finiz
Singidunum University International Scientific Conference
Međunarodna naučna konferencija Univerziteta Singidunum

PAPERS FROM THE THEMATIC AREAS OF THE CONFERENCE
Corporate Governance
Professional paper

# THE INFLUENCE OF PANDEMIC COVID-19 ON CYBER-SECURITY ON THE SERBIAN COMPANIES

Lidija Barjaktarović[1]*,
Sanja Kekić[2]

[1]Singidunum University,
Belgrade, Serbia

[2]ISACA Belgrade Chapter,
Belgrade, Serbia

Abstract:

The subject of the research is to determine the influence of pandemic COVID-19 on cyber-security of the Serbian companies. The aim is to stress the importance of cyber-security risk management in today's business world and permanent learning and investing in cyber-security risk prevention and detection controls. Two online researches conducted in the second quartile of 2020 (with almost 70% response rate) by using Zoom Pulling Feature had the following conclusions: the pandemic of COVID-19 has had influence on cyber-security of Serbian companies in terms of increased number of employees that had access to the corporate network from home, introduced risk management measures for mitigation of potential cyber-attacks and intensity of cyber-attacks on the company's system.

Keywords:

cyber-security, cyber-security risk management, COVID-19, lock-down.

## 1. INTRODUCTION

The subject of the research is to determine the influence of pandemic COVID-19 on cyber-security (CS) of the Serbian companies. The aim is to stress the importance of CS risk management in today's business world and permanent learning and investing in CS risk prevention and detection controls.

Business risks are part of a company's life. Global and local markets are exposed to different risks, and it has impact on a company's performances (Barjaktarovic, 2015). Business risk assessment and management is being impacted by "Black swans" (Taleb, 2010), and currently global situation, including the Republic of Serbia, can be described the same. Especially, in terms of influence of pandemic COVID-19 on CS of the Serbian companies.

In previous period there were different surveys related to the top ten risks in company's business where CS risks were recognized as increasingly significant in the future period.

According to the Federation of European Risk Management Association (FERMA) in 2016 cyber-attack/data privacy was ranked as 7 of 10 top business risks. They estimated low level of satisfaction with mitigation strategies. 2018 was in digital transformation, while 2019 was in preparing for cyber insurance. They stated that in the practice the only positive effect of cyber-event is that companies had become aware of cyber risks they face and that they need to manage their CS exposure. However, many companies are trying to find the most convenient way to do it. (FERMA, 2018) According to Bacanin Dzakula & Strumberg (2018), the cloud organization can be protected if they understand and know from what they should be protected, and can quantify potential damage which can be caused by the attack.

Correspondence:
Lidija Barjaktarović

e-mail:
lbarjaktarovic@singidunum.ac.rs



DOI: 10.15308/finiz-2020-89-96

BDO's survey found out that cyber-attacks are on the 6 of top 10 major risks for the likelihood of occurrence in 2017. They stressed that cyber risks are the third challenge for managing in the next years, and recommended adaptive agility strategy for risk management (BDO, 2017). BDO's Report (2019) suggested that concerns had narrowed from general to more specific. The risk of computer crime such as hacking or malicious viruses comes second, with economic slowdown and slow recovery ranking third.

Allianz Risk Barometer has recognized the importance of cyber-incidents in the top two risks since 2018. In 2018 top two risks were: business interruption – cyber incidents, and cyber incidents – such as new threats like "cyber-hurricanes ". In 2019 and 2020, cyber joins business interruption as a leading global risk for companies for the first time. Other important risks are business interruption and climate change.

AXA's survey (2019) findings are that CS risks were in top ten risks in terms of significance, with increasing impact and challenge for managing. PROTIVITI's study (2019) identified the following 3 top risks for 2019: cyber-threats (as 4-ranked), rapid speed of disruptive innovations and new technologies (as 6-ranked) and privacy/identity management and information security (as 7-ranked). EY & IIF survey (2019) identified as the top main risks in the following decade: protecting privacy to maintain trust (as 3-ranked) and fighting a cyber war in banks and across the system (as 4-ranked). Deloitte's survey (2019) key risk findings were: 1) overriding significance of cyber-risks, 2) increasing focus on non-financial risks and 3) data is the main priority for risk management and IT systems.

It can be concluded that managing CS risk will be a big challenge for all companies in the future.

