AGORA International Journal of Economical Sciences, http://univagora.ro/jour/index.php/aijes
ISSN 2067-3310, E-ISSN 2067-7669
Vol. 17, No. 2 (2023), pp. 27-33

POLICIES AND STRATEGIES AIMED AT ENSURING THE SECURITY OF BANKING INSTITUTIONS AND THEIR IT SYSTEMS

M.A. BUTCOVAN, R. IVAN

Marinela Adriana Butcovan[1], Rica Ivan[2]
[1] Romanian Court of Auditors – Bihor Branch, Romania
E-mail: adriana.butcovan@rcc.ro
[2] Faculty of Electrical Engineering & Information Technology, University of Oradea, Romania
E-mail: rika_ivan2005@yahoo.com

***Abstract**: With the development of the banking system, its security and, implicitly, security policies emerged as critical factors in the entire banking sector. In the context of the current technologicaldevelopment, the vulnerability of banking institutions has increased dramatically. For both bank employees and customers, cybersecurity, operational security and data privacy have become top priorities. Therefore, a central concern for banks is the prompt detection of threats and the development of measures aimed at eliminatingsuchdangers, which might both considerably increase the level of security in the banking sector.*

***Keywords:** banking security, banking strategy, fraud, cyber-terrorism, banking system, international transactions, IT security.*

1. INTRODUCTION

In time, the concept of security and its component elements have undergone essential changes, along with the attitude of the states towards the means whereby this notion can be transposed into life, in relation to the changes that occur at the global level.

The term "security", derived from the Latin words *securitas-securitatis*, represents "the state of beingprotected against danger; the feeling of security that one associates with the absence of any type ofrisk". Security also means "protection, defence".

In principle, security represents “that state of affairs that protects any community or country from any external and internal danger, following specific measures, which are adopted and can ensure the existence, independence, sovereignty, territorial integrity of the state and the respect for fundamental interests". (*Mica enciclopedie de politologie*- The Little Encyclopaedia of Politics, 1977)

Starting from the general understanding of security as the absence of physical violence, while progress is seen as material development related to the standard of living in a continuous process of improvement, Mary Kaldor observes that "both concepts encompass the idea ofexemption from fear and the absence of needs" (Marty Kaldor, 2010)

The concept of security applies to all levels in the organization of a society, from the individual to the state andto the international system. Security is based onboth economic and political stability. Thus, a viable security system can only be built if the two components are strengthened. Certainty, trust, and tranquillityare associated not only with the absence of dangers, but also with the idea of keeping them under control.

The banking sector operates in an environment characterized by instability and uncertainty, and losses can generate significant disturbances within the banking sector. The reputation and stability of banks depend on their ability to cope with the unstable economic environment, whether such instability is associated with money laundering, terrorist financing, corruption or fraud, or if it is generated by globalization or economic crises.

In the case of banks, security is an essential issue, being characterised by a state when even the smallest dangers might be anticipated. With the development of the banking system, security and, implicitly, the security policy was categorically imposed in the entire banking system.

Although a remarkable subject, bank security continues to be an impenetrable area, associated particularly with the idea of securing the banking system, but also with other issues. The economic environment is constantly evolving while also being subject to a state of perpetual uncertainty. The economic and banking events of the last period brought to the fore the fact that the accentuation of specific risks generate the problems experienced by the entire banking system. Consequently, credit institutions must comply with legislative acts, norms and regulations that include provisions regarding the security of information. The need to ensure security at the level of the system involves ensuring minimum security requirements for each participant, since the security problems of a participant can affect the functioning of the entire system.

As a result, cyber security is not only a protection factor, but also an element of trust and stability for financial institutions.

2. Policies and strategies regarding the security of banking systems

Any financial-banking operation involves a series of risk factors. Exposure to risk is inherent tothe banking system; therefore, the objective of risk management is to mitigate risk. Only the banks that succeed in accepting and managing risks have the possibility to anticipate the evolution of future events.

The bank security policy is an essential document regarding the security of banking institutions and includes considerable aspects, guidelines, as well as requirements that the management considers appreciable in order to maintain its security. At the same time, it includes a set of rules, norms and procedures that regulate the manner of managing, using, protecting and distributing resources in the banking institution. This policy applies to all activities, processes, procedures, directives, regulations, products, assets and decisions associated with the institution, since they may all influence the secure way in which a bank operates.

