CYBERLOAFING BEHAVIOR IN THE WORKPLACES AND MANAGEMENT PRACTICES

A THESIS SUBMITTED TO

THE INSTITUTE OF SOCIAL SCIENCES

OF

ANKARA YILDIRIM BEYAZIT UNIVERSITY

BY

YASEMIN KASAP

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN THE DEPARTMENT OF MANAGEMENT AND ORGANIZATION

MAY 2019

Approval of the Institute of Social Sciences

_____

Assoc. Prof. Dr. Seyfullah YILDIRIM

Manager of Institute

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Sciences.

_____

Prof. Dr. Nilay ALÜFTEKIN SAKARYA

Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master Sciences.

_____

Prof. Dr. Kerim ÖZCAN

Advisor

Examining Committee Members

Prof. Dr. Kerim ÖZCAN	(AYBU, Management)	_____
Assoc. Prof. Hasan E. ŞENER	(AYBU, Management)	_____
Assoc. Prof. Çağdaş H. ALADAĞ	(Hacettepe University, Statistics)	_____

I hereby declare that all information in this thesis has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work; otherwise I accept all legal responsibility.

Name, Last name : Yasemin Kasap

Signature :

ACKNOWLEDGMENT

I am very grateful to Prof. Dr. Kerim Özcan, for his dedication and valuable contribution at each stage throughout my graduate study. It has been a great honor to prepare this study within your guidance.

I would like to express my gratitude to my jury members Assoc. Dr. Hasan Engin Şener and Assoc. Dr. Çağdaş Hakan Aladağ for their valuable contributions to this study. I am also very thankful to Prof. Dr. Orlando Rua for his guidance in my exchange semester in Portugal.

I dedicate this dissertation to my father Kemal, my mother Semahat and my brother Orçun. I appreciate your love, support, understanding, endurance, and sharing my milestones on this master study. Last but not least, I would like to express my special thanks of gratitude to Markus who has supported and encouraged me in every part of my life since Portugal and Maşide as well as my other friends who were always with me in this journey.

Yasemin KASAP

Ankara, 2019

ABSTRACT

CYBERLOAFING BEHAVIOR IN THE WORKPLACES AND MANAGEMENT PRACTICES

Yasemin Kasap

Master, Department of Management and Organization

Supervisor: Kerim Özcan

May 2019, 89 Pages

Within the widespread use of information technologies in the workplaces, cyberloafing has become one of the greatest problems of the organizations and negative aspects of this behavior have led business managers to develop control mechanisms. However, in recent years, there has been a controversial perspective regarding the effectiveness of these control mechanisms such as computer monitoring and organizational policies. Therefore, within this research, it is aimed to broadening our understanding of cyberloafing behavior in the workplaces and how management practices affect cyberloafing intention of employees. The data were collected through a web-based survey from 380 employees of bank branches in Ankara province and collected data were analyzed with IBM SPSS 22 program. The findings support the general deterrence theory and reveal that intentions for cyberloafing behavior may be reduced by enforcing the organizational sanctions and computer monitoring systems. The findings are expected to contribute to the development of human resources practices and management strategies to be more effective in dealing with cyberloafing behavior.

Key Words: Cyberloafing, Organizational Behavior, Control Strategies, Counterproductive Work Behavior

ÖZET

İŞYERLERİNDEKİ SİBER AYLAKLIK DAVRANIŞI VE YÖNETİM UYGULAMALARI

Yasemin Kasap

Yüksek Lisans, Yönetim ve Organizasyon Bölümü

Danışman: Kerim Özcan

Mayıs 2019, 89 Sayfa

İşyerlerinde bilişim teknolojilerinin yaygın biçimde kullanılmaya başlanması ile birlikte, siber aylaklık organizasyonların en büyük sorunlarından biri haline gelerek, bu davranışın olumsuz yönleri işletme yöneticilerini çeşitli kontrol mekanizmaları geliştirmeye yöneltmiştir. Ancak, son yıllarda, bilgisayar izleme ve organizasyon politikaları gibi kontrol mekanizmalarının etkinliğine ilişkin tartışmalı bir bakış açısı görülmektedir. Bu nedenle, bu araştırma kapsamında, işyerlerindeki çalışanların siber aylaklık davranışı hakkındaki bilgilerimizi zenginleştirerek, siber aylaklık davranışını azaltmak amacıyla geliştirilen yönetim uygulamalarının, çalışanların siber aylaklık yapma niyetini nasıl etkilediğini araştırmak amaçlanmaktadır. Araştırmada kullanılan veriler, Ankara ilindeki 380 banka şubesi çalışanları ile web tabanlı bir anket aracılığıyla toplanmış ve toplanan veriler IBM SPSS 22 programı ile analiz edilmiştir. Bulgular, genel caydırıcılık teorisini desteklemekte ve kurumsal yaptırımlar ve bilgisayar izleme sistemlerini kullanarak çalışanların siber aylaklık davranışını gösterme niyetlerinin azaltılabileceğini ortaya koymaktadır. Bulguların, insan kaynakları uygulamalarında ve siber aylaklık davranışıyla başa çıkmada daha etkili olması için yönetim stratejilerinin geliştirilmesine katkıda bulunması beklenmektedir.

Anahtar Kelimeler: Siber Aylaklık, Organizasyonal Davranış, Kontrol Stratejileri, Üretken Olmayan Davranış

TABLE OF CONTENTS

ABBREVIATIONS

CWB:	Counterproductive Work Behavior
GDT:	General Deterrence Theory
SPSS:	Statistical Package For The Social Science
WDB:	Workplace Deviant Behavior

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

Developments in information and communication technologies and widespread use of the internet at the workplaces have created certain advantages for the organizations by reducing the operational costs, accelerating and facilitating the business operations and creating an innovative business environment. On the other hand, digitalized workplaces and internet access have raised some concerns regarding productivity and performance of employees, cybersecurity, organizational liability and misuse of information technology resources of the organization. Considering the high volume of competition in the industries within globalization trends, it has become a necessity for organizations to use the time in an effective way beside the organizational resources they have in order to sustain their existence. Therefore, in order to achieve organizational goals, employees have been expected to use their working time effectively and reduce deviant workplace behaviors which do not benefit the organization while performing their duties and responsibilities (Fındıklı, 2016). For this reason, as a new form of workplace deviant behaviors, "cyberloafing" has attracted great attention as it refers to non-work related internet activities of employees during working hours and it has positive and negative impacts on individuals and organizations.

Researchers revealed that employees spend up to 60% of their working hours on non-work related activities on the internet (Koay and Soah, 2018) such as sending and receiving e-mails, shopping, playing online games, conducting personal businesses, using social networks and other types of browsing activities (Weatherbee, 2010). Scholars mainly have two different counter-views regarding impacts of cyberloafing behavior on individuals and organizations. Particular cyberloafing behaviors have been found as constructive for organizations in terms of enhancing work-related knowledge, providing recovery from work stress and motivating the employees to be more creative and innovative which leads to an increase in the productivity and performance (Ivarsson and Larsson, 2011). Conversely, a considerable amount of studies emphasize the destructive side of cyberloafing which may cost a billion dollars to the organization by inefficient time management and misuse of the information technologies (Henle & Blanchard, 2008). Furthermore, cyberloafing activities may cause vulnerabilities and information security threats as well as legal problems which may create additional costs to organizations. Additionally, compared to offline slacking

activities which may be recognized by employer easily, cyberloafing behavior is more difficult to control, as employees could engage cyberloafing activities at the same time being present at their work station. Therefore, the vast majority of organizations develop and implement several controlling and deterrence mechanisms such as organizational policies, computer monitoring strategies (Giles, 2015) and sanctions to regulate cyberloafing behavior of the employees.

Considering the advancements on information and communication technologies, cyberloafing domain has been changed in the last decades. Today, employees are able to engage cyberloafing activities not only with work computers or other electronic devices which are provided by the company but also with their personal electronic devices such as smartphones, tablets and smartwatches (Saraç and Çiftçioğlu, 2014). Moreover, compared to other types of offline slacking activities, for instance, having coffee breaks, cyberloafing is more difficult to recognized by management as employees are present in their workplace. When these facts are taken into consideration, companies face great challenges to have control over employees' internet activities. Therefore, the effectiveness of control mechanisms has great importance for human resource management and middle managers, in order to cope with cyberloafing behavior of employees in the best way (Abbasi,2018).

Since existing studies in the literature have more concentrated on cyberloafing behaviors' antecedents and consequences on organization within a scope of the public sector and students, there has been a gap in the literature regarding effectiveness of the deterrence mechanisms on cyberloafing behavior intention in the workplaces. In this context, this study aims to broaden our understanding regarding cyberloafing behavior in the workplaces and examine the causal relationship between managerial practices and cyberloafing intention of the employees by the means of General Deterrence Theory.

In light of these objectives, the literature review constitutes three parts to shed light onto cyberloafing behavior and theoretical background of the research area. In the first part, deviant workplace behaviors and as a new type of workplace behavior, the emergence of cyberloafing behavior have explained. In the second part of the literature review, by synthesizing existing studies in the literature, cyberloafing behavior's typologies, the motives of the behavior, the impacts on individuals and the whole organization and management practices towards the negative side of this behavior were covered in detail. In

the last part, cyberloafing behavior has been approached by General Deterrence Theory and components which are sanction (detection) certainty and sanction severity have been explained in detail.

In order to achieve the aim of the research, quantitative research method web-based survey has been conducted on employees in the banking industry and statistical analysis has been implemented. Based on findings of the research, the relationship between control mechanisms and cyberloafing intention of individuals have been evaluated and the valuable suggestion has been made for managerial implications and future studies.

2. LITERATURE REVIEW

2.1. Deviant Workplace Behavior

Organizations are entities which are consisting of a group of people from different background, personality and behavioral patterns for a particular purpose. The acts of employees may have positive or negative consequences on other employees, whole internal or external environment of the organization and even on the business operations. Therefore, every organization adopts a set of rules and norms in order to regulate individual behaviors within the organization and ideally, employees are expected to comply with these regulations. However, occasionally employees tend to violate these expectations and show deviant workplace behavior (DWB) alias counterproductive work behavior (CWB). Workplace deviance defined by Robinson and Bennett (1995) as "voluntary behavior that violates significant organizational norms and in so doing threatens the well being of an organization, its members or both". Similarly, Sackett and DeVore (2002) defined counterproductive work behavior as "intentional acts of the individuals on the part of an organization member viewed by the organization as contrary to its legitimate interests".

In the literature different terminologies are used to define deviant workplace behavior such as counterproductive work behavior (Fox and Spector, 2005), dysfunctional work behavior (Robinson, 2008), organizational misbehavior (Vardi and Weitz, 2004) and non-compliance workplace behavior (Alter, 2015). However, each of these terms represents similar non-related work activities by employees which could have various impacts on organization and individuals. Furthermore, in the literature, WDB and CWB are the most common terms used interchangeably. Therefore, throughout this thesis, the term workplace deviance behavior and its abbreviation will be used referring to the intentional not work-related acts of a member of an organization which does not comply with regulations.

The deviant workplace behavior contains a large scale of activities which may range in minor activities such as chatting with colleagues to serious activities such as defalcating money from the company (Bennett and Robinson, 2000). By analyzing the literature, Gruys (1999) introduced 87 different types of deviant behaviors and divided them into 11 categories such as theft, damage of property, misuse of organizational sources, time and information, inappropriate absences, verbal and physical actions, poor quality of work and noncompliance

with safety procedures and using illegal or addictive substances. Each type of deviant behavior is defined by similar characteristics which are mostly intentional, unethical, undesirable, violation of rules of behaviors, noncompliance of organizational policies or even illegal (Gruys, 1999). Although each behavior has similar properties, it may differ in severity, target, and consequences on the organization, for this reason, each type of behavior evaluated with its consequences on the organizations.

DWB has been examined by scholars mainly in two aspects as positive and negative deviant workplace behaviors. While negative deviant workplace behavior represents negative consequences for the well-being of an organization, positive workplace deviant behavior refers to the positive outcome of the deviant behavior which may help the organization to reach its operational and financial goals (Appelbaum, Iaconi and Matousek, 2007). However, in the literature, negative deviant workplace behaviors have attracted a great deal of interest as it is important to find the motives behind these behaviors and prevent them to avoid undesired negative impacts on the organization.

By improving preliminary concepts on negative deviant workplace behaviors, Robinson and Bennett (1995) introduced conclusively detailed and comprehensive classification which brought a broader perspective in workplace deviant behavior typologies in literature. The authors defined four quadrant labels for the types of deviance behaviors and used two dimensions to evaluate the impact levels of the deviant behaviors on organizations. While serious versus minor dimension represents the severity of the workplace deviant behaviors, organizational versus interpersonal dimension represents the target domain of the deviance behavior.

- *Property Deviance*: This type of deviance behaviors refer to damaging acts of the individuals to the organizational assets without the permission of the management (Hollinger and Clark, 1983) and it can have severe effects on organizations (Robinson and Bennett, 1995). Damaging physical assets, involving bribery, misinforming about working hours, stealing company properties for self-use or interest are some forms of the property deviance. Some of these acts can result in disruption of work as the equipment needs to be replaced.
- *Production Deviance*: These types of workplace deviance behaviors defined by Hollinger and Clark (1983) as “Behaviors which violate the formally proscribed

norms delineating the minimal quality and quantity of work to be accomplished." Starting late and leaving early, working less or slower, using organizational resources in vain, taking sick leaves for no reason are the typical production deviance behaviors (Robinson and Bennett, 1995).

- *Political Deviance*: As one of the interpersonal deviant behavior, political deviance is defined by Robinson and Bennett (1995) as "Engagement in social interaction that puts other individuals at a personal or political disadvantage". Destructive competition between co-workers, nepotism, unfriendly behaviors against colleagues is some of the examples.

- *Personal Aggression*: As one of the serious and interpersonal deviant behavior, personal aggression refers to demonstrating aggressive and unfriendly behaviors towards other co-workers. Misbehaving and cast aspersion on co-workers, verbal or physical abuse, hindering work-related aims and success of co-workers are some of the most observed personal aggression forms (Robinson and Bennett, 1995).

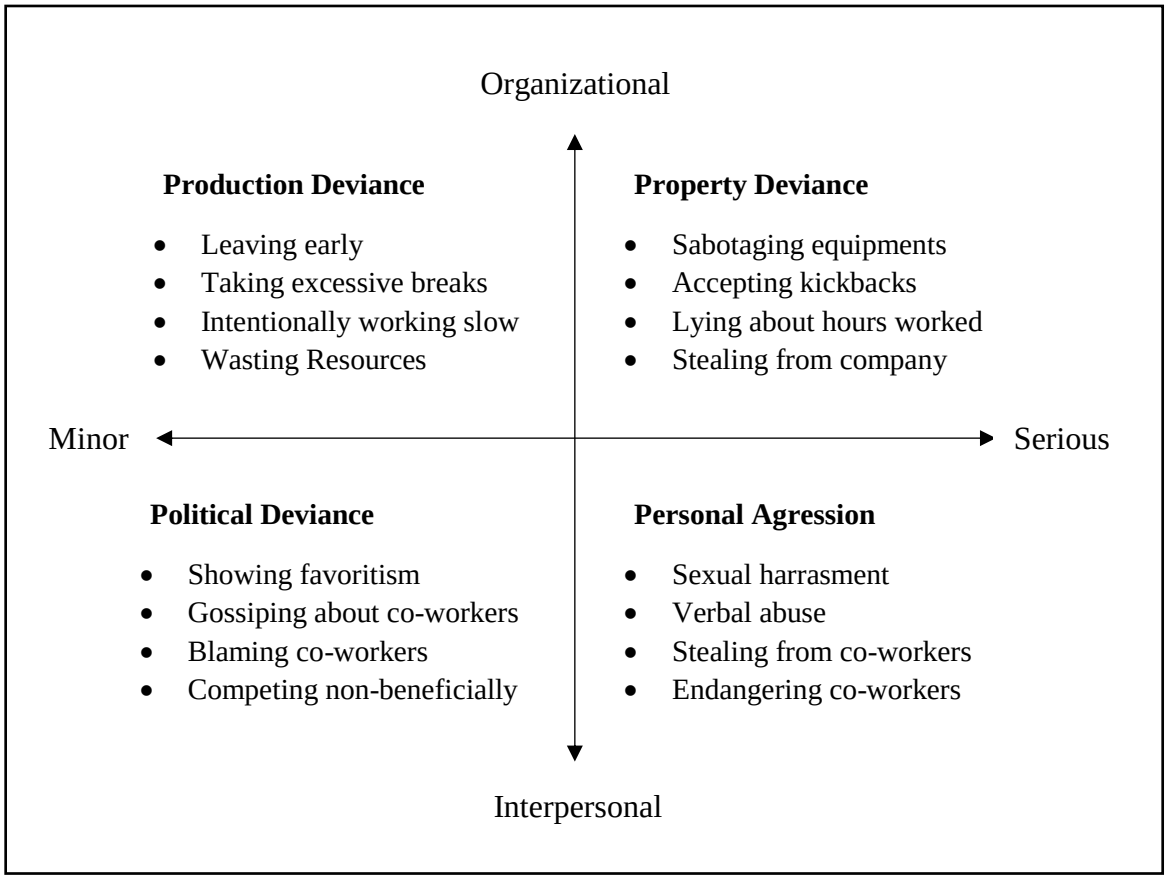

Figure 1. Deviant Behavior Typology

The common feature of all negative deviant behaviors is that they have negative impacts on businesses, organizations, and individuals. From a business perspective, Coffin (2003) states that up to 75 percent of all employees steal from company's properties at least one time and workplace deviant behaviors such as theft and fraud costs billion dollars to businesses in the United States. From an organizational perspective, Greenberg and Barling (1999) found out than 82 percent of the employees experienced psychological aggression acts against a coworker which can create interpersonal conflicts in organizations. Respectively, from a personal perspective, employees engaged with workplace deviance activities may suffer from stress-related problems, having a problem within their performance and motivation.

Most studies in the field of workplace deviance have identified numbers of deviance behaviors and focused on only negative impacts of deviant behaviors in the workplace which may be harmful to organizations. Nevertheless, there are also positive impacts of work deviance behaviors which could result in an advantage for work-related success and organizational goals. Positive deviant behavior in the workplace is defined by Spreitzer and Sonenshein (2003) as ''intentional behaviors that depart from the norms of a referent group in honorable ways" which may support to the organization in order to reach its business and financial goals. According to Vadera, Pratt, and Mishra (2013), some of the constructive behaviors are given below.

