Юридична Газета Multimedia online
ВСЕУКРАЇНСЬКЕ ЩОТИЖНЕВЕ ПРОФЕСІЙНЕ ЮРИДИЧНЕ ВИДАННЯ

Cyber security in the bank sector: can IT outsourcing help?

Anastasiya Pavlovska
«Sayenko Kharenko, ЮФ» Associate

Zarina Khalimon
«Sayenko Kharenko, ЮФ» Junior associate

Recently, the functioning of information systems in the world has revealed the problem of insufficient protection against computer viruses. BadRabbit, WannaCry, Petya and others unexpectedly surprised and paralyzed the computer systems of various institutions and enterprises. Their developers, although they had different purposes and methods of implementing viruses, have been basing their efforts on common ground - the shortcomings and weaknesses of cyber security systems. The mechanism of action of the virus Petya, which in a few days caused millions of dollars of losses both to Ukrainian businesses and government institutions, is the most illustrative in this issue. The virus affected a popular accounting software program M.E.Doc., gaining access to the administrative rights controlling computer systems and freely distributing its own copies.

Banking institutions were not an exception, even though they may have seemed to be protected by modern technical security systems. The worldwide experience of virus attacks and significant financial losses should have inevitably stimulated financial institutions to search for gaps in their own systems of cyber protection and engaging in constant updating. However, 2017 year has shown the unwillingness of Ukrainian banks to protect themselves from such interventions in their information systems. A general assessment of the events of 27-29 June 2017 shows that 70% of Ukrainian banks to some extent have been affected by the virus Petya. The consequences of such attacks were the following: stopping the work of terminals, payment systems, bank branches, as well as limited access to Internet banking and international transfers. Although banks continue to argue that attacks had a negative impact only on the infrastructure of the Windows system and the virus did not receive access to personalized customer databases, nobody can be sure that a more "sophisticated" program will not be able to do this.

The fact that banks did not withstand cyber attacks leads to the conclusion that the problem lies not only in the IT department of each individual bank. Underestimation of potential threats, lack of proper software and neglect of proper budgeting for the cyber security systems of banks - all this points to the lack of a systematic approach to cyber security.

NBU resolution No. 95 and its consequences

On 28 September 2017, the National Bank of Ukraine adopted resolution No. 95 "On Approval of the Provision on the Organization of Measures to Ensure Information Security in the Banking System of Ukraine" *(the "Resolution")*, which obliged banks to take measures during 2018 to strengthen their cyber security. This act contains two stages:

1. till 1 March 2018, banks have to carry out organizational changes, such as the mandatory creation of a collective body on the issues of implementation and functioning of information security management systems *(the "ISMS")* in order to ensure representation of the members of the bank's management and appointment of a responsible person for information security, as well as to update their basic information security systems and bring them into compliance with the International standards ISO/IEC 27001, ISO/IEC 27002 *и* PCI DSS, which are the basis of the Regulation.
2. till 1 September 2018, banks have to carry out additional measures to enhance information security – work with media carriers, the functioning of bank servers and the use of centralized monitoring tools.

The most significant changes were due for implementation by 1 March 2018. First of all, it is important for banks:

1. to ensure proper distribution of the rights of access to information systems of the bank and the frequency of their control;
2. to ensure the use of multi-factor authentication mechanisms;
3. use of appropriate encryption standards;
4. provision of centralized management of the bank's network;
5. provision of appropriate levels of documentary processing of information security processes.

Thus, within a few weeks, banks should be prepared to submit their updated cyber security systems that are required to comply with more than a hundred requirements of the Regulation.

At the same time, the Resolution does not prescribe special sanctions for violations of established requirements. However, according to the Article 73 of the Law of Ukraine "On Banks and Banking Activities", it is possible to distinguish several types of sanctions for the violation of banking legislation that can be applied precisely where failure to meet the requirements on improvement of cyber defence systems are identified:

1. written prevention;
2. restriction, suspension or termination of certain types of activity performed by the bank, including transactions with related parties;
3. imposition of fines;
4. temporary removal of the bank official from position (until the violation is resolved).