When it comes to operations and security, financial organizations should use a multi-level, layered approach, which nevertheless involvesseveral challenges. The pressure to improve and secure IT systems in financial institutions is enormous, since cyber-attacks on banks are on the rise.

The policy of the authorities and the obligation of the banks is to disclose and prevent the trafficking of illegally obtained funds. The threat of terrorism is a problem for all of humanity. This phenomenon is hard to detect because the sources of funding can be both illegal and legal. Those who intend to prepare various terrorist attacks seek to find new

sources, relying on the vulnerability of the financial and banking system, but also that of the legal system. In most cases, financial transactions are neutral; they come to the attention of specialized institutions only when suspicious persons are involved.

As far as money laundering is concerned, this phenomenon, which has already acquired an international character, leaves even deeper traces not only in the activities of banking institutions, but also in their image, which represents a crucial factor. Criminals, in their attempt to hide values gained from illegal acts, make use of banking institutions, by means of bank transactions. Thus, illegally obtained profits are "laundered" much more easily. However, the damages resulting from the crime of money laundering affect the economy worldwide. With the development of organized crime, the profits obtained also increased, and the banking circuit has become involved into the transfer of illegally acquired funds; for those involved in money laundering, technological progress has been a means whereby financial advantage can be obtained.

The banking system is, without a doubt, one of the economic systems dramatically affected by financial globalization. In their attempt to cope with all the changes in the economic environment, banks sought to implement new strategies and policies; their purpose was to protect themselves from criminals and the risks associated with the activities carried out, but also to survive the competition.

Crises, along with other social phenomena, become problematic only when they affect the social order, and their effects can no longer be controlled. These crises negatively affect the entire economic system. Along with it, the banking system has also suffered from desecurization and destabilization caused by these crises.

Most banking institutions, as well as other types of institutions, have recently operated in an environment characterized by uncertainty and instability, and the destruction or losses can cause serious disturbances to the activities of the institutions concerned. Considering the crime situation at global level, which has accentuated dramatically, while also taking into accountthe IT system, geographical location, and the community of employees and customers, the banking system is more exposed and vulnerable than other economic systems. The banking institution, as actor on the capital market and credit institution, is exposed to vulnerabilities. Therefore, a significant part of its activity requires special security measures.

In order to solve security- related problems, many innovative schemes have been developed (Singh & Malhotra, 2004; Rombel, 2003). Some authors have proposed the inclusion of biometric features in authentication schemes (Arumuga, 2006).

Maintaining banking stability and security is a fundamental requirement for the successful conduct of banking operations, but also a requirement that must be treated with particular care. The consequencesgenerated by either natural disasters or the human factor have shown that it is hard to anticipate the totality of the potential causesthat might generate an undesirable event. Instead, it should be pointed out here that the damage caused by these disasters can be compared in terms of value to the destructive effects of cyber-attacks.

Banking institutions that do not have a well-developed security policy, according to the standards in force, may face situations that negatively influence their existence and reputation, and the resulting effects also impact their financial situation.

The security policy must provide support, inspire credibility, but also demonstrate efficiency in the efforts that banking institutions make with the view of protecting their

resources. Maintaining the security of a banking institution is the daily task of every bank employeewho holds a position of either executor or bank manager, in conformity with the duties of their specific position and related skills. In order to ensure its security, the banking institution in question will proceed in accordance with the legal regulatory framework in force. Every standard, recommendation, and good practice, experience and information that can contribute to improving security will be evaluated and appreciated.

3. IT security in banking institutions

In the current global business environment, where information systems have effectively penetrated all organizations, the importance of information technology is widely accepted and recognized. The increasing dependence of most organizations on information systems, in conjunction with the risks, benefits and opportunities they bring, make information security control a critical component for the general administration of the organization.

Information is a vital resource of any organization and must be protected accordingly, by ensuring confidentiality, integrity, and availability. In the interconnected business environment, information is currently exposed to an increasing number and a much wider variety of threats and vulnerabilities.

Nowadays, information security is a fundamental pillar in the banking environment. Banks face various and multiple threats, caused by internal or external factors. Financial institutions must ensure the protection of data relating to corporate customers, clients' personal information and their financial resources. In the absence of security, the trust of customers and business partners can be easily compromised or lost. In addition, risk management and compliance requirements must be assessed constantly.

