Neobanks Operations and Security Features

Conference Paper · October 2019

DOI: 10.1109/PICST47496.2019.9061268

3 authors:

Larysa Gorodianska
National Taras Shevchenko University of Kyiv
18 PUBLICATIONS **20** CITATIONS
SEE PROFILE

Nosenko Tetiana
Borys Grinchenko Kyiv University
5 PUBLICATIONS **10** CITATIONS
SEE PROFILE

Viktoriia Vember
Borys Grinchenko Kyiv University
32 PUBLICATIONS **73** CITATIONS
SEE PROFILE

Neobanks Operations and Security Features

Gorodianska Larisa
Department of Financial Support of Troops
Military Institute of
Kyiv National University of Taras Shevchenko,
Kyiv, Ukraine
gorod_lv@knu.ua

Nosenko Tetiana, Vember Viktoriia
Department of Computer Science and Mathematics
Kiev Boris Grinchenko University,
Kyiv, Ukraine
t.nosenko@kubg.edu.ua, v.vember@kubg.edu.ua

***Abstract*—There is a steady tendency in the world to increase the level of use of the latest information technologies in the financial sphere, in particular new forms of banks - digital and neobank are gaining popularity. Such a business is promising, attractive to young people, people from remote places, so it is actively developing and is already a subject of interest of cybercriminals. Modern banks use open application programming interfaces to ensure the reception and transmission of information between information systems of different organizations through standard data transmission protocols. The use of open application interfaces affects the information security of banks, namely the security of information assets. Attackers who attack neobank information systems want to gain control of the information assets in order to further engage in illegal transactions or compromise the bank at the request of unfair competitors. Therefore, information banking systems must be protected against threats to internal and external interference and implement a comprehensive security strategy. This strategy should provide security and include technical solutions and procedures that will protect the security of all components of neobank information systems - electronic payment systems, electronic workflow, payment card services, banking software systems, remote systems, networking and more. The banking system security strategy must ensure high-performance processing of large volumes of information without loss of speed, tool collection, incident data analysis and response to security events, as well as reliability and fault tolerance.**

Keywords—digital bank; neobank; Application Programming Interface; information security of the bank; the latest information technologies; innovations.

I. INTRODUCTION

The processes of globalization of the international economy, the development of Internet and digital technology contribute to the active attraction of innovations to the banking sector and the emergence of virtual forms of banks that have gained popularity in the world and in Ukraine. Currently, there is a steady tendency in the world to increase the level of use of the latest information technologies in the financial sector. Current bank customers live at a fast pace and do not have the time and desire to visit the banks. Internet communication and mobile applications are their choice and lifestyle. In conditions of significant competition, banks are forced to actively innovate, develop modern information strategies for business development, attract investment and invest in developing new types of communication with customers. Banking services are increasingly moving into virtual space.

One of the first banks that began customer service with the use of telephone in 1989 was the British First Direct Bank, applying the concept of work without offices. Banks without banking centers have been called neobanks or challengers, unlike conventional banks, which are also actively using modern information technology in their business, so they are usually called digital.

Analysis of recent studies and publications. The peculiarities of the functioning of digital and neobanks in Ukraine and in the world were studied by domestic and foreign scientists: Barclay Ballard [1], Nathaniel Popper [2], V.S. Morina, Ezangina I.A. [3], CrouwdfundUp team [4], E.I. Bulatova, V.A. and Shein [5], M. Kovalev, and G.Golovenchik [6], A.T. Kearney[7], N. Panthilieva, S. Krinitsia, [13], H. Arslanian, F. Fischer [15] and others.

There are different interpretations of the "neobank" definition. For example, neobank is considered a kind of direct bank, which is 100% digital and serves customers through mobile applications and personal computers. Digital banks are just the online player of a larger bank in the financial sector, while the neobanks are completely digital, and they operate independently of traditional banks [8]. Neobanks work through software that facilitates the administration of accounts and credit cards and is fully based also on the mobile platform. They do not have typical bank branches and affiliates that can be visited, and exist exclusively on the Internet. Due to the use of state-of-the-art IT technologies, neobanks provide services at cheap rates, their processing time and delivery algorithms are significantly reduced, new types of activities appear, such as financial robot-advisers, P2P lending, crypto currency [8].

Neobanks are virtual form of banks that actively use modern gadgets, including mobile platforms. Such a business is perspective, attractive for young people, people from remote places and cities, other categories of users, therefore, it is actively developing and is already the subject of interest of cybercriminals.

