
GAZİ ÜNİVERSİTESİ
Gazi
1926

ÖRGÜT KÜLTÜRÜNÜN BİLGİ GÜVENLİĞİ ALGISI ÜZERİNE ETKİSİ: TÜRKİYE'DEKİ DEVLET ÜNİVERSİTELERİNDE BİR ARAŞTIRMA

Ertuğrul AKTAN

DOKTORA TEZİ
YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

EYLÜL 2017

Ertuğrul AKTAN tarafından hazırlanan "Örgüt Kültürünün Bilgi Güvenliği Algısı Üzerine Etkisi: Türkiye'deki Devlet Üniversitelerinde Bir Araştırma" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ / OY ÇOKLUĞU ile Gazi Üniversitesi Yönetim Bilişim Sistemleri Anabilim Dalında DOKTORA TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. Belgin AYDINTAN

İşletme, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum/onaylamıyorum ……..

Başkan : Prof. Dr. Türksel KAYA BENSGHİR

Yönetim Bilişim Sistemleri, TODAİE

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum/onaylamıyorum ……

Üye : Prof. Dr. Alptekin SÖKMEN

İşletme, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum/onaylamıyorum ……

Üye : Doç. Dr. Aykut GÖKSEL

İşletme, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum/onaylamıyorum ……...

Üye : Doç. Dr. Mehmet ALTINÖZ

Büro Yönetimi ve Yönetici Asistanlığı, Hacettepe Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum/onaylamıyorum ……

Tez Savunma Tarihi: 20/09/2017

Jüri tarafından kabul edilen bu tezin Doktora Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

.....

Doç. Dr. Bünyamin CİYLAN

Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Ertuğrul AKTAN

20/09/2017

ÖRGÜT KÜLTÜRÜNÜN BİLGİ GÜVENLİĞİ ALGISI ÜZERİNE ETKİSİ: TÜRKİYE'DEKİ DEVLET ÜNİVERSİTELERİNDE BİR ARAŞTIRMA

(Doktora Tezi)

Ertuğrul AKTAN

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Eylül 2017

ÖZET

Bu çalışmada, Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profilinin Rekabetçi Değerler Modeli ekseninde Cameron ve Freeman Örgüt Kültürü Türleri Modeli'ne göre örgüt kültürü türleri hiyerarşi, pazar, klan ve adhokrasi temelinde tanımlanması, akademik personelin bilgi güvenliği algısının bilgi güvenliği prensiplerinden gizlilik, bütünlük, erişilebilirlik ve sorumluluk boyutlarında değerlendirilmesi ve örgüt kültürünün bilgi güvenliği prensipleri boyutlarında bilgi güvenliği algısı üzerine etkisinin incelenmesi amaçlanmıştır. Bu bağlamda örgüt kültürü ve bilgi güvenliği konularını ele alan ve bu konularda nicel yöntemlerle araştırma yapan çalışmaların alanyazın taraması gerçekleştirilmiştir. Alanyazın taramasında elde edilen örgüt kültürünü ve bilgi güvenliği yönetimini ölçümleyen anketlerden yararlanmak suretiyle çalışmaya özgün yeni bir anket hazırlanmıştır. Araştırmanın evreni olarak Türkiye'deki devlet üniversitelerinde çalışmakta olan akademik personel seçilmiştir. Bu kapsamda Türkiye'deki 106 devlet üniversitesinden anket yöntemi ile veri toplanmış olup, araştırmanın örneklemi 3023 akademik personelden oluşmuştur. Elde edilen bulgulara göre, hiyerarşi kültürünün Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profilinde baskın olduğu, hiyerarşi kültürünü sırasıyla pazar, adhokrasi ve klan kültürlerinin takip ettiği, akademik personelin bilgi güvenliği algısı profilinde ise erişilebilirlik algısı düzeyinin diğer bilgi güvenliği prensipleri algılarına göre yüksek çıktığı, erişilebilirlik algısını sırasıyla gizlilik, bütünlük ve sorumluluk algılarının takip ettiği sonucuna ulaşılmıştır. Çoklu doğrusal regresyon analizi sonuçlarına göre önem sırasıyla, bilgi güvenliği algısı üzerinde hiyerarşi, pazar, klan ve adhokrasinin; gizlilik algısı üzerinde hiyerarşi, pazar ve klanın; bütünlük algısı üzerinde hiyerarşi, pazar, klan ve adhokrasinin; erişilebilirlik algısı üzerinde hiyerarşi ve pazarın; sorumluluk algısı üzerinde ise klan, hiyerarşi, adhokrasi ve pazarın olumlu yönde etkiye sahip olduğu görülmüştür. Analiz sonuçları bir bütün olarak ele alındığında, örgüt kültürünün bilgi güvenliği algısı üzerinde olumlu etkiye sahip olduğu sonucuna ulaşılmıştır. Bu bağlamda elde edilen sonuçların, araştırmanın evrenini temsil eden devlet üniversitelerinin yanı sıra diğer örgüt türleri için de anlam ifade edeceği değerlendirilmektedir.

Bilim Kodu : 114601
Anahtar Kelimeler : Örgüt kültürü, rekabetçi değerler modeli, bilgi yönetimi, siber güvenlik, bilgi güvenliği, bilgi güvenliği algısı
Sayfa Adedi : 163
Danışman : Doç. Dr. Belgin AYDINTAN

THE EFFECT OF ORGANIZATIONAL CULTURE ON THE PERCEPTION OF INFORMATION SECURITY: A RESEARCH IN GOVERNMENT UNIVERSITIES IN TURKEY

(Ph. D. Thesis)

Ertuğrul AKTAN

GAZİ UNIVERSITY

INFORMATICS INSTITUTE

September 2017

ABSTRACT

In this study, it was aimed to define the general organizational culture profile of government universities in Turkey on the basis of hierarchy, market, clan and adhocracy culture types according to Cameron and Freeman Organizational Culture Types Model on the Competing Values Framework axis, to evaluate the academicians' perception of information security in dimensions of information security principles confidentiality, integrity, availability, accountability and to examine the effect of organizational culture on the perceptions of information security in dimensions of information security principles. In this context, a literature survey was conducted covering organizational culture and information security issues and of quantitative researches on these issues. By using the questionnaires obtained from the literature survey, which measures the organizational culture and the information security management, a new questionnaire for this study was originally prepared. As the research universe, the academicians working at government universities in Turkey were selected. In this context, data were gathered from 106 government universities in Turkey via survey method and the sample of the research was composed of 3023 academicians. According to the findings, it was concluded that, in general organizational culture profile of the government universities in Turkey, hierarchy was dominant culture, followed by market, adhocracy and clan cultures respectively and in the academicians' perception of information security profile, the perception level of availability was the highest one, followed by perception levels of confidentiality, integrity and accountability respectively. According to the results of multiple linear regression analysis, it was seen that, on the perception of information security, hierarchy, market, clan and adhocracy; on the perception of confidentiality, hierarchy, market and clan; on the perception of integrity, hierarchy, market, clan and adhocracy; on the perception of availability, hierarchy and market; and finally on the perception of accountability, clan, hierarchy, adhocracy and market had positive effects respectively. When the results of the analysis were considered as a whole, it was concluded that the organizational culture had a positive effect on the perception of information security. In this context, it is evaluated that the findings obtained will also be meaningful for other type of organizations as well as government universities representing the research universe.

Science Code : 114601
Key Words : Organizational culture, competing values approach, information management, cyber security, information security, perception of information security
Page Number : 163
Supervisor : Assoc. Prof. Dr. Belgin AYDINTAN

TEŞEKKÜR

Bu çalışmanın hazırlanması sürecinde desteğini hiçbir zaman esirgemeyen, değerli yardım ve katkılarıyla beni yönlendiren, kendisiyle çalışmaktan onur duyduğum danışman hocam Doç. Dr. Belgin AYDINTAN'a, yine tavsiye ve önerileriyle çalışmama yön veren değerli hocalarım Prof. Dr. Türksel KAYA BENSGHİR ve Prof. Dr. Alptekin SÖKMEN'e ayrı ayrı teşekkür ederim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklama**
β	Standartlaştırılmış regresyon katsayısı
λ	Özdeğer
N	Örneklem büyüklüğü
p	Anlamlılık değeri
r	Korelasyon katsayısı
R^2	Determinasyon katsayısı (Açıklanan varyans)

Kısaltmalar	**Açıklama**
ABD	Amerika Birleşik Devletleri
ANOVA	Varyans Analizi (Analysis of Variance)
AR-GE	Araştırma ve Geliştirme
BGYS	Bilgi Güvenliği Yönetim Sistemi
BS	İngiliz Standardı (British Standard)
BSI	İngiliz Standartlar Enstitüsü (British Standards Institute)
CEO	Genel Müdür (Chief Executive Officer)
CI	Koşul İndeksi (Condition Index)
CISSP	Sertifikalı Bilgi Sistemleri Güvenlik Uzmanı (Certified Information Systems Security Professional)
COBIT	Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri (Control Objectives for Information and Related Technology)
FISMA	Federal Bilgi Güvenliği Yönetimi Yasası (Federal Information Security Management Act)
HIPAA	Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (Health Insurance Portability and Accountability Act)
IBM	Uluslararası İş Makineleri (International Business Machines)
IC3	İnternet Suçları Şikâyet Merkezi (Internet Crime Complaint Center)

Kısaltmalar	Açıklama
IP	İnternet Protokolü (Internet Protocol)
ISACA	Bilgi Sistemleri Denetim ve Kontrol Birliği (Information Systems Audit and Control Association)
ISO	Uluslararası Standartlar Teşkilâtı (International Organization for Standardization)
İŞKUR	Türkiye İş Kurumu
OCAI	Örgüt Kültürü Değerlendirme Aracı (Organizational Culture Assessment Instrument)
PCI DSS	Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (Payment Card Industry Data Security Standard)
SOX	Sarbanes Oxley Yasası (Sarbanes Oxley Act)
SPSS	Sosyal Bilimler için İstatistiksel Paket (Statistical Package for the Social Sciences)
SSL	Güvenli Giriş Katmanı (Secure Sockets Layer)
TBD	Türkiye Bilişim Derneği
TDK	Türk Dil Kurumu
TS	Türk Standardı
TSE	Türk Standardları Enstitüsü
TV	Tolerans Değeri (Tolerance Value)
VIF	Varyans Büyütme Faktörü (Variance Inflation Factor)
YBS	Yönetim Bilişim Sistemleri
YÖK	Yükseköğretim Kurulu

1. GİRİŞ

Yakın zamana kadar, bilgi sistemlerinde güvenliğin sağlanması için sarf edilen çabaların çoğu teknoloji odaklıydı. Bununla birlikte son yıllarda insan faktörünün bilgi güvenliğinin tesisinde merkezî bir rol oynadığı ortaya çıkmaya başlamıştır. Bilgi güvenliği kapsamında insan, bilgi sistemleri kullanıcısı, bilginin sahibi veya bilgi sistemleri saldırganı gibi çeşitli rollerde görülebilmektedir (Safa, Solms ve Futcher, 2016). Bu nedenle modern bilgi sistemlerinde uygun güvenlik yapısının kurulması için, sadece teknoloji ile ilgili konuların değil aynı zamanda güvenlik politikalarıyla şekillenen insan davranışlarının ve örgütle ilgili konuların da üzerinde durulması gerekmektedir. İş süreçlerinin bilgi teknolojisi ile sıkı bir ilişki içinde olmasından dolayı son dönemde güvenlik konuları ön plana çıkmıştır. Bilgi güvenliğinde, örgütsel ve insan davranışlarıyla ilgili konulara vurgu yapılmaya başlanmıştır (Trcek, Trobec, Pavesic ve Tasic, 2007).