The deterioration of the economic situation, together with the inefficient activity of the institutions responsible for the financial security of the country, will affect the quality of assets in the banking sector and generate new challenges for financial institutions. At the same time, the volatility of the foreign exchange market and the low trust in public and financial institutions represent a risk for the stability of the banking sector.

Risks can have an obvious impact on the value ofboth financial and banking institutions, dueto its effects on staff, partners, clients, or the banking authority, or because it might take the form of direct losses. In the banking sector, risk should be understood as a conglomerate of threats, which are often interdependent and might have common causes. At the same time, the emergence of one type of risk can generate the appearance of a succession of other risks. (Gheorghe Manolescu, Adriana Sîrbea Diaconescu, 2001)

When it comes to operations and security, financial organizations should use a multi-level, layered approach that presents a number of challenges. The pressure to improve and secure IT systems in financial institutions is enormous, with cyber-attacks on banks being on the rise.”

Both financial institutions and consumers agree upon the fact that financial fraud and attacks are becoming more complex, since they are perpetrated by a different class of criminals, who use increasingly sophisticated methods, where technology is part of their

strategy. Moreover, experts predict that the current global crisis is likely to increase the frequency of internal fraud and security breaches.

Banking institutions must focus on preventing security events as the best means of ensuring security. In order to establish security, a bank must develop a clear and consistent regulatory environment, but also avoid exceptional procedures. When customers are inquired about their expectations in relation to the banking institution they work with, two aspects are generally mentioned: security of operations and cyber security, as well as confidentiality of information.

The need for the cyber-security of banking institutions has increased simultaneously with the total computerization of banking activity. The implementation of an IT security policy gives the management of a banking institution the security of a quantifiable and controllable system.

Computer system vulnerabilities are basically weaknesses that can be exploited by a possible threat at any time. Thus, we can say that information security is not only a technical problem, but also a managerial problem.

Following the emergence of situations related to criminality in the banking cyber system, as well as customer panic, banking institutions have increased their measures and efforts to protect the IT infrastructure. Maintaining IT security has never been more important than now. There are more sophisticated and lethal cybercrime trends that the banking sector should pay attention to. Internet fraud is currently the most practiced type of fraud at international level. The phenomenon is booming, correlated with the increase in the number of users and, at the same time, in electronic transactions.

These events can cause financial damage, IT infrastructure damage, but most importantly, reputation damage. In such cases, banking institutions should not wait for legislation or government decisions to find solutions to suchproblems but reactpromptly instead. (Cindy Collins-Taylor, 2013) Investments in software and hardware solutions, however, remain a necessity, as by such means institutionsare ablerespond quickly to IT threats. And the training and testing of both employees and customersmay contribute to reducing computer fraud.

Concerns for IT security increased in direct proportion to the increase in the number of users, but also in the value of transactions made by banking institutions.

Along with technological development, the security of information systems has also developed. At the same time, attackers managed to develop their skills and opportunities to penetrate deeper and faster into information systems, the effects of their actions being most often particularly serious. Thus, it can be stated that computer security is a constant and continuous process, because in order to increase security, one should always return to the starting point.

Innovative technologies and ideas constantly require an update of the IT security policy. Once connected to the Internet, banking institutions become more accessible to the public, but also vulnerable, in the face of unforeseen attacks, caused by unauthorized penetration into the IT system.

In order to achieve the protection objectives of the IT system, banking institutions must hire reliable personnel, who have the necessary skills and qualifications, while also being prepared for critical events. The continuous training of employees who use the

computer system is also of significant importance, so as they might constantly update their knowledge and reaction skills. The employees should also receive information about new methods used by cybercriminals with the view of penetrating the banks' IT system. Each user of the IT system is responsible, in one way or another, for ensuring the security of the data. A well-implemented and selected IT security strategy can help the institution avoid undesirable events, with impact upon the information resources of a banking institution.

The security requirements are constantly changing due to the developments of the banking system in recent years. Such prerequisites include the expansion of electronic communication channels with customers and partners, the electronic payment system, the reporting systems to the National Bank of Romania, the development and integration of payment systems, etc. In this context, in addition to the individual demands that relate toensuring information security, there is also the issue of the risks that a properly unsecured component induces in the system and the need to ensure the safety of the entire banking system.Each banking institution, in part, must implement its own information security system. Its management can be achieved by implementing practices, tools, procedures, policies, organizational structures, or software functions. Following the emergence of situations related to criminality in the banking cyber system, which generate panic among customers, banking institutions have intensified their measures and efforts to protect the IT infrastructure.