- Extra-role behaviors: The intentional act of an employee which is beyond his/her task to be beneficial to the organization.

- Creative performance: The emergence of new ideas, innovations, solutions for the organizational problems although it may be against norms or policies of the companies.

- Prosocial rule breaking: Employees' intentional act to promote the organization's welfare or its stakeholders while violating the regulations or policies.

- Issue selling: Dutton and Ashford (1993) defined issue selling as "Individuals' behaviors that are directed toward affecting others' attention to an understanding of issues". In organizations, by concealing and sharing the information about the particular issue, using the resources in a particular way, it can be seen that lower level managers can take attention to some issues.

Based on a considerable amount of literature has been published shows that not every positive deviant behavior creates a positive outcome although the intention of the employee is positive. Moreover, some deviant behaviors may be categorized as constructive (positive) or destructive (negative) at the same time due to the business case (Appelbaum et al., 2007). For example, whistleblowing may be perceived as negative deviant behavior, but it may be also categorized as positive when an employee makes a disclosure to its supervisors about illegal activities of other co-workers.

As a result of developments in information technologies and widespread use of the internet and smart devices in the workplaces, workplace deviant behaviors shifted to cyber spaces and the new term which is called "cyberloafing" has arisen. Although the main logic is the same with other deviant behaviors, cyberloafing is differentiated from other workplace deviant behaviors by the environment which it occurs in. Cyberloafing refers to any types of non-work related activities which are carried out by individuals via the internet, during working hours (Brock et al., 2013) In the literature, there is no specific categorization agreed upon for cyberloafing activities among other deviant behaviors but scholars mainly classified cyberloafing as a form of WDB or workplace procrastination behavior (Metin, Taris, and Peeters, 2016). Considering the typology of deviant behaviors which is presented by Robinson and Bennett (1995), cyberloafing can fall under production and property deviances. Using work computers and internet connection for personal interests, taking excessive breaks for cyberloafing activities can be seen as a part of production deviance while engaging cyberloafing activities in working hours and misinform the management about actual working duration may be categorized under property deviance. For this reason, by and large, in the literature and in this thesis cyberloafing has been categorized under workplace deviant behaviors which examines an individual's behavior related to misuse of the computer resources and internet which is provided by the company.

As it is mentioned more detailed in the next part of the thesis, cyberloafing may be also constructive or destructive and minor or serious depending on the situation. On the one hand, the different types of cyberloafing activities found positively associated with relieving the stress, increasing the creativity, reducing the operational costs and more (Warren, 2003). On the other hand, destructive cyberloafing activities may damage legitimacy, create conflict in the organization, cause security issues and data leakage within the company. Moreover, in a similar way with other workplace deviant behaviors, cyberloafing also creates high costs for

business owners. By synthesizing the cyberloafing reports in different countries, Lim and Chen (2012) reported that in the UK employees spend half of their working hours with cyberloafing activities which cost to business approximately £150 Million per year. Another research revealed that engaging with cyberloafing activities may reduce the productivity of employees by up to 37 percent (Verton, 2000). Since the internet and smart devices became inevitable for a business environment, it has been crucial to minimize the negative impacts and support the effective and proper use of information technologies in accordance with rules. For this reason, day by day cyberloafing is becoming a popular concept among other deviant behaviors and companies develop specific deterrence mechanisms against to detrimental impacts of this behavior.

2.2. Cyberloafing

2.2.1. Definition of Cyberloafing Behavior

Slacking off during working hours has been always a big issue for companies. Before the usage of Internet and computers, employees were "slacking off" in offline ways such as coffee brakes, booking meeting rooms for resting, having smoking breakes and doing other activities which are not work-related. Within the advances in information technologies, at the beginning of the 1990s, internet and computers started to be used in workplaces and in accordance with this, employees started using computers for playing games, browsing the internet, reading newspapers, watching videos or carrying their own personal works. In addition to computers, the emergence of mobile phones and its transformation to smartphones also increased the "cyberloafing" acts in the workplaces.

Cyberloafing is a compound term which is derived from a prefix "cyber" and activity "loafing". "Cyber" refers to a prefix relating to computers, information science or internet and "loafing" means an activity which is conducted by a person who spends his or her time in an aimless-idle way. As a term, cyberloafing has been widely used since the middle of the nineties. In their research, Lim, Teo, and Loo (2002, p.67) defined cyberloafing as "any voluntary act of employees using their company's Internet access during office hours to surf non-work-related web sites for non-work purposes, and access non-work related email". Cyberloafing simply refers that individuals' use of work computers and internet access to spend their time during working hours for non-work related activities instead of working.

There are various terms and concepts has been used to describe cyberloafing activities such as cyberslacking (Beugre, 2003), personal internet usage (Lee, Lee & Kim, 2004), junk computing (Guthrie and Gray, 2007), internet abuse (Anandarajan, 2002), and internet addiction (Kim and Bryne, 2011) as it is shown in Table 1. However, although the terms can vary, the scholars agree on these activities that have three common facts, namely, cyberloafing activities performed by employees voluntarily through organizational IT sources or within their personal mobile devices, for non-work related personal purposes and during working hours (Jiang, 2016). In this respect, cyberloafing is dissociated from other types of deviant behaviors as it allows employees to present physically in the workplaces while they are loafing and taking a break from their tasks through internet activities.

Term	Definitions	Author
Cyberloafing	"Employees voluntary non-work related use of company provided email and Internet while working."	Blanchard and Henle, 2008, p.1068
	"The deliberate usage of IT for non-business affairs in the workplace."	Jandaghi, Alvani, Zarei Matin, Fakheri Kozekanan, 2015, p.337
Junk Computing	"An employee`s usage of organizational IS resources for personal purposes, not directly related to organizational goals."	Bock and Ho, 2009, p.125
Personal Web Usage	"Voluntary online Web behaviors during work time using any of the organization's resources for activities outside current customary job/work requirements."	Anandarajan and Simmers, 2004, p.19
Cyberslacking	"The overuse of the Internet in the workplace for purposes other than work."	Whitty and Carr, 2006, p.237
	"The usage of e-mail and Internet opportunity unrelated to a job in office hours for the aims that are supplied to workers."	Phillips and Reddie, 2007

Table 1. Typologies of Cyberloafing Term

Furthermore, although cyberloafing typologies have been developed on the basis of computers at workplaces, there can be many kinds of communication tools to engage with cyberloafing. Within the advancements in the information and communication technologies, smartphones, tablets, smart watches enable users to access internet and cyber-spaces without time and location restrictions (Giles, 2015). Statista (2019) research revealed that by the end of 2019, the number of smartphone users will reach 2.1 billion in worldwide. Moreover, according to Digital 2019 in Turkey report, 77% of the population use smartphones, 25% of the population has tablets and 9% of the individuals own wearable tech devices such as smartwatches. These statistics show that cyberloafing domain has been changed in recent years and not only work computers, employees may also engage cyberloafing activities through their personal electronic devices (Askew, 2012).

In addition to the distinctive characteristics, cyberloafing has a solid presence in the organizations. Research by Vault.com (2000) revealed that nearly 88% of employees use the internet for non-work-related Web sites and 82% of the employees send and receive personal emails during working hours (Henle and Blanchard, 2008). According to the result of the American Management Association's research, more than 50% of the internet activities are non-related with work (Greenfard, 2000). Similarly, a study from the Wisconsin School of Business indicates the amount of time employees spend cyberloafing is estimated to range from three hours a week to as much as two and a half hours per day. More recent research by Salary.com (2018) reported that 64% of employees stated that they browse the internet for non-work related activities every day and among the various types of internet activities, it was found that participants mostly spend their time on the internet via visiting websites such as news, social media, online shopping, entertainment and lifestyle, sports and travel.

2.2.2. Types of Cyberloafing

As individuals have different background, values, interests, and personalities, cyberloafing behaviors may vary from person to person. Individuals may use the internet for surfing, shopping, personal communication, playing a game or personal business purposes. In literature cyberloafing mainly categorized based on types of behavior and activities.

As a type of behavior, cyberloafing may be classified into four different categories such as development behavior, recovery behavior, addiction behavior and deviant behavior (Doorn, 2011).

- *Deviant behavior:* As it has been discussed in the first chapter of this thesis, many scholars argued that cyberloafing with negative consequences on the organization can be categorized under deviant behaviors considering these types of behaviors are undesired behaviors of individuals from organizations side (Weatherbee, 2010).

- *Recovery behavior:* Particular cyberloafing behaviors may reduce anxiety and work-related stress and help employees to relax their mind. Consequently, cyberloafing activities may have positive on employees' mental health and work performance and these types of cyberloafing activities may be classified as recovery behavior.

- *Development behavior:* Cyberloafing activities considered as development behavior when employees use the internet for learning new things and improving their

knowledge which is related to work (Brakel, 2016). These types of cyberloafing activities may be beneficial for employees to perform their tasks and create positive impacts on the organization in general.

- *Addiction behavior:* Employees who have internet addiction in their personal life may also cause problems in work-life regarding interpersonal relationships and productivity. Therefore, when employees engage in cyberloafing activities because of their addiction to the internet, such cyberloafing behavior may be categorized under addiction behavior. From the organizational side, these types of behaviors are undesirable as it affects employees work satisfaction and mental health in a negative way.

On the other hand, scholars categorized cyberloafing activities mainly based upon their functions, relations to productivity and impacts on organizations which are presented in Table 2.

Based on workplace deviance typology which is developed by Benett and Robinson(1995), Blanchard and Henle (2008) categorized cyberloafing activities in two sections as minor and serious cyberloafing activities. The researchers defined minor cyberloafing activities as common usage of email and the Internet at work, for instance; personal communications via email, visiting personally interested websites; banking, sports, shopping related websites or non-internet loafing behaviors such as chatting with friends, phone calls, reading newspaper and coffee break (Blanchard and Henle, 2008). These types of cyberloafing activities considered as harmless by researchers in contrast to serious cyberloafing activities. Serious cyberloafing activities are described as serious forms of cyberloafing those behaviors which are abusive and potentially illegal such as online gambling, visiting adult-oriented websites and other illegal activities through the Internet (Case and Young, 2002).

Lim and Chen (2002), divided cyberloafing activities into two categories as browsing activities and email activities. Within browsing activities they covered browsing sports related websites, investment related websites, entertainment related websites, general news sites, non-work related websites, downloading non-work related information, shopping for personal interests, adult-oriented (sexually explicit) websites. Additionally, the scholars examined the impacts of browsing and emailing activities on employees' emotion and found

that browsing activities affect positively while emailing activities have negative impacts on employee's emotions (Lim and Chen, 2012).

Authors	Type of Cyberloafing Activities
Blanchard and Henle (2008)	• Minor cyberloafing activities • Serious cyberloafing activities
Lim and Chen (2002)	• Browsing activities • Emailing activities
Mahatanankoon, Anandarajan, and Igbaria (2004)	• Purchasing and personal business • Seeking and viewing information • Interpersonal communication • Interactive entertainment and pass time • Personal downloading
Li and Chung (2006)	• Social function • Informational function • Leisure function • Virtual emotional function
Mastrangelo, Everton, and Jolton (2006)	• Non-productive activities • Counterproductive activities
Ramayah (2010)	• Personal communication • Personal information research • Personal downloading • Personal e-commerce

Table 2. Types of Cyberloafing Activities

Furthermore, Mahatanankoon, Anandarajan and Igbaria (2004) classified cyberloafing activities in five different categories as purchasing and conducting personal business, seeking and viewing information, interpersonal communication, interactive entertainment and pass time activities and personal downloading. According to their research, an individual can demonstrate cyberloafing behaviors in order to conduct personal financial activities, shopping, reading news, researching on personal interests, participate online chat groups, online auctions or downloading some contents.

Alternatively, Li and Chung (2006) proposed four different functions of the internet in order to explain why people use the Internet. The functions are; a social function which is the

purpose of communication between individuals, informational function to gain knowledge and exchanging the information via Internet, leisure function for entertainment activities for individuals and virtual emotion function to build emotional relationships between individuals (Doorn, 2011).

Mastrangelo, Everton, and Jolton (2006) brought a different perspective to literature and differentiated the cyberloafing activities as their results when they are performed. First one is non-productive cyberloafing activities which are consists of spending the time to connect socially or engaging non-harmful unrelated work activities. The second one is counterproductive activities which are socially undesirable behaviors such as gambling at work, downloading pornography, asking co-workers for dates, and violating confidentiality. These counterproductive activities can be very harmful for the organization and information security (Mastrangelo et al., 2006).

Based on Mahatanankoon et al. (2004) research, Ramayah (2010) categorized cyberloafing activities similar to previous researches as personal communication, personal information research, personal downloading and personal e-commerce.

2.2.3. The Antecedents of Cyberloafing

As cyberloafing behavior has positive and negative impacts on organizations, it is crucial for the organizations to understand motives behind of this behavior to effectively cope with employees' internet usage at workplaces (Liberman et al., 2011). In the literature, the antecedents of cyberloafing commonly divided into personal factors, situational (work) factors and organizational factors.

- Organizational Factors

  Organizational factors which may have an influence on cyberloafing behaviors of employees are varied mainly as employee's perception regarding organizational justice, organizational commitment, and policies which include new working concepts.

  - *Organizational Justice*

    Organizational justice refers to the perception of employees regarding the fairness of procedures, outcomes and interpersonal relationships at the workplace

(Baldwin, 2006). According to previous researches, organizational justice has been classified into three categories as distributive justice, procedural justice, and interactional justice.

Distributive justice is one's perception regarding the equity and fairness of an outcome or allocations such as promotions, salary or additional benefits (Mey, Werner, and Theron, 2014). Procedural justice is one's perception regarding the fairness of procedures which are used to determine the allocation of the resources and it is expected by employees that the decisions are consistent and justified for each allocation. Interactional justice is one's perception regarding the quality of interpersonal communication between coworkers and managers' attitude for their employees (Everton, Mastrangelo and Jolton, 2005).

Several researchers revealed that the employees who perceive organizational injustice, more tend to engage cyberloafing activities (Henle, Kohut and Booth, 2009; Liberman et al., 2011) Similarly, Lim (2005) found that when employees perceive organizational injustice, they more likely to use neutralization techniques to justify their engagement in cyberloafing activities. Contrast to prior researches, Garrett and Danziger (2008) reported there is no significant relationship between interactional justice and cyberloafing constructs.

- Organizational Commitment

Organizational commitment is defined by Porter, Steers, Mowday, and Boulian (1974) as "An attachment to the organization, characterized by an intention to remain in it; identification with the values and goals of the organization; and a willingness to exert extra effort on its behalf". There is a consensus among social scientists that organizational commitment characterized within three factors such as acknowledgment and reliance on values and objectives of the organization, readiness to make great efforts in the interest of the organization and powerful willingness to maintain relationship within the organization (Mowday, Steers and Porter, 1979). By drawing on the concept of organizational commitment, Meyer and Allen (1991) introduced affective, continuance and normative commitment as three components of the organizational commitment.

Affective commitment refers to employees' emotional connection and identification within the organization and the degree of involvement in the organization (Meyer and Allen, 1991). The higher degree affective commitment represents a stronger desire to be a part of the organization, embrace organizational aims and values and demonstrates a positive work attitude.

Continuance commitment is cost-based consideration of employees in case of leaving the company or rewards in return of their continuance commitment (Allen and Meyer, 1991). When the continuance commitment degree is high for an employee, this means that employee will stay because of some worries such as no job alternative, gained specific skills in the current job and cannot use these skills within other company, unwillingness to lose benefits or relationships.

Normative commitment refers to perceived obligation feeling by employees to maintain their employment with the company (Allen and Meyer, 1991). A higher level of normative commitment means although the employee is not happy or get better offers from other companies, the employee will not leave because it is the right thing to do. Previous studies have reported, this type of commitment is related to a person's previous and current experiences, personal characteristics, family and social environments and organization's investment.

In the literature, there have been very few studies which analyze or explain the direct relationship between organizational commitment and cyberloafing behavior. Previous researches indicated that organizational commitment and three subdimensions are negatively associated with cyberloafing activities (Niaei, Peidaei, and Nasiripour, 2014). In the same vein, Garrett and Danziger (2008) argued that employees who possess a higher level of affective commitment to the organization, less likely to misuse the internet in the workplace.

A number of studies have stated that both cyberloafing and organizational commitment has been associated with role stressors and organizational justice components (Meyer et al., 2002). When the employee experience a higher degree of affective and normative commitment, less likely to experience role stressors and organizational injustice (Sage, 2015). Conversely, when an employee

demonstrates a higher degree of continuance commitment, the employee is more likely to experience role stressors and organizational injustice. Lim (2002) reported the employees who perceive a high degree of organizational injustice and role stress, more tend to cyberloaf. In these premises, it can be said that affective and normative commitment is negatively correlated with cyberloafing while continuance commitment is positively correlated with cyberloafing.

- Sanctions

Organizations develop various sanction and punishments in order to prevent employees to engage with illegal, unethical and harmful internet activities towards other individuals or organization. Depending on the extent of behavior, the severity of these sanctions may also change from a verbal warning to employment termination. However, Henle and Blanchard (2008) illustrated that when employees perceive no or little sanctions against their non-compliant behavior, they are more tend to cyberloaf.

- *Policies*

Policies refer to the set of rules, guidelines, principles which are designed or adopted by organizations to regulate and affect employees´ behavior and define the roles of employees in order to reach organizational long-term goals. As technological tools and internet are used by the companies to maintain their daily business operations, they develop their own internet usage policy, electronic devices usage policies and guidelines.

To prevent security incidents, cyberloafing activities and to have control over the employees, organizations mainly adapt internet policies into their organizations. Internet policies serve the goal to regulate the behavior of the employee and are proven to play an important role in cyberloafing behavior (Lim and Theo, 2005). In the literature, some researchers found that the presence of a formal Internet usage policy can serve as deterrents to cyberloafing behavior. (Jia, Jia, and Karau, 2013). However, when the norms, rules or the policies of the organization supports personal internet usage and accept conducting personal

business during work hours, employees are more tend to cyberloaf (Askew et al., 2014).

One of the newest trends in the workplaces, Bring Your Own Devices is a term which refers to the policy of permitting employees to bring personally owned devices (laptops, tablets, and smartphones) to their workplace, and to use those devices to access privileged company information and applications (Lee, Crossler and Warkentin, 2013). Although this concept benefits companies to save their capital and operating expenses, at the same time it creates difficulty to have control over employees actions on their devices. One of the types of this concept is Bring Your Own Hardware (BYOH) concept allows employees to buy the hardware from the budget instead of getting from the organization. According to research which is carried out by Doorn (2008), it is found that; the internet policy has a negative relation with Bring Your Own Hardware concept and the presence of this concept related to more leisure activities and cyberloafing.

