.com/social-engineering-human-threat/
7. Deception of Phishing: Studying the Techniques of Social Engineering by Analyzing Modern-day Phishing Attacks on Universitie Date 2016-05-05 Author Walker, Lauren Elizabeth