Maintaining IT security has never been more important than now. Sometimes, the banking system might encounter difficulties in controlling the increasingly sophisticated and lethal cybercrime trends. These events can cause financial damage, IT infrastructure damage, but most importantly, reputation damage. In such cases, banking institutions should not wait for legislation or government decisions to find solutions to these problems, but to react immediately. Investments in software and hardware solutions, however, remain a necessity, so as banks might be ready to respond to cyber threats. And the training and testing of employees, but also the instruction of customers, is a solution to reduce computer fraud.

4. CONCLUSIONS

In the current climate, banks are called upon to implement strategies and business models that make them stronger and more competitive in a market heavily involved in innovation. At the same time, they must strengthen customer trust and loyalty.

Most often, companies avoid sufficient investment in IT security because their perception is that the threats do not justify a very high level of expenses. However, the costs of a computer breach and the loss of confidential data, as a result of large-scale cyber-attacks, arevery important issues. The creation of a security culture is essential to any organization. This can be achieved by the continuous instruction and training of the staff, through permanent collaboration with partners for a common approach to security issues, and by constantly making customers aware of the risks regarding information security.

The security of the computer system can be increased by building and improving collaborations between banking institutions, governments and institutions specialized in combating computer crime. It is also important to adapt the national security strategy to these cyber issues, as well as to expand IT security in order to support both banking and national or global security.

Banking institutions must determine and develop IT tolerance, in a context where protection will never be enough and tolerance should be high. Depending on the level of risk and protection, the level of investment necessary to reach the comfortable level of protection is determined. But no one knows the cost associated with the aim to reduce the risk.

According to the commitments assumed, Romania has undertaken measures to develop the national normative framework in the field of cyber security, harmonized with the provisions of EU legislation, which will meet international requirements, facilitate bilateral cooperation and the exchange of information among the competent authorities.

To fully ensure the safety and security of critical data and systems, financial institutions should use a robust privileged access management solution in order to protect both themselves and their customers against attacks. Since it is necessary to comply with this large number of regulations, standards and requirements, information security must be considered a crucial concern for the organization, which requires the involvement of the management at the highest level and the active engagement of all the structureswithin the organization, from professionals in the domain to the final users of data.

REFERENCES

1. Arumuga, S., 2006. Effective method of security measures in virtual banking. Journal of Internet Banking and Commerce [online], Available at: http://www.arraydev.com/commerce/JIBC/2006-04/VB.asp

2. Cindy Collins-Taylor, New Cyber Security “Rules of the Road” for the Financial Services Industry, Television, April 2013, p. 2, www.aspenpublishers.com

3. Dumbrava, Dumitru, Agresiunile în spațiul cibernetic (Aggressions in cyberspace), in Revista Română de Studii Intelligence (Romanian Journal of Intelligence Studies), No. 06, 2011;

4. Gheorghe Manolescu, Adriana Sîrbea Diaconescu, Management bancar (Banking Management), Bucharest, The Publishing House of the Foundation “România de Mâine”, 2001, p. 123

5. Lică-Banu, Laura-Susana, Apariția și Proliferarea finanțării terorismului (Emergence and Proliferation of Terrorism Financing), Bucharest, Universul Juridic Publishing House, 2010;

6. Marty Kaldor, Securitatea umană (Human Security), Editura CA Publishing, 2010, p. 39;

7. Mica enciclopedie de politologie (The Little Encyclopedia of Political Science), Enciclopedic Publishing House, Bucharest, 1977, page 402;

8.Nagy, Agnes, Benyovszki, Annamaria, Provocările crizei asupra sistemului bancar (Challenges of the Crisis on the Banking System), Theoretical and Applied Economics, Vol. 20, No. 4 (581), 2013;

9. *** Manual de management al fraudelor în activitatea de creditare (Handbook on the Management of Fraud in Crediting Activity), 2012;

10. Rombel, A., 2003. Next step for Internet Banking. [online]. Available at: http://www.gfmag.com/archives/87-87-february-2003/2176-features--next-step-forinternet-banking.html#axzz0IhUm79xl;

11.Singh, B. & Malhotra, P., 2004. Adoption of Internet banking: an empirical investigation of Indian Banking sector. Journal of Internet Banking and Commerce, [Online]). Available at: http://www.arraydev.com/commerce/JIBC/9909-05.htm