International Journal of Business and Management Review
Vol.5, No.8, pp.43-52, October 2017
Published by European Centre for Research Training and Development UK (www.eajournals.org)

# LEVELS OF CORPORATE APPROACH TO CYBERSECURITY İN MEDIUM AND LARGE ENTERPRISES İN GAZIANTEP

**Mehmet Aytekin[1] and Ahmet Bozgeyik[2]**

[1]Gaziantep University
[2]Hasan Kalyoncu University

**ABSTRACT**: *In this study, the levels of corporate approach to cybersecurity in the context of reducing the risk of cybersecurity have been investigated using survey method in medium and large enterprises in Gaziantep. In this context, as a result of the analysis of the data obtained from 63 enterprises, it has been found out that the enterprises within the scope of the research have a low level of corporate approach to cybersecurity. Also, it has been determined that there are differences in the level of corporate approaches to cybersecurity according to the demographic characteristics of the enterprises covered by the research.*

**KEYWORDS:** Cybersecurity, Corporate Approach, Medıum and Large Enterprıses, Gazıantep

## INTRODUCTION

Emerging technologies offer unique opportunities, but they also lead to cyber threats that can cause unpredictable, complex, and irreparable damages. Businesses are beginning to use technology in different areas and their cyber assets are now under multidimensional threats and risks. These threats and risks are much more intractable than the traditional threats to the business assets (theft, physical deterioration, wearing out, etc.) (Alter & Sherer, 2004; Carr, 2003; Goel & Chen, 2008). Businesses must take precautions to prevent seizure or manipulation of any kind of information that belongs to them by unauthorized people. At this point, the measures taken for cybersecurity should be managed by an institutional perspective and they should not aim solely physical security or technological investment.

Investigations have shown that cyber threats are increasing day by day and the losses organizations face due to cyber threats are also increasing (Marinos, Belmonte & Rekleitis, 2016; Ponemo Institute Research, 2015; Verizon, 2016). Businesses must take the necessary precautions to combat cyber threats and relevant abuses that cause unrecoverable loss. Many researchers have suggested that technological investments will be inadequate, the desired results of those investments will not be achieved and they will result in failure, if the investments which are intended for eliminating possible threats are made without sufficient study (Dhillon & Backhouse, 2001, Baskerville, 1993, Straub & Welke, 1998, Şişaneci et al., 2013). It would therefore be appropriate that those who use the technology especially for public, commercial, and strategic purposes and who are engaged in storage, transmission, and processing activities through these technologies begin combating cyber threats with institutional methods that are far less costly rather than technological investments.

The installation, use, and management of the cybersecurity systems are viewed as an area with little regulation or guidance. A number of studies emphasize that managers have not understood this issue correctly, they have not given enough attention to the issue and their level of awareness has been insufficient.(Vural & Sağıroğlu, 2008; Barrett, 2003; Kudat, 2007).



ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

This situation delays the acquaintance of the enterprises with the concept of corporate cybersecurity management and negatively affects the development of management tools and the safe and efficient use of technology. In cases where senior management in the organizations has begun to value the cybersecurity, we can see that they usually make another mistake by appealing to quick fixes and day-saving remedies and by focusing on technology-based solutions (Richardson, 2008). Cybersecurity can only be achieved by blending technological and managerial elements of combat against cyber threats and using those elements complementarily. In other words, businesses will be more successful and productive if they deal with cyber threats at the corporate level.

In this study, levels of corporate approach to cybersecurity in medium and large enterprises in Gaziantep was investigated by using survey method. With the data obtained in this study, the level of corporate approach related to cyber safety of the companies was determined and whether a difference in the corporate approach to cyber safety exists according to the demographic characteristics was defined.

**Corporate approach to cybersecurıty**

Cybersecurity is a broad concept that expresses the precautions taken against any threats and risks to the information assets of businesses. In the literature, cybersecurity is used in the same sense as the concept of information security since the consequences of a negative event in cybersecurity will affect the information security (Solms & Niekerk, 2013).