The problem statement. Modern banks use the API to provide reception and transmission of information between the information systems of different organizations through standard data transfer protocols. The use of open APIs affects the information security of banks, in particular the security of information assets. Criminals who attack information systems of banks, including neobanks want to gain control over their information assets with a view to conducting illegal operations or compromise the bank at the request of unfair competition. Therefore, the problem of safety of non-bays, their protection against threats to the internal and external environment is acutely raised.

The article's goal is the disclosure of the features of the neobanks operation in the conditions of globalization and assessment of factors that affect the security of the bank.

978-1-7281-4184-8/19/$31.00 ©2019 IEEE

II. THE THEORETICAL BACKGROUNDS

Digital and neobanks have their own characteristics (table 1) and, unlike traditional banks, offer more attractive services to customers. In particular, they provide higher rates and minimum fees compared to competitors, since the neobanks have the ability to minimize their own costs due to the withdrawal of bank branches. In addition, custom software (mobile applications, sites and networks) has an intuitive and easy interface - the quality and variety of services depends on it. This includes, for example, the ability to get instant approval of credit applications and other documents or blocking an account with a single click of a button. Neobanks use artificial intelligence to track expenditures and can send warnings to their customers, check their transactions in real time, quickly detect and respond to fraud cases.

TABLE I. FEATURES OF FUNCTIONING OF THE LARGEST DIGITAL AND NON-BANK IN THE WORLD

Name of the bank	Date of establishment	Branch	Web-banking	Provision of services through:	Security measures	Country of registration
Atom Bank	2014	-	-	Mobile application	Voice, face Recognition	United Kingdom
WeBank	2015	-	-	Social Network WeChat, Mobile application	Face Detection	China
MYbank	2015		+	Mobile application	Face Detection	China
Simple	2009	-	-	Mobile application	Face Detection	Argentina Serves the United States
N26	2015		+	Mobile application	Face Detection	Germany
FidorBank	2009, 2015		+	Mobile application Payment system Ripple	Face Recognition	Munich, United Kingdom
StarlingBank	2014	-	-	Mobile	Face Detection	London, United Kingdom
MonzoBank	2015	-	-	Mobile Application	Face Recognition	United Kingdom
Tandem Bank	2013	-	+	Mobile Application	Face Recognition	United Kingdom

The number of neobanks in the world as of 2016 is presented in Fig.1.

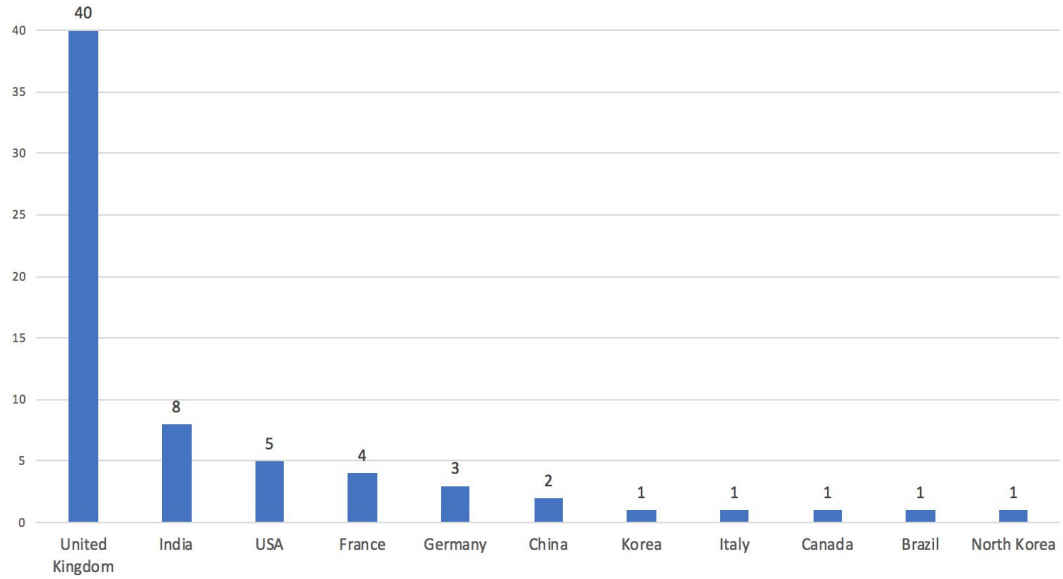

Fig. 1. The number of neobanks as of October 2016, according to Forbes

According to data [10], neobanks have a significant potential (see Fig. 2). Banking information systems store and process a large amount of data on finances and activity of individuals and legal entities, have financial transaction management tools that lead to financial consequences and cannot be completely closed, since they must meet modern requirements to the level of service (to have an online banking system, a network of ATMs, connected to public communication channels, etc.).

