JOURNAL OF ENGINEERING MANAGEMENT AND COMPETITIVENESS (JEMC)
VOL. 11, NO. 2, 2021, 85-95

CRM AND CUSTOMER DATA: CHALLENGES OF CONDUCTING BUSINESS IN DIGITAL ECONOMY

UDC: 005.346:004.6.056
Original Scientific Paper

Mihalj BAKATOR[1], Dejan ĐORĐEVIĆ[2], Dragan ĆOĆKALO[2], Milenko ĆEHA[3], Srđan BOGETIĆ[4]

[1]University of Novi Sad, Technical faculty "Mihajlo Pupin" in Zrenjanin, 23000 Zrenjanin, Đure Đakovića bb, Republic of Serbia
E-mail: mihalj.bakator@uns.ac.rs
[2]University of Novi Sad, Technical faculty "Mihajlo Pupin" in Zrenjanin, 23000 Zrenjanin, Đure Đakovića bb, Republic of Serbia
[3]Ministry of Interior, 11000 Belgrade, Republic of Serbia
[4]Belgrade Business and Art Academy of Vocational Studies, 11000 Belgrade, 73, Kraljice Marije, Republic of Serbia

Paper received: 03.04.2021.; Paper accepted: 16.04.2021.

Enterprises are facing difficulties in achieving and maintaining competitive ability amidst globalized markets. In the modern business environment, an effective CRM is an imperative for retaining customers. As CRM systems rely on customer data, it is important to secure data integrity. This paper thoroughly analyses the challenges of enterprises, CRM and customer data. The main goal of this paper is to provide an overview of existing literature and business practice in the domain of CRM. In addition, a model for improvement of CRM is developed. The model is based on the results of conducted review, and as such, it presents an approach towards enhancing CRM systems while taking into consideration the integrity of customer data.

Keywords: CRM; Customer data; Globalization; Digital economy; Data security.

INTRODUCTION

Competitive ability of an enterprise is a determining factor of long-term survival on globalized markets. Enterprises and their competitiveness are not determined by their size and country of origin, as smaller enterprises can obtain a solid competitive position despite the presence of large corporations present on the same market (B. Fleaca, E. Fleaca, & Maiduc, 2017; Kotler, Kartajaya, & Setiawan, 2017). Achieving competitive ability amidst the globalization of markets and the digitalization of business processes has proved to be a challenge for enterprises (Bakator, Đorđević, & Ćoćkalo, 2019; Bakator et al., 2018). In these conditions, where rapid changes of market trends are the default state, enterprises have to develop products and services, and flexible long-term strategies in order to develop and maintain competitive ability (Sipa, Gorzeń-Mitka, & Skibiński, 2015; Ungerman, Dedkova, & Gurinova, 2018). Digitalization does not only affect business activities, but every aspect of human activity as well. From the aspect of competitiveness and economy, digitalization has brought digital platforms (e-commerce sites, collaboration software, etc.), which made it possible for enterprises from smaller countries to actively participate on the international market (Yeganeh, 2019). Competitiveness of enterprises is an integral part and one of the main goals of conducting business. With the rapid development of information on-communication technologies (ICTs) enterprises have to adapt and conduct business in the digital economy (Ćoćkalo et al., 2019). Permanent changes of the business environment are mainly the result of technological advancement (Bogetić et al., 2018). The processes of digital enterprises do not have to rely heavily on financial assets or to be more precise, human resources and intellectual capital were more used

ISSN 2217-8147 (Online)

Available online at http://www.tfzr.uns.ac.rs/jemc

compared to financial resources in these transformations (Ansong & Boateng, 2019).

With the goal to achieve and maintain strong competitive positions on the market in modern business environment, enterprises have to apply advanced information systems alongside various tools designed to obtain and process information from the market (Pomffyová & Bartková, 2016). This information can provide an insightful overview on market trends and more importantly, on customer satisfaction. Information on customer satisfaction plays a crucial role in customer relationship management (CRM) systems. CRM aims at achieving and maintaining good relationships with customers with the goal to develop loyalty over time (Nyadzayo, & Khajehzadeh, 2016). Enterprises are realizing the enormous potential and necessity for obtaining customer and market data. Through data analysis approaches such as big-data analysis enterprises can create value for the customer and increase customer retention (Benoit, Lessmann & Werbeke, 2020).

However, if the collected customer data, and employee data as well would fall under a data breach, the consequences could put an enterprise out of business. The main negative points of data breaching are reputation of the enterprise and legal repercussions are a more severe negative side and market monopoly (Lafuente, 2015; Nuccio, & Guerzoni, 2018). Security issues include access control, application security, cryptography and authentication. Enterprises have to apply multiple methods such as system integrity checks or remote system management in order to increase data security (Wang & Jones, 2020). In order to reduce implementation costs, enterprises can opt for a cloud-based service to acquire and manage customer data. Now, as a large amount of information is transferred through these cloud services, data security is a challenge and enterprises have to implement user-oriented policies, data storage security, network security, and application security (Tabrizchi & Kuchaki Rafsanjani, 2020). Effective data security solutions are an imperative for enterprises that collect, apply and store customer data. As modern CRM relies on customer data, data security solutions within enterprises should be a new "norm" of how enterprises conduct business with their customers. Namely, existing policies such as the EU General Data Protection Regulation (GDPR) provide a solid framework, and enterprises should integrate their own policies that would complement broader sets of guidelines.

