IMPROVING THE BANK INFORMATIONAL SYSTEMS SECURITY IN THE REPUBLIC OF MOLDOVA THROUGH IMPLEMENTATION OF INNOVATIONS

Stela CIOBU, assoc. prof., Ph.D., AESM
e-mail: stela.ciobu@gmail.com

Banks should always take into consideration the fact that when informational security masterminds think they developed the best informational security systems, the cyber criminals will always be a step forward. This reality should be recalled daily in order to ensure the best informational protection, and banks, as the most valuable field in the state and economy, should be obliged to keep up with the best informational security protocols.

There are five key factors are contributing to the increasing vulnerability of banks' information resources, making it much more difficult to secure them: (a) the evolution of the informational systems' resource from mainframe-only, today's complex, interconnected and interdependent, wirelessly networked business environment; (b) modern computers and storage devices continue to become smaller, faster, cheaper, and more portable, with greater storage capacity; (c) the computing skills necessary to be a hacker are decreasing; (d) international organized crime is taking over cybercrime and (e) lack of management support. With these factors keep growing and developing, it became an urge for banks to establish the security of their informational systems as one of their top priorities.

After analyzing the international experience, the following steps should be undertaking in order to ensure the security of the informational system of the bans of the Republic of Moldova:

- adopt a risk-based approach of the informational systems: the most severe banking risks in this century – the risks of the informational systems;
- work towards improving the national legal framework related to the banking informational security field;
- get informational security governance right - the greatest security prevention tips and action plans come from a proper corporate governance: from top management to the regular employees, everybody should acknowledge their responsibility on keeping information safe;

- establish and rationalize access control models for applications and sensitive information – the best protection against threats and vulnerabilities begin with proper access control management;
- identify the existing weaknesses and address them –banks of Moldova must make efforts to address them efficiently as soon as possible, because cyber threats are developing on daily basis;
- develop secure products and services – before launching new products or services, banks must be sure that they are cyber secured and fully protected against the existing risks and threats;
- invest in the best hardware and software security solutions –it is very important to keep technology up-to-date, as threats and vulnerabilities are developing with a tremendous speed;
- continuously educate employees about security best practices of informational system management – employees which have the proper informational security training are the basis of the informational security management in banks;
- educate and inform their clients about the potential risk and threats and the ways they can pass them by – bank's customers should be also aware of the existing risks and threats and to understand the responsibility they have when using banking products or services which involve informational systems;
- Live CDs or Linux integration - banks should think about alternative methods of ensuring the security of informational system, like isolating the PC/operating systems on which transactions are performed from the regular PC or operating systems, because this software isolation contributes to a higher protection against threats and attacks;
- cooperate with other banks or informational security experts;
- consider organizing specialized informational security competitions – Moldavian banks could benefit from the knowledge exchange during these competitions, and both identify their weaknesses and address them, and find skilled experts;
- biometrics implementation – the largest Moldavian banks seem more than prepared to innovation implementations, and the usage of biometrics not only will ensure them a higher level of security, but will improve their reputation. In order to take in

consideration this possibility, banks should at least cooperate with Moldavian telephone network providers and/or international manufacturers of biometrics enabled ATMs and POS-terminals for finding the most cost effective and secure solution.

The implementation of these technologies seem more like a strategic purpose of Moldavian banks, rather than a measure that could be implemented in the following years. However, this does not exclude the fact that Moldavian banks are not capable to prove that they can develop and implement high technologies at the same level as international banks. The decision of introducing biometrics in enhancing bank's informational security could become one of the greatest turning points into increasing customer's confidence and increasing bank's profitability overall, and this kind of results are worth the resources invested in them and created large benefits and opportunities to the whole banking system, not only for one particular bank from the Republic of Moldova.

Bibliography:

1. European Union Agency for Network and Information Security Threat Landscape 2014, Overview of current and emerging cyber threats. Heraklion, Greece 2013. 70 p. ISBN: 978-92-9204-112-0.

2. Forget fingerprints – banks are starting to use vein patterns for ATMs [online], [quoted 22.12.2016]. Available: http://www.theguardian.com/money/2014/may/14/fingerprints-vein-pattern-scan-atm.

3. Planet Cash: Europe's first biometric ATM shared network launched in Poland based on successful collaboration between ITCARD and Hitachi [online], [quoted 18.12.2016]. Available: <http://www.hitachi.co.uk/about/press/pdfs/Press_Release_Hitachi_ITC_14%20May%202014%20FINAL%20r.pdf>.