NEW TRENDS IN INSURANCE INFORMATION SECURITY TECHNOLOGIES

Stanislava Veselovská[249]
Eva Jančíková[250]

https://doi.org/10.31410/itema.2018.652

Abstract: *Innovations in the information security technologies within financial institutions represent very important criteria in the competition. They are part of the success at the financial markets as they provide information about the client. Innovations into a suitable information system secure the stability of the insurance portfolio and safety for a client before discreet information outflow. An appropriate processing of the project and keeping of right principles in the field of the projection and implementation of the innovative security technologies and by application of the SkyMinder service the insurance company secure enough information about the client, his commercial partners and a sufficient security for the client. The aim of this paper is to define the new trends in insurance information security technologies and discus how these new technologies are accepted by insurance industry. To achieve this aim we are using qualitative methods such as analysis, synthesis and comparison. This paper is the output of the project "Modernisation and consolidation of R&D infrastructure in the area of financial security information technologies "(Code of the project: 2623012000) and the project GAAA 11_2/2016 „A comparison of the business environment in selected countries in terms of individual market segments ".*

Keywords: *innovation, insurance, information technologies, security technologies.*

1. INTRODUCTION

Innovation through new technologies is a key driver of change in the financial sector and this has led to immeasurable efficiency gains, even though these changes can initially be accompanied by uncertainty and doubt. In recent years, such innovation has happened on the back of new technological developments, with the phenomenon often being described as "FinTech". As financial services deal in intangible products, it is well suited for technological innovation to lower transaction costs and expedite the delivery of services.[7] Together with digitization and the development of new technologies, they are creating new opportunities for entrepreneurship in a volatile, uncertain, complex and ambiguous VUCA environment, resulting into revolution of demand and supply in the field of energy supply side, which requires an adequate transformation of existing business models. .[8]

There are new forms of processes that may be improving the efficiency of intermediation and claims management. Most insurance start-ups involved in distribution have sites with well-developed contents, often accompanied by the application of artificial intelligence or robo-advice. These are intended to give an improved customer experience and lower commission/fees for when products are sold, although the initial fixed cost will likely be higher.

[249]Pan-European university, Faculty of Economics, Tematinska 10, 851 05 Bratislava 5, Slovakia
[250]University of Economics in Bratislava, Faculty of International Relations, Dolnozemská cesta 1, 852 35 Bratislava 5, Slovakia

Some outlooks predict the number of insurance employees will drop as a result of some of these evolutions. [3]

The competition in the insurance market is one of the strongest on the financial market. On one side existing players are trying to innovate on the other side new ones enter the market usually focus on online and non-traditional channels of distribution. Customer retention and cost optimization are becoming very critical. Consumers expect the same kind of service what they experience from leading online companies such as Netflix, Amazon and Airbnb.

Insurance companies are starting to leverage multiple parallel channels, often working hard to minimize channel conflicts. Some of the fastest growing channels are bancassurance, affinity and retail partners. Online and mobile channels are also growing in importance, although in most countries mostly for comparison shopping / information gathering. In Europe, insurance products are starting to be bundled and sold with banking products. Pure-play European insurance companies are at a disadvantage from a distribution perspective. In addition, direct-to-consumer online channels are also becoming more important as the internet pervades the daily lives of most consumers. [2]

For years now, digital advances have been transforming a range of industries. [3] Innovations in the information security technologies within the financial institutions represent very important criteria in the competition. They are part of a success at the financial markets as they provide information about the client. Innovations into a suitable information system secure the stability of the insurance portfolio and safety for a client before discreet information outflow. An appropriate processing of the project and keeping of right principles in the field of the projection and implementation of the innovative security technologies and by application of the SkyMinder service the insurance company secure enough information about the client, his commercial partners and a sufficient security for the client. The aim of this paper is to define the new trends which are expected to absorb the insurance industry and help those who follow them stay on top of the competition and satisfy both their and their customers´ needs, define the insurance information security technologies and discus how these new technologies are accepted by insurance industry. To achieve this aim we are using qualitative methods such as analysis, synthesis and comparison.

2. INNOVATIONS IN INSURANCE TECHNOLOGIES

Artificial intelligence and machine Learning. Insurers are exploring and investing in machine learning and automation during the whole product lifecycle: from marketing, through underwriting and customer service to claims processing, fraud management and reimbursement. While automation and machine learning have been present in the insurance industry for years, only simple processes that require low decision-making skills such as data entry, compliance checks, standard customer communications, and managing rule-based decisions, used to be a subject of automation.[2]

The information systems of insurance companies are able to explore the automation perspectives of more complex processes such as personalized customer interactions, property assessment, fraud detection and claims verification and processing. In today's business, we are experiencing many technological trends, so cyber security is needed to protect the companies from threats.[6] Some insurers are even using drones for automated property and claims assessment.