- *Remote Working Concept*

Due to the high amount of cost and inadequate working place, in some industries, business owners introduce a remote working concept to their organization. Remote access working concept allows employees to work remotely without location restriction. The concept's itself and its policy are becoming popular for companies to reduce the cost and increase the flexibility of the workplace. However, it is found that as employees have less supervision, they are more tend to engage with cyberloafing activities during remote working (O'Neill, Hambley, and Bercovich, 2014).

- Individual Factors

Based on existing literature, individual characteristics may predict which individuals are more tend to engage with cyberloafing activities. The main individual factors consist of individual's perceptions and attitudes of the employees, personality traits, gender, age, income level, and other demographic components.

- *Demographic Factors*

Demographic factors such as gender, age, tenure, and education are one of the important antecedents of cyberloafing behavior.

Previous researches in the literature found that gender differences may indicate the frequency of performing the cyberloafing activities and type of cyberloafing (Garrett and Danziger, 2008; Vitak, Crouse and LaRose, 2011; Ozler and Polat, 2012). On the one hand several studies reported that male employees tend to engage in cyberloafing activities more than female employees (Garrett and Danziger, 2008; Lim and Chen, 2012; Jia, Jia, and Karau, 2013; Vitak, Crouse and LaRose, 2011) and male employees have higher possibility to use the internet at work for non-work related personal purposes (Everton, Mastrangelo and Jolton, 2005). Similarly, Lim and Chen (2012) found that men were more likely to cyberloaf for longer periods throughout the day than women employees. On the other hand, a number of authors argue that men and women are equally likely to cyberloaf (Stanton, 2002; Ugrin, Pearson and Odom, 2008). As a result, there is not enough empirical evidence to determine if gender differences are significantly related to cyberloafing activities or not (Weatherbee, 2010).

Researches indicate that younger employees tend to engage in cyberloafing more than older employees (Vitak, Crouse and LaRose, 2011), and use the internet in the workplaces for personal purposes (Everton, Mastrangelo, & Jolton, 2005). This may be one of the results of the information era, where the younger individuals are more qualified using the technological tools and ethical considerations are less worried by younger individuals so that they are more tend to violate the norms (Zhang, 2005).

Regarding job tenure, Hollinger, Slora, and Terris (1992) found that employees with less tenure are more likely to commit counterproductive behaviors such as theft. This notion is also supported by other researchers and stated as organizational tenure is also likely to be related to cyberloafing and as employees who have been with their organization longer have been found to commit less counterproductive behaviors in the workplace (Hollinger et al.,1992; Martin et al., 2010).

The research is conducted by Garrett and Danziger (2008) revealed that education level positively associated with cyberloafing activities. As education positively related to moral awareness and ethical behavior, employees who have a higher education level are less likely to develop unethical behaviors. However, in numerous researches, it is found that although top managers are well educated and against to unethical behavior of their employees, they are more also tend to engaging cyberloafing activities (Ugrin et al., 2007).

- *Personality Traits*

Personality traits are "individual attributes that consistently distinguish people from one another in terms of their basic tendencies to think, feel, and act in certain ways" (Ones, Viswesvaran and Dilchert, 2005). Every individual possesses several personality traits and therefore personality traits are helpful to understand individuals' attitudes and behaviors in the workplace (John and Srivastava, 1999). Although there are many different frameworks about personality traits, The Big Five Model is the most common model which is used in literature as a representative of cognitive and behavioral patterns. The model consists of five main traits such as extraversion, agreeableness, conscientiousness, emotional stability, and openness to experience.

Extraversion refers to the comfort level of an individual regarding interaction and communication with other individuals. The characteristics of extraverted individuals are sociable, assertive and positive while introverted ones tend to be quiet and reserved (Brinkman, 2013). Agreeableness is the ability of an individual to involve in a group of people and it consists of tendencies to be kind, gentle, trusting and trustworthy, and warmth (Judge and Iles 2002). Conscientiousness defined as an individual's self-control that facilitates compliance and goal-oriented behavior, such as following norms and rules, organizational plans and programs (John and Srivastava, 1999). Emotional stability embodies even-temperedness in contrast with negative emotionality that includes feelings such as sadness, anxiousness, insecurity, anger, and nervousness (John and Srivastava, 1999). Openness to experience refers to the degree of willingness to experience new things and possessing a broad

perspective and curiosity (Hough and Furnham, 2003). Individuals who open to experiences are considered as more creative, curious and flexible.

The main finding of the prior researches is that individuals‘ personality traits predict engagement with cyberloafing activities. A number of studies have found that extraversion personality trait is positively linked to cyberloafing activities (Krishnan, Lim, and Teo, 2010; Jia et al., 2013). As extraverted individuals are more social, friendly and active compared to introverted individuals, they are more tend to spend more time on the Internet and mobile devices. Similarly, Andreassen, Torsheim, and Pallesen (2014) reported that employees who have unstable emotions are more likely to get anxiety and stress which leads them to cyberloaf. On the contrast, there is a consensus among researchers that conscientiousness is negatively related to cyberloafing activities as conscientious individuals are less tend to engage counterproductive behaviors and violate the rules (Salgado, 2002; Andreassen et al., 2014). In the same vein, agreeableness is negatively correlated with cyberloafing, as agreeable individuals show more compatible, cooperative and trustful behaviors in the organization and less tend to demonstrate non-compliance behaviors (Jia et al., 2013; Wyatt and Phillips, 2005).

- Work Factors

Individuals’ work and task-related factors may also affect personal internet use at workplaces. Role stressors and the characteristics of the job are the most common work factors.

- *Role Stressors*

Blanchard and Henle (2008) identify role ambiguity, role conflict and role overload as main role stressors which can interfere with employee’s productivity, motivation or wellbeing.

Role ambiguity referred to unclear guidance about roles, tasks or responsibilities regarding the work. It is found that greater level of role ambiguity can lead to

higher level engagement cyberloafing activities as employees do not have clear guidance about their tasks and responsibilities.

Role conflict occurs when employees face with incompatible tasks or demands simultaneously. Role conflict can arise in different situations such as the conflict in one's personal values and work duties or between organizational rules and work duties. According to research which is conducted by Blanchard and Henle (2008) role conflict increase, cyberloafing activities as employees are not able to cope with the multiple tasks at the same time and they tend to take a break from the work.

Role overload is excessive work demands in a given time period and resources. relation to available resources. Henle and Blanchard (2008) argued that role overload has a negative correlation with cyberloafing activities as an employee has no or a little time to take a break from work. Unlike prior research, Runing, Hunik and Cahyadin (2012) found no relationship between role overload and engagement with cyberloafing activities.

- *Job Characteristics*

A number of studies examined the relationship between cyberloafing activities and job characteristics such as skills variety and autonomy.

Skills variety is defined as a wide range of skills that the employee needs to obtain in order to perform a task. (McKnight, Phillips and Hardgrave, 2009) The studies found that when a task requires limited activities and skills, the employee can be unsatisfied within the tasks and become more tend to engage with deviant behaviors. In contrast when a job requires different activities to be done and various skills to obtain, these can keep away the employees from the cyberloafing or any other counterproductive work behavior (Arshad, Aftab, and Bukhari, 2016).

Autonomy is an ability and independence for employees to control and take a decision regarding his or her task. Researches on this topic show that autonomy is beneficial for developing the sense of self-responsibility in employees, on

contrast higher level autonomy leads to engagement with cyberloafing activities (Garrett and Danziger, 2008; Jian, 2013).

2.2.4. Consequences of Cyberloafing Activities

In terms of its positive and negative impacts on employees and organization, cyberloafing has been categorized commonly into two types by scholars. Cyberloafing behavior is defined as destructive when it has negative outcomes for the organization and company such as cost, data leakage, privacy threats, and productivity loss (Beugre and Kim, 2006). In contrast, cyberloafing may be perceived as constructive when it has a positive outcome for the organization which can lead to higher productivity, innovative and creative work behavior, job satisfaction or acquire new information. Each type of cyberloafing behavior has different impacts on employees and the organization. Therefore, in this study consequences of cyberloafing examined from organizational and individual perspectives.

Destructive cyberloafing behavior refers to non-work related internet activities which have negative consequences on employees and organizations. Misuse of email services, hacking, downloading illegal software programs, visiting adult-oriented websites, unauthorized access to information, uploading confidential company information and plagiarism is the several examples of cyberloafing activities which are considered as destructive. From an organizational perspective, destructive cyberloafing behavior may have threaten legitimacy and liability of organization, cause data security and confidentiality issues in corporate level, decrease the productivity and performance of the employees which increase the cost for the organization (Henle et al. 2009; Wagner et al., 2012; Beugre and Kim, 2006). The deterrence mechanisms such as compliance training and computer monitoring systems which are used by organizations to prevent and regulate cyberloafing behavior also create additional expenses for organizations.

Negative Consequences of Cyberloafing Activities	
Individual Perspective	Organizational Perspective
The decrease in performance	Increased costs
Loose of focus on tasks	Inefficient usage of resources
Task postponement	Legal issues
Disciplinary actions	Risks for corporate confidentiality
Negative impacts on mode and emotions	Security threatens

Table 3. Negative Consequences of Cyberloafing

The most striking aspect of destructive cyberloafing behavior is the cost that it creates for businesses. According to prior researches, due to cyberloafing activities, the productivity of employees decreases to %30 which costs billions of dollars every year for the companies (Lara, Tacoronte and Ding, 2006). In the same vein, Jandaghi et al. (2015) found that today cyberloafing cost companies approximately $183 billion considering the loss in productivity, security and internet related incidents, legal actions and other related costs.

In addition to financial costs, cyberloafing activities cause employees to complete their task in a longer period of time. For instance, in order to take a break from work and use the internet or mobile devices for non-work related activities, employees mostly postpone their tasks (Bock et al., 2010) and afterward, transition from cyberloafing to work takes a large amount of time and employees mostly to experience to difficulty in focusing on their task which results in lost productivity and job satisfaction (D'Abate and Eddy, 2007).

From an individual perspective, particular cyberloafing activities affect employees mode and emotion negatively, cause work inefficiency and lower task performance which leads to a loss in productivity (Askew, 2012). In her research, Lara (2012) emphasized the impacts of different cyberloafing activities on individuals and stated that employees who engage with email activities experience boredom and affected negatively while browsing the internet for leisure purpose gives joy and effects employees mode on positively. Similarly, it was found that approximately up to 30% of employees find sending and receiving emails are distracting

as it requires personal resources such as time and energy (Fallows, 2002) and up to half of the employees did not switch to their work-related tasks after emailing as it is distracting and tiring (Macklem 2006).

Previous studies in this area of research have reported that cyberloafing or personal internet use is not always harmful to individuals and organizations. Constructive cyberloafing refers to non-work related activities which have positive impacts on organizations. From an organizational perspective, by engaging cyberloafing activities, employees recover from work and they return their tasks as more motivated which affects their performance and job engagement positively (Westman & Etzion, 2001) and in the longer term, it creates advantages for the organization in terms of work efficiency. Furthermore, constructive cyberloafing activities provide a more collaborative atmosphere in the workplace, give a chance to grasp opportunities within the sector and monitoring trends on the market (Belanger and Slyke, 2002) that benefits organizations become more profitable.

Positive Consequences of Cyberloafing Activities	
Individual Perspective	Organizational Perspective
The increase in performance	Grasp opportunities related business
The increase in productivity	Efficient usage of IT sources
Recovery from work	The innovative and flexible work environment
Innovative and creative work behavior	Cost reduction and increased profit
Self-improvement regarding work	Higher quality of work
Positive impacts on mode and emotions	Motivated and satisfied employees

Table 4. Positive Consequences of Cyberloafing

From an individual perspective, a considerable amount of researches has been published on positive impacts of cyberloafing mainly points out that constructive cyberloafing positively associated with productivity and work satisfaction level of employees (Vitak et al., 2011; Coker, 2011). This notion supported by İnce ve Gül (2011) and found that minor cyberloafing activities positively affect employees' job satisfaction, hinder work efficiency

and it reduces the resign desires. Similarly, Hamermesh (1990: 121) stated in his research that "time spent on the job relaxing can increase workers' productivity by enabling them to rest when they are physically or mentally fatigued". So, when an employee recovery from the work, it increases his/her well being, reducing the stress (Westman & Etzion, 2001) and increasing the engagement for the task (Sonnentag, 2003).

Moreover, Belanger and Van Slyke (2002) argued that if employees use the internet for playful web browsing, they gain a better understanding of the organization and they improve their knowledge more accurate. By the same token, computer and online games also decrease anxiety and encourage employees to involve more experimentation (Oravec, 2002). This is because browsing on the Internet for pleasurable activities help employees to cope with the stressful work environment and negative experiences which are related to work or the organization

2.2.5. Management Practices to Control Cyberloafing Behavior

There is a considerable amount of published studies reporting that employees spent certain amount of their time with non-work related activities on internet at the workplace (Garrett and Danziger, 2008; Lim and Teo, 2005) Although these activities may have positive impacts on individuals or business operations, at the same time it may cause time and money loss, serious security issues, damage the legitimacy of the company, create conflicts in organization. Therefore organizations develop their own control mechanisms to control and reduce the cyberloafing intention of organization members. Based on empirical studies and much of the current literature shows that internet usage policies and computer monitoring systems are effective and most commonly used management practices which are implemented by companies for cyberloafing mechanisms (Wang et al., 2013).

One of the main strategies of organizational control is bureaucratic control refers to the use of rules, policies, legitimate authority, standards, any written documentation, and other control mechanisms in order to control and standardize the behavior and performance of an employee (Daft, Murphy and Willmott, 2010). Particularly, policies and rules regulate the behavior of individuals in the workplace, outline the responsibilities and expectations, protect employee's right, create uniformity regarding human resources practices and ensure consistency and stability within operational procedures. Therefore, every organization adopt

operational and administrative policies such as code of conduct, health and safety, intellectual property and evolve these policies through a process trial and error.

Within the introduction of computers and the Internet at business, besides the benefits, new threats such as security issues, illegal activities, misuse the information systems has arisen in the workplaces. In order to eliminate these threats, set guidelines for appropriate usage and regulate the activities of employees through the internet, computer and internet usage policies has become necessary for the organizations. Moreover, some of these policies inform individuals regarding the deterrence mechanisms which are used by the organization and the possible consequences in case of non-work related or illegal activities on the Internet. Although the terms may vary such as Electronic Use Policies (Henle, Kohut and Booth, 2009), Internet Acceptable Usage Policy, Network Usage Policy in this thesis Internet Usage Policy (IUP) is adopted as it is commonly used in the literature.

According to Lichtenstein and Swatman (1997), as a part of security policies, Internet Usage Policies reinforce two functions of the organizations; usage of the internet which is compatible with business objectives of the company and value-added business. Furthermore, from a individuals perspective, the presence of well defined and comprehensive computer usage guidelines and policies have positive impacts on ethical behavior intention of the individuals in the workplace, who do not possess high moral values. Similarly, several scholars pointed out the awareness of the existence and clarity of the internet policies and stated in their research most of the misuse of internet activities are consequences of low perception of the policies or unclear policy contents (Lichtash, 2004; Foltz, Cronan and Jone, 2005).

In their paper, Siau, Nah, and Teng (2002) examined different types of cyberloafing activities and points out the important points while developing internet usage policies to discourage organization members to engage with non-work related activities on the Internet. They suggested that ideal internet usage policy should be complementary to company values and code of ethics, strongly emphasize that computer resources should be used only for the business purpose and forbid any type of unauthorized use of the internet or confidential and unethical data storage. More importantly, in the IUP, organizations should state their rights to control and monitor internet activities of the employees, enforce the policy steadily in all

over the organization and ensure sanctions in case of violation of the rules (Siau, Nah and Teng, 2002).

As the presence of IUP does not assure the perception and acceptance by individuals, researchers suggest that involving employees in the development process of policies raises greater awareness regarding the regulations (Foltz, Cronan and Jones, 2005). Moreover, the individuals who have a higher awareness of IUP, tend to use information systems more effective and secure way (Doherty, Anastasakis and Fulford., 2011).

In general, the purpose of these policies is to keep the employees' activities through computers and the Internet under control through specific rules.

According to Salary.com's (2018) survey which is conducted of 3200 employees in the United States, 64% of employees visit non-work related websites and engage cyberloafing activities every day during working hours. Therefore, today, most of the companies utilize the monitoring strategies as well as internet usage policies to prevent cyberloafing activities and minimize the risk to their business. As a type of workplace surveillance, computer monitoring refers to controlling systems which observe, record and regulate the activities of individuals through the Internet and computers. In 2007 the American Management Association conducted a survey with 304 companies in the United States and concluded that 66% of them monitor internet connection of employees and 84% of these companies, informed their employees regarding Internet monitoring systems.

Computer monitoring practices may vary according to the industry that business operates in, risk and security management strategies, company objectives or even workplace conditions. Some of the monitoring practices can be given as follows.

- *Internet Activities Monitoring*: As internet and computers became indispensable elements of daily businesses, companies set up their own business networks and connect their business to the Internet by using an Internet Service Provider. Any internet activities which are connected to an individual's workstation over the company network can be monitored and stored by the employer.

- *Keystroke Logging*: Within specific software programs every keystroke activity on a keyboard of individuals can be captured and stored in the databases.

- *E-mail Monitoring*: Most of the companies use their own e-mail hosting services and each individual has his/her own work email and while this creates formality for the employees, at the same it helps companies to keep incoming and outcoming emails under control. As it is supported by judicial decisions, the correspondence of the employees via email accounts can be monitored by the employer. Moreover, in order to minimize the security issues and prevent misuse the e-mail services, particular contents may be filtered out automatically by the information systems which are set before by security offices.

- *Screen Monitoring*: After employees log into their network accounts via work computers, the display of the screen can be captured at intervals or recorded continuously over a certain time which is determined by the employer.

- *Software Monitoring*: Any types of software on computers or electronic devices including applications, communication tools, web browsers may be monitored and content of these software programs can be stored in databases.

A number of researches have found that computer monitoring strategies are effective to reduce cyberloafing behavior and when employee is aware of monitoring, they more tend to comply with rules regarding Internet usage and decrease the time they spend on the Internet for non-work related activities (Urbaczewski and Jessup, 2002; Stanton and Weiss, 2000). Moreover, Rahimnia and Mazidi (2015) have reported monitoring strategies to create bigger impacts on individuals who do not possess a high level of self-control.