The article consists of 4 chapters. Introduction is the first chapter. Methodology is explained in the second chapter. Research results are presented in the third chapter. The conclusion is the last chapter.

## 2. METHODOLOGY

On 04/27/2020 and 06/04/2020, ISACA Belgrade Chapter (ISACABC) organized panel discussions related to the influence of pandemic COVID-19 on CS, during which online questionnaires by using Zoom Pulling Feature. Both panels were in the function of continuous education. Therefore, participants had to fulfil application form with relevant personal data in order to get a proper certificate after the panel. ISACABC sent invitation on 176 email addresses and statistics were as follows: 1) on the first panel: 102 applications, 79 participants, 55 respondents; 2) on the second panel: 79 applications, 54 participants, 37 respondents.

Response rates in comparison with the number of present participants were: 1) 69.62% on the first panel, 2) 68.52% on the second panel; and they are relevant for making adequate conclusions. On both panels participants: 1) came from following industries: financial sector – 47%, telecommunication sector – 21%, information technology – 23%, consulting – 7% and other -2%; 2) had predominant expertise in following fields: information security (22%), audit (21%), information technology audit (20%), implementation of security solutions (19%) and risk management (18%).

Both questionnaires had 6 questions with offered answers. Questionnaires were prepared in cooperation between ISACABC and Singidunum University Belgrade (SUB). Questions will be presented in the Research Results chapter. The data analysis employed the use of descriptive statistics. There were two online surveys in order to compare the difference between two periods during COVID -19, i.e. defined as at the time of COVID-19 lock-down and one month after it.

## 3. RESEARCH RESULTS

On the first panel, on the first question related to the increase of number of employees that had access to the corporate network from home, 89% of participants answered positively, i.e. it had increased (Table 1). It goes in line with research of the AM Cham Serbia (2020) where 95% companies- members allow work from home.

25% of participants said that 80% - 100% of employees worked from home. Two equal groups of participants (20% each) answered that 40-60% and 60%-80% of employees worked from home. 13% of participants said that 100% of employees had access to the corporate network from home. Two equal groups of participants (11% each) answered that 0% and 20-40% of employees worked from home.

**Table 1.** Review of answers on the question: How much has the number of employees accessing to the corporate network from home increased in your company?

| Offered answers | No of participants | Relative participation (%) |
|---|---|---|
| 0% | 6 | 11 |
| 20% - 40% | 6 | 11 |
| 40% - 60% | 11 | 20 |
| 60% - 80% | 11 | 20 |
| 80% - 100% | 14 | 25 |
| 100% | 7 | 13 |

On the second question related to the intensity of cyber-attacks on the company's system at the time of COVID-19, 41% of participants answered that it was increased (Table 2). It is below global trend, 58% ISACA Global research / ISACAGR/participant members said that it was increased (ISACA, 2020). This difference could show us concern that some of the cyber-attacks were not detected.

In terms of increased intensity of cyber-attacks, the structure of answers was as follows: 20% of participants said slightly increased, 16% of participants answered increased but not significantly and 5% of participants said significantly increased. 33% of participants said that according to the company's policy it is prescribed not to answer on this type of question. 25% of participants answered that the intensity of cyber-attacks at the time of COVID-19 stayed the same.

**Table 2.** Review of answers on the question: To the best of your knowledge in your company, what was the intensity of cyber-attacks at the time of COVID-19?

| Offered answers | No of participants | Relative participation (%) |
|---|---|---|
| Company's policy prescribed not to answer on this type of question | 18 | 33 |
| Same | 14 | 25 |
| Increased but not significantly | 9 | 16 |
| Slightly increased | 11 | 20 |
| Significantly increased | 3 | 5 |

On the third question related to the types of cyber-attacks at the time of COVID -19, 60% of participants answered mainly the same (Table 3), where 45% of participants said the same but used COVID-19 as the main word and 15% answered the same. 25% of participants said that types of cyber-attacks happened at the time of COVID-19 were somehow different. 15% of participants said that according to the company's policy it is prescribed not to answer on this type of question.