Bilgi güvenliği uygulamalarının anlaşılması için, öncelikle bilgi güvenliğinin temelini oluşturan "bilgi" ve bilgiyle yakından ilişkili olan "enformasyon" kavramlarının ele alınması gerekmektedir. Bilgi, bilişim alanındaki sözlük anlamı bakımından "kurallardan yararlanarak kişinin veriye yönelttiği anlamdır" (Türk Dil Kurumu [TDK], 2017). Diğer bir ifadeyle bilgi, işlenmiş ve anlamlı hâle getirilmiş veri olup belirli amaçlara ulaşmak veya belirli bir anlayışı geliştirmek adına verilerin, bir dönüşüm süreci sonucu yöneticiler için faydalı biçime sokulmuş şeklidir (Gökçen, 2011: 20). Enformasyon ise anlam katılmış veriler topluluğu olup bilginin kaydedilmiş ve iletilmiş formudur (Yılmaz, 2009). Bilginin enformasyondan farkını ortaya koyan tanım itibarıyla bilgi, enformasyon akışından doğmakta ve sahibinin fikir ve inançlarına bağlı olarak organize edilmektedir. Bu durum, bilginin önemli bir yönü olan insan faktörü ile bağını vurgulamaktadır (Nonaka, 1994). Diğer bir ifadeyle bilgi, karar verme ve eyleme geçmede kullanılan yüksek değere sahip enformasyondur (Davenport, Long ve Beers, 1998). Türkçe alanyazına bakıldığında bilgi ve enformasyon kavramlarının ne olduğu konusunda tam manasıyla fikir birliği oluşmadığı, bu iki terim arasında hâlâ süregelen bir kavram kargaşasının yaşandığı görülmektedir. Bu kavram kargaşasının temel nedeni, yabancı alanyazında bilginin karşılığı olarak "knowledge", enformasyonun karşılığı olarak da "information" sözcüklerinin kullanılıyor olmasıdır. Türkçe alanyazında da çoğu zaman bu iki sözcüğün birbirinin yerine kullanıldığı ve her ikisinin de Türkçeye "bilgi" olarak tercüme edildiği

görülmektedir (Yılmaz, 2009). Ayrıca Türkçede “information” sözcüğünün karşılığı olarak bazen “enformasyon” bazen de “bilgi” terimi kullanılmaktadır. Bu noktada, çoğu kimsenin “bilgi” terimini kullandığı zaman “information” ya da “knowledge” ayrımını gözetmediği görülmektedir (Tonta, 2004). Bununla birlikte bilgi ve enformasyon terimleri arasında süregelen kavram kargaşasının bir sonucu olarak da yabancı alanyazında sıkça karşılaşılan "information security" kavramının Türkçe alanyazına "enformasyon güvenliği" yerine "bilgi güvenliği" olarak aktarıldığı, bu bağlamda bilgi güvenliği kapsamında enformasyon güvenliğini konu alan çalışmaların yol gösterici olduğu ve bilgi güvenliği konusunun, genellikle elektronik ortamlarda tutulan bilginin, bir anlamda enformasyonun güvenliği merkezinde ele alındığı görülmektedir. Enformasyonun, bilginin kaydedilmiş ve iletilmiş formu olduğu, enformasyon güvenliğinin ise basılı veya elektronik bilginin güvenliğini kapsadığı ve dolayısıyla bilgi güvenliği süreçlerinin teknolojik boyutunu oluşturduğu dikkate alınarak bu tez çalışmasında, enformasyon ve bilgi kavramları, bilgi başlığı altında birleştirilmiş ve bu bağlamda yabancı alanyazında yer alan enformasyon güvenliği konulu çalışmalar bilgi güvenliği boyutunda değerlendirilmiştir.

Günümüzde bilgi ve iletişim teknolojilerinde çeşitli uygulamaların artarak kişilerin günlük yaşantılarının vazgeçilmez bir parçası hâline gelmesiyle birlikte birçok örgüt, hizmet sunumunu, zaman ve coğrafi sınırlılıkların ortadan kalktığı, anlık iletişim ve bilgi paylaşımının sağlanabildiği siber ortamda gerçekleştirmektedir (Yaşar ve Çakır, 2015). Siber ortam, dünya çapında dağıtık vaziyette bulunan bilgi ve iletişim teknolojisi cihazları ve bu cihazların bağlı olduğu ağlar tarafından desteklenen, İnternet üzerinde insanların, yazılımların ve servislerin etkileşiminden kaynaklanan karmaşık bir çevreyi ifade etmektedir (International Standard [IS], 2012: vi). Günümüzde 3 731 973 423 adet İnternet kullanıcısı bulunmaktadır (Internet World Stats, 2017). Bu istatistiki değer, siber ortamın örgütlerin sınırlarını aşan genişlikte bir çevreye sahip olduğunu ortaya koymaktadır. Bilgi güvenliği, bir varlık olan bilginin veya bilgi sistemleri kaynaklarının çeşitli tehdit ve zafiyetlerden kaynaklanabilecek olası zararlardan korunmasıyken, siber güvenlik sadece siber ortamın kendisinin korunması değil, aynı zamanda siber ortamın kaynaklarından yararlanan insanların ve topluma ait olan diğer varlıkların korunmasıdır. Bu bağlamda siber güvenlik, bilgi ve iletişim teknolojilerinin kullanımında bilgi güvenliğinin sınırlarının genişletilmiş hâli olarak görülmelidir (Solms ve Niekerk, 2013). Nitekim örgütler ve servis sağlayıcıları arasındaki iletişimin gerçekleştiği siber ortamı destekleyen cihazlar ve bu cihazların bağlı olduğu ağlar, her biri kendine özgü işlere sahip ve farklı düzenlemelere

tabi birçok örgütün sahipliğindedir (IS, 2012: vi). Dolayısıyla siber güvenliğin sağlanmasında, teknolojik, örgütsel, yasal ve insani yöntemler (öncelikli olarak ahlaki ve etik değerler) bir bütün olarak ele alınmalıdır (Malyuk ve Miloslavskaya, 2016). Kültürel açıdan değerlendirildiğinde de siber güvenlik kültürü toplumsal boyutta, bilgi güvenliği kültürü ise örgütsel bağlamda ele alınmaktadır (Reid ve Niekerk, 2014). Örgütsel bakış açısına göre kurumların önemli bilgilerini ve bilgi sistemlerini koruyabilmesi, risklerini en aza indirebilmesi ve sürekliliğin sağlanabilmesi adına bilgi güvenliği yönetim sisteminin (BGYS) kurumlarda hayata geçirilmesi gerekliliği ortaya çıkmaktadır (Vural ve Sağıroğlu, 2008). Bu tez çalışmasında da siber güvenliğin örgüt sınırları dâhilinde yer alan bilgi güvenliği boyutu, BGYS standartları ölçüsünde ve bilgi güvenliğinin gizlilik, bütünlük, erişilebilirlik ve sorumluluk prensipleri temelinde ele alınmıştır.

Örgütlerde bilgi güvenliği riskini azaltmak için, teknolojik yönlerin yanı sıra bilgi güvenliğinin insan yönü de dikkate alınmalıdır. İnsan davranışlarının modellenmesinde insan algılarının anlaşılması en zorlu kısımdır. İnsan davranışlarının anlaşılmasında algılar yol gösterici olmaktadır. Algı, bir zihniyet hâlidir ve bir değişiklik gerektirecek durum olmadıkça akılda değişmeden kalmaktadır. Değişim ise gerçek ve algılanan değerler arasındaki tutarsızlıktan kaynaklanmaktadır (Trcek ve diğerleri, 2007). Algılama kişisel bir olgudur. Buradan hareketle algılama kişinin karakterine, yaşına, cinsiyetine, eğitimine, deneyimine, yaşadığı sosyal çevreye ve kültüre göre değişiklik göstermektedir. Algılamanın olduğu sırada insan beyni, diğer duyu organlarından gelen duyularla birlikte edinilen bilgileri, beklentileri, toplumsal ve kültürel değerleri de hesaba katarak gelen duyuları seçer ve yorumlar (Çağlayan, Korkmaz ve Öktem, 2014). Bu bağlamda örgüt kültürü, kişinin düşüncesinin ve doğal yargısından ayırt edilmesi zor olan algısının üzerinde büyük bir etkiye sahiptir (Lacey, 2010).

