Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 169 (2020) 314–319

Procedia Computer Science

www.elsevier.com/locate/procedia

Postproceedings of the 10th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2019 (Tenth Annual Meeting of the BICA Society)

New cyberattacks vectors of Russian critical infrastructure enterprises: domestic private banking sector view within AI protection methods

Alexey Gusev[a,*]

[a] *National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe shosse 31, Moscow 115409, Russia, Department of cybernetics*

Abstract

The growing anti-Russian sanctions list can seriously change the situation within the cyber threats priorities for Russian enterprises of critical infrastructure, demonstrating in recent years the advanced rates of development directly associated with the practice of import substitution. The introduction of the most advanced methods of protection against possible cyberattacks should be carried out taking into account the imbalance in the corporate strategy of Russian business evolution: between the current level of corporate relations development, and the existing methods of IS. Thus domestic private banking solutions can be quite successful with effective protection against cyber threats.

Keywords: Information security; Cyberattacks; Information security management, private banking; VIP-clients; anti-Russian sanctions.

* Corresponding author. Tel.: +7-916-959-63-31.
E-mail address: AIGusev@mephi.ru

1877-0509
10.1016/j.procs.2020.02.189

INTRODUCTION

The outstripping rapid of the accelerated development of Russian critical infrastructure and industry enterprises related to the implementation of import substitution practices turn them into a potentially attractive target for cyber attacks and significantly increasing the overall level of cyber threats. Russian business that has not previously encountered serious cyber attacks will have to develop and implement adequate IS measures in a short time. Thus, the paper's goal is to present the possibilities for building effective protection against cyber threats, in which it is necessary to take into account not only the Russian practice of building successful IS techniques, but also prime features the development of corporate relations development.

Such unadequate IS measures makes them the most attractive target for cyberattacks not only in the near future, but even now. Hense, the most interesting now are AI solutions from domestic private banking within its target customers - owners of Russian industrial enterprises.

1. THE OVERALL LEVEL OF CYBER THREATS TO THE RUSIAN INDUSTRY ENTERPRISES COULD GROW SIGNIFICANTLY

New vectors and new methods of IS for critical infrastructure enterprises (especially in the Russian industry sector), have recently become the subject of a separate, very close and substantive discussion and not only at specialized conferences. This year, such topics were for the first time discussed at financial conferences in Moscow related to the specifics of domestic private banking development (especially at the 9th Adam Smith Institute's "Wealth Management & Private Banking Summit — Russia & CIS" summit in late April 2019 and at "Intax Expo Russia 2018" in September). They became the subject of serious discussion not only on the specialized IS sections, but also on round sections devoted to various aspects of client policy, tax planning and development strategies of the entire Russian private banking market in general, with the active participation of the author as not only a participant, but also a moderator within these events.

Among the issues directly related to cybersecurity, the most actively discussed topics were the revision and reassessment of priorities in the analysis of vulnerabilities and the subsequent construction of an effective protection of the external and internal perimeters of the enterprise. Moreover, this problem reflects the position of not only the corporate structure of IS of industrial enterprises, but directly of a private banking unit, focused on the long-term service of this particular enterprise within the framework of banking services and extremely interested in increasing the demand for its own services by finding ways to stimulate demand for IS solutions to the mutual benefit of both parties, not excluding the business of the client itself – as the owner of the enterprise.

The traditional private banking approach of building long-term customer service here, through the establishment of long-term relationships with him, in this case implies a more thorough substantive analysis of the long-term corporate needs of the owner, after which he is offered appropriate solutions from the private banking product line. And the solutions, primarily designed for the same duration and constant support, ensure the continuity of business development, to which are now added various IS methods, both of the private banking department and its contractors. And it is precisely the point of view of private banking that allows us to look at the organization of corporate structure of IS in a different way, that is much closer to the current needs of the local business.

In fact, in the past few years, the main risks in terms of IS, have been associated with other sectors of the economy and areas of cyber attacks that are more profitable for attackers This trend will continue in the near future, if we analyze the general trends of cyber threats according to the annual IS reports and forecasts over the past few years from SANS, PriceWaterhouseCoopers, Kaspersky, Positive Technologies and Group IB. And even despite the obvious intensification and complication of attacks against critical infrastructure (with certain attacks on energy companies in recent years), all of this does not look so dramatic against the background of quantitative and qualitative growth of cyber threats in general.

When building effective protection against cyber threats in Russia, this still allows, as a matter of priority, to implement -made basic solutions from other sectors of economy that are more susceptible to cyber attacks. And only then slowly adapting these well tested and easily replicable solutions to the specifics of critical infrastructure and

industry enterprises. That, in itself, is much preferable to the initial development and implementation of narrower and more expensive niche specific solutions, especially now, when the overall landscape of attacks on critical infrastructure by attackers largely coincides with the landscapes of these sectors.