**Table 3.** Review of answers on the question: To the best of your knowledge, which types of cyber-attacks happened at the time of COVID 19?

| Offered answers | No of participants | Relative participation (%) |
|---|---|---|
| Same | 8 | 15 |
| Same just use COVID-19 as main word | 25 | 45 |
| Company's policy prescribed not to answer on this type of question | 8 | 15 |
| Something different | 14 | 25 |

On the fourth question related to the company's number of employees in charge of CS, 98% of participants answered positively i.e. the company has one or more employees in charge of CS (Table 4). Two equal groups of participants: 1) (24% each) said that they had 1 and 1-3 employees in charge of CS, 2) (18% each) answered that they had 5-10 and above 10 employees responsible for CS. 14% of participants answered that they had 3-5 employees in charge of CS. 2% of participants said that they do not have an employee in charge of CS.

Although the answers show a positive result in the sense that companies have employees in charge of CS, it also shows a worrying result, because 50% of companies do not have or have one to three employees in charge of CS. It goes in line with global trends, only 51% ISACAGR participant members are highly confident in their security team's ability to detect and respond to cyber threats during the pandemic (ISACA, 2020).

**Table 4.** Review of answers on the question: To the best of your knowledge in your company, how many employees are in charge for CS?

| Offered answers | No of participants | Relative participation (%) |
|---|---|---|
| 0 | 1 | 2 |
| 1 | 13 | 24 |
| 1- 3 | 13 | 24 |
| 3 - 5 | 8 | 14 |
| 5 - 10 | 10 | 18 |
| above 10 | 10 | 18 |

On the fifth question related to the company's attitude toward CS prevention after COVID 19, 56% of participants said better, 40% of participants answered the same and 4% said worse (Table 5).

**Table 5.** Review of answers on the question: What will be the company's attitude toward CS prevention after COVID-19?

| Offered answers | No of participants | Relative participation (%) |
|---|---|---|
| Better | 31 | 56 |
| Same | 22 | 40 |
| Worsted | 2 | 4 |

On the sixth question related to the reporting line responsibility of the company's Chief Information Security Officer (CISO), 82% of participants answered to the higher managing and ownership function (Table 6). 27% of participants said that the CISO reports to the Executive Director. 20% of participants answered that the CISO reports to the General Manager. 18% of participants said that the CISO reports to IT Directors. 16% of participants said that the CISO reports to the Group CISO. Two equal groups of participants (9% each) answered that the CISO reports to the Executive Board i.e. Supervisory Board and the owner of the company.

**Table 6.** Review of answers on the question: To whom report the CISO in your company according to the organizational structure?

| Offered answers | No of participants | Relative participation (%) |
|---|---|---|
| IT Directors | 10 | 18 |
| General Manager | 11 | 20 |
| Group CISO | 9 | 16 |
| Executive Director | 15 | 27 |
| Executive Board i.e. Supervisory Board | 5 | 9 |
| Owner of the company | 5 | 9 |

It can be concluded that: 1) there was the increased number of employees which had access to the corporate network from home (89% of participants); 2) the intensity of cyber-attacks on the company's system at the time of COVID-19 was increased (41% of participants). It is below global trend (58%), and this difference could show us concern that some of the cyber-attacks were not detected. 3) Types of cyber-attacks at the time of COVID-19 were mainly the same (60% of participants) i.e. 45% of participants said the same but used COVID-19 as the main word and 15% answered the same. 4) The company's attitude towards cyber security prevention after COVID 19 would be better (56% of participants); 5) there was majority of companies which had one or more employees in charge of CS (98% of participants). This can be considered at the same time as positive and worrying result. It is positive in a way that companies have employees in charge of CS; and it is worrying in a way that 50% of companies do not have or have one to three employees in charge of CS. It goes in line with global trends (51%). 6) CISO's reporting line responsibility is to the higher managing line and ownership function (82% of participants).

On **the second panel,** on the first question related to the decreased number of employees that had access to the corporate network after the lock-down, 65% of participants answered positively i.e. the number had decreased (Table 7). In terms of decreased number of employees, the structure of answers was as follows: 24% of participants said it was 0%-20%, 19% of participants answered it was 20%-50%, 14% of participants said it was 50%-80%, 5% of participants answered it was 100% and 3% of participants said it was 80%-100%. 35% of participants answered that there was no decreased number of employees accessing to the corporate network from home in their company after the lock-down.