Kültür, insanların çevreye ve değişen koşullara uyum sağlamalarında gizli ya da açık baş etme yolları veya mekanizmaları sunmaktadır. Örgüt kültürü, örgüt içinde görevlerin yerine getiriliş sırasını ve genel örgütsel yapıyı etkilemekte, doğruyla yanlışı ayırt etme noktasında yönlendirici temel kuralları oluşturmakta ve insanların yaşam biçimini şekillendirmektedir. Tanım itibarıyla örgüt kültürü, örgütün yerleşmiş, belirli bir zaman içerisinde oluşmuş, gelişmiş ve birtakım göstergelerle (sembol, norm, değerler vb.) kendini ifade eden karakteristikleridir (Erkmen, 2010: 9, 11, 15). Benzer bir ifadeyle örgüt kültürü, bireylerin örgütün işleyişini anlamalarına yardımcı olan ve böylelikle onlara örgütteki

davranış normlarını gösteren paylaşılmış değerler ve inançlar örüntüsü olarak tanımlanmaktadır (Deshpande ve Webster, 1989).

Modern örgütlerin ve örgütsel davranışların incelenmesinde en hızlı büyüyen araştırma alanı örgüt kültürüdür (Harris, 1984). Örgüt kültürü ve örgüt kültürünün diğer örgütsel değişkenler üzerine etkisini konu alan araştırmalar 1980'li yıllarda yaygınlaşmaya başlamıştır (Ahmadi, Salamzadeh, Daraei ve Akbari, 2012). Kültürün örgütsel bir değişken olduğu görüşünden hareketle yürütülen araştırmalar, yönetimsel amaçlara uyumlu bir şekilde örgüt kültürünün nasıl şekillendirileceği ve değiştirilebileceği üzerine gelişim göstermektedir. Akademisyenler için kültür, mikro ve makro analiz seviyeleri arasında kavramsal bir köprü oluşturmaktadır. Örneğin kültür kavramı ele alınarak örgütsel davranış modelleri ve stratejik yönetim çıkarları arasında bir köprü kurulabilmektedir (Smircich, 1983). Örgüt kültürü üzerine yürütülen birçok araştırmada, konu çeşitli yönleriyle ele alınmış ve örgüt kültürünün farklı nitelikleri incelenmiştir. Araştırmalarda genel olarak örgüt kültürünün örgüt başarısını etkileyen önemli bir değişken olduğu sonucuna ulaşılmıştır (Uzun ve Tamimi, 2007).

Yapılan alanyazın taramasında bir örgütün özelinde veya birden fazla farklı örgütün genelinde örgüt kültürünün nicel yöntemlerle tanımlanabilmesi için Rekabetçi Değerler Modeli'nden (Competing Values Framework) yararlanıldığı görülmektedir. Rekabetçi Değerler Modeli temelinde geliştirilen Örgüt Kültürü Türleri Modeli'ne göre örgüt kültürü, içsel devamlılık - dışsal konumlama ve organik süreçler - mekanik süreçler boyutlarında, hiyerarşi, pazar, klan ve adhokrasi olarak dört türde ortaya çıkmaktadır. Hiyerarşi kültürü, içsel devamlılık ve mekanik süreçler üzerine kurulu olup formel işleyiş süreçlerine hâkim resmî ve katı bir çalışma ortamını yansıtmaktadır. Pazar kültürü, dışsal konumlama ve mekanik süreçlere yönelik bir kültürü ifade etmektedir. Klan kültüründe ise içsel devamlılık ve organik süreçlere vurgu yapılmakta olup, dışsal konumlama ve organik süreçler altında yer alan dördüncü örgüt kültürü türü de adhokrasi olarak adlandırılmaktadır. Rekabetçi değerler terminolojisi gereğince klan kültürünün içerdiği değerler pazar kültürününkilerle, adhokrasi kültürünün içerdiği değerler de hiyerarşi kültürününkilerle zıtlık teşkil etmektedir (Cameron ve Freeman, 1991). Bu tez çalışmasında da örgüt kültürünün ölçümü için Rekabetçi Değerler Modeli temelinde geliştirilen Cameron ve Freeman Örgüt Kültürü Türleri Modeli'nden yararlanılmıştır.

Bilgi teknolojisi, örgütlerin amaç ve hedeflerine ulaşmasını destekleyen bir platform veya yöntemdir. Bununla birlikte teknoloji projeleri, hedeflere ulaşma yolunda tehditlere maruz kalmakta ve başarısızlıkla karşılaşılma potansiyelini de beraberinde getirmektedir. Dolayısıyla yönetimsel olarak bilgi güvenliğinin uygulanıyor olması, örgüt başarısı için vazgeçilmez bir husustur. Bilgi güvenliğinin temel amacı işletmeyi tehditlere karşı korumak, günlük iş uygulamalarında başarıyı elde etmek, gizlilik, bütünlük ve erişilebilirliğin korunması suretiyle de işletmelerin arzu edilen düzeyde güvenilirlik ve üretkenliğe ulaşmasında yardımcı olmaktır. Bu manada bilgi güvenliği, bilginin gizlilik, bütünlük ve erişilebilirliğini koruma platformudur (Istikoma, Fakhri, Ain ve Ibrahim, 2015). Bilgi güvenliği konusunda gizlilik, bütünlük ve erişilebilirlik olmak üzere üç temel bilgi güvenliği prensibinden söz edilmekte ise de temel bilgi güvenliği prensiplerine ek olarak sorumluluk prensibini de bilgi güvenliğine dâhil eden çalışmalar mevcuttur (Canbek ve Sağıroğlu, 2006; Chang ve Lin, 2007; Grzebiela, 2002; Hande ve Mane, 2015; Harris, 2013: 298; Kanday, 2012; Türk Standardı [TS], 2006: 4; Türkiye Bilişim Derneği [TBD], 2006: 3). Gizlilik, bilginin sadece yetkilendirilmiş kullanıcıların erişimine açılması iken bütünlük, bilginin ve bilgi işleme metotlarının doğruluğunun ve tamlığının korunmasıdır. Erişilebilirlik sayesinde kullanıcıların, bilgiye erişim yetkileri dâhilinde istenildiği zaman ulaşabilmesi sağlanmaktadır. Sorumluluk prensibi ile de kullanıcıların faaliyetlerinden dolayı sorumlu tutulması ve bilgi sistemlerine erişim faaliyetlerinin sonradan analiz edilmesi için kayıt altına alınması hedeflenmektedir.

Bilginin korunması, tipik olarak bilgi güvenliği tehditlerine ve zayıflıklarına karşı önlemlerin alınması yoluyla gerçekleşmektedir. Alınacak önlemlere örnek olarak güvenlik duvarı, yetkilendirme ve kimlik doğrulama sistemleri gibi teknolojik süreçlerin ve mekanizmaların uygulanması, şifre kontrolü ve bilgi işleme usulleri üzerine örgütsel politikaların zorunlu tutulması gibi caydırıcı prosedürlerin oluşturulması verilebilir. Bununla birlikte rutin olarak alınan önlemlere rağmen bilgi güvenliği ihlalleri ve olaylarının arttığı görülmektedir. Bu ihlaller, bilginin, kişisel kayıtların veya diğer verilerin kaybına sebep olmakta, dolayısıyla bilgi varlığının değerini olumsuz yönde etkileyen sonuçlar doğurmaktadır. Bu konuya ilişkin yürütülen birçok çalışmada, bilgi güvenliği olaylarının, öncelikli olarak teknolojik sorunlar veya prosedürel eksikliklerden ziyade paydaşların güvenlik önlemlerine karşı uyumsuz tutum sergilemelerinden kaynaklandığı ileri sürülmektedir (Tajuddin, Olphert ve Doherty, 2015). Çalışanların uyumu ile bilgi güvenliğinin sağlanması için oluşturulan global anlamda yasalara ve düzenlemelere, lokal

anlamda da örgütsel politikalara uygun davranış sergilenmesi kastedilmektedir. Bilgi sistemlerinin güvenliği bugün birçok örgütün önem verdiği bir konudur. Uyum ise elektronik ortamda tutulan bilginin güvenliğini sağlayan süreç ve kontrollere görünürlük kazandırmaktadır (Cavallari, 2011).

Bilgi güvenliği kavramı sadece teknoloji temelli olarak algılanmamalıdır. Teknolojik yatırımlarla birlikte kullanıcıların bilgi güvenliği ile ilgili davranış perspektiflerine daha fazla önem verilmelidir (Tang, Li ve Zhang, 2016). İstenilen düzeyde bilgi güvenliği seviyesine ulaşılabilmesi için, bilgi güvenliği farkındalığına ve güvenlik kontrollerine gereksinim duyulmaktadır. Bununla birlikte güvenlik önlemleriyle uyarlanan örgüt kültürünün daha iyi bir şekilde anlaşılıyor olması da önemlidir. Bu bağlamda bilgi güvenliğinin, örgüt kültürü içerisine gömülü olması ve örgüt misyonunu desteklemesi gerekmektedir (Koskosas, Kakoulidis ve Siomos, 2011).

Bilgi güvenliği ihlallerinin büyük çoğunluğu örgütsel bilgi güvenliği rehberlerine uymayan çalışanlardan kaynaklanmaktadır. Son zamanlarda yürütülen anket çalışmaları, bilgisayar ataklarının %78'inin e-posta eklerinde gelen zararlı yazılımlardan kaynaklandığını göstermektedir. Bilinmeyen kaynaklardan gelen e-posta eklerini açan çalışanlar, kendi bilgisayarlarına ve aynı ağı kullanan diğer bilgisayarlara zararlı yazılım bulaştırabilmektedir. Bu nedenle çalışanların bilgi güvenliğine karşı uygunsuz davranış sergilemelerinin nedenini öğrenmek için daha fazla özen gösterilmelidir (Chan, Woon ve Kankanhalli, 2005).