Information security is focused directly on the protection of the information on the information technology systems. But in cybersecurity, the main standards of information security, which are privacy, integrity, and accessibility, are being addressed in a wider way, including information and communication tools, systems, and technologies that provide access to information on interconnected networks (Whitman & Mattord, 2009).

Corporate information security can be considered as taking precautions by carrying out necessary security analyses in order to determine institutions' vulnerabilities by identifying information assets and by protecting them from unwanted threats and risks. Corporate information security is composed of complex processes that must be managed under one roof, where many factors such as security, human factor, education, technology influence. The process of standardization in the management of corporate information security around the world is rapidly proceeding in order to manage these processes, to structure security systems according to international standards and to provide information security at a high level (Chang et al., 2001). The corporate information security policy is a set of instructions that encompasses and directs all information security activities to ensure information security in institutions and organizations, and consists of documents that include rules which must be complied by all employees who are authorized to access corporate information resources. Although information security policies differ for each organization, they usually contain general expressions of employee responsibilities, security audit tools, goals and objectives of those tools, and rules and regulations governing the management, protection, distribution and maintenance of important functions of corporate information assets (Kalman, 2003). Today, the standards and practices of methods, tools and audits that can combat cyber threats and risks are being developed every passing day in order to remove them or at least reduce them to an acceptable level.

Cybersecurity can only be achieved by blending technological and managerial elements of



ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

combat and using those elements complementarily (Berghel, 2005; Sundt, 2006). Şişaneci et al. have listed the cybersecurity components that should be based on the development of the cybersecurity capacity in each institution according to its own needs as follows (Şişaneci et al., 2013):

- The cybersecurity approach should be holistic.
- Flexible management style should be adopted.
- Risk management based, continuous improvement methods should be applied.
- For security, besides achieving the coordination of public, private, academic circles, it should also be focused on non-governmental organizations, international cooperation and information sharing.
- Transparency, accountability, ethical values and freedom of expression should be considered.
- It should be able to adjust the balance between security and practicality.

There are not enough studies in the literature about the corporate approach to the cybersecurity. For example, in some studies it is emphasized that managers have not understood cybersecurity correctly, they have not given enough attention to the issue and their level of awareness has been insufficient (Vural & Sağıroğlu, 2008; Barrett, 2003; Kudat, 2007). Segev et al. emphasized the importance of focusing on non-technological elements in the battle against cyber threats in organizations, and highlighted non-technological components (Segev, et al., 1998). Von Solm noted that cyber threats can only be tackled on the basis of organizational and institutional qualifications, legal requirements, best sectoral practices and security technologies (Von Solms, 2000).

Since there is not enough study about the corporate approach to cybersecurity, the level of corporate approach to the cybersecurity of medium and large enterprises in Gaziantep is being investigated in this study. Therefore, it is expected that the findings of this study will contribute to the literature. Based on the assumptions that the levels of corporate approach of the businesses are low, and the levels of corporate approach differs according to the demographics of the enterprises, the following hypotheses will be tested in this study:

Hypothesis 1: The levels of corporate approach of businesses to cybersecurity are low.

Hypothesis 2: The levels of corporate approach of enterprises to cybersecurity differ according to their demographic characteristics.

## RESEARCH METHODOLOGY

In this study, broadly the levels of corporate approach of the businesses in Gaziantep to cybersecurity and whether their approaches to cybersecurity differ according to their demographic characteristics are investigated. Therefore, the scope of this research is limited to those subjects. This work was made in medium and large scale manufacturing companies operating in Gaziantep province of Turkey in 2017. A 5-point Likert scale was used as the data collection method in the study. The cybersecurity corporate approach scale used in the work



ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

was adapted from the study of the Japan Information Technology Promotion Agency's Information Security Management Benchmarking System (http://www.ipa.go.jp).