Although monitoring strategies attract great attention from the business environment, certain aspects of these strategies are still matters of debate. Martin and Freeman (2003) investigated seven main arguments related to electronic monitoring;

- *Security:* By monitoring, organizations have a greater chance to detect and prevent data breaches and security issues.

- *Productivity:* In some extent, monitoring increases productivity and decrease the cyberloafing activities. Conversely, monitoring may have resulted in some physiological problems such as boredom, depression and high tension.

- *Liability:* As approved by recent courts, particular acts of employees are under the responsibility of employers. Therefore monitoring is a helpful tool for organizations to diminish undesirable acts of employees such as sexual harassment, unethical internet usage, illegal uploads and downloads, violation of copyrights and so on. In this way, while companies use monitoring as a risk management tool and protect themselves from possible lawsuits, employees are protected from transgressions.

- *Privacy:* There are two main theories which measure privacy in different ways. Control Theory defines privacy as "an amount of control that we have over our own information" and Restricted Access Theory measures privacy within "the level of access others have to our information." Therefore, on the one hand, monitoring may be seen as a loss of control and privacy violation by employees. On the other hand, as information technologies are given to employees for work purpose, within his/her activities through the internet in the workplace; employees have control over the personal information that can be accessed.

- *Creativity:* Monitoring may reduce creativity, as employees feel forced to comply with the desires of the observer and filter out of communication by not sharing different and radical ideas.

- *Paternalism:* Monitoring may have negative impacts on perceived trust and employees' morale which may push employees to act childlike.

- *Social Control:* Monitoring may change how employees act, talk, think and participate in the organization. As there is no obligation for the employers to inform their employees regarding monitoring systems, even there is no monitoring, employees could still change their behaviors to avoid the possible threat of observer.

Besides the facts which are given below, the legality of monitoring is also a very important aspect for the companies to develop their own strategies. Legislation and principles of monitoring may vary depending on region or country, but in most of the countries, computer monitoring in the workplace is legal and employer's rights are protected by the laws to a certain extent. Moreover, while in the USA consent of the employee is not required, in EU countries, the purpose, process, frequency and another type of guidelines regarding monitoring should be stated in company policies, the employee must be informed and the

consent of employee should be taken. In Turkey, according to 2009/447 numbered decision of Supreme Court of Appeals in 2010, employers also have a right to monitor employee's computer, email and other electronic devices which are given by the company for work purposes. However, it should be noted that although monitoring is entitled as legal, monitoring practices should comply with constitutional and human rights.

In addition to computer monitoring and organizational policies to reduce and control cyberloafing behavior of individuals, there are alternative management practices in organizations. Chen, Chen and Yang (2008) point out that the most effective practice to reduce Internet misuse behavior is to educate employees about potential security risks, negative consequences and create awareness about their responsibilities. In the same vein, Vitak et al. (2011) argue for by strengthening and restructuring self-control on cyberloafing behavior it is possible to prevent and control this behavior.

In view of all that has been mentioned so far, controlling strategies have been used by organizations to decrease cyberloafing behavior and control employee's activities through work computers. However, implementation of the countermeasure strategies may not always successful vice versa create an adverse effect on individuals. According to Sheikh et al. (2015), organizational sanctions and punishments against non-work related internet activities strengthen individuals' ability to hide cyberloafing behavior. Moreover, as individuals more tend to use their smartphones and tablets for non-work related internet activities such as visiting social network websites, from organizations side, it is unlikely to control cyberloafing activities of employees (Sheikh et al., 2015).

2.2.6. Ethical and Legal Considerations Regarding Cyberloafing Behavior

As one of the types of professional ethics, business ethics inspect ethical and moral principals in a business environment (Warren, 2011). It applies to all aspects of business and individual behaviors and eventually the whole organization. It aims to prevent unethical behaviors such as cyberloafing activities in workplaces. Increasing unethical behaviors related to computer and internet usage has raised the necessity of ethical codes, regulations, and educations regarding usage of information technologies in the workplaces.

In their research, Massera et al. (2011) emphasized the importance of training and educations related to the ethical use of work computers and Internet access. Similarly, Young (2010)

argued that educations which are conducted periodically may strengthen an individual's responsibility and moral integrity during the time spent on the Internet. Moreover, Peterson (2002) pointed out the importance of policies and investigated an interaction between computer guidelines and moral beliefs and found that the presence of clear computer guidelines has positive impacts on ethical intentions of professionals with lower moral beliefs.

Regardless of the severity and impact of the cyberloafing behavior, organizations may tolerate or impose a sanction based upon their own rules and regulations regarding acceptable internet usage. Researches show that between twenty percent and thirty percent of the organizations get fired at least one of their employee because of the cyberloafing activities during work hours (Blanchard ve Henle, 2008: 1068). Moreover, at certain times code of ethics or computer guidelines may be insufficient to prevent cyberloafing behavior. In these cases, employers may take legal action against the employee who shows non-compliant behavior.

There are several examples of cyberloafing behaviors that result in dismissal of employees or legal actions in all over the world. As one of the financial service company in Boston, Fidelty Investment fired nine of the employees in 1998 because of excessive use of internet and misuse of email services of the company. More recently, companies such as Xerox, HP and New York Times after warning their employees regarding their internet activities and consequently terminated their contracts within the company who were unresponsive to these warnings (Saraç and Çiftçioğlu; Piscotty et al., 2016).

One of the leading case decision has been taken by the Supreme Court precedent in Turkey, 9th Court of Appeals Law office 2007/27583 in 17.03.2008 2008/5294 number of a decision.

> "*In the workplace without permission of the employer, explicitly or implicitly, usage of the Internet as a special purpose is forbidden. However, an exception to this prohibition, in case of an emergency or for reasons relating to the business the rule can be drilled in a legitimate way. If the employees use the Internet for non-related work activities despite it is explicitly forbidden by the employer, the employment contract of the employees can be terminated without prior warning. Additionally, there is no need for a prior warning in case the*

employees download or install pornographic images, videos, and contents to the company's data carrier.".

Based on this decision, in Turkey, the employer has a right to restrict the usage of the internet regarding non-work-related activities and take disciplinary actions in case of unauthorized internet activities of employees.

2.2.7. Review of Theories in Cyberloafing Literature

In cyberloafing studies, scholars established their conceptual framework based on numerous theories. There are six popular theories in the literature which are mainly used in cyberloafing studies such as Control Theory, Theory X/Y, Deterrence Theory, Social Capital Theory, Theory of Planned Behavior and Theory of Interpersonal Behavior.

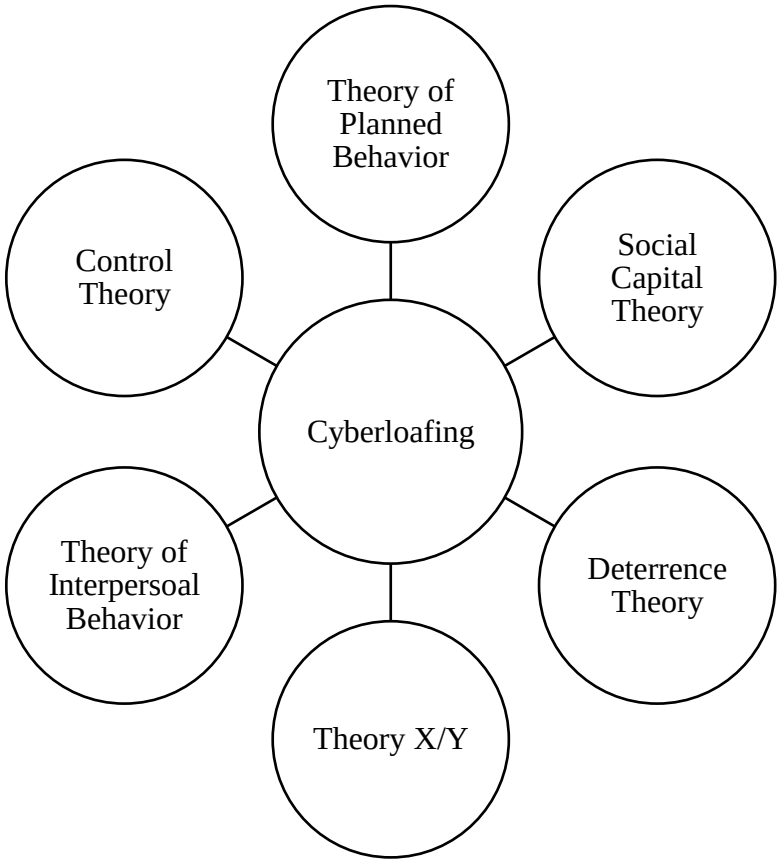

Figure 2. Theories in Cyberloafing Studies

Theory of Planned Behavior, Theory of Interpersonal Behavior and Social Capital Theory has been used for explaining the motives of cyberloafing behavior. On the other hand, within Deterrence Theory, Theory X/Y and Control Theory, scholars have explained the ways of discouraging cyberloafing behaviors.

- Control Theory: The theory posits there are certain control factors which refrain individuals from deviant workplace behaviors. Applied to cyberloafing studies, organizational control discourage cyberloafing behavior intention.

- Theory of Planned Behavior: According to theory, an individual's intentions or behaviors are linked to their attitude, perceived social norms and perceived organizational control. Similarly, theory in cyberloafing studies states that employee's intention for cyberloafing behavior related to their attitude against personal computer use at the workplace, organizational control regarding employee's computer use and acceptance of the cyberloafing behavior by others (Askew et. al., 2014).

- Theory of Interpersonal Behavior: The theory posits that individual's behaviors or intentions are shaped by their personal habits, intention, and presence of facilitating conditions. In cyberloafing studies, it has been seen that cyberloafing behavior intention increases when employees access internet sources without any restriction or difficulty and when they perceive benefits from their internet activities (Chang and Cheung, 2001).

- Theory X/Y: Based on this theory which is formulated by Douglas McGregor, there are two different types of employees and according to these types, organizations should revise their human resources strategies. Theory X assumes employees intrinsically do not like working, thus in order to reach organizational goals, managers should enforce sanctions and coercive control strategies in order to force employees to work. On the other hand, Theory Y posits that employees are willing to reach organizational goals and they do not need to receive external and coercive control to perform their task. In cyberloafing studies, it has found that cyberloafing behavior decreases when employees aware of their internet and computer activities monitored by the organization which supports Theory X (Urbaczewski and Jessup, 2002).

- Social Capital Theory: According to the theory, the community becomes stronger when its members have more common values and features. Applied to cyberloafing behavior, a recreation of computer and internet use lead to increased productivity and more of the organization (Oravec, 2002).

- Deterrence Theory: GDT suggests in order to discourage deviant behaviors, organizations should apply sanctions against employee's non-work related behaviors. Similarly, it has been seen that employees are less prone to engaging cyberloafing activities when they perceive sanctions against their non-work related internet activities (Hassan, Reza, and Farkhad, 2015).

In this thesis, the General Deterrence Theory has been used in order to examine the effectiveness of control mechanisms on cyberloafing behavior intention. The theory has explained in the section in more detailed.

2.3. General Deterrence Theory

One of the prominent conception of behavioral psychology, GDT (General Deterrence Theory) is a theory which asserts undesirable acts of individuals may be controlled or prevented through fear of punishment (Gibbs, 1975). The theory is originally grounded and started to use as a military strategy throughout the Cold War. By using the perception of nuclear superiority and massive retaliation, it was aimed to dissuade the adversary states from attacking or taking an unwanted action. In later times, the theory examined in the context of criminology and several studies found that the high level of fear punishment is negatively associated with crime commitment intention of individuals (Kuhalampi, 2017). Based on previous researches, scholars start emphasizing GDT concept that can be also used for the organizations to control and prevent any type of incompatible behaviors with the rules of the organization.

The preliminary works on GDT identified three components of the deterrence mechanisms: severity, certainty, and celerity.

- *Severity:* The degree of a sanction which could be low to high.
- *Certainty*: The possibility of a sanction.
- *Celerity:* The velocity of sanction enforcement.

The theory suggests that when individuals engage with an unwanted act, there should be a certain sanction for his or her behavior, the sanction should be severe enough to discourage this behavior and it should be immediate before the act is actualized (Williams and Hawkins, 1986). Comparison of the researches conducted so far shows that sanction severity and sanction certainty are two prominent and effective components of the deterrence theory, while celerity is an ignored concept due to inadequate empirical analysis (Nagin and Pogarsky, 2001). Therefore in this thesis, sanction severity and sanction (detection) certainty were used as the main components of the deterrence theory.

Every organization adopts some rules and policies in order to prevent undesirable actions of employees. However, the existence of these rules has only a small impact on individuals' behavior, if they are not enforced in the right way (Peace, Galletta & Thong, 2003). The GDT asserts formal sanction against an undesirable act of individuals and directs them to

comply with organizational policies (Han and Jie, 2010). Likewise, many scholars supported this notion with findings which prove that perceived sanction severity and detection certainty associated with the behavioral intention for misuse of the Internet (Hollinger and Clark, 1983; Gibbs, 1975).

In organizational studies, sanction severity simply refers to the individual's perception that the punishment for the engagement with deviant behavior will be severe (Kuhalampi, 2017). As sanction severity generally corresponds to the severity of the undesired behavior, it can vary from a verbal or written reprimand, short or long term suspension to termination of the employment contract. According to rational choice and deterrence theories, the perceived sanction severity positively correlated with the perceived cost of deviant behavior and neutralize the attractiveness of deviant behavior. This means that if the sanction severity is high, individuals will be less tend to engage with deviant behaviors (Liao et al., 2009).

However, in the literature, the scholars found different results regarding the perceived sanction severity and intention of misuse of the Internet or work computer. A number of studies suggest that perceived sanction severity has a positive relationship with compliance of the internet and security policies and influence employees to not engage with deviant behavior. (D'Arcy et. al, 2009; Straub and Nance, 1990) On the other hand, several studies could not find or very significant impact of sanction severity on employees intention for misusage of the internet or computers. (Liao et al., 2009; Lowry et al., 2014) The reason for this can be explained with individuals who have high personal norms are influenced by extrinsic enforcements such as rules and punishments very little.

Although sanction severity is found as effective for deterring particular behaviors, in his research Bosword (2005) states that if a sanction is too severe, it will not decrease the behavioral intention vice versa, it will increase, as the excessive punishment will be perceived as unjust by individuals. In the same way, if a sanction is not severe enough corresponding to behavior, then it will not deter individuals from engaging deviant behaviors.

The second component of deterrence theory sanction probability refers to the possibility of caught and receive sanctions when the employee engages with cyberloafing activities and detection may include computer monitoring, audit software or physical monitoring by supervisors or colleagues. As the cyber systems in the workplaces are given to the employees

for working purpose, companies have a certain extent right to control and verify the usage of these tools are comply with the rules and policies. Nevertheless, the detection strategies which are used by companies must be applied in accordance with the laws and it can vary from country to country.

Much of the available literature on perceived sanction certainty argues that sanction certainty negatively associated with misusage of internet and computer (Hollinger and Clark, 1983; Cheng et al., 2014) While low level of detection probability points out the increased deviant behaviors such as theft, internet abuse, software piracy, high level of detection probability demonstrates high level of compliance of the policies. By the same token, several researches claim that sanction certainty has a stronger impact on employees compare to sanction severity (Hasan et al., 2015). Together these researches provide an explanation that when employees are aware of the possibility of getting caught, they are less tend to engaging deviant behaviors.

In conclusion, within general deterrence theory, it is intended to eliminate the perceived benefits of engaging deviant behaviors and strengthen the perceived deterrents against deviant behaviors. With a balanced sanction strategy, organizations will be able to preclude undesired behaviors of individuals.

2.4. Hypotheses Of The Study

A number of studies have investigated the countermeasures for improper usage of the internet and outlined four strategies such as deterrence, prevention, detection and remedial (recovery) measures (Straub & Welke, 1998). These measures have been used mostly in the information security area to reduce the systems risks and personal internet usage for non-work related activities.

- *Deterrence measures*: These types of measures refer to policies, guidelines and other written documents regarding misusage of the internet.

- *Prevention measures*: Physical or cyber prevention mechanisms such as blocking particular websites, requiring a password for accessing online and offline environment via work computers are some examples to prevent individuals to engage in illegitimate behavior in cyberspace.

- *Detection measures*: In the case of the previous measures are inadequate, the detection measure is proposed to be implemented to detect misusage of the Internet and take action to prevent it. Computer and system monitoring, Internet activity reports are system audits are common mechanisms to detect an individual's computing activities and online behaviors in the workplaces.

- *Remedial measures*: When controlling and preventing strategies are failing to reduce and prevent the misusage of internet, formal punishments such as verbal or written warning, termination of the contract may be effective to correct the undesirable behavior.

In their research, Straub and Welke (1998) suggest that ideally, organizations should adopt deterrence measures as a precaution and when this measure is not functional, organizations should continue following the prevention and detection measures. When individuals cannot be prevented, then as a result of their unwanted action, remedial measures should be implemented (Griffiths, 2010). However, in contrast to their framework, researchers found that monitoring and blocking the access are the most effective two deterrence actions compare to written rules or formal remedial actions which are implemented by organizations (Straub and Welke, 1998).

Based on the literature review and in view of all that has been mentioned so far, this study identified eight variables which compose the main points of the conceptual framework and in accordance with previous studies and filling the gap in the literature, seven hypotheses have been proposed. H_4 and H_5 hypotheses were established to represent the link between cyberloafing behavior intention and awareness of computer monitoring and organizational policies.In research area regarding misuse of the Internet, organizational policies and computer monitoring strategies have been found negatively associated with misuse of the internet. Therefore in this study, it was assumed that computer monitoring and organizational policies have negative impacts on cyberloafing behavior intention of employees. Additionally, as General Deterrence Theory emphasizes the effectiveness of sanctions against deviant workplace behavior (Han and Jie, 2010), H_6 and H_7 hypotheses were developed to test whether GDT components have a negative impact on cyberloafing behavior intention of individuals. The other three hypotheses, H_1, H_2 and H_3 were used to define the relationship between demographic characteristics of individuals such as age, gender, and education level differences and cyberloafing behavior intention.

H_1: There is a significant difference between cyberloafing intentions of individuals by their gender.

H_2: There is a significant difference between cyberloafing intentions of individuals by their age.

H_3: There is a significant difference between cyberloafing intentions of individuals by their education.

H_4: There is a negative relationship between user awareness of organizational policies and cyberloafing intention.

H_5: There is a negative relationship between user awareness of computer monitoring and cyberloafing intention.

H_6: There is a negative relationship between perceived detection certainty and cyberloafing intention.

H_7: There is a negative relationship between perceived severity of sanctions and cyberloafing intention.