Son zamanlarda örgüt içi kaynaklı bilgi güvenliği tehditlerinin, sayıca örgüt dışı kaynaklı olanlarının önüne geçtiği görülmekte ve bu durum bilgi güvenliğinin, teknolojik çözümlerin yanı sıra insan faktörünü de kapsadığı gerçeğini ortaya çıkarmaktadır. Dolayısıyla kullanıcı farkındalığı ve davranışları, bir örgütün bilgi güvenliği performansının önemli bir parçası durumundadır (Albrechtsen ve Hovden, 2010). Bu noktada örgüt kültürü, norm ve değerler vasıtasıyla bireylere nasıl davranmaları gerektiği konusunda yol göstermekte, bireyleri örgüt amaçları çevresinde birleştirmekte, belirsizliklere karşı örgüte güvenilir bir ortam sağlamakta, örgüt içi ve örgüt dışı ilişkileri yönlendirerek düzenlemektedir (Erkmen, 2010: 21). Örgüt kültürünün temelini teşkil eden bilinçaltı varsayımlar bireylerin algılama sürecini etkilemekte, algılamada meydana gelecek değişimler de insan yaşamına ve davranışlarına yansımaktadır. Bu bağlamda örgüt

kültürü çalışanların bilgi güvenliğine ilişkin algı ve tutumlarını etkilemektedir (Knapp, Morris, Marshall ve Byrd, 2009). Bilgi güvenliği prensipleri temelinde insan davranışlarının şekillenmesi için, bilgi güvenliği algısında bilgi güvenliği bakış açısına uyumlu değişimlerin yaşanması gerekmektedir. Bilgi güvenliği algısının kültürel değerler ve varsayımlar doğrultusunda değişime uğrayacağı vurgusundan hareketle, değerler ve varsayımlar örüntüsü konumunda olan örgüt kültürünün bilgi güvenliği algısı üzerindeki etkisi, incelenmesi gereken bir konu olarak karşımıza çıkmaktadır. Örgütlerin sahip olduğu kültür profiliyle çalışanların bilgi güvenliği algısı arasındaki ilişkinin düzeyi, bilgi güvenliği uygulamalarında başarıyı elde etmede üst yönetime rehber niteliği taşımaktadır. Çalışanların bilgi güvenliği algısını etkileyen örgüt kültürü türlerini belirlemek ve örgüt kültürü türleri ile çalışanların bilgi güvenliği algısı arasındaki etki düzeyini anlamak, bilgi güvenliği uygulamalarında kullanıcı farkındalığı oluşturulmasında ve bilgi güvenliği yönetimindeki başarının sağlanmasında kilit rol oynamaktadır. Bu açıdan değerlendirildiğinde örgüt kültürü, bilgi güvenliği başarımının sağlanmasında stratejik bir öneme sahip olmaktadır.

Araştırmanın Amacı

Bu araştırmada, Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profilinin Cameron ve Freeman'ın (1991) Örgüt Kültürü Türleri Modeli'ne göre hiyerarşi, pazar, klan ve adhokrasi temelinde tanımlanması, üniversitelerde çalışan akademik personelin bilgi güvenliği algısı düzeyinin ise bilgi güvenliği prensiplerinden gizlilik, bütünlük, erişilebilirlik ve sorumluluk boyutlarında değerlendirilmesi ve örgüt kültürünün bilgi güvenliği prensipleri boyutlarında akademik personelin bilgi güvenliği algısı üzerine etkisinin incelenmesi amaçlanmaktadır. Bu amaçla araştırmada aşağıdaki sorulara yanıtlar aranmıştır.

Araştırmanın Problemleri

Araştırmada cevap aranmakta olan problemler aşağıdadır:

1. Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profilinin, hiyerarşi, pazar, klan ve adhokrasi örgüt kültürü türleri temelinde görünümü nedir?

2. Türkiye'deki devlet üniversitelerinde çalışan akademik personelin bilgi güvenliği algısı profilinin, gizlilik, bütünlük, erişilebilirlik ve sorumluluk prensipleri temelinde görünümü nedir?
3. Türkiye'deki devlet üniversitelerinde örgüt kültürünün akademik personelin bilgi güvenliği algısı üzerinde etkisi var mıdır?
4. Türkiye'deki devlet üniversitelerinde örgüt kültürünün akademik personelin gizlilik prensibi algısı üzerinde etkisi var mıdır?
5. Türkiye'deki devlet üniversitelerinde örgüt kültürünün akademik personelin bütünlük prensibi algısı üzerinde etkisi var mıdır?
6. Türkiye'deki devlet üniversitelerinde örgüt kültürünün akademik personelin erişilebilirlik prensibi algısı üzerinde etkisi var mıdır?
7. Türkiye'deki devlet üniversitelerinde örgüt kültürünün akademik personelin sorumluluk prensibi algısı üzerinde etkisi var mıdır?

Araştırmanın Önemi

Son yıllarda elektronik ağlarda ve bilgisayar tabanlı bilgi sistemlerinde yaşanan hızlı gelişmeler, sayısal verilerin birçok iş alanında işlenmesi, depolanması ve iletilmesinde yüksek düzeyde yetenekler sağlamıştır. İletişim ve bilgi teknolojilerindeki değişiklikler örgütsel bilgi varlıklarının korunmasıyla ilgili birtakım kaygıları da beraberinde getirmiştir. Bir örgütte farklı paydaşlar arasında bilgi sistemleri için alınacak güvenlik önlemlerine ilişkin fikir birliğine ulaşmak, ortaya çıkabilecek birçok teknik problemi çözmekten daha zor olmaktadır. Bu manada teknik konularda görüş birliğinin oluşturulması için, bilgi güvenliğinin doğasının iyi anlaşılıyor olması gerekmektedir (Dhillon ve Backhouse, 2000).

Yeni teknolojilerin ortaya çıkması modern toplumları sürekli olarak değişime maruz bırakmaktadır. Bunlardan en etkili olanı bilgi teknolojileridir. Bilgi teknolojileri iş sahipleri için güçlü bir araç konumundadır ve hızlı bir şekilde iş yapış şekillerini, aktiviteleri ve etkileşimleri değiştirmektedir. Dolayısıyla bilgi ve bilgi teknolojileri örgütlerde kritik bir faktör olarak düşünülmektedir (Ebrahimi ve Naini, 2012). Örgütler, etkin operasyonel kontrollerin ve stratejik yönetimin, yüksek kalitede bilginin erişilebilirliğine ve kullanımına bağlı hâle geldiği, rekabet düzeyinin giderek arttığı bir ortamda hayatta kalmak ve daha da gelişmek istiyorsa bilgi sistemleri ve teknolojilerinden

yararlanmak zorundadır (Fulford ve Doherty, 2003). Bilgi teknolojisi modern yaşamın ayrılmaz bir parçası hâline gelmiştir. Bugün, bilgi kullanımı hem iş hem de özel hayatın her alanına nüfuz etmektedir. Dolayısıyla bilgi varlıklarının korunması konusunun ciddiyetle ele alınması gerekmektedir. Bilgi varlıklarının korunması için ihtiyaç duyulan süreçlerin birçoğu büyük ölçüde insanların işbirliği içinde sergiledikleri davranışlara bağlıdır. Çalışanlar kasıtlı ya da ihmalkârlıkla, çoğunlukla da bilgi eksikliğinden dolayı bilgi güvenliği için en büyük tehdit kaynağı durumuna gelmektedir. Bilgi güvenliği ile uyumlu örgütsel bir kültürün kurulmasının, bilgi güvenliği ile ilgili insan faktörünü yönetmenin anahtarı olduğu yaygın bir şekilde kabul edilmektedir. Bu nedenle bir örgütün bilgi güvenliği stratejisinde, "insan faktörü" kapsamlı bir şekilde ele alınmalıdır (Niekerk ve Solms, 2010). Yetkili veya yetkisiz olarak bilgi güvenliği ile alakalı faaliyetleri yürüten örgüt çalışanlarının karmaşık, dinamik ve belirsiz özelliklerini anlamak çok önemli ve zor bir görev olarak kabul edilmelidir (Alfawaz, Nelson ve Mohannak, 2010).

Bilgisayar sistemlerine ve ağlarına yönelik gerçekleştirilecek saldırılar neticesinde örgütlerin para, zaman, prestij ve bilgi kaybı ile karşı karşıya kalmaları kaçınılmazdır. Dolayısıyla tüm iş süreçleri zarfında bilgisayar sistemlerine olan bağımlılık, elektronik ortamda tutulan bilginin güvenliğinin sağlanması ihtiyacını gündeme getirmektedir. Şifreleme sistemleri, anti virüs yazılımları, kimlik doğrulama mekanizmaları ve güvenlik duvarları gibi teknik çözümler, bilgiye karşı oluşabilecek tehditlerin azaltılmasında tek başına yetersiz kalmaktadır. Bilgisayar sistemlerinin güvenliğinin sağlanmasında insan faktörü önemli bir rol oynamaktadır (Metalidou ve diğerleri, 2014). Kullanıcı adını ve parolaları çalışma arkadaşları ile paylaşmak, masa üzerindeki veya monitöre yapıştırılan not kâğıtlarında yazılı hâlde bırakmak, bilinmeyen e-postaları ve e-posta eklerini açmak, İnternet'ten yazılım indirmek ve bilgisayar sistemlerini oturum açık vaziyetteyken terk etmek bilgi güvenliği alanında yaşanan insan hatalarının başlıca örneklerindendir. Gerçekten de kullanıcılar, kasıtlı ya da istemeden de olsa bilgi varlıkları için büyük bir tehdit oluşturmaktadırlar. Pek çok durumda, örgütsel bilgi güvenliği politikalarına karşı gösterilen duyarsızlık, ihmal, farkındalık eksikliği, zarar verici yaklaşımlar ve direnç, bilgi güvenliği olaylarının temelinde yer almaktadır. Öte yandan çalışanlar, bilgi güvenliği ihlallerine karşı çabalarını, yeteneklerini ve bilgilerini bir araya getirebilirler. Bu bağlamda bilgi güvenliği kapsamında çalışanlar tarafından sergilenecek tecrübe paylaşımı, işbirliği, bilinçli davranışlar, bilgi güvenliği politika ve prosedürlerine uyum, örgütlerin bilgi güvenliği riskini azaltacak insan ile alakalı etkili yaklaşımlar olarak ele alınmaktadır (Safa

ve diğerleri, 2016). Günümüzde, bilgi güvenliği sorunu yalnızca bilgi güvenliği uzmanları için değil aynı zamanda şirket yöneticileri ve üniversite personeli de dâhil olmak üzere geniş bir topluluk için önemli bir öncelik hâline gelmiştir (Stanciu ve Tinca, 2016).