As of January 2017, there are 324 medium and large scale manufacturing enterprises registered in the Gaziantep Chamber of Industry. Therefore, these 324 enterprises constitute the main mass of the work. Convenience sampling method was used in the study and by utilizing this method, 63 surveys were conducted through face-to-face interview. The data obtained from 63 enterprises were analyzed in the SPSS statistical package program. In this context, the data obtained in the study analyzed through descriptive statistics, factor and reliability analyses, Kruskal-Wallis (H), and Mann-Whitney (U) tests.

## FINDINGS

The data obtained in the study were analyzed using the SPSS 22 statistical program. The findings of those analyses are as follows:

**Table 1. Findings Related to Demographic Characteristics**

| **Number of Employees** | **F** | **%** | **Quantity of Critical Information of the Company** | **F** | **%** |
|---|---|---|---|---|---|
| 50-249 | 32 | 50,8 | Almost no critical information. | 3 | 4,8 |
| 249 + | 31 | 49,2 | Small amount of the information is critical | 13 | 20,6 |
| **Annual Turnover of the Company (USD)** | | | Half of the information is critical. | 44 | 69,8 |
| 100.000–1.000.000 | 3 | 4,8 | Most of the information is critical. | 3 | 4,8 |
| 1.000.000–10.000.000 | 26 | 41,3 | **Dependency Level to Informatics in Business Activities** | | |
| 10.000.000–100.000.00 | 16 | 25,4 | Less than %25 | 11 | 17,5 |
| 100.000.000 + | 18 | 28,5 | %25–%50 | 22 | 34,9 |
| **Cyber Threats Encountered** | | | %50–%75 | 8 | 12,7 |
| Companies That Encountered | 55 | 87,3 | %75 + | 22 | 34,9 |
| Companies That NOT Encountered | 8 | 12,7 | **Total** | **63** | |

As seen in Table 1, 50.8% of enterprises participating in the survey are large enterprises (over 250 employees) and 49.7% are medium scale enterprises (50-249 employees). 53.9% of these enterprises have an annual turnover of more than 10 million USD and 41.3% of them have an annual turnover between 1 and 10 million USD. 82.5% of the participating enterprises have 25% or more dependency on informatics. In other words, these businesses have a high IT dependency and any problem can negatively affect business activities to a great extent. More than half of the information asset of the 74.6% of the businesses which participated in the study



ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

are critical. In addition, 87.3% of the businesses participated in the study encountered a cyber threat. The vast majority of the enterprises covered by the survey are highly dependent on informatics and they are exposed to cyber threats. This suggests that businesses should pay more attention to cybersecurity in order to avoid disruption in business activities and any unrecoverable losses.

**Table 2. Descriptive Statistics, Factor and Reliability Analysis**

| Corporate Approach to Cybersecurity | Mean | St. Dev. | Factor Loading | Alpha |
|---|---|---|---|---|
| Our organization has written rules and policies regarding information security. | 1,74 | 1,015 | 0,832 | 0,911 |
| Our organization has taken into account the risks and security vulnerabilities that may arise in critical areas while creating written rules and policies on information security. | 1,73 | 1,034 | 0,922 | |
| The rules and policies regarding our organization's information security comply with the relevant laws and regulations in our country. | 1,74 | 1,046 | 0,803 | |
| Information technologies that our organization owns are managed by classifying them according to their importance. | 2,39 | 0,833 | 0,793 | |
| Our organization takes the necessary security precautions at all stages of the information life cycle (Information life cycle: creation, usage, storage, transmission, processing and destruction of information). | 2,41 | 0,612 | 0,684 | |
| Our organization incorporates necessary security measures in the clauses of the contracts while purchasing services regarding information technologies. | 1,69 | 0,835 | 0,855 | |
| All of our employees are clearly informed about their information security responsibilities. | 2,25 | 0,761 | 0,648 | |
| Our organization regularly provides information security trainings to all employees. | 1,55 | 0,798 | 0,738 | |
| **General Average** | 1,94 | 0,867 | | |

Factor and reliability analyses were conducted for the variable scale of the corporate approach to cybersecurity which is used in the research. As can be seen in Table 2, the factor loadings of this variable are generally high and the variables are loaded into the relevant factor. This shows that the survey questions used to measure this variable have a unity and they were loaded into the relevant variable correctly. Furthermore, it can be said that as the Cronbach alpha value (0,911) is high, the scale used in reliability analysis is highly reliable.