In conclusion, this study has four main and three sub-hypotheses in order to analyze the effectiveness of control mechanisms to discourage cyberloafing behavior and whether demographic characteristics predict cyberloafing intention of employees. The proposed hypotheses and conceptual framework has been shown and explained in the Methodology chapter in more detailed.

3. METHODOLOGY

3.1. Research Purpose

The purpose of research can be examined in three different groups; exploratory research aims to explore a new subject, descriptive research focuses on the description of a social phenomenon and explanatory research seeks an explanation regarding why things are the way they are (Saunders, Lewis and Thornhill, 2012). As the aim of the research may differ due to change in time, new aspects of a topic or different research methods, research may have multiple research purposes.

As a result of developments in information technologies, internet and computer technologies have become an indispensable element of the workplaces and has been beneficial to organizations in terms of cost reduction, facilitation and acceleration of business operations, encouragement of innovative and creative way of thinking. On the other hand, computerized technologies brought some disadvantages along such as security breaches, unproductivity, ineffective time management which may cause a large amount of cost and legitimacy issues for the organization. For this reason, in order to reduce the negative impacts and control the computer and internet usage at workplaces during work hours, organizations adopt several strategies. As current cyberloafing studies focus mostly on one-sided regarding its impacts and antecedents, there is a gap in the literature related to management practices regarding cyberloafing behavior and the effectiveness of these practices. Therefore, the following research questions of this study were addressed:

- Are the deterrent mechanisms effective in preventing cyberloafing behavior?
- Which deterrence mechanisms play a more effective role in reducing cyberloafing?
- Do demographic characteristics of employees predict the intention of cyberloafing?

By presenting the research questions, the main purpose of this study is to examine the relationship between cyberloafing behavior and deterrent mechanisms which are implemented by organizations. Another purpose of the thesis is to present a comprehensive guideline study that examines the cyberloafing behavior in all aspects. The findings are expected to contribute to the development of human resources practices, management, and

analysis of the training needs of an organization to be more effective in dealing with cyberloafing behavior.

Taken together, since the cyberloafing phenomenon is not a recent research area, the purpose of this thesis is not exploratory. However, as the research examines the effectiveness of business practices on cyberloafing behavior intention which is based on a General Deterrence Theory the thesis has a strong explanatory and descriptive research purposes.

3.2. Research Approach

Based on the research purposes and problems, research approach plays an important role in data collection and data analysis processes. Data collection consist of quantitative and qualitative methods and data analysis comprise inductive and deductive research approaches.

In social researches by using quantitative and qualitative methods, the connection between data and concepts can be examined. The main difference between these two approaches, quantitative research approach use and produce data in forms of numbers, while qualitative research use and produce non-numerical dataset. In this thesis, the quantitative research method has been used and the advantages of this method are given below (Neuman, 2014; Rowley, 2014).

- Highly structured research tools in the data collection phase
- A large and broad sample representative of a population
- Usage of advanced statistical techniques to measure and analyze the data
- Based on statistical analysis hypothesis testing
- Generalization of the results to the target population
- Predict future behaviors/intentions (Rowley, 2014)

There are three main quantitative research techniques for data collection such as survey research, experimental research, and non-reactive research (Neuman, 2014). The survey research method applied in this thesis to gather information through a questionnaire from a large number of the sample at one time.

After the data collection process, analysis of the obtained data can be performed by deductive an inductive research approaches. Deductive research approach mostly emphasizes causality between constructs, aims to verify or falsify a theory which based on previous literature, starts with a hypothesis and generalizing from general to specific (Saunders et al., 2012) In contrast, inductive research approach focuses on seeking new phenomena, aims to generate and build a theory, starts with a research question and generalizing from specific to general. In this thesis, deductive research has been adopted since the study found on the General Deterrence Theory within previous literature and aims to test hypotheses which have been developed to explain the relationship between independent variables (control mechanisms) and the dependent variable (cyberloafing behavior intention).

3.3. Data Collection

Traditionally, for the data collection, the sources of data can be classified as primary data and secondary data. Primary data is a raw data which is collected for the first time by a researcher for a specific research purpose. On the other hand, secondary data refers to processed data that is retrieved from a source which was originally collected and used for another specific purpose. In this thesis, two data collection sources used together. In order to give comprehensive information about the research topic and gain a better understanding of theory, scientific journals, articles, and other literature resources have been used as secondary data. At the same time to answer the research question and test the hypotheses of the research, the primary data was gathered through a questionnaire with employees of bank branches in Ankara, Turkey.

As one of the primary data collection methods, the questionnaire is the most commonly used research instrument in social sciences and it refers to the set of questions which is designed to gather and analyze the data about a specific topic. These set of questions predominantly close-ended designed, and both questions and answers are pre-coded. The main advantages of the questionnaire is that makes easier to reach a large audience in a shorter time, effort and cost. Besides this, it benefits to produce standardized data within more reliable statistical results and allows researchers to compare the different populations and cases. The questionnaire may be distributed in a sample via online tools, e-mail or printed versions.

In this thesis, the online questionnaire method was used as primary data sources. As the measurement of research has a strong impact on the quality of the research, scholars suggest

adopting scales which already exist in the literature and tested by prior researchers. Therefore measures were used in the thesis were selected from the scales that were proven in terms of reliability and validity. “Cyberloafing intention” was assessed by three-item scale which was adopted from a research of Moody and Siponen (2013), the General Deterrence Theory components of “sanction certainty” measured by two-item scale and “sanction severity” were assessed by two-item scale which was both retrieved from a study of Li, Zhang, and Sarathy (2009). Finally, to measure “organizational policies” and “computer monitoring” four-item scale and six item scale adopted from the research of D'Arcy, Hovav, and Galletta (2009). Composite reliabilities for each scale has given below.

- Organizational Policies: 0,88
- Computer Monitoring: 0,96
- Sanction Certainty: 0,95
- Sanction Severity: 0,80
- Cyberloafing Intention: 0,90

To measure the constructs, a five-point Likert scale which ranges between 1=strongly disagree, 2=disagree, 3=neutral, 4=agree, and 5=strongly agree multi-item approach was used. The final version of the questionnaire comprises of five sections and 20 questions in total. In the first section, it was aimed to measure the awareness of organizational policies regarding internet and computer usage at work and in the second section, the aim of the research was measuring individual’s awareness of the computer monitoring practices which is implemented by management. In the third and fourth sections, it was aimed to measure perceived sanction certainty and severity in case of engagement with cyberloafing activities. Finally, in the fifth section, the intention for the cyberloafing activities of individuals was the aim of the understanding. The measurement’s items have been shown in Table 5.

Scale	Codes	Items
Organizational Policies	OP1	My organization has specific guidelines that describe the acceptable use of the internet.
	OP2	My organization has established rules of behavior for use of computer and internet resources.
	OP3	My organization has a formal policy that forbids employees from accessing computer systems that they are not authorized to use.
	OP4	My organization has specific guidelines that govern what employees are allowed to do with their computers.
Computer Monitoring	CM1	I believe that my organization monitors any modification or altering of computerized data by employees.
	CM2	I believe that employee computing activities are monitored by my organization.
	CM3	I believe that my organization monitors computing activities to ensure that employees are performing only explicitly authorized tasks.
	CM4	I believe that my organization reviews logs of employees' computing activities on a regular basis.
	CM5	I believe that my organization conducts periodic audits to detect the use of unauthorized software or website access on its computers.
	CM6	I believe that my organization actively monitors the content of employees' e-mail messages
Sanction Certainty	PC1	The probability that I would be caught is high.
	PC2	The likelihood that my organization would discover that I use work computers for non-work-related activities is high.
Sanction Severity	PS1	The punishment would be severe by my organization.
	PS2	The probability that I would be reprimanded by my supervisor is high.
Cyberloafing Behavior	CBI1	I intend to use the Internet at work for non-work-related purposes in the future.
	CBI2	If opportunities allow, I will use the internet for non-business purposes in the future.

Table 5. Measurement Items

3.4. Sample Selection Strategies

In quantitative studies, sampling has vital importance as it refers to select a small set of units which represent the characteristics of a large collection of units that are called population

(Neuman, 2014). The population of this thesis is the employees who work at bank branches which are operated in Ankara province. As it is impracticable to conduct research on the whole population in terms of time, cost and access limitations, the representative sample was selected.

There are two types of sampling strategies to choose a sample from a population which are probability and non-probability sampling strategies. Each of the strategies has different methods of the sampling but the main difference between two strategies is in probability sampling, each case or unit has the equal chance to be selected while in the non-probability selection of the units are unknown (Bryman and Bell, 2011). Moreover, probability sampling techniques are named as "gold standard" which is considered more suitable for creating a representative sample of a population compared to non-probability sampling techniques.

For this study, probability and non-probability sampling techniques were used together. Primarily, within purposive non-random sample, the sample elements who will be the best representative of a population are selected according to criteria which are determined by the researcher (Saunders et al., 2012). In this research, in the first instance, the participants were chosen from full-time employees of a company which operates in the banking industry that is located in Ankara. In the banking industry daily business operations are carried out through computers and employees are using their computers regularly during working hours. Moreover, in terms of providing service to the internal and external environment of the company, velocity and information security play an important role in the banking industry. For this reason, companies attach great importance to compliance of rules and productivity of employees. Considering all these facts, banking industry employees have been found ideal to be a sample of this study. Following the criteria, by using snowball probable sampling technique, the interrelationships of the reference person in the bank branches are utilized and reached more sample elements from a population. Furthermore, by using simple random probable sampling technique within some of the sample bank branches the questionnaires are distributed to employees randomly by the human resources department.

A sample size of the research is another important issue to be covered as it should be large enough to reflect the population. In this research, based on the dataset which was provided by the Bank Association of Turkey, the population constitutes approximately 18.000 people. There is a consensus among scholars that considering a 95% level of confidence and 5%

margin of error, the sample size 378 found as an appropriate. Additionally, at the beginning of the research, a pilot test conducted with 96 employees from different branches to test the first version of the questionnaire.

3.5. Research Ethics

Ethics in researches refers to following moral procedures during the research process. The main ethical principles composed of ensuring the privacy of the participants and obtaining the consent of the participants regarding voluntary participation in the research process and informed about the aspects of the research.

Moreover, the permission of the scholars has been obtained to use of each scale of the measurement in this study and by contacting with the scholars directly, necessary information has been acquired regarding the scales.

In this thesis, participants of the research were informed about the content and the aims of the study within an informed consent statement. Additionally, at the beginning of the research consent of voluntary participation were asked and participants were informed that they could withdraw from the questionnaire at any time without any issue. The participants of the research were also ensured that the obtained data will remain as confidential and anonymous and not shared with third-parties. Moreover, the research design of this thesis was guided and approved by the Social and Human Sciences Ethics Committee and the research process started after the approval.

3.6. Contributions

This study makes several noteworthy contributions to cyberloafing phenomenon by synthesizing the prior studies and providing comprehensive information regarding cyberloafing behavior and deterrence mechanisms. Moreover, by conducting quantitative research method, the study has aimed to fill the gap in the literature and explore the effectiveness of deterrence mechanisms on cyberloafing intention.

Moreover, most of the studies in the research area has been used a different theoretical background such as the theory of planned behavior, and self-control theory in order to examine motives of cyberloafing behavior and its consequences on individuals and organizations. In contrast, by using general deterrence theory this study brings a new point

of view to research area regarding deterrence mechanisms and cyberloafing behavioral intention.

3.7. Conceptual Framework and Hypotheses

The purpose of this study to examine the causal relationship between control mechanisms and cyberloafing behavior intentions. Therefore in accordance with prior studies regarding management practices against deviant workplace behaviors such as misuse of the Internet and considering the General Deterrence Theory, organizational policies, computer monitoring, sanction (detection) certainty, sanction severity have been identified as independent variables. Likewise, to answer the main research questions, cyberloafing behavior intention has been identified as a dependent variable. Furthermore, gender, age, and education level of employees have been included in the conceptual framework.based on the extensive literature review, the following conceptual framework and hypotheses were proposed.

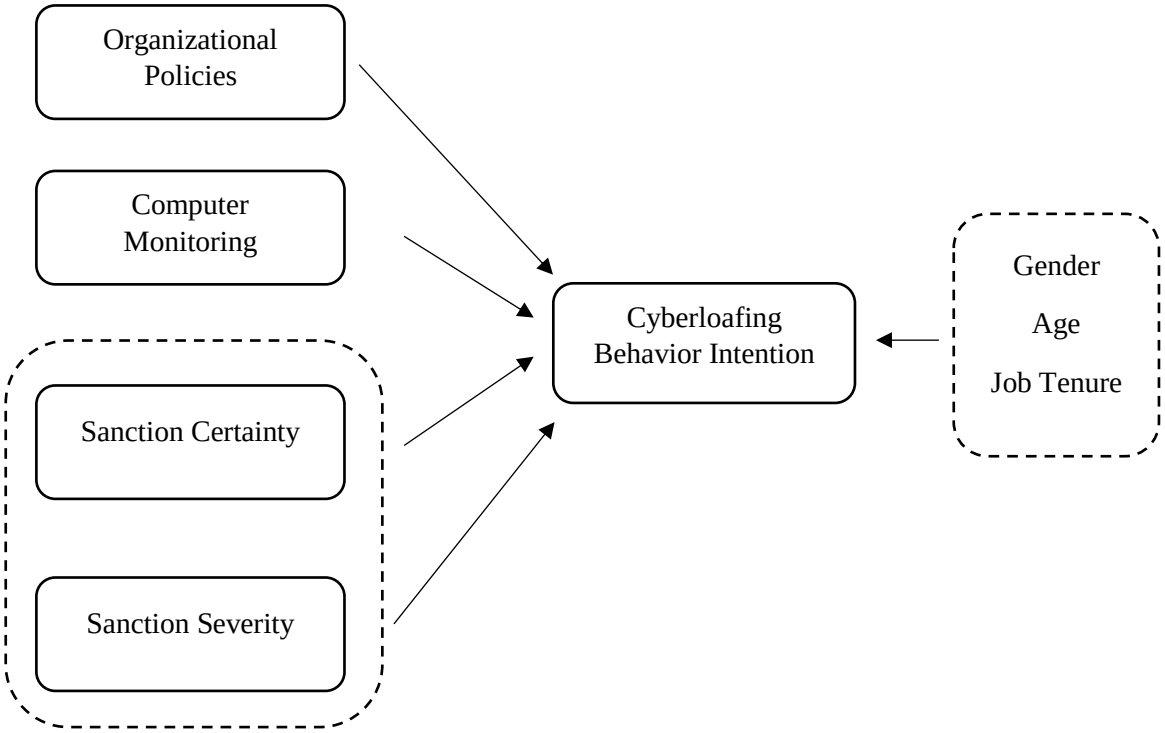

Figure 3. Conceptual Framework

H_{01}: There is no significant difference between cyberloafing intentions of individuals by their gender.
H_{11}: There is a significant difference between cyberloafing intentions of individuals by their gender.

H_{02}: There is no significant difference between cyberloafing intentions of individuals by their age.
H_{12}: There is a significant difference between cyberloafing intentions of individuals by their age.

H_{03}: There is no significant difference between cyberloafing intentions of individuals by their education.
H_{13}: There is a significant difference between cyberloafing intentions of individuals by their education.

H_{04}: There is no significant relationship between user awareness of organizational policies and cyberloafing intention.
H_{14}: There is a negative relationship between user awareness of organizational policies and cyberloafing intention.

H_{05}: There is no significant relationship between user awareness of computer monitoring and cyberloafing intention.
H_{15}: There is a negative relationship between user awareness of computer monitoring and cyberloafing intention.

H_{06}: There is no significant relationship between perceived detection certainty and cyberloafing intention.
H_{16}: There is a negative relationship between perceived detection certainty and cyberloafing intention.

H_{07}: There is no significant relationship between perceived severity of sanctions and cyberloafing intention.

H_{17}: There is a negative relationship between perceived severity of sanctions and cyberloafing intention.

3.8. Data Analysis

For this thesis, IBM SPSS Statistics 22 and AMOS Graphics software packages were used for the evaluation of the data. Initially, the reliability and validity analysis was conducted to test internal reliability and convergent and discriminant validity. Based on these analyses, the latest version of the questionnaire was developed and collected data from the participants. Afterward, descriptive analysis was employed to give information about the characteristics of the obtained data and demographic features of the participants. Thereafter, correlation analysis was conducted to reveal the relationship between dependent and independent variables. In the end, multiple regression analysis was employed to test hypotheses and examine the causal relationship between constructs.

4. FINDINGS

4.1. Sample Characteristics

This study collected data from 380 employees of bank branches in Ankara province between the periods of March 2019 to April 2019.

From the Table 6, it can be seen that the vast majority of findings were obtained from employees under thirty-five years of age and bachelor level of education which may demonstrate employees' familiarity with information technologies and ability to use electronic devices.

Moreover, compared to male participants, the number of female participants is higher and the majority of the participants have experience in their institution less than eight years. Taken together, the findings of this study is consistent with the official statistics of The Banks Association of Turkey.

In more detailed, a number of female participants (63.9%) is higher than male participants (36.1%) which shows that female employees constitute the majority of the total number of participants.

The table shows that %59.5 of participants were between the ages of 26-35 and 19.7% of the participants were between 18-25 ages; followed by 17.6% of the participants were between 36-45 ages and 3.2% which is a minority of the participants were above the age of 4.5.

Sample characteristics illustrate, in total, only 27.1% of the participants are working in their institutions for more than 8 years and 72.9% of participants have job tenure for less than 8 years.

Lastly, the majority of the participants' education was at bachelor level with 76.4%; followed by a master degree level with 18.4% and high school and an associate degree with 4.7%.

The table below illustrates the demographic characteristics of the participants which are obtained from the descriptive analysis.