Güvenlik gerekliliklerinin artık tek başına teknolojik araçlar tarafından karşılanamayacağı yaygın bir şekilde kabul görmüş durumdadır. Bilgi güvenliğinde başarı ihtimalinin, insanlar tarafından önemli ölçüde etkileneceği düşünülmektedir (Furnell, Jusoh ve Katsabas, 2006). İnsanları hedef alan bilgisayar korsanlığı, genellikle insanların kandırılmasına dayanan, teknik olmayan bir saldırı türüdür. Bu tür saldırıların etkisi, bilgi teknolojileri alanında sürekli kaygı uyandırmaktadır. Bilgi güvenliğinde en zayıf halka olarak görülen, daha önceden şüphe uyandırmamış kişiler üzerinden ağlara sızmak için yaygın olarak kullanılan bu saldırı türü nedeniyle bilgi teknolojileri zarar görmektedir. Davranışsal değişikliği meydana getiren kullanıcı güvenlik farkındalığı, çalışanların güvenlik zafiyeti oluşturmasını azaltmakta, çalışanların güvenlik zafiyetinden yararlanan tehditlere karşı koruma sağlamakta ve bilgi varlıklarıyla ilgili risklerin azaltılması adına genel olarak olumlu bir etkiye sahip olmaktadır (Okenyi ve Owens, 2007). Dolayısıyla bilgi güvenliğinin istenilen düzeyde sağlanabilmesi için, teknolojik çözümlere yatırım yapılması kadar çalışanların bilgi güvenliği hususundaki farkındalıkları, örgütsel bağlılıkları ve herkesçe bilgi güvenliği amaçlarının anlaşılıyor olması gittikçe önemli bir hâl almaktadır. Bilgi güvenliği farkındalığı, kullanıcıların kurallara tam manasıyla uydukları, olası bilgi güvenliği ihlal olaylarının farkına vardıkları, sorumluluklarının önemini anladıkları ve bu çerçevede davranış sergiledikleri bilinç hâli olarak adlandırılmaktadır (Ahlan, Lubis ve Lubis, 2015). Bilgi güvenliğinin etkin bir şekilde tesis edilmesi ve geliştirilmesi için, çalışan farkındalığının oluşturulması gereklidir (Alhogail ve Mirza, 2014a). Bilgi güvenliği anlayış, davranış ve tutumlarını yönlendiren farkındalık düzeyi üzerinde kişilik gibi bireysel faktörlerin, kültür gibi örgütsel faktörlerin ve eğitim gibi dışsal müdahale faktörlerinin etkisi olmaktadır (Parsons ve diğerleri, 2017).

Örgütlerin, çalışanların doğru güvenlik yaklaşımlarını desteklediği kültür yapısını oluşturması, sürdürmesi ayrıca güvenliği örgüt yapısı, iş süreçleri ve servisleri içerisinde yer alan her bir bireyle bütünlük içinde örgüt kültürüne aşılaması gerekmektedir. Bilgi güvenliği ile ilgili çalışanların günlük olarak karşılaştıkları sorunlar anlaşılmalı ve çözülmelidir. Bu manada bilgi güvenliği farkındalığının önemi hakkında çalışanların eğitilmesi örgütün bir önceliği olmalıdır (Metalidou ve diğerleri, 2014).

Örgütsel verinin korunması alanında veritabanı ihlalleri, şifrelerin çalınması ve kimlik hırsızlığı gibi önemli sorunların yaşanmaya devam ediyor olması ele alınması gereken en önemli konular arasında yer almaktadır. Bu noktada, yöneticilerin genellikle bilgi güvenliği yönetimini, kurumsal yönetimden ayrı tutarak bilgi işlem birimlerinin yetkisi altında tanımlıyor olmaları ve bu bağlamda güvenlik konusunun bir "eklenti" olarak ele alınıyor olması büyük bir sorundur. Halbuki güvenlik bir öncelik hâline getirilerek örgüt kültürünün ayrılmaz bir unsuru olmalıdır. Bu çerçevede oluşturulacak güvenlik entegrasyonu üstten aşağıya doğru yapılandırılmalı ve örgütteki herkesi kültürel formda kapsamalıdır (Corriss, 2010).

Örgüt kültürü olgusunu önemli kılan ve birçok çalışmaya konu olmasını sağlayan birincil neden, örgüt kültürünün zaman içinde öğrenme ve algılama yoluyla kalıplaşmış ve bir anlamda kurumsallaşmış gelenekleri sonraki nesillere ve dönemlere aktarma işlevini üstlenmesidir. Örgüt kültürü oldukça rasyonel bir yapıda görünebilmektedir. Fakat esas itibarıyla örgüt kültürü, algısal ve durumsal bir yapı üzerine kuruludur. Algılama, davranış sergileme, bağlılık ve uyum yaratma gibi kavramlar örgüt kültürünün temelini teşkil eden değerleri anlamlı bir bütüne dönüştürmektedir. Algılama bireyin çevresindeki olay, nesne ve tepkileri fark etmesi ile kültürel çevresi içinde gözlemlerine ve ilişkilerine anlam vermeye başlaması sürecidir (Öztürk, 2015). Örgütün bilgi güvenliği iklimi hakkında çalışanlarda oluşan algı ve çalışanların bilgi güvenliği hususundaki öz yeterlilikleri, çalışanların bilgi güvenliği bakış açılı davranışlarını pozitif yönde etkilemektedir. Bu durum, bilgi güvenliği prensipleriyle uyumlu davranış sergilemenin örgütsel ve kişisel faktörlere bağlı olduğunu göstermektedir (Chan ve diğerleri, 2005).

Bilgi güvenliği yönetiminin etkin bir şekilde tesis edilmesinde, bilgi güvenliği politikalarının geliştirilmesi ve uygulanmasında yürütülen üst yönetim faaliyetleri, farkındalık ve uyum eğitimleri, kurumsal bilgi mimarisi, bilgi teknolojileri altyapısı, bilgi teknolojileri ile uyumlu iş süreçleri ve insan kaynakları yönetimi önemli derecede etkiye sahiptir (Soomro, Shah ve Ahmed, 2016). Nitekim yürütülen birçok çalışmada bilgi güvenliği sosyo-teknik bir konu olarak ele alınmaktadır. Teknik sistemlerin insanlar tarafından kullanıldığı düşünülecek olursa BGYS'yi etkileyen teknik olmayan faktörlere, özellikle de insan faktörüne daha fazla dikkat edilmesi gerekliliği doğmaktadır. Bireylerin örgütteki davranışlarının örgüt kültürü formunda ortaya çıkmasından dolayı etkin

faktörlerden biri olan örgüt kültürünün bilgi güvenliği yönetimini nasıl etkilediğini incelemek önemli bir konu olmaktadır (Ebrahimi ve Naini, 2012).

Bilgi güvenliği yönetiminde başarının elde edilmesi, teknolojik çözümlerden ziyade öncelikli olarak örgütteki bireylerin sergiledikleri davranışlara ve bireylerde istenilen düzeyde bilgi güvenliği algısının oluşturulmasına bağlıdır. Bireylerin davranışlarını ve algılama sürecini etkileyen ana unsur ise örgüt kültürünün temelini teşkil eden bilinçaltı varsayımlardır. Dolayısıyla örgüt kültürünün bilgi güvenliği algısı üzerindeki etkisinin anlaşılması, çalışanların bilgi güvenliği ile uyumlu davranış sergilemeye sevk edilmesinde yol gösterici olacaktır. Bu bağlamda bu tez çalışmasında elde edilen sonuçların, Türkiye'de devlet üniversitelerindeki akademik personelin davranışlarının bilgi güvenliğine uyumlu hâle getirilmesinde örgüt kültürünün etkisinin anlaşılması açısından faydalı olacağı değerlendirilmektedir.

Varsayımlar

Araştırma ölçeğinin hazırlanmasında yararlanılan örgüt kültürü ve bilgi güvenliği yönetimini ölçümleyen veri toplama araçlarının, kullanıldığı geçmiş çalışmalarda geçerliği ve güvenirliğinin sağlanmış olmasından dolayı ölçülmek istenen özellikleri doğru olarak ölçtüğü varsayılmıştır.

Ölçeği cevaplayan üniversite akademik personelinin tüm soruları içtenlikle ve doğru olarak cevapladığı varsayılmıştır.

2. KAVRAMSAL ÇERÇEVE

Bu bölümde, tez çalışmasının altyapısını oluşturan kavramsal çerçeve sekiz alt bölümde sunulmuştur. Birinci alt bölümde kültür kavramı ve seviyeleri, ikinci alt bölümde örgüt kültürü kavramı, örgüt kültürünün unsurları, katmanları, fonksiyonları ve ölçümü ele alınmıştır. Üçüncü alt bölümde örgüt kültürünü ölçümleyen Rekabetçi Değerler Modeli'ne, dördüncü alt bölümde de bu modelin referans alınmasıyla oluşturulmuş olan Cameron ve Freeman Örgüt Kültürü Türleri Modeli'ne yer verilmiştir. Cameron ve Freeman Örgüt Kültürü Türleri Modeli kapsamında örgüt kültürü türleri hiyerarşi, pazar, klan ve adhokrasi anlatılmıştır. Beşinci alt bölümde Rekabetçi Değerler Modeli boyutunda bu kültür türleri arasındaki yaşam döngüsüne değinilmiştir. Bilgi güvenliği kavramı altıncı alt bölümde ele alınmış ve bilgi güvenliği boyutları kapsamında gizlilik, bütünlük, erişilebilirlik ve sorumluluk kavramlarının anlatımına da yedinci alt bölümde yer verilmiştir. Sekizinci ve son alt bölümde ise örgüt kültürü ve bilgi güvenliği ilişkisi ele alınmıştır.

2.1. Kültür

"Kültür" (culture) kelimesi genellikle anlam bakımından, "kimlik" (identity) kelimesiyle eşleştirilmektedir. Profesyonel hayatta kullanılan birçok kelime gibi yabancı alanyazında yer alan "kültür" ve "kimlik" kelimlerinin kökeni Fransızca ve Latinceye dayanmaktadır. Kimlik, Latinceden gelen benzersiz, tekrar eden anlamlarını taşımaktadır. "Kültür" ve kültürle ilgili türetilmiş "kültürlü" (cultured), "yetiştirmek" (cultivate), "yetiştirme" (cultivation) gibi tüm terimler de Fransızca "culture" ve Latince "cultura" kelimelerinden türetilmiştir. Bu sözler temelde, emek ve bakım ile arazinin başarılı bir şekilde işlenmesi, ekin üretiminin geliştirilmesi anlamına gelmekteydi. Her ne kadar günümüzde bu sözcüklerin anlamı değişmiş olarak gözükse de sembolik olarak verimli topraklar, çoğumuzun bugün kullanmakta olduğu kültür kelimesinin anlamının gizli veya bilinç dışı olarak temelinde yatmaktadır. Arazi ile olan anlam ilişkisi şimdiye kadar devam etmekte ise de 13. ve 14. yüzyıllarda kültürün anlamı, insanların öncelikle eğitim ve öğretim yoluyla geliştirilmesini içerecek şekilde genişletilmiştir (O'Hagan, 1999).