Interactive technologies are becoming more pervasive, and enterprises collect, apply and store customers' personal data in a covert manner and fewer resources (Plangger & Montecchi, 2020). In the same study it was noted that customers have tradeoff their personal data in order to enjoy the benefits given by an enterprise that applies such data.

The application and development of information communication technologies (ICTs) affect and change economic trends and economic activity (Goldfarb & Tucker, 2019). Namely, within the digital economy enterprises have to accommodate and adapt to dynamic communication and distribution channels. If competitiveness is the goal, then obtaining, processing and analyzing customer data are the key. This data is further applied for effective CRM. Given the risks of storing customer data, enterprises have to manage customer data securely. It is evident that enterprises face challenges in the digital economy, and issues such as data security have to be addressed. This topic invites new research, as the matter of CRM and data security is becoming a matter of survival on the market within a digital economy. This paper focuses on improvement of CRM through data security, as an important tool for gaining competitiveness. The paper addresses four main research questions as guidelines for the research:

- How is the digitalization of the economy affecting enterprises?
- How important are modern CRM systems for achieving competitiveness?
- How important is data security when it comes to CRM systems?
- How can CRM be improved through data security?

The aim of this review paper is to develop a theoretical model for improvement of CRM through data security mechanisms. The paper consists of four main sections (excluding the Introduction and Conclusion sections). First, the research methodology is explained in more details. Next, the results (information, data, etc.) of the review process are presented. In the third section the theoretical model for improvement of CRM through data security is presented. Finally, the model and the research questions are discussed.

METHODOLOGY

Review Process and Flow Diagram

The PRISMA structured protocol flow diagram was used to conduct the review process (Moher et al., 2010). Literature was obtained through the Google Scholar service and the KoBSON service. The review process started with searching and downloading scientific articles in the domain of CRM, data security, Industry 4.0 and the digital economy. Afterwards, duplicates were removed. Next, a thorough screening process was conducted with the goal to determine the articles addressing the subjects of interest to the systematic review. Irrelevant literature sources were excluded. The structured flow diagram of the review process is presented in Figure 1.

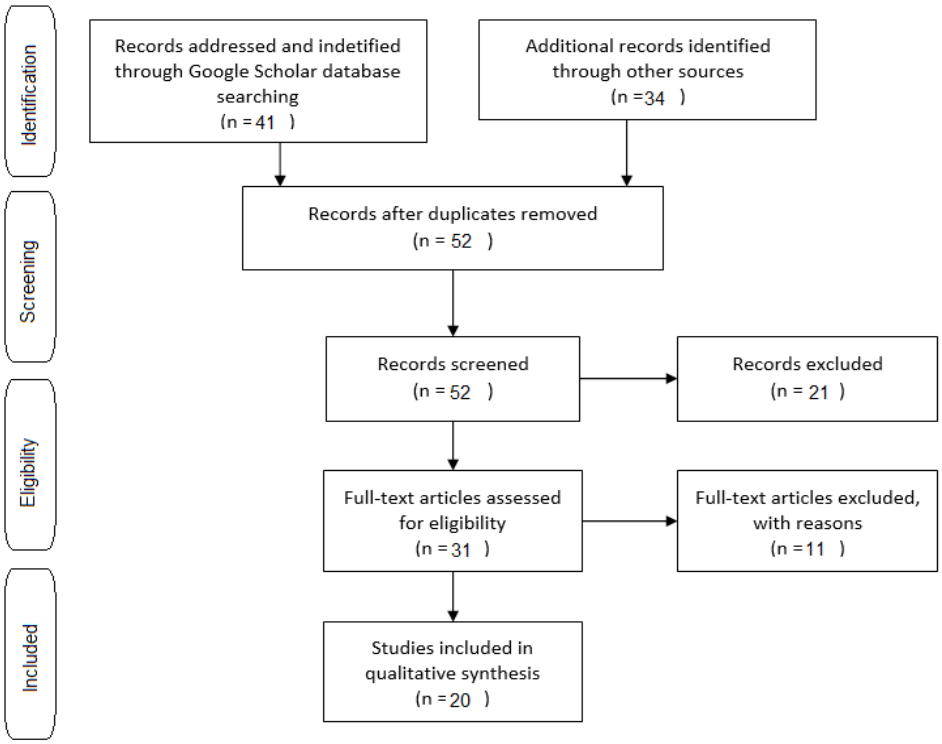

Figure 1: Protocol flow diagram

Literature Eligibility Criteria

Articles published between 2015 and 2020 were taken into consideration for review. Every article is published in credible scientific and peer-reviewed journals. The main subjects included in these articles are:

- customer relationship management,
- digital economy,
- domestic enterprises and globalization,
- globalization and Industry 4.0,
- global economy and competitiveness,
- SMEs and CRM,
- CRM and data security,
- data security and customer data

Furthermore, articles in the review process are not taken into consideration. Similarly, articles published in journals conducting predatory practices were not taken into consideration. The majority of scientific journals are in the domain of CRM, management, customer satisfaction, economy and competitiveness. Details on specific literature sources are provided in the section of References.

Data Collection, Search and Study Selection

In the first step, articles were searched through the Google Scholar service. Based on the title and abstract, articles were downloaded through KoBSON or directly from the journal archive if it was an open access. Within this step, articles and conferences were checked if they were labelled "predatory". Articles filling the requirements of the review were downloaded and stored on the personal computer of the author.