In Table 2, the mean and the standard deviation values of the corporate approach to cybersecurity variable and the findings related to the factor and reliability analyses are given. Participants' levels of involvement related to their organizations' corporate approach levels of cybersecurity were measured by responses between 1 and 5 (1 = lowest, 5 = highest



ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

participation) in the study. As is evident from the table, it was found that the average values of the variables regarding the corporate approach levels to the cybersecurity of the enterprises are under 2.5 and the general average is 1.94. This suggests that the levels of corporate approach to the cybersecurity in the surveyed enterprises are generally low. Hence, among the hypotheses tested in the context of the research, the hypothesis of "enterprises have low levels of corporate approach to cybersafety" has been supported.

The second hypothesis of the study was analyzed by the H and U tests because the data obtained within the study were not normally distributed (at the result of Kolmogorov Smirnov test) and the sample size was insufficient for some groups (n <7).

**Table 3. Kruskal-Wallis (H) Tests**

| **Dependency Level to Informatics in Business Activities** | | | | | |
|---|---|---|---|---|---|
| | Frequency | Mean Rank | DF | $X^2$ | Sig. |
| Less than %25 | 11 | 23,59 | 3 | 36,185 | 0,000 |
| %25 - %50 | 22 | 18,82 | | | |
| %50 - %75 | 8 | 30,56 | | | |
| %75 + | 22 | 40,91 | | | |
| **Quantity of Critical Information of the Companies** | | | | | |
| | Frequency | Mean Rank | DF | $X^2$ | Sig. |
| Almost no critical information | 3 | 23,00 | 3 | 1,764 | 0,623 |
| Small amount of the information is critical | 13 | 32,50 | | | |
| Half of the information is critical | 44 | 31,76 | | | |
| Most of the information is critical | 3 | 42,33 | | | |
| **Annual Turnover of the Company (USD)** | | | | | |
| | Frequency | Mean Rank | DF | $X^2$ | Sig. |
| 100.000 – 1.000.000 | 3 | 17,00 | 3 | 19,575 | 0,000 |
| 1.000.000 – 10.000.000 | 26 | 23,40 | | | |
| 10.000.000 – 100.000.000 | 16 | 32,63 | | | |
| 100.000.000 + | 18 | 46,36 | | | |

As shown in Table 3, there is a statistical difference of 1% in the corporate approaches of cybersecurity of business activities according to their dependency levels to informatics. That is, the levels of corporate approach of businesses to cybersecurity differs according to their dependency levels to informatics in their activities. To determine among which groups this difference exists, Tamhane test was utilized. As a result of the analysis made, there is a difference of 1% between the enterprises with a dependency level of more than 75% to informatics and with the enterprises less than 25% and between 25% and 50%. In the same way, there is a difference of 5% between the enterprises with the levels of 50% and 75%. There is not any statistical difference between the other groups. According to this result, the



ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

enterprises with a dependency level of more than 75% to informatics in their activities have higher levels of corporate approach to cybersecurity than the other enterprises.

It has been found that there is no statistically significant difference between the levels of corporate approach to cybersecurity according to the amount of critical information that the businesses possess. To put it another way, the levels of corporate approach of the enterprises to the cybersecurity in the study do not depend on the amount of critical information possessed. In other words, the levels of corporate approach of these groups to the cybersecurity is statistically same.