Written prevention is likely to be the initial type of sanctions to be imposed by the NBU in case of detecting a non-compliance with the provisions of the Regulation and provides for a further additional period for the introduction of new cyber security systems. In the event of further systematic failure to meet its obligations, banks will risk restrictions on certain types of activity that are most vulnerable to the consequences of cyber attacks or the temporary dismissal of officials directly responsible for implementing the provisions of the Resolution on the activities of the bank. Moreover, the functioning of such banks will attract the attention of the NBU, because the bank's unwillingness to protect its information systems from possible cyber attacks poses a real threat to the personal data both of customers of the bank and the entire banking system.

Implementation IT outsourcing

Are banks ready to independently develop, finance and introduce all the necessary measures in such a short time? After all, such innovations require both significant financial expenses and the involvement of qualified IT specialists. Although the search and implementation of the software itself do not provide for significant challenges, it is much more difficult to find specialists who could conduct a competent assessment of the system's shortcomings and the associated risks for cybersecurity. Whereas the market of international integrating companies (for example, Windows) have a full range of necessary software and hardware, the market of national specialists in the field of cybersecurity remains quite narrow.

Hence, not every bank maintaining its own IT department will be able to withstand the next virus attack. Nevertheless, the strongest security factor for the bank remains preparatory work, as well as the continuous updating of systems and the analysis of deficiencies that require a comprehensive assessment by a subject matter expert.

Other negative factors which affect the capacity of banks to independently improve their own systems of cybersecurity include:

1. "inadequacy" of expert opinions of IT departments on the introduction of modern methods of protecting information systems;
2. significant financial expenses for the employment of subject matter experts;
3. inappropriate implementation of international ISO standards;
4. insufficient external independent assessment of the bank's security systems.

This is why IT outsourcing for banks becomes increasingly popular as the fastest way to bring information protecting methods in compliance with the Regulation. First of all, such services are offered by several IT companies which conduct general technical audits and assessment of the regulatory maintenance of the bank’s protection systems. Such an assessment primarily includes a “penetration test”, which is aimed at identifying the technical weaknesses of information systems and determining the list of required protection systems.

However, is this assessment sufficient to identify all potential risks? A preliminary comprehensive audit is indeed a determining factor for understanding the weaknesses of the information systems of the bank, but is only the first stage towards assessing all possible risks. Along with the information and technological aspect, it is also necessary to assess the risks of management and legal regulation that affect the general policy of the bank on information security assurance.

Unfortunately, an assessment of regulatory maintenance alone is not able to identify all the risks of improper work of personnel on information security assurance and, in general, the attitude of the bank's administration to preventing attacks on information systems.

Thus, the cybersecurity of the bank requires a comprehensive, well-planned, step-by-step project to improve its protection systems. This should include three main approaches to identify threats to the functioning of information systems of the bank:

1. technological – first-priority audit, implementation of updated security methods and further optimization of the entire IT infrastructure of the bank - with the aim not only to eliminate shortcomings, but also to prevent them in future;
2. personnel and administration development – at this stage it is necessary not only to confirm the proper regulatory support of the operation of information systems, but also to carry out further explanatory work with personnel. On the other hand, this step will engage the top management of the bank for better understanding of all the possible risks of the further cyberattacks and sanctions of the NBU for non-compliance with the provisions of the Resolution;
3. legal groundwork that would allow for proper regulation of the confidential relationships between the bank and the IT company.

The development of such an integrated project would help to establish long-term relationships between banks and specialized IT companies which render services in the field of cybersecurity. Even though the implementation of measures bringing the information systems of banks into line with the provisions of the Resolution is quite possible by certain IT companies, it remains the case that further protection from possible cyberattacks will not be fully provided. After all, only continuous work on preventing viral threats can protect banks from possible material losses.

There is a need for banks to understand that the NBU's sanctions are the least significant threat to their operation and existence compared with a viral attack which can strike personal customer databases and lead to more extensive consequences for the functioning of the entire banking system.