From here, duplicates were removed and article screening was conducted. If an article did not aim towards the goal of this review paper, then it was removed from further review. Articles including data on CRM systems, customer satisfaction, competitiveness, data security, digital economy, Industry 4.0 and globalization were taken into consideration. The data and information obtained from these articles are applied for development of relations between the model's elements. As stated at the beginning of the paper, the main goal of the review process is to identify crucial elements of CRM improvement and to develop a model for improvement of CRM through data security. Such approach is a necessity in the modern business environment where business is conducted within the framework of a digital economy.

REVIEW RESULTS

Information from the reviewed articles are categorized into two groups: base reference (BR) and supporting reference (SR). Base references directly address a certain relation/connection/ element of the model, while supporting references indirectly address a specific model relation/ connection/element.

These labels along with adequate numbering are used in the development process. The model consists of several elements and the relations between these elements are based on the results of the review (for example, BR1, BR4, SR2, etc.). Further, the information noted from the review process are as follows:

1. Effective CRM systems are necessary for development of good relationships with customers. Continuous good relationships may lead to customer loyalty, which has an increasingly positive effect on long-term business performance (Budianto, 2019). From here, it is arguable that enterprises should possesses well-developed (Base reference - BR1).
2. Enterprises have to implement security management systems in accordance with standardized procedures. The implementation and application of ISO/IEC Standard 15408 (Information Technology - Security Techniques - Evaluation Criteria for IT Security), which consists of three main parts (Introduction and General Model; Security Functional Requirements; and Security Assurance Requirements) can have a positive result when it comes to detection and management of risks and countering threats (Dotsenko et al., 2019). (Base reference - BR2)
3. Data security should not only be the responsibility of IT sector in an enterprise, but rather, the business infrastructure should be defined in a manner that integrates data security as a default mechanism (Spremić & Šimunic, 2018). (Base reference - BR3)
4. In order to increase cyber security in enterprises and within their CRM systems, it is necessary to implement awareness programs for employees and minimize security fatigue (He & Zhang, 2019). (Base reference - BR4)
5. Besides the adequate equipment necessary for an effective data security system, it is important to increase employee awareness regarding data security social engineering, as these attacks can often lead to authorization access compromised (Aldawood & Skinner, 2019). Therefore, effective employee training should be periodically introduced within the enterprise. (Supporting reference - SR1)
6. Cyber-attacks are mainly motivated by potential financial gain (through fraud, ransom, blackmail, intellectual property theft, industrial espionage, etc.) (Tao et al., 2019). (Base reference - BR5)
7. If a cyber-attack should arise and customer data be stolen, the enterprise can have severe consequences not only in the form of bad press, but also in a more legal sense, where customers collectively sue the enterprise for not securing sensitive customer information. A cyber-attack can easily result in big losses for the enterprise, as these attacks may steal credit card information or other sensitive data. For example, the chain store Target has experienced a 46% loss of profit, in addition to the loss of trust and loyalty of customers, lenders and existing and potential investors (Manworren, Letwat, & Daily, 2016). Now, this attack was aimed at Target - a big enterprise with over 1,700 stores. (Base reference - BR6)
8. As there is a tremendously increasing number of cyber-attacks each year, enterprises have to implement data security systems mainly consisting of several main components. These components are analysis (analyzing and identifying potential internal and external risks); defense (the data security system has to effectively annul internal and external attacks); detection (effective detection of internal or external threats and ongoing or conducted attacks); revival (restoring and recovering data

after the attack); and oversight and development (monitoring all employees, business activities, data routes, and alerts; conducting timely security updates and patches; developing security awareness) (Aboelfotoh & Hikal, 2019). (Base reference - BR7)

9. Data security systems should integrate a prevention protocol consisting of recipient-initiated report of malicious e-mail; storage of cyber-attack records; aggregating and analyzing databases; publicize senders of malicious e-mails; developing and setting up inbound and outbound filters (Lee et al., 2020). (Base reference - BR8)
10. Risks in security can be categorized into network/platform provider vulnerabilities, availability and data control from a third party. In these cloud-based security systems, data should be secured with authentication and authorization as firewalls do not always ensure data security (Wang & Wang, 2017). (Base reference - BR9)
11. With the goal to prevent, detect and respond to cyber-attacks, enterprises have to consider technological tools, implementation of security standards, firewalls, Intrusion Detection System, Intrusion Prevention System, antivirus and anti-malware software, and develop an overall capability to respond to incidents (Maglaras, et al., 2019). (Base reference - BR10)
12. Data security systems for securing data (customer, employee, market, financial, etc.) are affected by various factors. Especially in the developing countries. These factors may include financial resources, management support, awareness, IT education, pirated software, usage patterns, etc. (Kabanda, Tanner, & Kent, 2018). In order to effectively manage such security systems adequate optimization is needed. (Base reference - BR11)
13. Furthermore, modern ICTs have made it possible for enterprises to collect, process and analyze data from customers. The information extracted from these data makes it possible for enterprises to develop effective CRM systems. In other words, through use of ICTs, enterprises can use customer and market data for development of short-term and long-term strategies to attract and retain customers. CRM is an important factor for long-term enterprise sustainability, as it was found that CRM can improve efficiency, customer satisfaction, brand reinforcement, cost reduction and customer loyalty (Pohludka & Štverková, 2019). (Supporting reference - SR2)
14. SMEs have to realize the value of customer data and the value of retaining, processing and analyzing that data for financial gain and for development of competitiveness (Li, Nirei, & Yamana, 2019). Namely, customer data has a significant role in an effective CRM system. (Base reference - BR12)
15. In order to develop and distribute the right products at the right time, enterprises have to identify the noted specific market segments. On the global, digitalized market, SMEs are competitors of big corporations, and vice-versa. However, dynamic changes on the market may take a bigger toll on big corporations. This is due to the size and complexity of organization and organization processes. Namely, larger organizations have to implement more changes (Andersson et al., 2018) compared to SMEs. (Base reference - BR13)
16. With the goal to safely manage customer data, enterprises have to address five major security factors within their network security. These are confidentiality (not accessible to unapproved personnel); availability (must be easily available to approved clients, and secured from unapproved clients); authentication (client confirmation through passwords, biometric information, documents, etc.); integrity (the data cannot be adjusted/modified in the distribution and transmission process); and non-repudiation (both the sender and receiver know the source of the data) (Adlakha et al., 2019). (Base reference - BR14);
17. As devices used in business and connected to the Internet can be the subject of cyber-attacks (unauthorized access; confidentiality; availability; transmission threats; and malicious code attacks) the following principles should be taken into consideration for guaranteed security: confidentiality (authorization through credentials); integrity (protecting information from attacks); availability (data should be available to authorized personnel, and not be limited); authenticity (different operations require different access authorization); nonrepudiation (trusted audit trail); and privacy (right to interact at desired level) (Ervural & Ervural, 2017). (Supporting reference - SR3)