Gender	Frequency	Percent	Cumulative Percent
Female	243	63,9	63,9
Male	137	36,1	100,0
Total	380	100,0	
Age			
18-25	75	19,7	19,7
26-35	226	59,5	79,2
36-45	67	17,6	96,8
45+	12	3,2	100,0
Total	380	100,0	
Job Tenure			
0-3 years	160	42,1	42,1
4-7 years	117	30,8	72,9
8-11 years	66	17,4	90,3
12+	37	9,7	100,0
Total	380	100,0	
Education Level			
High school/ Assoc.	18	4,7	4,7
Bachelor	290	76,4	81,0
Master	70	18,4	99,5
Doctorate	2	5	100,0
Total	380	100,0	

Table 6. Sample Characteristics

4.2. Descriptive Statistics

Descriptive Statistics			
Variable	Measures	Mean	Std. Deviation
Organizational Policies	OP1	3,71	1,06
	OP2	4,00	1,01
	OP3	4,20	1,06
	OP4	4,03	1,05
Computer Monitoring	CM1	4,08	1,15
	CM2	3,88	1,06
	CM3	3,99	1,07
	CM4	4,05	1,15
	CM5	3,81	1,07
	CM6	3,94	1,05
Sanction Certainty	PC1	3,82	1,02
	PC2	3,87	1,13
Sanction Severity	PS1	3,17	1,03
	PS2	3,74	1,06
Cyberloafing Intention	CBI1	2,11	0,96
	CBI2	2,34	0,94

Table 7. Descriptive Statistics

All scales were measured by a five-point Likert scale, ranging from strongly disagree (1) to strongly agree (5). The mean score for all five variables was found as follows; organizational policies are between 3.71 and 4.20, computer monitoring is between 3.81 and 4.08, sanction certainty is between 3.82 and 3.87, sanction severity is between 3.17 and 3.74, cyberloafing intention is between 2.11 and 2.34. Table 7 shows the means and standard deviations for all measurements.

The answers of the participants in the first part show that most of the participants are aware of the policies within their organizations which regulates internet and computer usage. Similarly, in the second part of the questionnaire, employees answered commonly "Agree" to questions which examine employees' perception regarding computer monitoring mechanisms within their organization. This shows that most of the bank branches utilize specific software and systems to control employees' internet activities and employees are aware of these mechanisms.

In the third and fourth parts participants' perceived sanction certainty (detection certainty) and sanction severity in their organization were measured. In these parts, participants have been asked whether if they engage with cyberloafing activities, this can be recognized by managers and there can be a severe sanction against this behavior. Findings revealed that the average of the answers was varied between "Undecided" and "Agree". This means employees slightly agree that if they engage in cyberloafing activities this can be notified by managers and based on their activities' consequences on the organization, the sanction against this behavior may be severe.

In the last part, participants' cyberloafing intention was measured and the average of the answers show that participants are not intended to engage in cyberloafing in the future regardless they have an opportunity.

4.3. Reliability

Reliability analysis has great importance in quantitative researches to evaluate stability and internal consistency of the constructs. In this thesis, the scale reliability of the variables was assessed by Cronbach alfa's test and Cronbach's alfa coefficient was found 0,852. The result of the analysis indicates the internal reliability of the measurement were proven to be acceptable as shown in Table 8.

		N	%	Cronbach's Alfa	N of Items
Cases	Valid	380	100,0		
	Excluded	0	,0	,898	16
	Total	380	100,0		

Table 8. Case Processing Summary and Reliability Analysis

4.4. Validity

In addition to reliability, measurement validity is another key component of research methodology to assure the integrity and quality of measurement (Kimberlin & Winterstein, 2008). The measurement validity defined as "relevancy and meaningfulness of a measurement" and in social sciences, it is mainly evaluated through construct validity and discriminant validity.

In this study to assess the measurement validity, two steps were followed. Primarily, exploratory factor analysis was performed on pilot sample data which is obtained from 96 bank employees and according to dimensionality and factor loading of the items, adjustments were made on the scales. As a result of the exploratory factor analysis, KMO measure of sampling adequacy was found 0,875 which shows that obtained data was appropriate and our sampling was adequate for factor analysis. Based on this analysis, the final version of the scale was created and applied to an actual sample of this study.

Analysis		Value
Kaiser-Meyer-Olkin Measure of Sampling Adequacy		,875
Bartlett's Test of Sphericity	Approx. Chi-Square	1211,702
	df	120
	Sig.	,000

Table 9. Exploratory Analysis

After data was obtained from the sample, in order to control the convergent and construct validity of the measurement, confirmatory factor analysis was conducted. The model of the research was evaluated through Chi-square to the degree of freedom (CMIN/DF), comparative fit index (CFI), the goodness of fit index (GFI), non-normal fit index (NFI) and root mean square error of approximation RMSEA goodness of fit indexes and shown in Table 10.

Model Fit Indices	Default Model	Recommended Criteria
CMIN/DF	1,729	< 3.00
CFI	,989	≥ 0.90
GFI	,947	≥ 0.90
NFI	,974	≥ 0.90
RMSEA	0,44	< 0.80

Table 10. Goodness Fit Statistics

Ideally, CFI, GFI and NFI indexes are expected higher than 0,90, RMSEA lower than 0,80 and CMIN/DF value lower than 3 which show a good fit with reasonable errors of approximation in the population. All model fit indices such as CMIN/DF (1,729), CFI (0,989), GFI (0,947), NFI (0,974) and RMSEA (0,44) were found as satisfactory regarding the recommended criteria and each of goodness-fit indices were achieved.

Moreover, the convergent validity of the research was evaluated by estimated factor loading, composite reliability (CR), and average variance extracted (AVE). In accordance with the rule of thumb, factor loadings supposed to be greater than 0,50, composite reliability should be greater than 0,70 and average variance extracted value should be greater than 0,50 (Fornell and Larcker, 1981). As Table 11 illustrates, for each variable factor loadings, composite reliability and AVE values comply with recommended criteria.

Variable	Measure	Factor Loading	CR	AVE
Organizational Policies	OP1	,70	0,88	0,66
	OP2	,84		
	OP3	,83		
	OP4	,86		
Computer Monitoring	CM1	,93	0,95	0,81
	CM2	,85		
	CM3	,92		
	CM4	,93		
	CM5	,85		
	CM6	,89		
Sanction Severity	PS1	,78	0,80	0,67
	PS2	,86		
Sanction Certainty	PC1	,94	0,94	0,89
	PC2	,95		
Cyberloafing Behavior	CBI1	,86	0,90	0,82
	CBI2	,95		

Table 11. Convergent Validity

In addition to convergent validity, discriminant validity was analyzed to evaluate the reflection of the measurement with other measurements that suppose to test another concept. To evaluate discriminant validity square roots of AVE value should be greater than correlation coefficients of each variable. In this study, square roots of AVE for organizational policies (0,81), computer monitoring (0,90), sanction severity (0,81), sanction certainty (0,94) and cyberloafing behavior (0,90) were found greater than each of variables correlation coefficient which refers discriminant validity was achieved.

Based on the result of confirmatory factor analysis, it can be said that the scale of the research which consists of five factors is verified and the reliability and validity of the measurement were proved.

4.5. Hypotheses Testing

Correlation Analysis

	Mean	S.D.	1	2	3	4	5
1. Organizational Policies	3,99	,90	-				
2. Computer Monitoring	3,96	1,00	,636**	-			
3. Sanction Certainty	3,85	1,09	,543**	,824**	-		
4. Sanction Severity	3,46	,96	,490**	,695**	,783**	-	
5. Cyberloafing Behavior Intention	2,22	,90	-,544**	-,766**	-,715**	-,647**	-

**p<0,05

Table 12. Correlation Analysis

According to Table 12, there is a significant and negative relationship between each independent variables and a dependent variable. In more detailed, computer monitoring, sanction certainty, sanction severity were found highly and negatively correlated with cyberloafing behavior intention. Similarly, awareness of the organizational policies also found correlated with cyberloafing significantly and negatively (*r* = -,544), but compared to the other dependent variables, in the lower level. Moreover, the correlation analysis revealed that there is a significant and positive correlation between dependent variables. The most surprising aspect of the analysis, while sanction certainty and computer monitoring were the highly correlated variables (*r* =, 824), organizational policies and sanction severity were the low-level correlated variables (*r* =, 490).

In order to examine the relationship between control variables and cyberloafing behavior, T-test and One-Way ANOVA analysis were conducted. According to the results of the T-test which was conducted to compare cyberloafing intentions between genders, it can be seen that the intention of cyberloafing of men and women was significantly different from each other ($p < 0,05$).

Gender	N	Mean	S.D.	t	df	*p*
Woman	243	2,17	0,96	-11,581	378	p < 0,05
Men	137	3,41	1,08			

Table 13. Results of T-Test Analysis

As it has been shown in the table, cyberloafing behavior intentions of men employees ($\bar{X} = 3,41$) were higher than women employees ($\bar{X} = 2,17$). Therefore H_{11} hypothesis which states "there is a significant difference between of cyberloafing intention by genders" was supported. In addition to gender, One-Way ANOVA Test was used in order to analyze the difference between cyberloafing intention and employees' ages and education levels. The result of the analysis is shown in Table 14.

	N	Mean	S.D.	S.S.	M.S.	F	*p*
18-25	75	2,82	1,23	15,18	5,06	3,77	*p*<0,05
26-34	226	2,68	1,16				
35-45	67	2,20	1,05				
45+	12	2,58	1,12				
High School	18	3,03	1,39	13,46	4,48	3,33	*p*<0,05
Bachelor	290	2,67	1,13				
Master	70	2,32	1,18				
Doctorate	2	1,50	0,70				

Table 14. One-Way ANOVA Test Analysis

It is apparent from this table that there is a significant difference between the ages of the employees and cyberloafing intention. As the age of the employees' increases, the intention of cyberloafing decreases. Although One-Way ANOVA analysis shows the overall differences between the control variables, in order to examine which group of ages and education levels differ from each other, post-hoc analysis was conducted.

There is a number of post-hoc analysis which is designed for the particular datasets and generally, post-hoc statistic analysis is considered in two different categories as the variance between the groups is equal and the variances are not equal. As can be seen from Table 15, in this research the dataset met the assumption of homogeneity of variances as p-value was found more than 0,05.

Levene Statistics	df1	df2	Sig.
2,049	3	376	$p > 0,05$

Table 15. Test of Homogeneity of Variances

As the variances were homogenously distributed, Gabriel Hochberg's GT2 methods were used for post-hoc analysis on control variables. Hochberg's GT2 statistic method commonly used when there the sample size of the groups are very different from each other. On the other hand, Gabriel post-hoc method is used when the sample size between groups are not very different.

As in this research the sample size of age groups not very different from each other Gabriel method was used. Based on results of Gabriel post-hoc analysis on age groups, it was found that there is a significant difference between employees under 34 years of ages and employees who are between 35-45 years old ages ($p < 0,05$). These results show younger employees have a greater intention for engaging cyberloafing activities compare to older employees.

	Age	Age	Mean Difference	Std. Error	Sig.
Gabriel	18-25	26-34	,13858	,15442	,926
		35-45	,61104*	,19479	,011
		45+	,23667	,36028	,979
	26-34	18-25	-,13858	,15442	,926
		35-45	,47246*	,16119	,014
		45+	,09808	,34327	1,000
	35-45	18-25	-,61104*	,19479	,011
		26-34	-,47246*	,16119	,014
		45+	-,37438	,36323	,843
	45+	18-25	-,23667	,36028	,979
		26-34	-,09808	,34327	1,000
		35-45	,37438	,36323	,843

Table 16. Gabriel Post-Hoc Analysis

On the other hand, in age groups, as the number of employees who have doctorate level of education is only two, in order to avoid from a bias, these data were excluded from the analysis. For the rest of the data, Hochberg's GT2 post-hoc analysis method was used as the sample size between education level groups are very different from each other. The results of the analysis have shown in Table 17.

	Education	Education	Mean Difference	Std. Error	Sig.
Hochberg's GT2	High School	Bachelor	,40920	,28219	,381
		Master	,76190*	,30701	,040
	Bachelor	High School	-,40920	,28219	,381
		Master	,35271	,15471	,068
	Master	High School	-,76190*	,30701	,040
		Bachelor	-,35271	,15471	,068

Table 17. Hochberg's GT2 Post-Hoc Analysis

It can be seen from the data in Table 17 that there is a significant difference between employees who have a high school or associate level of education and master degree level of education for cyberloafing intention. Gabriel test of analysis revealed that employees who have a higher level of education level are less tend to engaging cyberloafing activities.

In conclusion, H_{11}, $H_{12,}$ and $H_{13\ h}$ypotheses have been supported by the T-Test, One-Way ANOVA and Post-hoc analysis.

As correlation analysis shows only the presence of a relationship between two variables, multiple regression analysis have been conducted in order to examine the causal relationship between this study's dependent and independent variables.

Multiple Regression Analysis				
$F(4,375) = 153,888$	$p < 001$		$R^2 = ,62$	$R^2_{adjusted} = .61$
OP → CBI	$B_4 = -,080$	$t = -1,932$	$p = 0,51$	H_4: Not Supported
CM → CBI	$B_5 = -,433$	$t = -7,810$	$p < 0,05$	H_5: Supported
PC → CBI	$B_6 = -,132$	$t = -2,911$	$p < 0,05$	H_6: Supported
PS → CBI	$B_7 = -,142$	$t = -2,427$	$p < 0,05$	H_7: Supported

Table 18. Results of Multiple Regression Analysis for Hypotheses

Results of the multiple regression analysis show that 61% of the total variance in the dependent variable, can be explained by independent variables. According to Table 18 awareness of organizational policies do not predict cyberloafing behavior intention ($\beta_4 = -,080$, $t = -1,932$, $p = 0,51$). Therefore, H_{04} hypothesis was supported by the results of the analysis. This shows that organizational policies are not effective enough to prevent individuals from cyberloafing activities. H_5 hypothesis was supported since the relationship between computer monitoring awareness and cyberloafing behavior intention was found significant ($\beta_5 = -,433$, $t = -7,810$, $p < 0,05$). There is a negative relationship between computer

monitoring awareness and cyberloafing behavior intention. Therefore, the H_5 hypothesis is supported by the results of the analysis. When employees have awareness regarding their internet activities may be tracked and controlled by the organization, they are less prone to engage in cyberloafing activities. Similarly, H_6 hypothesis which is established based on General Deterrence Theory is supported by the analysis (β_6 = -,132, t = -2,911, p < 0,05). There is a significant and negative relationship between perceived sanction certainty (detection) and cyberloafing behavior intention. When employees perceive that if they engage in cyberloafing activities, this will be recognized by the management, they have less intention to conduct this behavior. Finally, H_7 hypothesis tests another component of General Deterrence Theory was supported which predict a significant and negative relationship between perceived sanction severity and cyberloafing behavior intention (β_7 = -,142, t = -2,427, p < 0,05). This shows, if employees have an intention to engage in cyberloafing activities and they face severe sanction according to their cyberloafing behavior, they will less tend to show this behavior again. It appears from the analysis when employees perceive organizational sanctions, they are less tend to engaging cyberloafing behavior.

Although it has been found that computer monitoring and organizational sanctions negatively affects cyberloafing intention, the relationships between independent and dependent variables have been found week as coefficients of the regression analysis were below than average. Moreover, compared to awareness of sanction severity and certainty, the perceived computer monitoring system has been found more effective to reduce cyberloafing intention. In conclusion, except H_{14} all hypotheses are supported with the achieved results of the multiple regression analysis.

Furthermore, the regression model formula has been given below.

$$Y = ß_0 + ß_1X_1 + ß_2X_2 + \ldots\ldots\ldots ß_nX_n + \varepsilon$$

$$CBI = ß_0 + ß_4.OP + ß_5.CM + ß_6.PC + ß_7.PS + \varepsilon$$

$$CBI = 5{,}262 + (-{,}080)OP + (-{,}433)CM + (-{,}132)PC + (-{,}142)PS + \varepsilon$$

5. DISCUSSION

Within the introduction of information technologies in the workplaces, cyberloafing has attracted great attention as it affects organizations negatively as well as positively. In order to cope with the negative aspects of this behavior, organizations have developed several countermeasure strategies and control mechanisms. However, in the literature, there was a gap regarding the effectiveness of these mechanisms as studies have focused commonly on antecedents and consequences of this behavior. Therefore, this study aimed to explain the causal relationship between control mechanisms and cyberloafing behavior intention. In order to achieve this aim, 7 hypotheses were proposed and analyzed by statistical analysis. The sample of the study was constituted of 380 employees of bank branches in Ankara and collected data were analyzed with IBM SPSS 22 program. In accordance with the results of the analysis, the hypotheses status is shown in Table 19.

	Hypotheses	Status
H_1:	There is a significant difference between cyberloafing intentions of individuals by their gender.	Supported
H_2:	There is a significant difference between cyberloafing intentions of individuals by their age.	Supported
H_3:	There is a significant difference between cyberloafing intentions of individuals by their education level.	Supported
H_4:	There is a negative relationship between awareness of organizational policies and cyberloafing intention.	Not Supported
H_5:	There is a negative relationship between awareness of computer monitoring and cyberloafing intention.	Supported
H_6:	There is a negative relationship between perceived sanction certainty of computer monitoring and cyberloafing intention.	Supported
H_7:	There is a negative relationship between perceived sanction severity and cyberloafing intention.	Supported

Table 19. Status of Hypotheses

Prior studies have noted organizational policies which include rules, possible sanctions and guidelines regarding acceptable use of the internet have a negative impact on cyberloafing intention of individuals. (Henle, Kohut and Booth, 2009). Therefore, based on earlier

findings, this study proposed that when individuals aware of the organizational policies, they are less likely to engage with cyberloafing behavior. Contrary to expectations, the current study did not find a significant relationship between awareness of organizational policies and cyberloafing intention which means organizational policies are not adequate to control mechanism to prevent cyberloafing behavior. The result of the analysis shows that employees' cyberloafing intention is not affected by the presence of policies. This can be interpreted in two ways. Firstly, the organizations may not have effective and comprehensive policies regarding acceptable internet usage behavior or it is not implemented in the correct way.

Another control mechanism that is highly debated in terms of ethics and the negative impacts on employees, computer monitoring has been found as an effective control strategy in reducing cyberloafing intention by many scholars (Mirchandani and Motwani, 2003; Lichtash, 2004). Therefore, this study proposed, individuals' awareness of computer monitoring mechanism is negatively related to the intention of cyberloafing behavior. In accordance with the previous findings, this study has demonstrated that when employees are aware of their activities through work computers are monitored and controlled by the employer, they are less tend to cyberloaf.

Moreover, the sixth and seventh of the hypotheses of this study proposed based on General Deterrence One of the prominent concepts in this research area, General Deterrence Theory suggests that by enforcing the sanction severity and detection certainty in the organization, workplace deviant behaviors such as cyberloafing can be prevented in some extent. (Ugrin and Pearson, 2013). Therefore, by reviewing the literature it is proposed that perceived sanction severity and sanction certainty negatively related to cyberloafing intention. Likewise, the finding of this study supports previous research into this area which states that when individuals perceive strong sanction severity and sanction certainty regarding their counterproductive behaviors, they are less likely to engage with cyberloafing behavior. This means, employees should be aware of if they engage in cyberloafing activities during work hours, there is a high possibility of getting caught and if they caught up the sanction will be severe.