**Table 7.** Review of answers on the question: How much has the number of employees accessing to the corporate network from home decreased in your company after the lock-down?

| Offered answers | No of participants | Relative participation (%) |
|---|---|---|
| 0% | 13 | 35 |
| 0-20% | 9 | 24 |
| 20% - 50% | 7 | 19 |
| 50% - 80% | 5 | 14 |
| 80% -100% | 1 | 3 |
| 100% | 2 | 5 |

On the second question related to the intensity of cyber-attacks after the lock down, 78% of participants answered the same, as it was in the previous period (Table 8). Two equal groups (11% each) said that it slightly decreased and noticeably decreased, but not significant.

**Table 8.** Review of answers on the question: To the best of your knowledge in your company, what was the intensity of cyber-attacks after the lock-down?

| Offered answers | No of participants | Relative participation (%) |
|---|---|---|
| Slightly decreased | 4 | 11 |
| Same, as it was during the lock-down | 29 | 78 |
| Noticeably decreased, but not significant | 4 | 11 |

On the third question related to the types of cyber-attacks happened after the lock-down, in comparison with the previous period, 85% of participants answer mainly the same (Table 9), where 55% of participants said the same and 30% of participants answered the same but they used COVID-19 as the main word. 15% of participants said different.

**Table 9.** Review of answers on the question: To the best of your knowledge, which types of cyber-attacks happened after the lock-down, comparing to the previous period?

| Offered answers | No of participants | Relative participation (%) |
|---|---|---|
| Different | 6 | 15% |
| Same | 20 | 55% |
| Same just use COVID-19 as main word | 11 | 30% |

On the fourth question related to the intensity of impact of cyber-attacks on a company's assets (damage) after the lock-down, 84% of participants answered mainly the same (Table 10), where 44% of participants said the same, 25% of participants answered slightly increased and 16% of participants said slightly decreased. 16% of participants answered significantly increased.

**Table 10.** Review of answers on the question: What is your opinion on the intensity of impact of cyber-attacks on a company's assets (damage) after the lock-down?

| Offered answers | No of participants | Relative participation (%) |
|---|---|---|
| Significantly increased | 6 | 16 |
| Slightly increased | 9 | 25 |
| Slightly decreased | 6 | 16 |
| Same | 16 | 44 |

On the fifth question related to the introduced measures for risk mitigation of potential cyber-attacks during and after the lock-down period (Table 11), 71% of participants answered yes, where 47% said it was applied essentially and 24% answered it was applied formally. 29% of participants said that companies didn't do anything comparing the lock-down period in terms of introducing appropriate measures in order to mitigate the risks of potential cyber-attacks during and after the lock-down period.

**Table 11.** Review of answers on the question: Did companies introduce appropriate measures in order to mitigate the risks of potential cyber-attacks during and after the lock-down period?

| Offered answers | No of participants | Relative participation (%) |
|---|---|---|
| Yes - formally | 9 | 24 |
| Yes - essentially | 17 | 47 |
| Nothing more comparing the lock-down period | 11 | 29 |

On the sixth question related to the probability of cyber-attacks consequences on the company's business after the lock-down (Table 12), 94% of participants answered mainly the same, where 53% said the same, 25% answered slightly increased and 16% said slightly decreased. 6% of participants answered significantly increased.

**Table 12.** Review of answers on the question: What is your opinion about the probability of cyber-attacks consequences on the company's business after the lock- down?

| Offered answers | No of participants | Relative participation (%) |
|---|---|---|
| Significantly increased | 2 | 6 |
| Slightly increased | 9 | 25 |
| Slightly decreased | 6 | 16 |
| Same | 20 | 53 |

It can be concluded that: 1) there was the decreased number of employees who had access to the corporate network after the lock-down (65% of participants); 2) the intensity of cyber-attacks after the lock down was the same as it was in the previous period (78% of participants); 3) the types of cyber-attacks happened after the lock-down, in comparison with the previous period were mainly the same (85% of participants), i.e. 55% of participants said the same and 30% of participants answered the same but COVID-19 is used as a main word. 4) The intensity of impact of cyber-attacks on a company's assets (damage) after the lock-down stayed mainly the same (84% of participants) i.e. 44% of participants answered the same, 25% of participants answered slightly increased and 16% of participants said slightly decreased. 5) The introduced measures for risk mitigation of potential cyber-attacks during and after the lock-down period were appropriate (71% of participants) i.e. 47% said it was applied essentially and 24% answered it was applied formally. 6) The probability of cyber-attacks consequences on the company's business after the lock-down stayed mainly the same (94% of participants) i.e. 53% said the same, 25% answered slightly increased and 16% said slightly decreased.