In addition, it allows to use well-tested and long-established critical infrastructure enterprises IS solutions as a basis for the same protection of industrial enterprises Moreover, the implementation of fairly stringent requirements of such solutions, when adapting existing both Russian and Western standards, within the overall growth of cyber threats and weak attacks upon industrial enterprises at the same time, allows us to work out different approaches for building effective protection nowdays, not only for the nearest future. Especially taking into account the adaptation of western experience in the protection of critical infrastructure enterprises where the total number of such attacks is greater.

However, the growing anti-Russian sanctions list can seriously change the situation within the cyber threats priorities. With each new phase of sanctions, the various discussions on the impact measures taken and those already taken, especially the assessment of their effectiveness, are becoming more public and accessible. So at the end of September 2018, Assistant Secretary of the Treasury Marshall Billingsley informed the US Congress Subcommittee on Financial Services and Trade of the House of Representatives of that the Russian economy is too large and well integrated into the international financial system, therefore the effect of comprehensive sanctions, as it were with respect to Iran or the North Korea, it will not be reached [4]. Moreover, there has been a significant growth within individual industries, sectors, and even specific enterprises of the Russian economy, and the current effect data can be compared with earlier ones, for example, mid-2015 data, when, for examle, Nobuo Sugahara from Japan Business Press already noted that if the Russian machine tool industry continues to develop at the same pace, western sanctions will lose all meaning in an article with the equally significant title “Sanctoins leading to a Russian industrial renaissance” [6]. This information on advanced development allows us to consider critical infrastructure and industry enterprises as if not one of the priorities, then at least one of the main cyber attack targets, with a corresponding reassessment of the degree of importance of cyber threats. And consider these enterprises as a means for further penetration into this sector of the economy, especially by novice, yet less professionally trained cybercriminals.

2. Domestic private banking solutions can be quite sucessful

Are Russian critical infrastructure and industry enterprises ready for such cyber attacks? Do they have enough safety margin to reflect the first trial, as well as the subsequent ones, if only the first ones prove successful, much stronger and more complex cyber attacks by more skilled groups of intruders with more advanced tools for targeted penetration?

In fact, Russian industry enterprises which prefer to use now well-tested and long-established critical infrastructure enterprises IS solutions as a basis for the same protection of industrial enterprises, will face attacks from a new groups of sophistcated attackers who previously ignored them. Moreover, they are already beginning to face this, as it follows from the above-mentioned assessments of domestic private bankers, who are forced to react such threats faster than traditional IS vendors. Besides, new IS solutions of domestic private banking for t protection of its target VIP-clients will be suitable for the other owners of Russian industrial enterprises.

The case is that it is the owner of medium-sized industrial enterprises, with real assets (just the wealthy person with whom it is preferable to establish long-term financial relations) since the beginning of the 2000s. is a long-standing and successful client of Russian private banking and quickly turning from the category of potential VIP-clients into the most preferred and target category of VIP-clients. Initially, the wealthiest Russians at the top of the wealth pyramid, representing traditional categories of domestic VIP clients from among the owners of the largest Russian private companies, officials and top managers of state-owned companies are too loyal to their own financial structures and banks in which they are already serviced, their attraction for service in a new bank, is too individual and expensive. Therefore, private banking was forced to pay special attention to representatives of alternative, less wealthy categories of VIP-clients, primarily to private owners of smaller and medium-sized industrial enterprises, with more transparent and replicable methods of attraction. In order to effectively such an owner, the domestic private banking has moved to manage not only of his personal fortune, but also his business, having evolved into a so-called “corporate loyalty program”, thus building his own positioning. The personal wealth and business of the owner is considered here together as the total capital of the VIP-client. This immediately provides good opportunities for the implementation

of complex capital servicing projects, especially now in a period of economy stagnation, when through the continuity of business processes, it is possible to provide longer-term service, establishing with the client the very long-term financial relations, to which the domestic private banking seeks for this target VIP-client category[1].

The corresponding positioning has proved useful not only in relation to other players in the banking sector, but also to financial advisors, offering specialized services, though more preferable to a wealthy client, but who consider his capital less aggregate. First of all, this manifested itself in solving complexly structured (essentially the same complex capital servicing projects), requiring the involvement of external companies-contractors, as well as taking into account the long-term consequences of recommendations provided to the client as a business owner. For example, when conducting an audit of the organizational and management structure of a business with its subsequent adaptation to new financial needs. The latter task turned out to be very popular on the part of the Russian owner, whose business is characterized by an artificially complicated hierarchical, less commonly networked corporate structure in the form of a set of functionally related Russian and foreign legal entities. What is more typical for private owners of not very large and medium-sized industrial enterprises, including critical infrastructure enterprises, considered domestic private banking as the target category of VIP-clients [2].