Kültür sözcüğü örgütsel çalışmalarda yaygın ve sıklıkla kullanılsa da kavramsal olarak kültürü tanımlamak çok da kolay değildir. Kültür, antropolojiden alınan bir kavram

olmakla birlikte anlamı konusunda tam bir fikir birliği bulunmamaktadır. Dolayısıyla örgütsel çalışmalardaki uygulamalarda çeşitli şekillerde yer alması da sürpriz olmamalıdır. Kültür, bilinçaltı ile ilgili psikolojik süreçlerin ifadesi olarak da görülebilir. Diğer bir ifadeyle kültür, bilinçaltının şeklini ortaya çıkarmaktadır (Smircich, 1983). Bazı antropologlar kültürü, insanı insan olmayanlardan ayıran bir kavram olarak algılarlar. Bazıları ise kültürü iletilebilen bir bilgi olarak düşünmektedirler. Bununla birlikte kültürden, insanlığın toplumsal yaşamı boyunca üretilen tarihsel başarıların bir toplamı olarak bahseden bazı antropologlar da bulunmaktadır (Wadia, 1965).

Kültür, bir grup tarafından paylaşılan, kabul edilmiş, çevrenin anlaşılmasını sağlayan ve çevreye karşı nasıl reaksiyon alınacağını gösteren kapalı varsayımlar kümesidir (Schein, 1996). Diğer bir ifadeyle kültür, bir grubun belirli bir süre boyunca öğrendiğidir. Bu öğretiler, grubun dış çevresinde hayatta kalma mücadelesiyle ilgili ve iç çevresinde entegrasyonla alakalı ortaya çıkan sorunları çözmesini sağlamaktadır. Bu tür öğrenme, aynı zamanda davranışsal, bilişsel ve duygusal bir süreçtir. İşlevselci antropolojik bakış açısına göre en derin kültür seviyesi, bir grubun paylaştığı algıları, dili ve düşünce süreçlerini yansıtan bilişselliktir. Bilişsellik seviyesi, duyguların, tutumların, benimsenen değerlerin ve davranışların nedensel bir belirleyicisidir (Schein, 1990).

Sosyal bilimlerin iki temel kavramı toplum ve kültürdür. Geleneksel olarak kültür terimi, insanı ve toplumu konu alan sosyal bilimlerle ilişkili olup sadece insan biyolojisi ile açıklanamamaktadır. Tanım olarak kültür, toplum üyeleri tarafından "paylaşılan" fikir, davranış, gelenek vb. şeylerdir (Johnson, 1983). Kültür, salt davranıştan ayrı bir kavramdır. Nasıl ki elektrik veya yerçekimini görmüyoruz fakat belirtilerini gözlemleyebiliyoruz; aynı şekilde, kültür de görülememekte fakat belirtileri gözlemlenebilmektedir (Wadia, 1965).

Geniş ya da dar manada olsun tek bir tanımlamayla kültür, sosyal tartışmalar için uygun değildir. Bu nedenle kültür kavramının değerlendirilmesinde, uygulamaya yönelik daha kapsamlı, kavramsal kategoriler içeren yaklaşımlardan yararlanmak gerekmektedir. Uygulamaya yönelik bir kültürel yaklaşımla aidiyet ve katılımın ortak yönlerinin göz önüne alınması gerekliliği kastedilmektedir. Bu manada en yaygın kültür anlayışı, bir sosyal sistem içinde yüksek seviyede içsel birlik anlayışıdır. Daha önceleri, bu kavram, etnisite veya ırk bağlamlarıyla sınırlı tutulmaktaydı (örneğin İtalyanların şık giyim tarzı). Günümüzde ise ortak özellikler genellikle çeşitli boyutlarda oldukça farklı sosyal

sistemlere dayanabilmektedir (örneğin Hıristiyan-Batı Avrupasının liberal değerleri, müşteri odaklı kurumsal kültür, kadınlar arasında ortak liderlik kültürü) (Rathje, 2009).

"Kültür" terimi, "ırk" temelli veya ten rengi gibi biyolojik özelliklere dayanmamaktadır. Çünkü kültür, öğrenilen davranış kalıplarını ifade etmekte olup "etnisite" veya "ırk" terimiyle karıştırılmamalıdır (Thomas ve Dyall, 1999). Kültür, etnisiteden ziyade bir topluluğun yeri ve zamanı nasıl kullandığı, yaşam biçimi, insanların nasıl örgütlendiği ve etkileşim içinde bulunduğu ile ilgilidir (Skemp, Dreher ve Lehmann, 2016). Bir bakıma kültür topluluktur. Bu, insanların birbirleriyle nasıl ilişki kurduklarının bir sonucudur. Aileler, köyler, okullar ve kulüpler gibi işletmeler de zaman içinde varlıklarını sürdüren ya da yıkıma uğratan sosyal etkileşim kalıplarına dayanmaktadır. Bu etkileşim kalıpları, ortak menfaatler ve karşılıklı yükümlülükler üzerine kurulmuş olup işbirliği ve arkadaşlıklar üzerine gelişmektedir (Goffee ve Jones, 1996).

Kültür kavramı günümüzde birçok farklı anlamlara gelmekle beraber genel olarak bir toplumun yaşama biçimini işaret etmek için kullanılmaktadır. Sözcük olarak kültür kavramı incelendiğinde de tarihsel süreç içinde belirli bir yaşam biçimini işaret ettiği görülmektedir. Kültür kavramını doğrudan konu alan disiplinlerin benimsedikleri tanım, sosyal antropoloji temeline dayanmaktadır (Doğan, 2012: 9, 13). Diğer bir ifadeyle kültür, bir insan grubunun üyelerini başka bir insan grubunun üyelerinden ayıran insan zihninin ortak programlamasıdır. Kültür bu anlamda, topluca tutulan bir değerler sistemi olup bir insan grubunun çevresine vermekte olduğu tepkiyi etkileyen ortak özelliklerin interaktif toplamı olarak da tanımlanabilir (Hofstede, 1981). Bununla birlikte kültür için, insanların birlikte yaşamalarından ortaya çıkan değerler tanımı yapılabilir. Bireyler, öğrenme sürecinin bir sonucu olarak karar verme esnasında kültürlerinden yararlanırlar (Balogh, Gaal ve Szabo, 2011). Bu bağlamda kültür, bireylerin ve tüm toplumun davranışlarını ve yaşam biçimlerini yöneten çok baskın bir faktördür. Bireysel yaşamda kültür, karar verme üzerinde güçlü bir etkiye sahiptir. Bireylerin tutum ve davranışlarının kültürlere göre gelişim sergilemesinde ve sadeleştirilmesinde kültürel olgular araç rolü üstlenir. Kültürün kural ve gelenekleri, insan hayatında önemli bir etkiye sahiptir (Gull ve Azam, 2012).

Kültür, karmaşık ve belirsiz ortamlarda başparmak kuralları doğrultusunda buluşsal (heuristics) olarak uygulanan karar verme aracıdır. Diğer bir ifadeyle kültür, tipik olarak değerler, inançlar veya sosyal normlar olarak ortaya konan bu buluşsal karar verme

yöntemlerini ifade etmektedir. Bu buluşsal yöntemler, tarihsel süreç içerisinde bireyler ve toplumlar arasında potansiyel olarak değişmekte ve şekillenmektedir. Tarihsel olaylar, farklı kültürel özelliklerin toplumdaki yaygınlığını etkileyebilmekte ve kültür üzerinde kalıcı etkilere neden olabilmektedir. Şayet kültürel özellikler ebeveynlerden çocuklara dikey olarak aktarılırsa kültürel etkilerin zamanla devam etmesi söz konusu olacaktır (Nunn, 2012).

Kültür, öncelikle davranışlara atıfta bulunmaktadır, ancak nedensel manada değer sistemlerine dayalıdır. Kültür toplu olarak paylaşılmaktadır. Dolayısıyla sadece bireysel tercihlerin ve önceliklerin bir yansıması değildir. Kültür, dili, gelenek ve görenekleri, kılık kıyafet tarzını, yemek yeme alışkanlıklarını, dinî uygulamaları, paylaşılan anlamları ve örgütleri içermekte, bu çerçevede kolektif değerlerin ve inançların ifadesi olan davranış kalıplarına yansımaktadır. Kültür sabit değildir; çevresel koşullara (örneğin azalan su kaynakları, artan hava kirliliği seviyeleri) ayak uydurmakta, gelişim göstermekte ve sonuçta kültürel olarak öngörülen bazı uygulamalar zamanla değişebilmektedir (Wallendorf ve Reilly, 1983).

2.1.1. Kültür seviyeleri

Kültür kelimesi, genel olarak toplumlar, etnik ya da bölgesel gruplar için kullanılmakla birlikte örgüt, meslek grubu ve aile gibi diğer insan toplulukları için de ayrı bir değer taşımaktadır (Hofstede, 1981). Genel kabul görmüş bir tanım olarak kültür, "öğrenilen ve paylaşılan değerler, inançlar, davranış özellikleri ve anlam taşıyan semboller toplamı" olarak ifade edilebilir. Bu ne kadar genişse kültür o derece genel veya üst kültür olma özelliğini taşımaktadır. Bu açıdan bakıldığında, bir genel toplumsal kültür içinde, değişik değer, inanç ve sembollerin paylaşıldığı alt kültürler oluşabilmektedir (Koçel, 2014: 162). Birçok ortak kültür özelliğini veya ögesini paylaşan bir toplum, grup veya ulusta, bir grubu diğerlerinden ayıran bazı karakteristik özellikler olabilir. Bu ayırt edici özellikler, yaş grubu, sınıf grubu, cinsiyet grubu veya ırk grubu gibi farklılaşmalar temelinde oluşan alt kültürler tarafından paylaşılmaktadır (Wadia, 1965).