In this article we look at three key ways that AI will drive savings for insurance carriers, brokers and policyholders, plugging into existing transformations within the insurance industry [12]:

- *Behavioural Policy Pricing:* Ubiquitous Internet of Things (IoT) sensors will provide personalized data to pricing platforms, allowing safer drivers to pay less for auto insurance (known as usage-based insurance) and people with healthier lifestyles to pay less for health insurance
- *Customer Experience & Coverage Personalization:* AI will enable a seamless automated buying experience, using chatbots that can pull on customers' geographic and social data for personalized interactions. Carriers will also allow users to customize coverage for specific items and events (known as on-demand insurance)
- *Faster, Customized Claims Settlement:* Online interfaces and virtual claims adjusters will make it more efficient to settle and pay claims following an accident, while simultaneously decreasing the likelihood of fraud. Customers will also be able to select whose premiums will be used to pay their claims (known as peer-to-peer (P2P) insurance).

The insurance industry is lagging behind tapping into AI´s potential compared to other industries such as life sciences, retail and manufacturing.

Blockchain – the key to secured transactions and fast data processing is one of the most powerful technology trends to revolutionize the insurance industry in the next couple of years.

The first area in the insurance industry, which the blockchain technology could have a lasting effect on, is underwriting. Since this is the department responsible for whether a claim is trustworthy or not and how much of it can be covered, it could use a trust worthy repository of data. Another aspect of the insurance industry that can be positively affected by the blockchain technology is the processing of claims. Considering the number of data points that need to be verified and the manual effort required, it is no surprise that the users find the process too long and tedious. By using blockchain all the necessary information needed for claims verification can quickly be processed. Insurers can track the usage of an asset by using the data available in the blockchain without tampering any information. [2]

3. THE SECURITY INFORMATION TECHNOLOGY IN INSURANCE COMPANIES AND THE CYBER SECURITY

Cyber security with focus on defining the cyberspace or cyber threat is currently a very frequent topic. [5] Innovations of security information systems and information systems of insurance companies are mostly governed by four principles in order to achieve the set goal effectively.

The first principle is the decision of the top management of the insurance company on the project of strategic importance to implement the security system and the management must unanimously support this project. The second principle is to undergo mandatory training for middle and senior management and the staff involved in the implementation, to review the status of the insurance company, describe the current situation, define the areas to be changed and create a project plan to achieve the expected outcome of the implementation itself. A third principle during the project is the need to use the tool to manage the level of expectation of all stakeholders. To make the project successful, they need to think about the expectation from the project. It is better not to have high expectations so that the outcome is not disappointing, but it is also not good to have expectations too low to make the result really implemented and exploited. The fourth principle is the need to maintain the equilibrium triangle "people -

processes - tools": Employees must undergo training, processes must be projected, deployed and adhered to in work procedures and in workload, and processes must be supported by appropriate software tools that are deployed and documented how they are used.

These principles must be respected; otherwise the project is unbalanced and wasteful of resources:

- If unnecessarily expensive software tools are deployed and employees are unable to use their capabilities because they have not completed the necessary training,
- If the processes that are deployed are correct but not supported by software tools, work procedures cannot be complied with, and work is complicated, even though the employees have completed the training because they are trying to bypass them,
- If the tools were not deployed, and therefore they are retreating from their use in the company. Investments are unnecessary, despite the fact that employees are trained and have knowledge of security information technologies.

Without information technology, information is not only inefficient, but also unimaginable today. Information security is the process of maintaining confidentiality and availability during processing, storing and transferring information. Information must be secured against misuse. The client must be certain that the money to protect the person and property he has entrusted to the insurance company and the operations with them is as safe as possible.

Information security is the process of maintaining confidentiality and availability during processing, storing and transferring information. Information must be secured against misuse. There are a number of reasons to protect the information system [10]:

- what software the insurance company uses,
- what means of communication and components,
- what privileges users have,
- how external influences affect information systems,
- what kinds of threats need to be provided for information systems,
- what impact this threat poses.

The insurance company should have multi-level security of the information system. This ensures that in case of attacking a security level, still further levels are intact, therefore the following security levels should be used [1]:

- physical access to the place of possible work with the information system,
- local access to work with PC,
- access to the bank's local computer network,
- access to the application software of the information system,
- access to the operating system.