As shown in Table 3, it has been found that there is a difference of 1% between the levels of corporate approach to cybersecurity of the enterprises according to their turnover. In other words, there is a difference in the levels of corporate approach to cybersecurity of the enterprises with different turnovers. To determine among which groups this difference exists, Tamhane test was utilized. As a result of the analysis, it was determined that there is a statistical difference of 1% between the enterprises having annual turnover of over 100 million USD and with the enterprises having annual turnover of between 100 thousand and 1 million USD and between 1 million and 10 million USD. Enterprises with an annual turnover of over 100 million USD have a higher level of corporate approach to cybersecurity than these businesses. This shows that the levels of corporate approach to cybersecurity increase with the rise of the incomes of enterprises. There is not any statistically significant difference between the other turnover groups in the study.

**Table 4 Mann Whitney (U) Tests**

| **Encounter with Cyber Threats** | | | | | |
|---|---|---|---|---|---|
| | Frequency | Mean Rank | Sum of Ranks | U | Sig. |
| Yes | 55 | 34,58 | 1902,00 | 78,00 | ,003 |
| No | 8 | 14,25 | 114,00 | | |
| Total | 63 | | | | |
| **Number of Employees** | | | | | |
| | Frequency | Mean Rank | Sum of Ranks | U | Sig. |
| Between 50 and 249 | 32 | 19,70 | 630,50 | 102,50 | ,000 |
| 259 or more | 31 | 44,69 | 1385,50 | | |
| Total | 63 | | | | |

As shown in Table 4, it has been found that there is a difference of 1% between the levels of corporate approach to cybersecurity according to the encounter of the enterprises to cyber threats and the number of employees. Within the scope of the research, it has been determined that the enterprises that have encountered cyber threats have higher levels of corporate approach to cybersecurity than those who have not encountered cyber threats. According to the number of employees of the enterprises covered by the research, it was found that the levels of approach to cybersecurity was higher in the enterprises with more than 259 employees. In other words, large enterprises have higher levels of corporate approach to cybersecurity.

The hypothesis “The levels of corporate approach of enterprises to cybersecurity differ according to their demographic characteristics”, which is tested in the study, is supported by



ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

the findings obtained through the H and U analyses (Table 3 and Table 4). When we take into consideration the demographics of the enterprises, it is determined that there are statistically significant differences between the levels of corporate approach to cybersecurity with one exception (according to the amount of critical information that enterprises have). This situation provides the sufficient condition to support the second hypothesis tested in the research. Because in order to support this hypothesis, the difference of the level of corporate approach to cybersecurity is sufficient according to at least one demographic characteristic.

## CONCLUSION

In this study, in general the levels of corporate approach to cybersecurity of enterprises are analyzed. In this context, as a result of the analysis of the data obtained from medium and large enterprises in Gaziantep province of Turkey through the survey method, the following conclusions can be drawn:

In this study, it is determined that the vast majority (87.5%) of the enterprises covered by the survey encountered cyber threats and the vast majority of these enterprises (82.5%) have a dependency level of more than 25% to informatics. On the other hand, it has been found that the levels of corporate approach of enterprises covered by the survey to cyber safety are low (1.94 out of 5). This suggests that the levels of corporate approach of enterprises to cybersecurity are inadequate. Because the majority of the enterprises covered by the survey encountered cyber attacks. It is therefore necessary for businesses to give more importance to cybersecurity and to approach to cybersecurity at corporate level in order to prevent the disruption of their business activities, and to avoid any unrecoverable losses and cyber attacks. Otherwise, they may have serious problems in their operations and in maintaining their assets.

It has been found out that there is a statistically significant difference between the levels of corporate approach of the enterprises to cybersecurity according to their dependency levels to informatics in their activities. That is to say, the corporate approach of businesses to cybersecurity differs according to their dependency levels to informatics in their activities. This difference was found to be between the enterprises which have a dependency level of more than 75% to informatics in their activities and the enterprises with a level of less than 25%, between 25% and 50%, and between 50% and 75%. There is no statistical difference between the other groups. The enterprises which have a dependency level of more than 75% in their activities have a higher level of corporate approach to cybersecurity than that of other enterprises. In other words, as the dependency level of the enterprises to informatics increases, their approach to cybersecurity is more institutionalized. This is a natural outcome.