Bireysel ve örgütsel davranışları etkileyen farklı kültür türleri veya seviyeleri mevcuttur. En üst kültür seviyesinde örneğin global düzeyde bir yarımküre kültürü ya da dinî kültür olabilir. Diğer kültür seviyelerinde ise ulusal kültürler, toplumsal cinsiyet kültürleri

(erkeklerin ve kadınların farklı bakış açılı değerlendirmelerini temel alan kültürler gibi), etnik grupların kültürleri, mesleki kültürler (hükümet kültürü gibi) veya sosyo-ekonomik grup kültürleri (zengin ve fakir ayrımını temel alan kültür türleri gibi) yer alabilir (Garcia, Sanchez, Cuevas, Hernandez ve Vargas, 2012).

Davranışları etkileyen farklı kültür türlerindeki en geniş kültür seviyesi dinî, kıtasal, ülkesel vb. farklılıklar temelinde oluşmaktayken bir alt genel kültürel seviye ise cinsiyet, meslek, sektör, kırsal ve kentsel yaşam alanı vb. farklılıklar temelinde oluşan alt grupların kültürel özelliklerini yansıtmaktadır. En alt dar kapsamlı kültürel seviye ise örgütün kişiliğini ortaya çıkaran örgütün değerlerini, baskın liderlik özelliklerini, dilini, sembollerini, prosedürlerini, rutin iş süreçlerini ve başarıyı nasıl tanımladığını ortaya koymaktadır. Örgüt içindeki fonksiyonel bölümler, üretim grupları, hiyerarşik seviyeler veya takımlar da kendilerine özel alt kültürleri oluşturmaktadır (Cameron ve Quinn, 2006:17). Diğer bir ifadeyle örgüt kültürü, örgütün içinde bulunduğu çevrenin bir alt kültürü olup, kendisi de birim ve bölümler şeklinde ortaya çıkan alt kültürlerden oluşmaktadır. Burada önemli olan husus, örgüt kültürünün içinde faaliyet gösterdiği çevrenin kültüründen etkilenmekte olan, ondan farklı fakat onunla uyuşmaya çalışan ve yine de ona ters düşmeyen bir olgu olduğudur (Erkmen, 2010: 23, 27). Örgütler büyüdükçe ve geliştikçe iş gücünü bölümleyip her biri kendine has çevreye sahip işlevsel, coğrafi ve diğer farklılıklar üzerine kurulu birimler oluşturmaktadır. Bunun doğal bir sonucu olarak da örgütler kendi alt kültürlerini oluşturmaya başlar. Bir anlamda örgütün yaşı ve büyüklüğü farklılaşmayı doğurmaktadır. Bir grupta birçok alt kültürün varlığı söz konusu olabilmekle birlikte grubun toplam kültürü, alt gruplarının etkileşiminin bir sonucu olarak ortaya çıkmaktadır (Schein, 1990).

2.2. Örgüt Kültürü

Örgüt kültürü teorisi, örgüt psikolojisi, toplum psikolojisi ve sosyal antropolojinin bileşiminden doğmaktadır (Scott, Mannion, Davies ve Marshall, 2003). Örgüt kültürü, örgütün kişiliğini ve kimliğini tanımlamaktadır (Erkmen, 2010: 9). Kültür olmadan, bir örgüt değerlerinden ve amacından yoksun kalır, yönünü kaybeder (Goffee ve Jones, 1996).

Örgüt kültürü, herhangi bir örgütün kendine özel karmaşık yönünü yansıtmaktadır. Örgüt yönetimi ve çalışanlar açıkça örgüt kültürünün farkında olmasalar dahi örgüt kültürünün

varlığı her zaman söz konusudur (Furnell ve Thomson, 2009). Sosyal bilimcilere göre örgüt kültürü kavramı, çalışanların davranışlarını düzenleyen resmî olmayan normlar ve değerler seti olarak tanımlanmaktadır. Bu manada örgüt kültürü, insanların işyerinde nasıl davranması gerektiğini, hangi görev ve hedeflerin önemli olduğunu gösteren, örgüt üyelerinin birçoğu tarafından paylaşılan birbiriyle ilişkili bir dizi inançlar bütünüdür (Baker, 1980). Diğer bir ifadeyle örgüt kültürü, bireysel seviyede paylaşılan örgüte özgü şemaların desenli bir sistemidir. Kültür ve şema dinamikleri, kültürel olarak şekillenen duygu dinamiklerinin grup ve birey seviyesindeki ilişkilerinin aydınlatılması işlevini üstlenmektedir (Harris, 1989).

Kültür, örgüt kültürünün tanımlanmasında temeldeki kavram olup, örgüt kültürünü ya bilişsel zeminde idrak edilme ve semboller vasıtasıyla ya da bilinç dışı cereyan eden süreçlerin bir ifadesi olarak sunmaktadır. Diğer bir ifadeyle örgüt kültürü, kültürün bilişsel, sembolik ve psikodinamik perspektiflerinde tanımlanmaktadır (Harris, 1998). Örgüt kültürü, örgütsel normların ve değerlerin algılanışıdır ve bu nedenle bireyde değil örgüt içinde bulunur. Dolayısıyla farklı geçmişleri olan veya örgütte farklı seviyelerde bulunan bireyler, örgütü benzer şekilde tarif etme eğiliminde olurlar (Koskosas ve diğerleri, 2011). Bu manada örgüt kültürü, örgüt üyeleri arasında paylaşılmış değerlerden, davranış kalıplarından, sembollerden ve sembolik eylemlerden meydana gelmektedir (Aydıntan, 2009: 130). Sosyal grupların üyeleri birbirleri arasında değer paylaşımında bulunarak, sosyal beklentilere veya normlara temel oluşturabilirler. Daha yaygın şekilde değer paylaşımı yapıldığında ise örgüt kültürü veya değer sistemi ortaya çıkmaktadır (O'Reilly, Chatman ve Caldwell, 1991).

Örgüt kültürünün sürdürülmesi, bireylerin örgütteki rollerini kabullenmeleri için gerekli olan değerleri, beklenen davranışları ve sosyal bilgileri öğrenmeleriyle bir anlamda sosyalleşmeyle sağlanmaktadır (Lunenburg, 2011). Kültür, gruba giren yeni üyelerin sosyalleşmesi yoluyla kendi kendini sürekli kılar ve çoğaltır. Sosyalleşme süreci, bir örgüte doğru varsayımlara, inançlara ve değerlere sahip yeni bireylerin katılmasıyla başlar (Schein, 1990). Örgüte yeni katılan bir üyenin örgütün değer sistemini, normlarını ve toplumun gerekli davranış kalıplarını öğrenme süreci olan sosyalleşme, genellikle örgüt içinde formel otorite sisteminin normlarına aykırı olarak gayriresmî şekilde gerçekleşmektedir. Dolayısıyla sosyalleşme sürecinin büyük bir kısmının, örgütün kültürü ile ilgili olduğu söylenebilir (Mintzberg, 1979: 97). Örgüt kültürü, örgütlerde sosyalleşme

süreçleri yoluyla öğrenilen, bireylerin davranışlarını yönlendiren özellikler içermektedir. Örgütler arası makro kültür özellikleri de farklı örgüt yapılarının üyeleri tarafından paylaşılmaktadır. Paylaşılan bu kültürel özellikler, örgütler arası işbirliği ve rekabeti etkilemektedir. Bir makro kültür içinde yer alan farklı örgütlerin üyeleri tarafından paylaşılan değer sistemleri ve inançlar, örgütler arası işbirliğini ve koordinasyon ilişkilerini kolaylaştırmakta ve karşıtlıkların, çatışmaların ve rekabetin azaltılması lehinde rol oynamaktadır (Garcia ve diğerleri, 2012).

2.2.1. Örgüt kültürünün unsurları

Örgüt kültürü, birbirinden ayırt edilebilir ancak birbiriyle ilişkili dört bileşenden oluşmaktadır. Bunlardan ilki bireylerin örgütün işleyişini ve özelliklerini anlamalarını sağlayan paylaşılan temel değerlerdir. İkinci bileşen, bu değerler tarafından üretilen bireylerin nasıl davranmaları gerektiğini gösteren davranışsal normlardır. Üçüncü bileşen, hikâyeler, anlaşmalar, ritüeller ve örgüt dili gibi değişik şekillerde kendini gösteren yapay dokulardır. Son bileşen ise örgütsel davranış örüntüleridir (Homburg ve Pflesser, 2000).

Tüm kuruluşların diğer kuruluşlardan ayırt edici nitelikte farklı bir kimliği, paylaşılan inanç ve değerlerden oluşan bir örgüt kültürü vardır. Örgüt kültürünü oluşturan olgular, örgüt üyelerinin düzenli veya nadiren gerçekleştirdikleri çeşitli prosedürleri ve faaliyetleri içermektedir. Dolayısıyla örgüt kültürü, bir örgütü oluşturan iletişim uygulamalarını ve davranışlarını açık bir şekilde tanımlamaktadır (Harris, 1984).

Örgüt kültürünün görünür belirtileri, örgüt içi biçimsel uygulamaları (maaş kademeleri, hiyerarşik yapı, iş tanımları), biçimsel olmayan uygulamaları (normlar), benimsenen değerleri, ritüelleri, örgütsel hikâyeleri, örgüt dilini ve fiziksel ortamı (ofis ve çalışma alanları, kılık kıyafet kuralları, mimari yapı) kapsamaktadır. Bu tezahürler çeşitli şekillerde yorumlanır, değerlendirilir ve uygulamaya konulur. Çünkü örgüt üyelerin ilgi alanları, deneyimleri, sorumlulukları ve değerleri farklıdır. Örgüt üyelerinin bu yorumlama farklılıkları, yorumlamaların altında yatan kalıplar ve uygulamaya konma biçimleri kültürü oluşturmaktadır. Örgüt kültürü, sadece yöneticilerin benimsediği değerler değildir. Aynı zamanda birçok çalışan tarafından paylaşılan değerleri de ifade etmektedir. Bu manada örgüt kültürü, tüm örgüt üyelerinin gündelik çalışma hayatlarında gömülü olarak yer almaktadır (Nicholson, Schuler ve Ven, 1998: 376).