Since 2010 banks have started opening information that has previously been considered a bank secret using the API (Application Programming Interface), which allows for the receipt and transmission of information between information systems of different organizations through standard protocols [11].The main consumers of the open API are business application developers (startups) and financial and technical companies that sell their customers with innovative services integrated into banking services.

By using the open interface of the API, banks expand the channels of representation of their financial products and services, and, consequently, increase the client base. Through access to open source software, rival banks are able to avoid possible errors, as well as track trends in banking services.

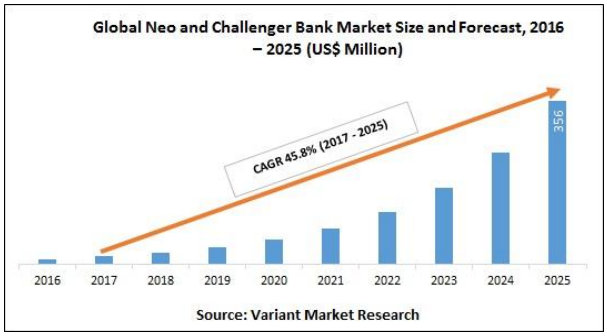

Fig. 2. Forecast for the development of the global neobanks market for 2016-2025 (millions of US dollars) [10]

Cybercrime destroys the principles of safe existence and interaction of all subjects of information relations, especially in the banking field. In connection with the growth of digital and neobanks cyber-threats, the incidents in the field of remote banking services take the first place in the world [11].

The use of the open APIs affects the information security of banks, namely, the state of the security of all their information assets.

The diagram presented in Fig. 3 shows that startups for neobanks occupy only 0.4% worldwide. At the same time, they currently have 5.3% in the Ukrainian segment [12]. This suggests that such FinTech-business in Ukraine is promising, and it will be actively developing, and therefore is the object of increased interest of cybercriminals [13]. Criminals, that are attacking information systems of banks, including neo, want to gain control over their information assets to further commit unlawful transactions or to compromise the bank to order unscrupulous competitors.