## 4. CONCLUSION

Researches conducted in relation to the influence of pandemic COVID-19 on CS of Serbian companies, in cooperation of ISACABC and SUB had good response rates (almost 70%).

98% of participants said that their companies had one or more full time employees in charge of CS area. This can be considered at the same time as positive and worrying result. It is positive because companies have employees in charge of cybersecurity; and it is worrying due to the fact that 50% of companies do not have or have one to three employees in charge of CS. It goes in line with global trends (51%).

82% of participants answered that the company's CISO reporting line responsibility is to the higher managing and ownership function.

There was the increase of number of employees that had access to the corporate network from home during and after the lock-down period. In initial phase there was an increase of 89%, after the lock-down it decreased up to 24%. It is important to notice that majority of companies has become virtual offices, which increases possibility for execution of cyber risks. It means that companies' assets are permanently exposed to damage caused by cyber-attacks, and it requires further education of employees in this field of expertise. Furthermore, it applies on further investments in adequate resources (people and tools) in order to obtain adequate CS risk management.

41% of participants answered that the intensity of cyber-attacks on the company's system at the time of COVID-19 increased. 78% of participants said that intensity of cyber-attacks after the lock down was the same, as it was in the previous period. It can be noticed that there exists concern that some of the cyber-attacks were not detected (comparing to global trends) and maybe companies' security teams are not enough to detect and respond to cyber threats during the pandemic.

60% of participants answered that types of cyber-attacks at the time of COVID -19 are mainly the same, where 45% of participants said the same but COVID-19 is used as the main word and 15% answered the same. 85% of participants said that types of cyber-attacks happened after the lock-down were almost the same, in comparison with the previous period. 55% of participants said the same and 30% of participants answered the same but they used COVID-19 as the main word.

Estimation of 56% respondents regarding the company's attitude toward CS prevention after COVID 19 would be better. Furthermore, 71% of participants said that their companies introduced adequate measures for risk mitigation of potential cyber-attacks during the lock-down. However, the way of applying the measures was different, i.e. 47% applied essentially and 24% formally.

84% of participants answered that the intensity of impact of cyber-attacks on a company's assets (damage) after the lock-down was mainly the same, where 44% of participants said the same, 25% of participants answered slightly increased and 16% of participants said slightly decreased.

Majority of respondents (94%) said that the probability of cyber-attacks consequences on the company's business after the lock-down would be mainly the same, where 53% said the same, 25% answered slightly increased and 16% said slightly decreased.

It can be concluded that pandemic of COVID-19 has had influence on CS of Serbian companies in terms of increased number of employees that had access to the corporate network from home, introduced risk management measures for mitigation of potential cyber-attacks and intensity of cyber-attacks on the company's system. Furthermore, it has had impact on further education of employees in CS field of expertise.

## 5. LITERATURE

Allianz Risk Barometar (2020) Cyber top peril for companies globally for the first time

Allianz Risk Barometar (2019) Cyber joins business interruption as a leading global risk for companies for first time

Allianz Risk Barometer (2018) Top ten ESG related risks for 2018

AM Cham Serbia (2020) Results of query related to the actual and expected economic influence of COVID-19 and measures which should be taken?

AXA (2019) Future risk report

Bacanin Dzakula, N., Strumberg, I. (2018) Cloud Computing, Singidunum University, Belgrade

Barjaktarovic, L. (2015) Risk Management, Singidunum University, Belgrade

BDO (2019) Global Risk Escape

BDO (2017) Global Risk Escape

Deloitte (2019) The future of risk – new game, new rules

EY & IIF (2019) An endurance course: surviving and thriving through 10 major risks over the next decade

FERMA (2018) Preparing for cyber insurance report, available on www.ferma.eu, date of access 06/24/20

FERMA (2017) European Risks and Insurance Report 2016

ISACA (2020) ISACA Survey: Cybersecurity Attacks Are Rising During COVID-19, but Only Half of Organizations Say Their Security Teams Are Prepared for Them

PROTIVITI - *Pool College of Management – Enterprise Risk Management Initiative* (2019) Executive prospective on top risks 2019

Taleb, N.Nicholas (2010). The Black Swan: the impact of the highly improbable (2nd ed.). London: Penguin Random House.