18. CRM collects data on customer satisfaction, customer retention rate, revenue per customer, information on perceived quality, brand loyalty and other significant metrics. After this data is analyzed, the obtained results are applied within CRM strategies that may increase customer satisfaction and customer retention (Soltani & Navimipour, 2016). (Base reference - BR15)
19. In order to improve integrated information systems, including CRM, it is necessary to conduct multi-layer data security that may include information gathering, information analysis, information evaluation, detection of risks, recovery and maintenance (Jafari Navimipour & Soltani, 2016). (Base reference - BR16)
20. CRM practices were found to positively affect customer relationship quality and customer satisfaction. CRM systems shorten the distance between the customer and enterprise, which positively affects development of customer loyalty (Santouridis & Veraki, 2017). In addition, in the same research it was noted that an effective CRM system has to provide value to the customer. (Base reference - BR17)

The information from the reviewed articles is used as base and support references for development of the model for improvement of CMR through data security. The model is presented in the next section.

MODEL FOR IMPROVEMENT OF CRM

Based on the thorough literature analysis a model for improvement CRM through data security is developed. The model is generic in nature in order to be applicable in various enterprises. The model includes several integral elements. The relations/connections between these elements are labelled in accordance with corresponding base (BR) or supporting reference (SR). The model is presented in Figure 2.

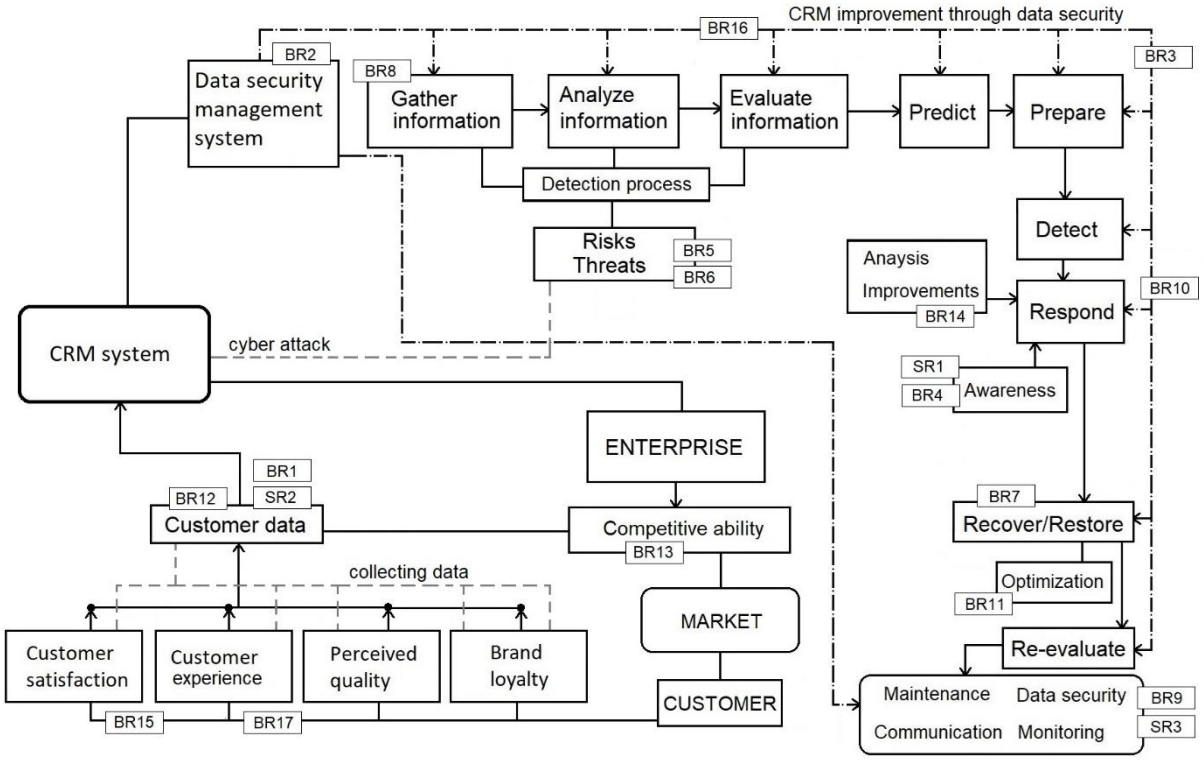

Figure 2: Model for CRM improvement

Based on the depicted model in Figure 2, it can be seen that the CRM system module is supported by the data security management system. The goal was to develop a rather generic model in order to make it suitable and modifiable for enterprises regardless of industry, size and business environment. The model is based and supported by the findings noted in the section of Results Review. The CRM improvement process is based on securing customer data and reassuring them that their data is secure.