Such an owner prefer to make decision of not only strategic, but also operational issues on himself, at best - on a limited circle of people who are not necessarily professionals, but whom he trusts. Usually these are relatives, classmates or old friends, less often - time-tested employees or partners for past business, and, only as a last resort, their own employees, hired employees-professionals. Despite the high internal costs of maintaining such an excessive and suboptimal organizational and management structure in certain cases, it is quite successful in ensuring the stability of the business, especially when trying hostile takeovers (especially by the state and state-owned corporations), as well as in a crisis situation (for example, when the business owner takes a loan not for the entire business, but for part of it, then writes off the loan and also comes with losses, written off for the forcibly bankrupt part of the business structure). Since 2009, almost continuous stagnation in the Russian economy has led to a steady decline in business margins and the emergence of a steady demand for optimizing the costs of maintaining the organizational and management structure. The need to optimize it has become obvious, although incomplete: the owners were ready to bear, albeit reduced, but still substantial enough, internal costs, which still ensure their sustainable development of their own business.

And here the domestic private banking was able to offer its customers quite competitive optimization services [3]. The fact is that by this time the loyalty of the business owner grew so much that it allowed him, practically the only one among the other players of the banking sector and financial consultants, to get almost full access to the previously closed and carefully protected organizational and management structure of the business. A high degree of trust from the target VIP client has provided private banking with the best opportunities to effectively identify redundant and non-optimal elements in organizational and management structure that could be safely removed. Moreover, if necessary, private banking could involve external companies-contractors to solve individual, more specialized tasks, while retaining overall control over the optimization procedure as a whole. Later, the owner got a demand for defoshorization of his business, and again it was necessary to carry out incomplete optimization of organizational and management structure of his business, where private banking was able to fully adapt all its previous developments on optimization services. Then two capital amnesties were announced (the latter was not over yet), and the anti-Russian sanctions mechanism was launched. This provided the domestic private banking with quite comfortable conditions for further improvement of methods of optimization of the corporate structure and further positioning itself as the main consultant not only for a narrow group of owners of industrial enterprises, but also for other VIP-clients, outside this target group, including those not previously considered – from the wealthier categories.

Furtermore the demonstration of trial, test solutions for the organization of an effective integrated cyber defense of the external and internal perimeter for the entire capital of the owner is quite a good way to demonstrate all the possibilities of effective transition from the development and implementation of ready-made IS solutions to solutions for optimizing organizational and managerial structuree in the tasks of ensuring inheritance rights [4].

As already mentioned, domestic private banking need to learn how to protect not only the client, but also his family members, traditionally - top-managers of owner`s corporate structure. Traditionally the owner prefer to make decision of not only strategic, but also operational issues on himself, at best - on a limited circle of people who are not necessarily professionals, but whom he trusts. Usually these are relatives, classmates or old friends, less often - time-tested employees or partners for past business, and, only as a last resort, their own employees, hired employees-

professionals. Despite the high internal costs of maintaining such an excessive and suboptimal organizational and management structure in certain cases, it is quite successful in ensuring the stability of the business, especially when trying hostile takeovers (especially by the state and state-owned corporations), as well as in a crisis situation (for example, when the business owner takes a loan not for the entire business, but for part of it, then writes off the loan and also comes with losses, written off for the forcibly bankrupt part of the business structure). Since 2009, almost continuous stagnation in the Russian economy has led to a steady decline in business margins and the emergence of a steady demand for optimizing the costs of maintaining the organizational and management structure. The need to optimize it has become obvious, although incomplete: the owners were ready to bear, albeit reduced, but still substantial enough, internal costs, which still ensure their sustainable development of their own business.

And here the domestic private banking was able to offer its customers quite competitive optimization services [3]. Moreover, if necessary, private banking could involve external companies-contractors to solve individual, more specialized tasks, while retaining overall control over the optimization procedure as a whole. Later, the owner got a demand for defoshorization of his business, and again it was necessary to carry out incomplete optimization of organizational and management structure of his business, where private banking was able to fully adapt all its previous developments on optimization services. Then two capital amnesties were announced (the latter was not over yet), and the anti-Russian sanctions mechanism was launched. This provided the domestic private banking with quite comfortable conditions for further improvement of methods of optimization of the corporate structure and further positioning itself as the main consultant not only for a narrow group of owners of industrial enterprises, but also for other VIP-clients, outside this target group, including those not previously considered – from the wealthier categories.

