Державний вищий навчальний заклад
«Українська академія банківської справи
Національного Банку України»

Препринт серії № UABS MEN/2014/024

Лопаткіна І.В., к.е.н., доцент кафедри менеджменту

THE EVOLUTION OF INFORMATION SECURITY STRATEGY IN BANKING INDUSTRY

I.V. Lopatkina, *PhD, Department of Management SHEI "Ukrainian Academy of Banking of the National Bank of Ukraine" in Sumy*
V.G. Lopatkin*, MBA program / Lincoln University of California (Oakland, USA)*

In the aftermath of the recent financial crisis global banking system has faced an array of required fundamental structural changes. Stricter financial; regulation together with lowered trust on the clients' part has generated the need for banks to invest in certain practices and policies that have long been abandoned. Information security is one of these areas that is being increasingly scrutinized by the governments all over the world.

Information security has always been one of the banking industry's highest priorities. Banks always realized that information and its integrity were some of the most important and sometimes valuable assets they have. However in the past several years banks realized that the depth of the risk structure has significantly increased and the old "information security" problem has acquired a number of new facets. As a part of international consolidated effort to move to a more viable, flexible and stress resistant financial industry banks all over the world embarked on developing and implementing the new strategies not only in the area of core business functionalities but in information security as well. According to multiple research strategic changes in this area are more often than not mandated by the executive level decisions rather than through and bottom-to-top approach. It has been noted that over 70% of decision making in the area of informational security has been a result of bank wide regulatory policy. This creates a more transparent and manageable environment for cooperation within banking industry and supervision from the government and non-government institutions.

It is important to note that not all the banks have realized the importance of developing a relevant data security strategy. Some organizations deal with potential risks on a "first come-first serve" basis, rather than proactively developing safeguards against potential issues in the future. It can be safe to assume that in most cases lack of strategy is caused by the fact that these banks have not fully recovered from the recent crisis and have yet to deal with more vital issues. In this case adapting strategies of other banking organizations could be a viable solution.

Understanding the structure of the potential risks and sources of risks is quite important. Multiple scandals in banking markets across the globe (most notorious reported in the United States and Great Britain) have revealed the new "enemies" of the information security and integrity. Historically banks have been using most of the resources to defend against the external threats. It is quite logical since even these days, external threats (hacking attacks, server failures, data lost in transactions etc.) constitute over 70% of total risk volume. However the internal causes have started playing an important role as well. Despite the fact that banks have done a great job in automating their business operation (specifically paper circulation) there is still a large share of work that is dependent upon the human input, analysis and processing. This in turn opens potential for user generated errors and potential data leakage. As multiple examples in the United States and Great Britain show, one person in charge of a significant portion of data can undermine a decade long process of information security protection. Client information represents one of the most valuable pieces of data banks own and it can be leaked relatively easily without proper policies being implemented. gregation of duties on workplace have been implemented in banking system ong time ago, but apparently current situation requires additional layers of protection.

Banks have also recognized the importance of the risk generated by banks clients. Clients represent a backdoor to banks vault like data security systems since they often underestimate the amount of information they hold. Without being fully aware of the consequences of inadequate data protection and potential damage that can be done if their information is hacked clients undermine banks information security efforts. Thus banks need to educate their clients on the importance of data security and make them a more integral part of the bank's data security system.

As it was mentioned before, government supervision plays its important role as well. Understanding the magnitude of the current threats, as well as awareness of the sources and direction of these threats can enable banking system to better manage the risks. Government can serve as a supervisor consolidating the policies and strategies within banking industry and across markets. One example of such supervision is the law implemented in some states in the United Stated that mandates all banks to report fraudulent activity and instances of data breach. As much as banks are tempted to resist such legislation, it is important to implement it to prevent the localized risk from becoming systemic.

Banking industry is entering its new round of rejuvenation after the devastating financial crisis of 2008-2011. Information security has acquired an important place in the ranks of the banking industry priorities. As each bank strives to develop the most impenetrable data security system on their own joint effort is a key to ensuring that the best practices are being implemented industry wide. Government role is essential as it could help consolidate cooperation within the industry and across markets and geographies.