Customer data includes the obtained, processed, analyzed and stored data on customers (IDs, e-

mails, information on gender, age, geographic location, address, phone number, credit card data, etc.). In addition, it contains semi-sensitive data on customer experience, customer loyalty, brand loyalty, customer intentions, customer satisfactions and perceived quality. This data is the core of the CRM system.

The CRM system represents the main system for management of customer relationships that has a goal to develop long-term customer loyalty and to also attract and retain customers. Within this model, the enterprise applies data security in order to protect customer data, which leads to an improved CRM.

Further, the data security management system represents the main core module of data security measures within the CRM system. Risks and threats regarding customer data are detected and an array of measures are conducted including: gathering information (information on the potential data breaches and hacks, passwords, authentication processes, ID registries, etc.), analyzing information (aims to detect vulnerabilities, security shortcomings or lack of awareness), evaluation (evaluation is conducted on potential threats and risks), prediction (future trends and predictions are projected), preparation (development of operational procedures for threats and risks), detection (detecting threats and risks), response (actions to annul existing and future threats and risks), awareness (increasing awareness of cyber threats and risks, among employees), analysis and improvements (analyzing the attack metrics), recover and restore (damage determination and conduct of data recovery), optimization (optimizing system modules that directly or indirectly use customer data), re-evaluation (thorough and continuous re-evaluation of the whole data security management system and the CRM system has to be conducted) maintenance, data security, communication and monitoring (the pillars of continuous improvement of the data security system).

As noted earlier, the model is generic in nature, and it is up to the enterprise what data security solution they will implement. The main concept of this model is continuous monitoring-evaluation-improvement cycle. The enterprise has to integrate, alongside with its CRM system an adequate data security system. In cloud-based CRM solutions, data security is most likely a "default" setting. The presented model provides an overview on how data security challenges can be addressed.

Depending on what type of data storage is used for customer data, the enterprise has to define and implement an effective data security management system. These systems can be based on data security policies, standards or hybrid non-standardized solutions. A CRM system supported with such data security is more effective in ensuring the enterprise's customers that their data is safe. This may further lead to increased customer satisfaction and development of long-term customer loyalty.

DISCUSSION

The challenge for enterprises when it comes to the digital economy lies in the dynamic changes of ICTs characterized by the fourth industrial revolution - Industry 4.0. (Kiyamov et al., 2019). Thus, conducting business within the frameworks of Industry 4.0 requires enterprises to apply modern ICTs (Gerbert et al., 2015). Technology can drastically improve quality, reduce manufacturing costs and increase overall competitiveness (Angelous Kotey & Yindenaba Abor, 2019).

Now, in today's digital economy, where the vast majority of business activities take place online, enterprises have to take into consideration the threats from cyber-attacks that can result in loss of sensitive data, stolen intellectual property, damage to the business public image, and damage to overall business performance (Raghavan, Desai, & Rajkumar, 2017). Therefore, when enterprises set up their CRM systems and when they collect customer data, it is important to take into consideration the users' concerns when it comes to their personal information and privacy. CRM is necessary for achieving competitive advantage on the market as enterprises gather, process, visualize, share and apply customer and market data provides user-friendly and specific information on metrics of interest (Holmlund et al., 2020). Without an effective CRM system with data security systems supporting it, enterprises may face difficulties in obtaining a competitive position on the market.

As social media data breaches occur from time to time, users/customers are getting more and more aware of the fact that enterprises collect and store their data and that this data is at risk from cyber-

attacks (Hu et al., 2018). Customer data is not vulnerable only on social media and other online platforms. Enterprises also face risks when it comes to the integrity of their customers' data (Powell, 2019; Raghavan, Desai, & Rajkumar, 2017). Therefore, it is evident that in order to improve CRM, enterprises have to secure customer data collected for development of good C2B relationships. Furthermore, based on these findings, the research questions are addressed:

1. How is the digitalization of the economy affecting enterprises? The modern business environments is "forged" in the changes brought by the globalization of markets and the framework of Industry 4.0. The rapid advancement of ICTs has changed the way how enterprises conduct business on the international market. Digitalization of the economy certainly puts a strain on enterprises as they have to adapt to new ways of conducting business. An online presence of almost any enterprise is an imperative for a chance to achieve competitiveness and satisfactory business performance. This online presence requires and effective CRM system that manages various metrics of customer relationships through obtained customer data.

2. How important are modern CRM systems for achieving competitiveness? Given the results of the thorough analysis of the existing literature in the domain of CMR and competitiveness, it can be argued that modern CRM systems are necessary for an advantage on the international market, while less sophisticated CRM solutions are necessary for survival on the domestic market.