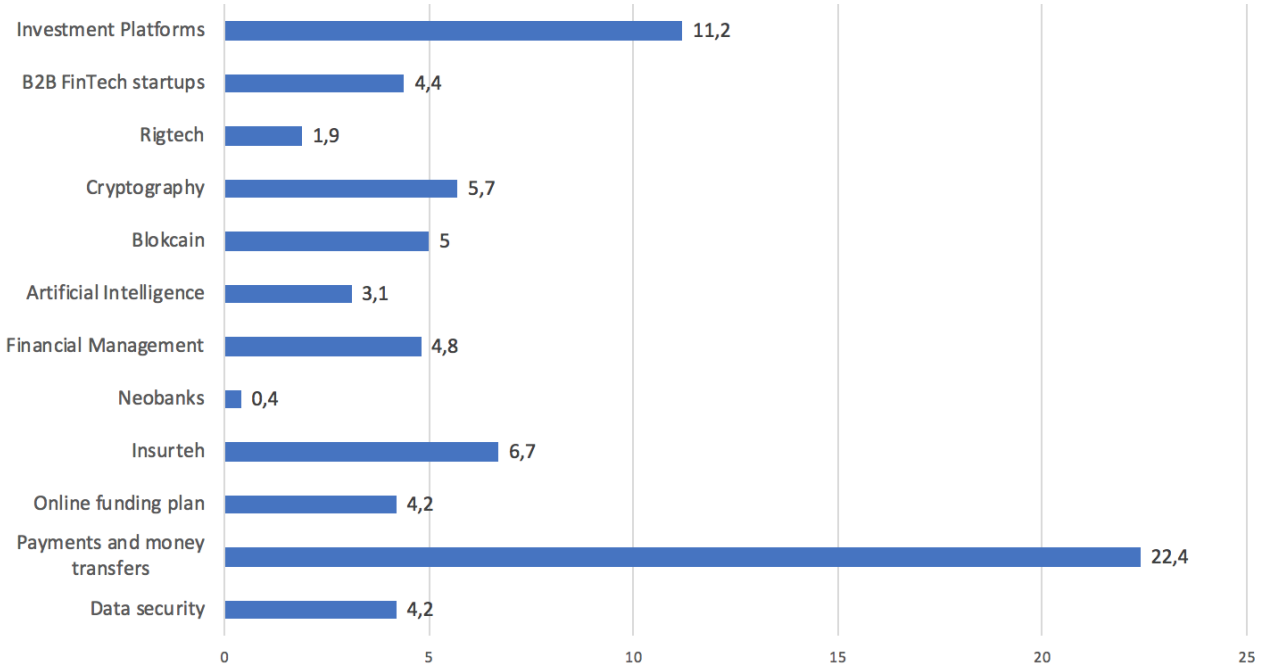

Fig. 3. Distribution of financial and technical startups by types in the global trend % [1

III. THE RESULTS

The work [13] summarizes possible threats to security in key information infrastructure systems. Modern digital banks and neobanks as their constituent are impossible without IT. Therefore, the threats connected with unauthorized access to data and information infrastructure by means of information technologies are at the forefront (Fig. 4).

Systemic information security measures can minimize risks [16], [17] (Fig. 5). The authors believe that ensuring the proper level of security of digital banks and neobanks must necessarily be of a systemic nature, and requires consideration of foreign and domestic experience, requirements of the current legislation, external and internal risks and observance of the basic directions of security [16], [18], [19].

IV. CONCLUSION

Thus, digital banks and neobanks security systems must adequately meet internal and external threats and provide an integrated approach to protection, namely: to include all necessary organizational and technical measures, to protect all components of the information systems of banks (electronic document management systems, servicing of payment cards, electronic payments, banking software, software and hardware complexes, remote maintenance systems, communication networks, etc.), provide high-performance workflow of large amounts of information without loss of performance, collecting tools, analyzing incident data and reacting to security events, being reliable and resistant to failures.

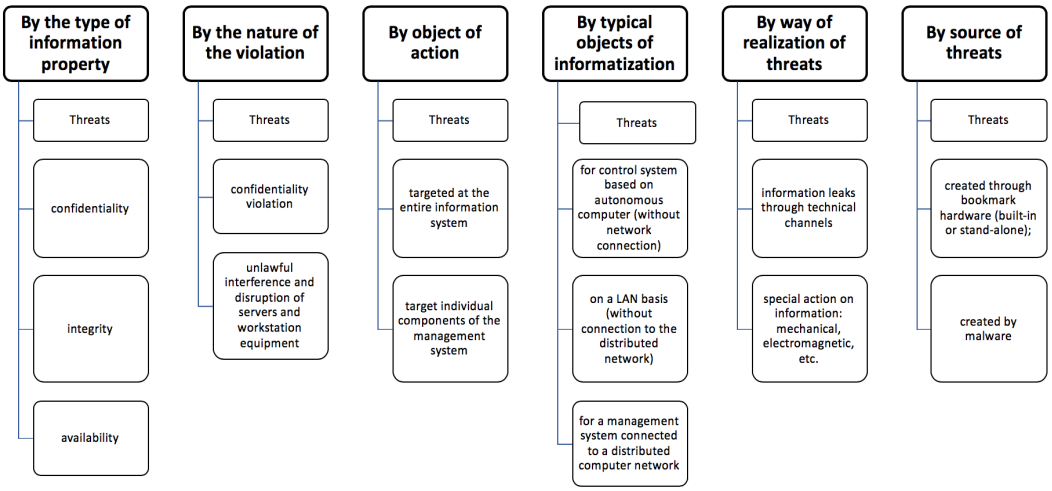

Fig. 4. Classification of threats to information security of digital banks and neobanks