The client must be sure that the money he has entrusted to the insurance company and the operations with them are as safe as possible. Security includes databases, data files, data and information, various manuals, procedures, but also software and programs, computer and technical equipment. The security department in financial institutions checks whether the data processed by an insurance company is secured against misuse or destruction, or whether the insurer's information system complies with the guidelines of the National Bank and the Treasury, and whether security is understood as a continuous process. The Bank's security policy is approved by the Board of Directors; it should include objectives, principles, powers and responsibilities.

The insurance company is required to contractually ensure the security of information accessed by a third party, i.e. an external company, which is used for example in the form of outsourcing. It must also ensure the design, implementation and operation of the insurance company. Another view is personal security, where a financial institution should reduce the human factor problem, reduce mistakes, thefts and human scams, and have well-informed and trained staff. An insurer should have procedures in place for software mistakes and failures or misconceptions.

For environmental safety, the premises of an insurance company are monitored only for eligible persons. This prevents the risk of space, whether due to data misuse or theft.

It is necessary to ensure the reliable and continuous operation of the information system in order not to disturb the insurance business.

The insurance company determines the possibilities of handling and disposal of portable devices, laptops, flash disks. All exchanges and transfers are contracted in order to mitigate security risks. Procedures for the use of electronic communication channels are also developed. The Security Department has the task of managing all people's access to information and services through various access and user registrations. Each employee logs in to the system with his / her password, after the subsequent identification and authorization, the system enters the system. Every employee has a unique approach under his settings, and each employee has access to the programs they need for their work.

Activities need to be continuously monitored to ensure they are adequately protected. The Bank should comply with the rules resulting from generally binding legislation, contracts and standards and report on the verification of information systems for the NBS. Nowadays, information technologies are being penetrated into all spheres, so it is also an important part of the security of information systems. In order to operate a secure information system, it is also necessary to have the objective of information security and to know the structure of threats and vulnerabilities in the systems.

It is necessary to create the safest information system which:

- ensure company data protection to avoid misuse,
- ensures the protection of personal data in order to prevent unauthorized disclosure of information,
- even if the environment of information systems changes, it can maintain the level of service provided in the required quality. [3]

With the increasing development of information technology, the more important information is processed, the more they must be protected so that:

- it was possible to get them every time it is necessary and only authorized persons,
- it was always possible to find out who, when, and what kind of interventions in the system did,
- Only true information was given to the system [4].

An insurance undertaking must ensure that the information system functions are accessible. Information systems operators are expected to provide protection for these systems. The fact that there are weak points is the result of errors in the development or implementation of the information system. The basis for successful communication and the achievement of the organization's goals is a properly developed information system to suppress potentially

vulnerable locations. The threat of the information system is the possibility of using a vulnerability in the system. Threats are the result of intense attacks or irresponsibility of the person who participated in the development, implementation, testing, installation, or operation of the system.

The insurance information system can be assured differently:

- only selected users have access to all of the information system functions, and it is easy and unambiguous to identify who has been and what has changed,
- not only names and passwords, but also chips are used. They allow secure login and encryption of data,
- monitoring all inputs, outputs, changes and usefulness of their use.

Insurance companies also protect their clients by using SkyMinder. It is an international service that provides access to information on over 200 million companies across 230 countries and world territories in the form of reports. The service serves in particular to assess creditworthiness, financial health and warning information about foreign business partners. It will help insurers, among other things, to find out about the ownership structure of the companies reviewed or their managers. SkyMinder is an international service with worldwide coverage and online availability; it provides access to financial, credit, and business information about businesses around the world, including countries designated as tax havens. SkyMinder has been the most effective intermediary between local reporting providers and users around the world. [9]

Another major emerging trend in the insurance industry is cyber security. It is an issue that insurers should look at from both the perspectives of a security provider and a client, since it affects them just as much, if not more, as their clients. While risk management is something that insurers deal with daily, they seem to be a bit behind in terms of cyber precautions, when compared to other financial sectors. Insurance agencies have not been the targets of hackers all that much, however, as other targets become more secure and inaccessible, attackers are moving on to more unprepared targets. Since insurance companies hold enormous amounts of sensitive personal information such as personal properties, health, etc. The other way cyber security could influence the insurance industry is through its inclusion in various policies. Because of the time and age we live in, many businesses and individuals alike are under risk of their virtual information being breached and the expectation for coverage arises. Whether it is included as an entirely standalone service or as an endorsement to an existing policy, companies would look to their current provider and definitely will not be happy with those who refuse.