Simply, domestic enterprises, and enterprises overall, have to know their customers and to effectively manage their relationships with them. The main focus of CRM systems is on development of customer loyalty that has one of the highest levels of customer retention. Without CRM systems, enterprises would have a hard time to determine the level of customer satisfaction, customer experience, customer loyalty, etc. Now, as for modern CRM systems, where big data analytics are applied, these represent a "powerful tool" for effective development and innovation of relationships with customers. This further positively affects new customer attraction and overall customer retention. However, modern CRM systems carry a larger risk of cyber-attacks, where customer data becomes a "two-edged sword" meaning that if data breaches occur, a significant loss of customer trust can follow after these cyber-attacks.

3. How important is data security when it comes to CRM systems? CRM systems carry the risk of cyber-attacks. Earlier in the paper it was noted that data breaches, fraud, blackmail and other types of cyber-attacks can severely affect customer trust that further negatively affect overall business performance. Therefore, enterprises in the digital economy, face challenges when it comes to building relationships with customers and at the same time securing the obtained and stored customer data as a part of their CRM.

The majority of enterprises have to implement a standardized or other type of policy regarding data security management within their CRM activities. From an enterprises' viewpoint, data security is a matter of economic stability in the long run. The long-term effectiveness of CRM is at risk if customer data is vulnerable. Therefore, when a specific CRM mechanism is developed, one of the main pillars should be data security.

4. How can CRM be improved through data security? An effective CRM system manages customer data in order to develop quality relationships with customers. Now, in order to protect customer, as noted before, data security mechanisms have to be in place. With the goal to improve CRM, which would indirectly improve customer relationships, leading further to customer loyalty, a model was introduced. From the model it is evident that the CRM system is supported by the data security management system including several modules for detection of risks and threats and procedures to eliminate them. Such configuration requires continuous evaluation and improvements. In addition, these extra security measures should be communicated to the customers as well, thus increasing their trust and satisfaction towards the enterprise.

The significance and contribution of this paper lies in its concisely conducted and structured review used for development of a model for CRM improvement through data security. Further, as for research implications, fellow researchers can address this paper as a basis for future empirical studies in the domain of CRM and customer data security. As for practical implications, enterprises can address this present paper in order to obtain an overview on the importance of securing customer data and other sensitive data regarding their

business activities. The social implications can be in the form of higher awareness of society on how enterprises obtain, apply and store data of their customers. Such awareness may lead to a more rational and safer distribution of personal information on the Internet.

CONCLUSION

The modern business environment puts pressure on enterprises when it comes to development of relationships with customers. Therefore, effective CRM systems are an imperative for long-term success on the market. However, an ever-increasing number of cyber-attacks on databases (storing customer data and other sensitive business information) is a major challenge for enterprises. These attacks can severely affect business performance and the overall survival of the enterprise on the market. It can be concluded that CRM is a necessary mechanism for achievement and maintenance of competitiveness, while adequate data security should be introduced in order to reduce risks and threats of cyber-attacks. Further, it can be seen that in the digital economy, enterprises almost do not have a choice when it comes to collecting, processing and storing customer data. Without these practices, their competitive position on the market would be uncertain. On the other side, customers tend to "flock" towards enterprises that "care" and "understands" them the most. This caring and understanding comes for price in the form of personal or semi-personal data. Ethical and moral aspects in these C2B relations are questionable. Therefore, for future research it would be interesting to analyze customers' opinions on how enterprises collect, process and store customer data.

The main limitation of this paper is the lack of survey data on how enterprises manage to stay afloat on turbulent markets. In addition, empirical data on domestic enterprises could have been included. However, this review paper still provides a concise overview on several CRM and customer data issues. In addition, it integrates the findings into a generalized model for improvement of CRM. Overall, this study makes a solid basis for future research in the domain of CRM and customer data security. As noted previously, future research can focus on customers and on enterprises activities regarding customer data in their C2B relationship. It is also recommended to conduct a survey with enterprise managers in order to investigate specific data security solutions and how they function within various enterprises. This approach may shed light on interesting perspectives when it comes to CRM and customer data security.

ACKNOWLEDGEMENT

This work is a part of current TR-35017 project funded by the Ministry of Education, Science and Technological Development of the Republic of Serbia.

REFERENCES

Aboelfotoh Aboelfotoh, S. F., & Hikal, N. A. (2019). A Review of Cyber-security Measuring and Assessment Methods for Modern Enterprises. *JOIV: International Journal on Informatics Visualization, 3*(2), 157-176. https://doi.org/10.30630/joiv.3.2.239

Adlakha, R., Sharma, S., Rawat, A., & Sharma, K. (2019). Cyber Security Goal's, Issue's, Categorization & Data Breaches. *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon).* https://doi.org/10.1109/comitcon.2019.8862245

Aldawood, H., & Skinner, G. (2019). Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering. *2019 Cybersecurity and Cyberforensics Conference (CCC).* https://doi.org/10.1109/ccc.2019.00004

Andersson, P., Axelsson, B., Jönsson, K., & Laurin, E. (2018). Marketing Reorganization in a Globalized Market: The Case of ABB Robotics. *Organizing Marketing and Sales,* 23–41. https://doi.org/10.1108/978-1-78754-968-520181002

Angelous Kotey, R., & Yindenaba Abor, J. (2019). The Role of Technology as an Absorptive Capacity in Economic Growth in Emerging Economies: A New Approach. *The European Journal of Applied Economics, 16*(2), 59-78. https://doi.org/10.5937/EJAE16-20133