Lastly, the differences between the demographic characteristics of employees and cyberloafing behavior intentions were examined. A number of studies have found that

particular demographic characteristics such as gender, age, education of employees are helpful to predict cyberloafing intention of the individuals. Lim and Chen (2012) reported that men are more likely cyberloafing than women, Vitak et al. (2011) have argued that younger employees more tend to use internet for non-work related activities compared to older employees and Garret and Danziger (2008) reported in their research that the individuals who have higher education, less prone to engage with cyberloafing activities. For this reason, three hypotheses proposed regarding there is a significant difference between age, gender, education level, and cyberloafing intention. In accordance with previous studies, it is found that men are more tend to cyberloaf than women, younger employees more likely to cyberloaf than older employees and as the level of education increases, the cyberloafing intention decrease. These findings are consistent with earlier studies and very important for human resource management to revise their strategies according to the characteristics of individuals.

In view of all that has been mentioned so far, the findings of this study revealed that computer monitoring systems are the most effective countermeasure mechanism for the organizations while organizational policies are insufficient to reduce cyberloafing intention. Furthermore, these findings support prior studies into this area which links General Deterrence Theory and cyberloafing intention which means when organizations enforce the sanctions towards the unwanted act of individuals, employees have the lower intention to cyberloafing behavior. Additionally, the gender, age, and education level of employees differences of employees create differences for cyberloafing intention.

6. CONCLUSION

To some extent use of internet and computer technologies in the workplaces are undoubtedly essential and beneficial for the organizations in terms of gaining a competitive advantage by accelerating the business operations, supporting innovative and creative ideas and decreasing the cost of units. On the contrary, the development of information technologies has been brought some drawbacks such as cyberloafing activities in the workplaces which lead to positive and negative impacts for employees and businesses. Although cyberloafing has become one of the popular phenomena in recent years, in the literature cyberloafing concept examined mostly about its consequences and antecedents. Only a few studies have been able to draw on structured research into controlling mechanisms and cyberloafing intention and much of the research up to now has been exploratory in nature with qualitative methods. Therefore the main aim of this study was examining the effectiveness of management practices to reducing cyberloafing behavior within a broader perspective. In order to achieve this aim, seven hypotheses were outlined and conceptual framework was developed regarding cyberloafing concept as a workplace deviant behavior, antecedents, consequences on organizations and control strategies toward cyberloafing behavior including General Deterrence Theory.

The findings of this study supported existing literature and indicated that awareness of computer monitoring is the most effective countermeasure mechanism for cyberloafing behavior. When individuals aware of their activities on the Internet or computerized data can be monitored and controlled by the organization, they are less likely to use the internet for personal purposes. In contrast to earlier findings, the present study did not find a significant relationship between the presence and awareness of organizational policies and cyberloafing behavior intention. This may be due to the fact that each organization implements these policies in their own way and the scope of these policies may differ. Furthermore, the findings of the current study regarding General Deterrence Theory and cyberloafing intention is consistent with prior studies in the literature. The results of this study confirm that perceived sanction severity and sanction certainty is negatively associated with cyberloafing intention and can be served as a deterrence mechanism. This shows that employees should be aware of the possible detection mechanisms if they engage in cyberloafing activities and these types of mechanisms should be updated due to advancements on information technologies which are used in workplaces. Moreover,

managers should apply sanctions according to the severity of cyberloafing behaviors fairly and consistently when employees engage with destructive cyberloafing activities. The severity of these sanctions should be varied based on the negative impacts of cyberloafing behavior on individuals and organizations.

Lastly, this study produced similar results regarding the differences between demographic characteristics may predict cyberloafing intention which corroborates the findings of a great deal of the previous work in this field. Based on the findings, women were found more likely to engage cyberloafing activities more than men, younger employees have a greater chance to cyberloaf compared to older employees and as the level of education increases, employees become less likely to engage cyberloafing behavior. Based on demographic characteristics human resources management may analyze internet use behavior of employees and conduct training to raise awareness between employees to use the internet for work-related tasks and self-improvement regarding work. Moreover, based on these characteristics, organizations may develop particular deterrence and control mechanisms and apply through the organization.

In summary, the results of the present study fully support the general deterrence theory and reveal that intentions for the cyberloafing behavior may be decreased buy enforcing the organizational sanctions and computer monitoring systems. Therefore, considering the positive and negative consequences of cyberloafing behavior, organizations should implement balanced controlling strategies to take advantage of beneficial aspects while avoiding the detrimental impacts.

6.1. Managerial Practices

A considerable amount of researches to date have shown that cyberloafing behavior has a negative impact on individuals and organization as well as positive (İnce and Gül, 2011). Therefore, instead of preventing cyberloafing activities, managers should find a balance in control practices to benefit from the constructive side of cyberloafing while avoiding the destructive aspects of the behaviors.

Instead of having generalized policies regarding computer use behavior, organizations should adopt more comprehensive and detailed policies which regulate the acceptable use of the internet. Policies should be specialized on employees' internet activities and state

specifically acceptable use of work computers and internet accesses. In the case of engaging destructive cyberloafing activities, policies should clearly point out the possible sanctions regarding the seriousness of cyberloafing behavior. Since the presence of the policy is not sufficient to prevent employees to cyberloaf, managers should ensure that these policies are implemented effectively and equally. Furthermore, the prior studies show that when employees take part in developments of policies, they are more tend to perceive these policies fair and more tend to comply with rules (Foltz, Cronan and Jones, 2005). Therefore organizations may encourage the group of people to represent other employees and contribute to the modification of the policies regarding internet use.

As study findings revealed that when individuals engaging cyberloafing behavior and they perceive, there is a high chance that it will be discovered and there will be a severe sanction regarding this behavior, they are less likely to engage with cyberloafing activities. From this point of view, organizations should enforce balanced organizational sanctions across the whole organization and create awareness of these sanctions against cyberloafing behavior. Employees' should be informed regarding detection mechanisms such as computer monitoring systems and ensured that destructive cyberloafing behaviors will not be tolerated by the organization. Moreover, certain websites and contents such as adult-oriented websites, gambling applications on the internet which may have negative impacts on organization or individuals should be forbidden and restricted by the organization.

In conclusion, although this study emphasizes the effectiveness of control strategies against detrimental impacts of cyberloafing behavior, it should be noted that there is a considerable amount of empirical findings which shows that cyberloafing also has positive consequences for individuals and organizations. Therefore, organizations should aim to take advantage of good aspects and protect from harmful aspects of this behavior and implement control strategies considering this situation.

6.2. Limitations and Future Research Suggestions

In spite of the fact that this study makes a considerable amount of contributions to the theory and managerial practices, the following limitations should be taken consideration for future researches.

The current study has only examined cyberloafing behavior in the workplace through work computers. However, considering the fact that almost every individuals use smartphone and internet become omnipresent via internet service providers, employees may also engage cyberloafing with their mobile phones. Therefore, future research should concentrate on the investigation of cyberloafing behavior in the workplace via smartphones and work computers together.

Moreover, this study has been used only computer monitoring and organizational policies to measure the effectiveness of deterrence mechanisms. Although these two strategies are the most applied and common practices to cope with cyberloafing behavior, in some organizations, there are various strategies such as compliance training and physical monitoring. Further experimental researches are needed to cover more broadly regarding managerial practices against cyberloafing behavior.

7. KAYNAKÇA

Abbasi, H. (2018). Organizational Information Security: Strategies to Minimize Workplace Cyberloafing for Increased Productivity. Doctoral Thesis, University of Walden.

Allen, N. J., & Meyer, J. P. (1990). The Measurement And Antecedents Of Affective, Continuance And Normative Commitment To The Organization. *Journal of Occupational Psychology, 63*(1), 1-18.

Alter, S. (2015). Beneficial Noncompliance and Detrimental Compliance: Expected Paths to Unintended Consequences, *Americas Conference on Information Systems,* 25.

Anandarajan, M. & Simmers, C. (2005). Developing Human Capital Through Personal Web Use in the Workplace: Mapping Employee Perceptions, *Communications of the Association for Information Systems*, (15), 776-791.

Anandarajan, M., Simmers, C. & Igbaria, M. (2000). An Exploratory Investigation Of The Antecedents And Impact Of Internet Usage: An Individual Perspective. *Behavior & Information Technology,* (19), 69–85.

Andreassen, C. S., Torsheim, T., & Pallesen, S. (2014). Use Of Online Social Network Sites For Personal Purposes At Work: Does İt İmpair Self-Reported Performance*? Comprehensive Psychology*, 3(1), 1-11.

Appelbaum, S.H., G.D. Iaconi & A.Matousek, (2007). Positive And Negative Deviant Workplace Behaviors: Causes, Impacts, And Solutions, *Corporate Governance: The International Journal Of Business In Society*, 7(5), 586-598.

Arshad, M., Aftab, M., & Bukhari, H.(2016). The Impact of Job Characteristics and Role Stressors on Cyberloafing: The Case of Pakistan. *International Journal of Scientific and Research Publications*, 6(12), 244-251.

Askew, K.L. (2012). The Relationship Between Cyberloafing and Task Performance and an Examination of the Theory of Planned Behavior as a Model of Cyberloafing. Graduate Theses and Dissertations, University of South Florida.

Askew, K., Buckner, E.J., Taing, M., Ilie, A., Bauer, J. & Coovert, M. (2014). Explaining Cyberloafing: The Role of the Theory of Planned Behavior. *Computers in Human Behavior*, 36, 510-519.

Baldwin, S.(2006). Organizational Justice, Brighton: Institute for Employment Studies.

Belanger, F. & Van Slyke, C. (2002). Abuse or Learning. *Communication of the ACM*, (45:1), 64-65.

Bennett, R. J., & Robinson, S. L. (2000). Development Of A Measure Of Workplace Deviance. *Journal of Applied Psychology*, 85(3), 349-360.

Beugré, C. D. (2003). Information Technology As A Double-Edged Sword: A Model Of Cyber Dysfunctional Behavior. *Proceedings of the Eastern Academy of Management Meeting*, April (3), Baltimore, MD.

Beugre, C.D. & Kim, D. (2006), Cyberloafing: Vice or Virtue? in Mehdi Khosrow-Pour-Ed.book, *Emerging Trends and Challenges in Information Technology Management*, 834-835.

Blanchard, A., & Henle, C. (2008). Correlates Of Different Forms Of Cyberloafing: The Role Of Norms And External Locus Of Control. *Computers in Human Behavior*, 24, 1067-1084.

Bock, G.W., Park, S.C. & Zhang, Y. (2010b). Why Employees Do Non-Work- Related Computing in the Workplace. *The Journal of Computer Information Systems*, (50:3), 150-163.

Bock, G.W., Park, S.C., & Zhang, Y. (2010). Why Employees Do Non-Work-Related Computing In The Workplace, *Journal of Computer Information Systems*, 50(3), 150-163.

Bock, G.W., Shin,Y., Liu,P. & Sun, H. (2010a). The Role of Task Characteristics and Organizational Culture in Non-Work-Related Computing: A Fit Perspective. *The Database for Advances in Information Systems*, (41:2), 132-150.

Bosword, M. (2005). Encyclopedia of Prisons & Correctional Facilities. Wesleyan University, SAGE Publications, 233-237.

Brakel, H. (2016). Cyberloafing: A Learning Tool for Senior Surfers? Master Thesis, Vrije Universiteit Amsterdam.

Brinkman, C. (2013). The Big Five Personality Model And Motivation In Sport. Master Thesis. Miami University.

Brock, M. E., Martin, L. E., & Buckley, M. R. (2013). Time Theft In Organisations: The Development Of The Time Banditry Questionnaire. *International Journal of Selection and Assessment,* 21, 309-322.

Bryman, B. & Bell, E. (2011). Business Research Methods, 3rd Edition, Oxford: Oxford University Press.

Case, C.J., Young, K.S. (2002). Employee Internet Management: Current Business Practices And Outcomes. *Cyberpsychology Behavior*, 5, 355-361.

Chang, M.K. and Cheung, W. (2001), Determinants Of The Intention To Use Internet At Work: A Confirmatory Study, *Information & Management*, 39(1), 1-14.

Chen,C.J., Chen, C.C., Yang, H. (2008). An Empirical Evaluation Of Key Factors Contributing To Internet Abuse In The Workplace. *Industrial Management & Data Systems*, 108(1), 87-106.

Cheng, L., Li, Y., Li, W., Holm, E. & Zhai, Qi.. (2014). Understanding The Violation Of IS Security Policy In Organizations: An Integrated Model Based On Social Control And Deterrence Theory. *Computers & Security*. 39. 447–459.

Coffin, B., 2003. Breaking The Silence On White Collar Crime. *Risk Management,* 50: 8.

Coker, B.L.S. (2011). Freedom to Surf: The Positive Effects of Workplace Internet Leisure Browsing. New Technology, Work and Employment, (26:3), 238-247.

D'Abate, C. & Eddy, E. (2007). Engaging In Personal Business On The Job: Extending The Presenteeism Construct. *Human Resource Development Quarterly*, 18 (3): 361-83.

Daft, R.L, Murphy, J. & Willmott,H. (2010). Organization Theory and Design. South-Western Cengage Learning: Singapore.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 20(1), 79-98.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2011). Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. International Journal of Information Management, 31(3), 201-209.

Doorn, O.N.V. (2011). Cyberloafing: A Multi-Dimensional Construct Placed In A Theoretical Framework. Master Thesis, Eindhoven University of Technology.

Dutton, J. E., & Ashford, S. J. (1993). Selling Issues to Top Management. *The Academy of Management Review*, 18(3), 397.

Eddy, E., D'Abate, C. & Thurston, P. (2010). Explaining Engagement In Personal Activities On Company Time. *Personnel Review*, 30 (5): 639-654.

Everton, W. J., Mastrangelo, P. M., & Jolton, J. A. (2005). Personality Correlates of Employees' Personal Use of Work Computers. *CyberPsychology & Behavior*, 8(2), 143–153.

Fallows, D. (2005). How Women And Men Use The Internet. *PEW Internet and American Life Project*, December, 1–45.

Fındıklı, M.A. (2016). Sanal Kaytarma Ve İş Performansı İlişkisi: Sağlık Ve Tekstil Sektörü Çalışanlarının Karşılaştırılması. *International Journal of Social Inquiry*, 9(1), 33-62.

Foltz, C. B., Cronan, T. P., & Jones, T. W. (2005). Have You Met Your Organization's Computer Usage Policy? *Industrial Management and Data Systems*, 105(1/2), 137146.

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models With Unobservable Variables And Measurement Error. *Journal of Marketing Research*, 18(1), 39-50.

Fox, S. & Spector, P. E. (2005). The Stressor-Emotion Model of Counterproductive Work Behavior. In S. Fox & P. E. Spector (Eds.), *Counterproductive Work Behavior: Investigations Of Actors And Targets*.Washington, DC, US: American Psychological Association, 151-174.

Garrett, R.K. & Danziger, J.N. (2008). Disaffection or Expected Outcomes: Understanding Personal Internet use During Work. *Journal of Computer-Mediated Communication*, (13), 937–958.

Gibbs, J.P. (1975). *Crime, Punishment, and Deterrence*. New York, NY: Elsevier.

Giles, C. (2015). Undergraduate Students' Perceptions Of Cyberloafing. Texas Christian University.

Greenberg, L., & Barling, J. (1999). Predicting Employee Aggression Against Coworkers, Subordinates And Supervisors: The Roles Of Person Behaviors And Perceived Workplace Factors. *Journal of Organizational Behavior, 20*(6), 897-913.

Greengard, S. (2000). The High Cost of Cyberslacking. *Workforce*. (12), 22-24.

Griffiths, M. (2010). Internet Abuse And Internet Addiction In The Workplace. *Journal of Workplace Learning*, 22(7), 463-472.

Gruys, M.L. (1999). The Dimensionality Of Deviant Employee Performance In The Workplace. Unpublished Doctoral Dissertation, University of Minnesota.

Hamermesh, D. S. (1990). Shirking Or Productive Schmoozing: Wages And The Allocation Of Time At Work. *Industrial and Labor Relations Review*, 43: 121–133.

Hassan, H.M., Reza, M.D., & Farkhad, M. (2015). An Experimental Study of Influential Elements On Cyberloafing From General Deterrence Theory Perspective. *International Business Research,* 8(3), 91-98.

Henle, C., Kohut, G. & Booth, R. (2009). Designing Electronic Use Policies To Enhance Employee Perceptions Of Fairness And To Reduce Cyberloafing: An Empirical Test Of Justice Theory. *Computers in Human Behavior*, 25 (4): 902–910.

Henle, C.A., & Blanchard, A.L. (2008). The Interaction Of Work Stressors And Organizational Sanctions On Cyberloafing. *Journal of Managerial Issues*, *20*(3), 383-400.

Hollinger, R. C. & J. P. Clark. (1983). Deterrence in the Workplace: Perceived Certainty, Perceived Severity, and Employee Theft. *Social Forces*. (62), 398-418.

Hollinger, R.C, Slora, K.B., & Terris, W. (1992) Deviance In The Fast-Food Restaurants: Correlates of Employee Theft, Altruism, And Counterproductivity. *Deviant Behavior: An Interdisciplinary Journal*, 13(2), 155-184.

Hough, L. M., & Furnham, A. (2003). Use of personality variables in work settings. In W. C. Borman, D. R. Ilgen, & R. J. Klimoski (Eds.), *Handbook of psychology: Industrial and organizational psychology,* 12, 131-169. Hoboken, NJ, US: John Wiley & Sons Inc.

Ince, M. & Gül, H. (2011). The Role Of The Organizational Communication On Employees' Perception Of Justice: A Sample Of Public Institution From Turkey. *European Journal of Social Sciences,* 21, 106-124.

Ivarsson, L. & Larsson, P. (2011). Personal Internet Usage at Work: A Source of Recovery. *Journal of Workplace Rights.* 16. 63-81.

Jandaghi, G., Alvani, S. M., Matin, H. Z., & Kozekanan, S. F. (2015). Cyberloafing Management in Organizations. *Iranian Journal of Management Studies*, 8 (3), 335-349.

Jia, H., Jia, R., & Karau, S. (2013). Cyberloafing and Personality: The Impact of the Big Five Traits and Workplace Situational Factors. *Journal of Leadership & Organizational Studies*, 20(3), 358–365.

Jian, G. (2013) Understanding the Wired Workplace: The Effects of Job Characteristics on Employees' Personal Online Communication at Work. *Communication Research Reports*, 30(1), 22-33.