In this study, no statistically significant difference between the levels of corporate approach to cybersecurity was found according to the amount of critical information that businesses possess. This result shows us that the levels of corporate approach of businesses to cybersecurity do not depend on the amount of critical information of the enterprises. In fact, as the amount of critical information that businesses possess increases, it is expected that the level of corporate approach to cybersecurity will be higher. However, as we could not draw such a conclusion from the study, this situation may result from the data obtained in the research or from the interpretation of the enterprises that all the information they possess as critical at the same level.



ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

As a result of the research, it was determined that the levels of corporate approach to cybersecurity differs according to the turnover of the enterprises. This result shows us that as the incomes of the enterprises increase, they approach institutionally to cybersecurity. In addition, it has been found that the enterprises that encountered a cyber threat have a higher level of corporate approach to cybersecurity than the ones that did not encounter a cyber threat. According to the number of employees of the surveyed companies, it was determined that the levels of approach to cybersecurity were higher in the enterprises with more than 259 employees. In other words, we can see that large enterprises have higher levels of corporate approach to cybersecurity.

## REFERENCES

Alter, S., & Sherer, S. (2004). A general, but readily adapable model of information system risk. Communicaitons of the AIS , 14(1),1-28.

Barrett, N. (2003). Penetration testing and social engineering: Hacking the weakest link. Information Security Technical Report, 8(4), 56-58.

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. ACM Computing Surveys, 25, 375–414.

Carr, N. (2003). It doesn't matter. Harvard Business Review 81 (5), 41-49.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal, 11, 127–153.

Goel, S., & Chen, V. (2008). Can business process reengineering lead to security vulnerability: analyzing the reengineered process. International Journal of Production Economics 115 (1), 104-112.

Kalman, S., "Web Security Field Guide", Cisco Press, Indianapolis, sf.36, 37, 2003.

Kudat, B. (2007). Kötü adamların hızına yetişen daha güvenli. BThaber, 6004:15.

Marinos, L., Belmonte, A., & Rekleitis, E. (2016). ENISA Threat Landscape 2015. European Union Agency For Network And Information Security.

Ponemo Institute Research. (2015). 2015 Cost of data breach study: Global Analysis. Ponemo Institute L.L.C.

Richardson, R. (2008). CSI/FBI Computer Crime & Security Survey. CSI.

Segev, A., Porra, J., & Roldan, M. (1998). Internet security and the case of Bank of America. Communications of the ACM, 41, 81–87.

Sisaneci, İ., Akin, O., Karaman, M., & Saglam, M. (2013, Eylül 20-21). A Novel Concept For Cybersecurity: Institutional Cybersecurity. 6th International Conference on Information Security and Cryptology, 89.

Solms, V., & Niekerk, V. (2013). From Information security to Cyber Security. Computers & Security 38, 97-102.

Straub, D., & Welke, R. (1998). Coping with systems risks: security planning models for management decision making. MIS Quarterly, 22, 441–469.

Verizon. (2016). Verizon's 2016 Data Breach Investigations Report. Verizon. http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf adresinden alınmıştır

Von Solms, B. (2000). Information security – the third wave? Computers & Security, 19(7), 615-620.

Vural, Y., & Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları üzrine bir inceleme. Gazi Üniversitesi Müh, Mimarlık Fakültesi Dergisi Cilt 23, No 2, 507-522.



ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)

Whitman, M. (2003). Enemy at the gate: threats to information security. Communications of the ACM, 46(8), 91-95.

Whitman, M., & Mattord, H. (2009). Princeples of Information Security 3rd Ed. Thomson Course Technology.

http://www.ipa.go.jp/security/english/benchmark_system.html



ISSN: 2052-6393(Print), ISSN: 2052-6407(Online)