Ansong, E., & Boateng, R. (2019). Surviving in the digital era – business models of digital enterprises in a developing economy. *Digital Policy, Regulation and Governance*. https://doi.org/10.1108/dprg-08-2018-0046

Bakator, M., Đorđević, D., & Ćoćkalo, D. (2019). Developing a model for improving business and competitiveness of domestic enterprises. *Journal of Engineering Management and Competitiveness (JEMC), 9*(2), 87-96. UDC: 658.562(497.11) 339.13(497.11)

Bakator, M., Đorđević, D., Ćoćkalo, D., Nikolić, M., & Vorkapić, M. (2018). Lean startups with industry 4.0 technologies: Overcoming the challenges of youth

entrepreneurship in Serbia. *Journal of Engineering Management and Competitiveness (JEMC), 8*(2), 89-101.

Benoit, D. F., Lessmann, S., & Verbeke. W. (2020) On realising the utopian potential of big data analytics for maximising return on marketing investments. *Journal of Marketing Management, 36*(3-4), 233-247. https://doi.org/10.1080/0267257X.2020.1739446

Bogetić, S., Đorđević, D., Ćoćkalo, D., & Vorkapić, M. (2018). Corporate social responsibility as a factor of global competitiveness. *Journal of Engineering Management and Competitiveness (JEMC), 8*(1), 11-19. UDC: 005.35:339.137.2

Budianto, A. (2019). Customer loyalty: quality of service. *Journal of Management Review, 3*(1), 299-305. https://doi.org/10.25157/jmr.v3i1.1808

Ćoćkalo, D., Đorđević, D., Bogetić, S., Bakator, M., & Bešić, C. (2019). Competitiveness of Domestic Enterprises in Changing Markets and Industry 4.0, In L. Monostori, V. D. Majstorovic, S. J. Hu & D. Djurdjanovic (Eds.), Proceedings of the *4th International Conference on the Industry 4.0, 5-7th June, 2019*, Springer Nature, Switzerland, pages 113-127, 2019, ISSN 2195-4356, https://doi.org/10.1007/978-3-030-18180-2_9

Dotsenko, S., Illiashenko, O., Kamenskyi, S., & Kharchenko, V. (2019). Integrated Security Management System for Enterprises in Industry 4.0. *Information & Security, 43*(1), 294-304. https://doi.org/10.11610/isij.4322

Ervural, B. C., & Ervural, B. (2017). Overview of Cyber Security in the Industry 4.0 Era. *Industry 4.0: Managing The Digital Transformation*, 267–284. https://doi.org/10.1007/978-3-319-57870-5_16

Fleaca, B., Fleaca, E., & Maiduc, S. (2017). Improving the Enterprise's Competitiveness by Applying the Functional Analysis Technique. *Procedia Engineering*, 181, 928–934. https://doi.org/10.1016/j.proeng.2017.02.489

Gerbert, P., Lorenz, M., Rüßmann, M., Waldner, M., Justus, J., Engel, P., & Harnisch, M. (2015). *Industry 4.0-The Future of Productivity and Growth in Manufacturing Industries.* Boston, MA: The Boston Consulting Group.

Goldfarb, A., & Tucker, C. (2019). Digital Economics. *Journal of Economic Literature, 57*(1), 3–43. https://doi.org/10.1257/jel.20171452

He, W., & Zhang, Z. (Justin). (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, 1–9. https://doi.org/10.1080/10919392.2019.1611528

Holmlund, M., Van Vaerenbergh, Y., Ciuchita, R., Ravald, A., Sarantopoulos, P., Ordenes, F. V., & Zaki, M. (2020). Customer experience management in the age of big data analytics: A strategic framework. *Journal of Business Research*. https://doi.org/10.1016/j.jbusres.2020.01.022

Hu, T., Wang, K.-Y., Chih, W., & Yang, X.-H. (2018). Trade off Cybersecurity Concerns for Co-Created Value. Journal of Computer Information Systems, 1–16. https://doi.org/10.1080/08874417.2018.1538708

Jafari Navimipour, N., & Soltani, Z. (2016). The impact of cost, technology acceptance and employees' satisfaction on the effectiveness of the electronic customer relationship management systems. *Computers in Human Behavior*, 55, 1052–1066. https://doi.org/10.1016/j.chb.2015.10.036

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

Kiyamov, I. K., Sabitov, L. S., Kabirova, G. I., Akhtyamova, L. S., & Iskhakova, L. S. (2019, July). Actual issues of digital transformation of the Russian economy in modern conditions. In *IOP Conference Series: Materials Science and Engineering 570*(1), 012056. https://doi.org/10.1088/1757-899X/570/1/012056

Kotler P., Kartajaya H., & Setiawan I. (2017). Marketing 4.0. Hoboken, NJ: John Wiley and Sons Inc.

Lafuente, G. (2015). The big data security challenge. *Network Security, 2015*(1), 12–14. https://doi.org/10.1016/s1353-4858(15)70009-7

Lee, J. K., Chang, Y., Kwon, H. Y., & Kim, B. (2020). Reconciliation of Privacy with Preventive Cybersecurity: The Bright Internet Approach. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-020-09984-5

Li, W. C., Nirei, M., & Yamana, K. (2019). *Value of data: there's no such thing as a free lunch in the digital economy*. US Bureau of Economic Analysis Working Paper, Washington, DC. https://www.rieti.go.jp/jp/publications/dp/19e022.pdf)

Maglaras, L., Ferrag, M. A., Derhab, A., Mukherjee, M., & Janicke, H. (2019). Cyber Security: From Regulations and Policies to Practice. *Springer Proceedings in Business and Economics*, 763–770. https://doi.org/10.1007/978-3-030-12453-3_88

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons, 59*(3), 257–266. https://doi.org/10.1016/j.bushor.2016.01.002

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & Group, P. (2010). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *International Journal of Surgery, 8*(5), 336-341.