John, O. P., & Srivastava, S. (1999). The Big Five Trait taxonomy: History, measurement, and theoretical perspectives. In L. A. Pervin & O. P. John (Eds.), *Handbook of personality: Theory and research*, 102-138. New York, NY, US: Guilford Press.

Johnson, R. & Rawlins, C. (2008). Employee Internet Management: Getting People Back To Work. *Journal of Organizational Culture, Communications and Conflict*, 12 (1): 43-48.

Judge, T. A., & Ilies, R. (2002). Relationship of personality to performance motivation: A meta-analytic review. *Journal of Applied Psychology*, 87(4), 797-807.

Kimberlin, C. L., & Winterstein, A. G. (2008). Validity And Reliability Of Measurement İnstruments Used İn Research. *American Journal of Health-System Pharmacy,* 65(23), 2276–2284.

Koay, K. Y., Soh, P. C.-H., & Chew, K. W. (2017). Do Employees' Private Demands Lead To Cyberloafing? The Mediating Role Of Job Stress. *Management Research Review,* 40(9), 1025–1038.

König, C. & E. Caner de la Guardia, M. (2014). Exploring The Positive Side Of Personal Internet Use At Work: Does It Help In Managing The Border Between Work And Nonwork?. *Computers in Human Behavior*, 30, 355-360.

Krishnan, S., Lim, V.K.G., & Teo, T.S.H. (2010). How Does Personality Matter? Investigating The Impact Of Big-Five Personality Traits On Cyberloafing. *International Conference on Information Systems Proceedings.*

Kuhalampi, M. (2017). Impact Of Deterrence Theory Methods On Employees' Information Security Behavior, Bachelor Thesis, University of Jyväskylä.

Lara, P. Z., Tacoronte, D. V., Ding, J. M. T. (2006). Do Current Anti-Cyberloafing Disciplinary Practices Have a Replica in Research Findings? A Study of the Effects of Coercive Strategies on Workplace Internet Misuse. *Internet Research*, 16 (4), 450-467.

Lee, J., Crossler, R. & Warkentin, M. (2013). Implications Of Monitoring Mechanisms On Bring Your Own Device (BYOD) Adoption. *International Conference on Information Systems* (ICIS 2013): Reshaping Society Through Information Systems Design. 3. 2096-2107.

Lee, Z., Lee, Y., & Kim, Y. (2004). Personal web usage in organizations. In M. Anandarajan and C. Simmers (Eds.), Personal Web Usage in the workplace: A guide to effective human resources management. Melbourne: Information Science Publishing.

Li, S. & Chung, T. (2006). Internet function and Internet addictive behavior. *Computers in Human Behavior*. 22. 1067-1071.

Liao, Q., Luo, X., Gurung, A., & Li, L. (2009). Workplace Management And Employee Misuse: Does Punishment Matter? *Journal of Computer Information Systems*, 50(2), 49-59.

Liberman, B., Seidman, G., McKenna, K. & Buffardi, L. (2011). Employee job attitudes and organizational characteristics as predictors of cyberloafing. *Computers in Human Behavior,* 27 (6): 2192–2199.

Lichtash, A.E. (2004). Inappropriate Use Of E-Mail And The Internet In The Workplace: The Arbitration Picture. *Dispute Resolution Journal*, February/April, 26-36.

Lichtenstein, S., & Swatman, P. M. C. (1997). Internet Acceptable Usage Policy For Organizations. *Information Management & Computer Security*, 5(5), 182-190.

Li, H., J., Zhang, Sarathy, R. (2010). Understanding Compliance With Internet Use Policy From The Perspective Of Rational. *Decision Support Systems*, 48, 635-645.

Lim, V., & Teo, T. (2005). Prevalence, Perceived Seriousness, Justification And Regulation Of Cyberloafing In Singapore: An Exploratory Study. *Information & Management*. 42(8), 1081-1093.

Lim, V.K.G. & Chen, D.J. (2012). Cyberloafing At The Workplace: Gain Or Drain On Work?. (2012). *Behaviour And Information Technology*. 31(4), 343-353.

Lim, V.K.G. (2002) The IT Way Of Loafing On The Job: Cyberloafing, Neutralizing And Organizational Justice. *Journal of Organizational Behavior*, (23), 675-694.

Macklem, K. (2006). You Got Too Much Mail. *Maclean's*, 119 (5), 20–22.

Mahatanankoon, P., Anandarajan, M., & Igbaria, M. (2004). Development of a Measure of Personal Web Usage in the Workplace. *CyberPsychology & Behavior*, *7*(1), 93-104.

Martin, K.E M. & Freeman, R.E. (2003). Some Problems with Employee Monitoring. *Journal of Business Ethics*, 43(4), 351-363.

Martin, L. E., Brock, M. E., Buckley, M. R., & Ketchen, D. J. (2010). Time Banditry: Examining The Purloining Of Time İn Organizations. *Human Resource Management Review*, 20(1), 26–34.

Mastrangelo P. M., Everton W., & Jolton J. A. (2006). Personal use of work computers: distraction versus destruction. *CyberPsychology and Behavior*, 9 (6), 730–74.

McKnight, D. H., Phillips, B., & Hardgrave, B. C. (2009). Which Reduces IT Turnover İntention The Most: Workplace Characteristics Or Job Characteristics? *Information & Management*, *46*(3), 167-174.

Metin, B., T.W., Taris and Peeters, C.W. (2016). Measuring procrastination at work and its associated workplace aspects. *Personality and Individual Differences*, 101, 254-263.

Mey, M., Werner, A., & Theron, A. (2014). The Influence Of Perceptions Of Organizational Trust And Fairness On Employee Citizenship. *Problems and Perspective in Management*, 12(3), 99–105.

Meyer, J. P., & Allen, N. J. (1991). A Three-Component Conceptualization Of Organizational Commitment. *Human Resource Management Review, 1(1), 61–89.*

Meyer, J. P., Stanley, D. J., Herscovitch, L., & Topolnytsky, L. (2002). Affective, Continuance, and Normative Commitment to the Organization: A Meta-analysis of Antecedents, Correlates, and Consequences. *Journal of Vocational Behavior,* 61(1), 20–52.

Moody, G. D., & Siponen, M. (2013). Using The Theory Of İnterpersonal Behavior To Explain Non-Work-Related Personal Use Of The Internet At Work. *Information & Management*, 50(6), 322-335.

Morrison, E.W. (2006). Doing The Job Well: An Investigation Of Pro-Social Rule Breaking. *Journal of Management*, 32, 5-28.

Mowday, R., Steers, R. & Porter, L. (1979). The Measure of Organisational Commitment. *Journal of Vocational Behavior,* 14(2), 224-247.

Nagin, D. & Pogarsky, G. (2001). Integratıng Celerity, Impulsivity, And Extralegal Sanction Threats Into A Model Of General Deterrence: Theory And Evidence. *Criminology*, 39(4), 865-892.

Neuman, W.L. (2014). Social Research Methods: Qualitative and Quantitative Approaches, 7th Edition, Pearson, The United States of America.

Niaei, M., Peidaei, M. & Nasiripour, A.A. (2014). The Relation between Staff Cyberloafing and Organizational Commitment in Organization of Environmental Protection. *Kuwait Chapter of Arabian Journal of Business and Management Review*, 3, 59-71.

O'Neill, T. A., Hambley, L. A., & Bercovich, A. (2014). Prediction Of Cyberslacking When Employees Are Working Away From The Office. *Computers in Human Behavior*, 34, 291–298.

Ones, D. S., Viswesvaran, C., & Dilchert, S. (2005). Personality At Work: Raising Awareness And Correcting Misconceptions. *Human Performance, 18*(4), 389-404.

Oravec, J.A. (2002), Constructive Approaches to Internet Recreation in the Workplace, *Communications of the ACM*, Vol.45, No.1, 60-63.

Ozler, D.E, & Polat, G. (2012). Cyberloafing Phenomenon In Organizations: Determinants And Impacts. *International Journal Of E-Business And E-Government Studies*, 4(2), 1-15.

Peace, A.G., Galletta, D. & Thong, J. (2003). Software Piracy in the Workplace: A Model and Empirical Test. *Journal of Management Information Systems*, 20(1), 153–177.

Piscotty, R., Martindell, E. & Karim, M. (2016). Nurses' Self-Reported Social Media And Mobile Device Use İn The Work Setting. *Online Journal Of Nursing Informatics*, 20(1).

Porter, L., Steers, R., Mowday, R., & Boulian, P. (1974). Organizational Commitment, Job Satisfaction, and Turnover Among Psychiatric Technicians. *Journal of Applied Psychology*, 59, 603-609.

Rahimnia, F., & Mazidi, A. R. (2015). Functions Of Control Mechanisms In Mitigating Workplace Loafing; Evidence From An Islamic Society. *Computers in Human Behavior, 48,* 671-681.

Rajah, R. & Lim, V.K.G. (2011), Cyberloafing, Neutralization, and Organizational Citizenship Behavior, PACIS 2011 Proceedings, Paper 152.

Ramayah, T. (2010), Personal Web Usage And Work Inefficiency, *Business Strategy Series*, 11(5), 295-301.

Robinson, S. (2008). Dysfunctional Workplace Behavior. In J. Barling & C. L. Cooper *The SAGE Handbook Of Organizational Behavior: Volume I - Micro Approaches*. London: SAGE Publications, 141-159.

Robinson, S.L. & Bennett, R.J. (1995), A Typology Of Deviant Workplace Behaviors: A Multidimensional Scaling Study. *Academy of Management Journal*, Vol. 38, No. 2, pp. 555-572.

Rowley, J. (2014). Designing And Using Research Questionnaires. *Management Research Review*, 37(3), 308-330.

Runing, S., Hunik, S., & Cahyadin, M. (2012). The Moderate Effect Of Commitment To Supervisor And Internet Expertise On Work Stressor And Employee Cyberloafing: The Study On Employee Of Local Government Of Surakarta. *Journal of Indonesian Economy & Business*, 27, 271-284.

Sackett, P. R. & DeVore, C. J. (2002). Counterproductive Behaviors At Work. In N. Anderson, D. S. Ones, H. K. Sinangil, & V. Viswesvaran (Eds.), Handbook Of Industrial, Work, And Organizational Psychology, London: Sage. Vol. 1., 145-164.

Sage, M. (2015). Cyberloafing: A Study Of Personality Factors And Organizational Commitment As Predictor Variables Of Cyberloafing And Perceived Organizational Acceptance. Master Thesis, East Carolina University.

Salgado, J. F. (2002). The Big Five Personality Dimensions and Counterproductive Behaviors. *International Journal of Selection and Assessment,* 10(1&2), 117–125.

Saraç, M. & Çiftçioğlu, A. (2014). What Do Human Resources Managers Think About The Employees' Internet Usage? *Anadolu University Social Science Journal*, 14(2), 1-12.

Saunders, M., Lewis, P. and Thornhill, A. (2012) Research Methods for Business Students. Pearson Education Ltd., Harlow.

Sheikh, A., Atashgah, M. S., & Adibzadegan, M. (2015). The Antecedents Of Cyberloafing: A Case Study İn An Iranian Copper İndustry. *Computers in Human Behavior,* 51, 172–179.

Siau, K., Nah, F. F.-H., & Teng, L. (2002). Acceptable Internet Use Policy. *Communications of the ACM*, 45(1), 75-79

Sonnentag, S., & Zijlstra, F. R. H. (2006). Job Characteristics And Off-Job As Predictors Of Need For Recovery, Well-Being, And Fatigue. *Journal of Applied Psychology*, 91, 330–350.

Spector, P. E. & Fox, S. (2002). An Emotion-Centered Model Of Voluntary Work Behavior: Some Parallels Between Counterproductive Work Behavior And Organizational Citizenship Behavior. *Human Resource Management Review*, 12(2), 269-292.

Spreitzer, G. M., & Sonenshein, S. (2004). Toward the Construct Definition of Positive Deviance. *American Behavioral Scientist*, *47*(6), 828–847.

Stanton, J. M. (2002). Company Profile of the Frequent Internet User. *Communications of the ACM*, (45),1, .55-59.

Stanton, J. M., & Weiss, E. M. (2000). Electronic Monitoring In Their Own Words: An Exploratory Study Of Employees' Experiences With New Types Of Surveillance. *Computers in Human Behavior, 16*(4), 423-440.

Straub, D.W.J., and Nance, W.D. (1990) Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, 14(1), 45-60.

Ugrin, J.C., J.M., Pearson, & M. D., Odom. (2007), Profiling Cyber-Slackers in the Workplace: Demographic, Cultural and Workplace Factors, *Journal of Internet Commerce*, 6(3), 75-89.

Urbaczewski, A., & Jessup, L. M. (2002). Does Electronic Monitoring Of Employee İnternet Usage Work? Communications *of the ACM*, 45(1), 80-83.

Vadera, A. K., Pratt, M. G., & Mishra, P. (2013). Constructive Deviance In Organizations Integrating And Moving Forward. *Journal of Management*, 1-56.

Vardi, Y., & Weitz, E. (2004). Misbehavior In Organizations: Theory, Research, And Management. Mahwah, NJ, US: Lawrence Erlbaum Associates Publishers.

Verton D (2000) Employers Ok With E-Surfing. Computerworld 34: 16.

Vitak, J., Crouse, J. & LaRose, R. (2011). Personal Internet Use At Work: Understanding Cyberslacking. *Computers in Human Behavior*, 27(5), 1751–1759.

Wagner, D. T., Barnes, C.M., Lim, V.K.G. and Ferris, D.L. (2012). Lost Sleep And Cyberloafing: Evidence From The Laboratory And A Daylight Saving Time Quasi-Experiment. *Journal of Applied Psychology*. 97 (5): 1068-1076.

Wang, J., Tian, J., & Shen, Z. (2013). The Effects And Moderators Of Cyber-Loafing Controls: An Empirical Study Of Chinese Public Servants. *Information Technology and Management*, 14(4), 269-282.

Warren, D.E. (2003). Constructive and Destructive Deviance in Organizations. *The Academy of Management Review*, 28(4), 622-632.

Weatherbee, T. (2010). Counterproductive Use Of Technology At Work: Information & Communications Technologies And Cyberdeviancy. *Human Resource Management Review*, 20 (1), 35-44.

Westman, M., & Etzion, D. (2001). The Impact Of Vacation And Job Stress On Burnout And Absenteeism. *Psychology and Health*, 16: 595–606.

White, M., Dionne, C., Koehoorn, M., Wagner, S., Schultz, I., Koehn, C., Williams-Whitt, K., Harder, H., Pasca, R., Hsu, V., McGuire, L. Schulz, W., Kube, D. & Wright, M. (2016). Physical Activity And Exercise Interventions In The Workplace Impacting Work Outcomes: A Stakeholder-Centered Best Evidence Synthesis Of Systematic Reviews. *The International Journal of Occupational and Environmental Medicine*, 7 (2): 61- 74.

Williams, K. & R., Hawkins. (1986). Perceptual Research on General Deterrence: A Critical Overview. *Law and Society Review,* 20, 545-572.

Wyatt, K. & Phillips, J.G. (2005), Personality As A Predictor Of Workplace Internet Use, Proceedings of OzCHI, Canberra, Australia, November 21-25.

Zhang, Y. (2005). Age, Gender, And Internet Attitudes Among Employees In The Business World. *Computers in Human Behavior*, 21, 1-10.

Internet Kaynakları

Salary.com (2018). Why & How Your Employees are Wasting Time at Work. Retrieved from https://www.salary.com/articles/why-how-your-employees-are-wasting-time-at-work/

Statista (2019) The Statistic Depicts The Total Number Of Smartphone Users Worldwide From 2014 to 2020. Retrieved from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

The Banks Association of Turkey (2018). Number of Banks and Branches. Retrieved from https://www.tbb.org.tr/en/home

8. APPENDICES

Appendix A – Questionnaire

As part of my Master's Thesis at Ankara Yıldırım Beyazıt University, I am conducting a survey that investigates the cyberloafing behavior in the workplaces and effectiveness of deterrence mechanisms which are implemented by organizations. I will appreciate if you could complete the following survey. All responses will be kept anonymous and no one will be identifiable in the research.

Thank you for your time.

Questions

Read each statement and select the response that best describes your behavior and awareness about deterrence mechanisms.
(1=strongly disagree; 7=strongly agree)

Policies

1. My organization has specific guidelines that describe acceptable use of internet.
2. My organization has established rules of behavior for use of computer and internet resources.
3. My organization has a formal policy that forbids employees from accessing computer systems that they are not authorized to use.
4. My organization has specific guidelines that govern what employees are allowed to do with their computers.

Monitoring

5. I believe that my organization monitors any modification or altering of computerized data by employees.
6. I believe that employee computing activities are monitored by my organization.
7. I believe that my organization monitors computing activities to ensure that employees are performing only explicitly authorized tasks.
8. I believe that my organization reviews logs of employees' computing activities on a regular basis.
9. I believe that my organization conducts periodic audits to detect the use of unauthorized software or website access on its computers.
10. I believe that my organization actively monitors the content of employees' e-mail messages.

Detection / Sanction Certainty

11. The probability that I would be caught is high.
12. The likelihood that my organization would discover that I use work computers for non-work-related activities is high.

Sanction Severity

13. The punishment would be severe by my organization.
14. The probability that I would be reprimanded by my supervisor is high.

Cyberloafing Intention

15. I intend to use the Internet at work for non-work-related purposes in the future.

16. If opportunities allow, I will use the internet for non-business purposes in the future.

Demographic Information

17. What is your gender?

Male o Female o Other o

18. What is your age?

18 - 25 o 26 - 34 o 35 - 45 o 45 or above o

19. What is your current level of education?

High school/ associate o Bachelor's o Master's o PhD o

20. How often do you use online shopping websites?

0-3 years o 4-7 years o 8-11 years o 12 or above years o

9. CURRICULUM VITAE

Personal Information

Surname, Name : Kasap, Yasemin
Nationality : Turkish
Birth of Place and Date : 18.08.1993 Germany
E-mail : yasemin.kasapp@gmail.com

Education

Degree	Institution	Graduation Date
Master	Ankara Yıldırım Beyazıt University	Ongoing
Bachelor	Gazi University	2015

Work Experiences

Year	Company	Position
2016-2017	Deutsche Bank Frankfurt/ Germany	Technology Intern
2013-2014	Goodgame Studios Hamburg/ Germany	CRM Intern

Language Skills

Turkish, English, German

Publications

Yasemin KASAP, (2017). Impacts of Electronic Word of Mouth Marketing on Consumer Purchase Behavior, *4th International Annual Meeting of Sosyoekonomi Society*, Vienna