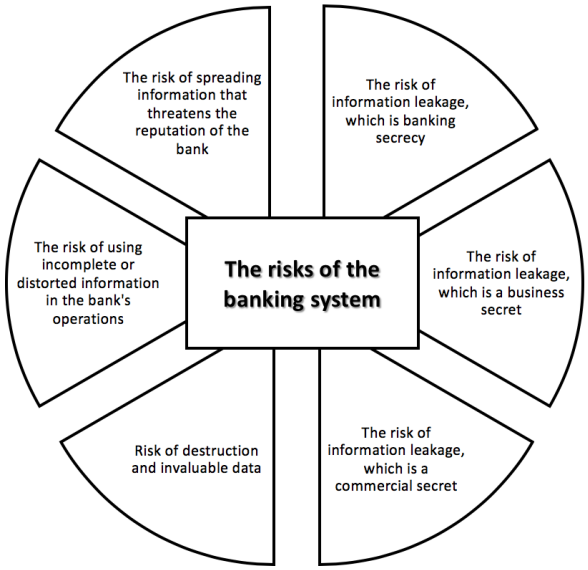

Fig. 5. Risks of the bank's information system

REFERENCES

[1] Barclay Ballard, "The unstoppable rise of neobanks," World Finance, Dec 2018. [Online]. Available: http://bit.ly/2GS1Zmn

[2] Nathaniel Popper, "The 'Neo-Banks' Are Finally Having Their Moment," The New York Times, Nov 2018. [Online]. Available: https://nyti.ms/2Tjmm0T

[3] V. S. Morina, I. A. Yezangina, "Neobank as an institution for the implementation of modern innovative technologies in the financial sector," Scientific almanac, Apr 2017. [Online]. Available: http://bit.ly/2ZNemaH017.04.01.191.pdf

[4] Crouwdfund Up team, "What is a Neo Bank and how are they disrupting traditional banking models?," Medium, Jun 2018. [Online]. Available: http://bit.ly/2ZNemaH

[5] E.I. Bulatova, V.A. Shein, "Neobanking as an Innovative Model for the Development of Modern Banks,". *Kazan Economic Newspaper*, Jan 2018 no. 33, pp.7-28.

[6] M. Kovalev, G. Golovenchik, "From financial companies - to digital banks. Banks and the Digital Economy," Aug 2018. [Online]. Available: http://bit.ly/2Kroq46

[7] A.T. Kearney, "Banking in a Digital World," ATKarney and Efm, 2013. [Online]. Available: http://bit.ly/33l5DPc

[8] M.Gudova, "Digital Banking and Neobanks," FinTech News, Sep 2018. [Online]. Available: http://bit.ly/2YSWu12

[9] Aditya D Menon, "Future of Banking," CEO Tallyx Inc., 2018. [Online]. Available: http://conferences.lafferty.com/doc/D317741.pdf

[10] Crouwdfund Up team, "What is a Neo Bank and how are they disrupting traditional banking models?," Medium, Jun 2018. [Online]. Available Available: http://bit.ly/2KFniIH

[11] Wellsoft, "How open API banks change the financial world," Hubr, Aug 2018. [Online]. Available: https://habr.com/ru/post/420253/

[12] Kovalenko V.V., "Development FinTech: threats and prospects for the banks of Ukraine," Priazovsky Economicman, 2018. Available: http://pev.kpu.zp.ua/journals/2018/4_09_uk/24.pdf

[13] N. Panthilieva, S. Krinitsia, "FinTech, Transformation of financial intermediation and financial stability," in *International Scientific and Practical Conference on Infocommunication Problems. Science and technology* (PIC S&T), 2018.

[14] Yu. Vasiliev, "Classification and analysis of threats to information security in key information infrastructure systems. Legal, normative and metrological provision of the information security system in Ukraine," [Online]. Available: http://pnzzi.kpi.ua/29/29_p56.pdf

[15] H. Arslanian, F. Fischer, "Fintech and the Future of the Financial Ecosystem," *The Future of Finance. Palgrave Macmillan, Cham*. 2019

[16] ARinteg, "Information security system of the bank," ARinteg. 2019. [Online]. Available: https://www.arinteg.ru/articles/informatsionnaya-bezopasnost-bankov-26722.html

[17] V. Lemeshko, O. S.Yeremenko, N. Tariki, "Improvement of flow-oriented fast reroute model based on scalable protection solutions for telecommunication network elements," *Telecommunications and Radio Engineering*. 2017. Vol. 76, Issue 6. P. 477–490

[18] O. Oxiyuk, I. Tereikovskiy, "Fundamentals of problems in the cloud authentication", in 4th *International Scientific-Practical Conference Problems of Infocommunications. Science and Technology* (PIC S&T), 2017, pp. 596-599.

[19] Gorbenko, M. Yesina, V. Ponomar, "Anonymous Electronic Signature Method,", in *Third International Scientific-Practical Conference Problems of Infocommunications. Science and Technology* (PIC S&T), Kharkov, Ukraine, 2016, pp.47-50.