Nuccio, M., & Guerzoni, M. (2018). Big data: Hell or heaven? Digital platforms and market power in the data-driven economy. *Competition & Change, 102452941881652*. Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & Group, P. (2010). Preferred reporting items for systematic reviews and meta-

analyses: the PRISMA statement. *International Journal of Surgery*, *8*(5), 336-341. https://doi.org/10.1177/1024529418816525

Nyadzayo, M. W., & Khajehzadeh, S. (2016). The antecedents of customer loyalty: A moderated mediation model of customer relationship management quality and brand image. *Journal of Retailing and Consumer Services*, 30, 262–270.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & Group, P. (2010). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *International Journal of Surgery*, *8*(5), 336-341. https://doi.org/10.1016/j.jretconser.2016.02.002

Plangger, K., & Montecchi, M. (2020). Thinking Beyond Privacy Calculus: Investigating Reactions to Customer Surveillance. *Journal of Interactive Marketing*, 50, 32–44.

Pohludka, M., & Štverková, H. (2019). The Best Practice of CRM Implementation for Small- and Medium-Sized Enterprises. *Administrative Sciences*, *9*(1):22. https://doi.org/10.3390/admsci9010022

Pomffyová, M., & Bartková, L. (2016). Take Advantage of Information Systems to Increase Competitiveness in SMEs. *Procedia - Social and Behavioral Sciences*, 220, 346–354. https://doi.org/10.1016/j.sbspro.2016.05.508

Powell, M. (2019). *11 eye opening cyber security statistics for 2019*. https://www.cpomagazine.com/tech/11-eye-opening-cyber-security-statistics-for-2019/

Raghavan, K., Desai, M. S., & Rajkumar, P. V. (2017). Managing cybersecurity and ecommerce risks in small businesses. *Journal of Management Science and Business Intelligence*, 9-15. https://doi.org/10.5281/zenodo.581691

Santouridis, I., & Veraki, A. (2017). Customer relationship management and customer satisfaction: the mediating role of relationship quality. *Total Quality Management & Business Excellence*, *28*(9-10), 1122–1133. https://doi.org/10.1080/14783363.2017.1303889

Sipa, M., Gorzeń-Mitka, I., & Skibiński, A. (2015). Determinants of Competitiveness of Small Enterprises: Polish Perspective. *Procedia Economics and Finance*, *27*, 445–453. https://doi.org/10.1016/s2212-5671(15)01019-9

Soltani, Z., & Navimipour, N. J. (2016). Customer relationship management mechanisms: A systematic review of the state of the art literature and recommendations for future research. *Computers in Human Behavior*, *61*, 667–688. https://doi.org/10.1016/j.chb.2016.03.008

Spremić, M., & Šimunic, A. (2018). Cyber security challenges in digital economy. In Proceedings of the *World Congress on Engineering,1*, pp. 341-346). ISSN: 2078-0958

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing*. https://doi.org/10.1007/s11227-020-03213-1

Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems.* https://doi.org/10.1016/j.future.2019.03.042

Ungerman, O., Dedkova, J., & Gurinova, K. (2018). The impact of marketing innovation on the competitiveness of enterprises in the context of industry 4.0. Journal of Competitiveness, 10(2), 132. https://doi.org/10.7441/joc.2018.02.09

Wang, L., & Jones, R. (2020). Big Data Analytics in Cyber Security: Network Traffic and Attacks. *Journal of Computer Information Systems*, 1–8. https://doi.org/10.1080/08874417.2019.1688731

Wang, L., & Wang, X. V. (2017). Challenges in Cybersecurity. *Cloud-Based Cyber-Physical Systems in Manufacturing*, 63–79. https://doi.org/10.1007/978-3-319-67693-7_3

Yeganeh, H. (2019). An Analysis of Emerging Patterns of Consumption in the Age of Globalization and Digitalization. *FIIB Business Review*, 231971451987374. https://doi.org/10.1177/2319714519873748

CRM I PODACI KORISNIKA: IZAZOVI POSLOVANJA U DIGITALNOJ EKONOMIJI

Preduzeća se suočavaju sa izazovima postizanja konkurentnosti usred globalizovanog tržišta. U savremenom poslovnom okruženju, efikasan CRM je neophodan za zadržavanje kupaca. Kako se CRM sistemi oslanjaju na podacima o korisnicima, važno je osigurati integritet podataka. Ovaj rad detaljno analizira izazove preduzeća, CRM i podatke o korisnicima. Glavni cilj ovog rada je pregled postojeće literature i poslovnih praksi u domenu CRM-a. Pored toga, razvijen je model za poboljšanje CRM-a. Model se zasniva na rezultatima pregleda literature i kao takav predstavlja pristup ka unapređenju CRM sistema, uzimajući u obzir integritet podataka o korisnicima.

Ključne reči: CRM; Podaci korisnika; Globalizacija; Digitalna ekonomija; Sigurnost podataka.