In the end, the owner is inclined to underestimate the level of cyber threats, which opens up good opportunities for appropriate pentesting of the external perimeter of his business, with subsequent rethinking of its components. That is why domestic private banking is beginning to actively raise issues of reassessing vulnerabilities and protecting the external and internal perimeters of critical infrastructure and industry enterprises. The goal is obvious - it is necessary to find in the person of the owner a partner who will be interested in optimizing a part of organizational and managerial structure to build an effective cyber security system. Private banking may well attract more specialized external contractors from the IS sector, which it has repeatedly demonstrated earlier on the example of no less complex and requiring a high degree of trust from the owner of optimization tasks.

In this way successful full protection against cyber threats is not only the technique of working with new group of stakeholders (protection of the tablet of the sister of the owner, who is still the chief accountant of one of his company’s categories in the holding’s structure)/ It is the task for well-known otimisation of organizational and managerial structure of the owner`s industrial enterprise, and with the same complexity metods which f domestic private banking implemented earlier within several tax amnesties.

Nowadays conservative domestic private banking can use AI solutions in order to find analogies of structure optimiation for the same industrial enterprise (or group of them) which used it earlier fot tax amnesty. At the 9th Adam Smith Institute's "Wealth Management & Private Banking Summit — Russia & CIS" where author was moderating “Digitalization and other technological disruptors in the private banking industry” section we discussed the firsts results of implementation Convolutional neural networks methods within ML. Besides, domestic private banking prefer not to hire unique data analysts yet because this year is the first when we spaek about several attempts to use ML for such complex problems as structure optimiation. That` s why the initial choise of such methods is based on previus experience within IBM Watson, widely used at european private banking for wealh advise. So, this system is being actively implemented now at investmet departments of domestic private banking, and some test tasks can be solved at corresponding area of structure optimiation. Even first test results demonstrate the potential of such approaches. But the further development of such methods will depend on additional free support of IBM Data Asset eXchange with free datasets for ML, that can stimulate domestic private banking to think about creating a separate AI unit or all-over ML prolems witin VIP-client advisory service.

That allows domestic private banking effectively solve not only private, specialized IS tasks, but with full access to its organizational and managerial structure to design and full protection against cyber threats of the entire business, and further, the entire capital of the owner as a whole. In addition to solving the tasks demanded by the owner, all this is a completely acceptable marketing move, which allows to increase trust and to offer the owner further solutions to more interesting private banking tasks to ensure inheritance rights, amnesty, etc. And sooner, after such proving that he can effectively replace the owner`s current private banking unit, he attract him for further service as a new VIP

client for himself.

CONCLUSION

The introduction of the most advanced methods of protection of Russian critical infrastructure and industry enterprises against possible cyberattacks should be carried out taking into account the imbalance in the corporate strategy of Russian business evolution: between the current level of corporate relations development, and the existing methods of IS. Thus domestic private banking solutions can be quite successful with effective protection against cyber threats with AI solutions within its target customers - owners of Russian industrial enterprises.

References

[1] Gusev A.I. “Rossijskij private banking: zapas prochnosti ischerpan // Upravlencheskij uchet i finansy (*Russian private banking: the margin of safety is exhausted*)”. *Upravlencheskij uchet i finansy*, 2017, vol. 46, no. 2, pp. 82–95. (in Russian).

[2] Gusev A.I. “Novye prioritety v upravlenii riskami pri restrukturizacii biznesa: opyt rossijskogo private banking (*New priorities in risk management of business restructuring by targeting interest of large industrial enterprises owners within Russian private banking*)”. *Upravlenie finansovymi riskami*, 2018, vol. 53, no. 1, pp. 44–51. (in Russian).

[3] Gusev A.I. “Sankcii protiv sostoyatel'nyh rossiyan sovsem ne pugayut VIP-klientov rossijskogo private banking (Sanctions against wealthy Russians do not scare VIP-clients of Russian private banking)”. *Bankovskoe delo*, 2018, vol. 297, no. 11, pp. 20–26. (in Russian)

[4] Statement of Assistant Secretary Marshall Billingslea Before the U.S. House Financial Services Subcommittee on Monetary Policy and Trade. Available at: https://home.treasury.gov/news/press-releases/sm496 (01.08.2019).

[5] N. Sugahara Sanctoins leadingTo a Russian Industrial Renaissance // Japan Business Press. Available at: http://jbpress.ismedia.jp/articles/-/50159 (01.08.2019).