General liability providers offer cyber risk coverage because of two specific reasons:
First, general liability is a large, profitable business for many insurers. If clients are not satisfied with the coverage provided by their current insurer, they can test the markets.
Second, cyber risk is and emerging trend and line of business that keeps growing, with potential to generate future revenue increases. [2]

4. CONCLUSION

As all the other members of the financial sector, the insurance industry is ever-changing and because of the plethora of competitors who offer similar services, one needs to follow the emerging trends in order to stay on top.

On the one hand, you have trends such as automation and blockchain, that drive your company towards higher efficiency, and on the other hand, you have trends such as the demand for more personalized premiums and cyber security policies, which can lead to the loss of both current and potential clients.

Every day, we encounter massive information about hackers who have disrupted the information systems of the various institutions, causing damage not only to property but also to the health of the world's population. It is therefore important to continuously upgrade security information systems and technologies in insurance companies and other financial institutions co-operating with insurance companies. It consists of protecting clients and consumers using the services offered by the financial institutions on the financial markets. Attention to the security of all processes and invested resources in the upgrading of security information technologies increases the security of the use of common electronic communication means for storing sensitive information, which is now almost done by computers and the Internet. That is why security technology innovation is important for our security.

Integrated supervision over all participants of the financial market, which is carried out by the National Bank of Slovakia, is currently risk-based and thus, one of its main goals is to promote the elimination of specific risks in supervised entities [11]. It is therefore quite substantiated that it is aimed at the prevention of legalization of criminal proceeds and of terrorist financing (or at enforcing the countermeasures against money laundering and terrorist financing).

REFERENCES

[1] Cummis, F.A**.** (2002) *Enterprise Integration*, John Wiley Sons, Inc., Canada, pp. 45-357.

[2] Guenov, I. (2018) *9 Emerging Trends that will transform the insurance industry until 2020,* Scalefocus, [online] available at: https://www.scalefocus.com/insights/business/insurance-industry-trends-2018-2020/.

[3] Johansson, S., Vogelgesang, U. (2015) *Insurance on the threshold of digitization:* [online]. Available at: *Implications for the Life and P&C workforce.* McKinsey https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/financial%20services/latest%20thinking/insurance/insurance_on_the_threshold_of_digitization.ashx

[4] Jonassen Hass, A.M. (2003) *Configuration Management principles and practice*, Person Education, Inc. Boston, pp. 159-317.

[5] Korauš, A., Veselovská, S., Kelemen. P (2017) *Cyber security as part of the business environment*, Conference proceedings International Scientific Conference, International Relations 2017: Current issues of world economy and politics, Smolenice 30. November - 1. December 2017, Ekonóm.

[6] Korauš, A.; Kelemen P. (2018) *Protection of persons and property in terms of cybersecurity*, Conference proceedings International Scientific Conference, Economic, Political and Legal Issues of International Relations 2018. Faculty of International Relations, University of Economics in Bratislava, 1. - 2. juni 2018, Virt, Ekonóm.

[7] OECD (2017) *Technology and innovation in the insurance sector.* [online]. Available at: https://www.oecd.org/pensions/Technology-and-innovation-in-the-insurance-sector.pdf.

[8] Pásztorová, J. (2018) *Transformácia obchodných modelov v energetike,* Economic, Political and Legal Issues of International Relations 2018, Virt, pp. 356-378 [online]. Available at: https://fmv.euba.sk/www_write/files/Virt_zborn%C3%ADk.pdf

[9] SkyMinder (2016) *Informácie o zahraničných firmách.* [online]. Available at: http://www.skyminder.sk/informacie-o-zahranicnych-firmach/.

[10] Tvrdíková, M. (2000) *Zavádění a inovace informačních systémů ve firmách*, prvé vydanie, Grada publishing, Praha, 2000, pp. 11-159.
[11] Veselovská S., Korauš A., Polák J (2018) *Money Laundering and Legalization of Proceeds of Criminal Activity*, Second International Scientific Conference on Economics and Management - EMAN 2018, March 22, 2018, Ljubljana, All in One Print Center, Belgrade. DOI: https://doi.org/10.31410/EMAN.
[12] Zagorin, E. (2017) *Artificial Intelligence in Insurance – Three Trends That Matter*, EMERJ, [online]. Available at: https://emerj.com/ai-sector-overviews/artificial-intelligence-in-insurance-trends/.