Örgütteki davranış biçimlerine yüzeysel seviyede bakıldığında bazı kültürel yorumlamalar elde edilebilir. Örneğin birçok yazılım şirketinde çalışanların gayriresmî tarzda elbise giyiyor olmalarının yaratıcılığın gömlek ve kravatla uyumlu olmadığı inancıyla ilişkili olduğu kolaylıkla algılanabilmektedir. Fakat daha derinlere doğru inildiğinde, yorumlamalarla etkinlikler arasındaki ilişkiyi anlamak sadece yabancılar için değil, aynı zamanda örgütte çalışan kişiler için bile zorlaşmaktadır (Mintzberg, Ahlstrand ve Lampel, 1998: 266). Bu nedenle örgüt kültürün yalnızca yüzeysel bir tezahürü olan örgütsel iklim üzerinde yapılan araştırmalar, örgütlerin nasıl işlediğiyle ilgili daha derin nedenselliklerin araştırılmasına yol açmıştır. Örgütsel iklim ve normlardaki çeşitliliklerin açıklanmasına duyulan ihtiyaç, nihai olarak örgüt kültürü gibi daha "derin" kavramların üzerinde durulması gerekliliğini doğurmuştur (Schein, 1990). Örgüt kültürü, yüzeysel tezahürlerin yanı sıra bir örgütün yazılmamış, hissedilerek anlaşılan alanını temsil etmektedir. Örgüt içindeki herkes kültür içinde yer alır, fakat kültür genelde örgüt üyelerince fark edilmemektedir. Ancak yöneticiler, temel kültürel normlara ve değerlere aykırı yeni stratejileri veya programları uygulamaya koyduklarında kültürel güçler ile yüz yüze gelinmektedir. Örgüt kültürü, temel olarak buz dağında olduğu gibi görülebilen ve görülemeyen iki farklı düzeyde tanımlanabilir. Buz dağının görünür yüzeyinde, insanların kıyafet ve davranış şekilleri, örgüt tarafından kullanılan denetim sistemleri ve güç yapısı türleri, örgüt üyelerinin paylaştığı semboller, hikâyeler ve törenler gibi görünür dokular ve gözlemlenebilir davranışlar yer almaktadır. Bununla birlikte görünür kültür ögeleri, örgüt üyelerinin zihin derinliklerinde yer alan değerleri yansıtmaktadır. Görünür yüzeyin altında kalan kısım, temel değerler, varsayımlar, inançlar ve düşünce süreçlerinden oluşmaktadır. Örgüt kültürünün bu görülemeyen bilinçaltı düzeyi gerçek kültürü tanımlamaktadır (Daft, 2010: 374-375).

Örgüt kültürü, örgüt üyelerinin düşünme, hissetme ve davranma biçimlerini etkileyen paylaşılan inançlar, değerler ve normlar bütünüdür. Örgütteki davranış standartları, çalışma gruplarında gelişmekte ve grup normları tarafından onaylanan davranışların etkisi davranış standartları olarak ortaya çıkmaktadır. Değerler açısından bakıldığında örgüt kültürü, örgütün elde etmeyi amaçladığı sonuçlardan (uç değerlerden) ve örgütün teşvik ettiği davranış şekillerinden (araçsal değerlerden) oluşmaktadır. Araçsal değerler, örgütün uç değerlerini elde etmesine yardımcı olmaktadır. Örneğin tüm öğrencilerin uç değer olarak yüksek başarı elde etmesi vurgulanan bir okulda, tüm öğrencilere ulaşmak adına çok çalışmak gibi araçsal değerler teşvik edilerek istenilen sonuca ulaşılabilir. Bu örnekten

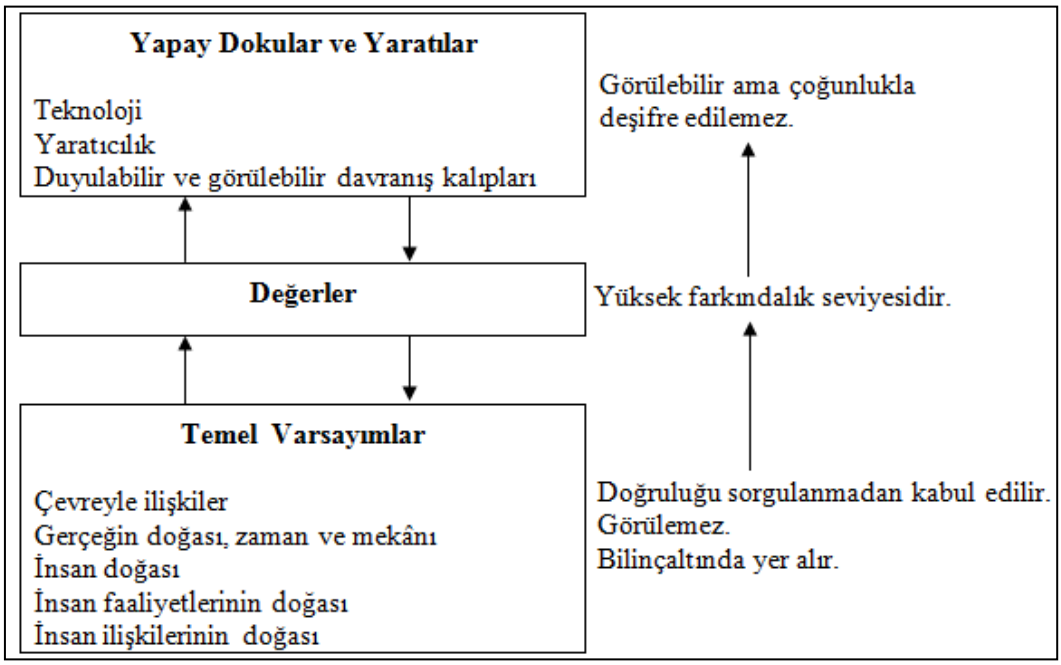
anlaşılacağı üzere örgüt kültürünün uç ve araçsal değerlerinin kombinasyonu örgüt başarısında etkili olmaktadır. Bununla birlikte kültür, değerler, kahramanlar, törenler, ritüeller ve iletişim ağları vasıtasıyla oluşturulmaktadır. Kahramanların hikâyeleri veya mitleri iletişim ağları vasıtasıyla iletilmektedir. Bu iletişim ağları örgütün kimliğinde rol alan farklı kişiler tarafından karakterize edilmektedir. Her örgütte olan biteni yorumlayan, örgütsel hikâyeleri anlatan kişiler bulunmaktadır (Lunenburg, 2011).

Kültür genel anlamda paylaşılan tutum ve davranış kalıplarıdır. Bu açıdan değerlendirildiğinde, örgüt üyelerinin örgütsel eylem ve süreçlere ilişkin tutum ve davranışlarının örgüt kültürü tarafından yönlendirildiği genel kabul gören bir görüştür (Doğan, 2012: 114). Örgüt kültürü, ayrıca örgüt üyeleri arasında paylaşılan inanç ve beklentiler örüntüsüdür. Bu inanç ve beklentiler, örgüt içindeki bireylerin ve grupların davranışlarını önemli ölçüde şekillendiren normları oluşturmaktadır (Schwartz ve Davis, 1981). Normlar, temel varsayımların görünür bir tezahürüdür. Unutulmamalıdır ki normların arkasında birçok örgüt üyesinin sorgulayamayacağı veya inceleyemeyeceği pek çok varsayım yatmaktadır (Schein, 1996). Ayrıca örgüt kültürü normları, örgütün yapısal tasarımında da önemli bir rol oynamaktadır (Mintzberg, 1979: 292). Mintzberg'e göre, örgüt yapısını altı temel öge oluşturmaktadır. Bunlar, operasyonel çekirdek, stratejik tepe, orta kademe, teknolojik yapı, destek personeli ve tüm bu ögeleri içine alan ideolojidir. Burada ideoloji, bir örgütü diğer örgütlerden ayıran gelenek ve inançlarını kapsayan örgüt kültürünü ifade etmektedir (Lemieux, 1998). Benzer bir ifadeyle örgütün genel görünüşü, örgüt kültürünü belirleyen unsurlar temelinde şekillenir. Bu unsurlar, örgüt kültürünün temel özellikleri, liderlik (yönetim), insan kaynakları yönetimi, örgütsel birlik, stratejik hedefler ve başarı kriterleridir (Lapina, Kairisa ve Aramina, 2015).

2.2.2. Örgüt kültürünün katmanları

Şekil 2.1'de görüldüğü üzere örgüt kültürü, Schein'in örgüt kültürü katmanları modeline göre üç farklı katmanda analiz edilmektedir. Başlangıç katmanı olan görülebilir dokular (yaratılar), örgütün yapısal çevresini, mimarisini, teknolojisini, ofis yerleşim düzenini, çalışanların giyim tarzını, görülebilir ve duyulabilir davranış örüntülerini, sözleşmeler, kontratlar gibi dokümanları, çalışan oryantasyonunda kullanılan materyalleri ve hikâyeleri yansıtmaktadır. Bu seviyedeki kültür ögelerinin elde edilmesi kolay fakat yorumlanması zordur. Bu katmanda grupların örgüt içinde nasıl bir çevre kurduğu ve hangi davranış

örüntülerinin bireyler arasında görülebilir olduğu tanımlanabilmektedir. Bireylerin neden süregelen şekilde davranış sergilediklerini analiz edebilmek için ise ikinci katmandaki davranışları şekillendiren değerlere bakılması gerekmektedir. Fakat değerlerin doğrudan gözlemlenebilmesi zor olup, değerlerin ne manaya geldiği, kilit örgüt üyeleriyle yapılacak görüşmeler ve yaratıların analizi ile elde edilebilmektedir. Bireylerin davranışları altında yatan esas sebepler ise gizli ve bilinçaltı ögeler olup üçüncü katmandaki temel varsayımlara dayanmaktadır. Kültürü gerçekten anlayabilmek ve grupların değerlerini bütünüyle kavrayabilmek için, grup üyelerinin nasıl algıladıklarını, düşündüklerini ve hissettiklerini belirleyen altta yatan bilinçaltı varsayımlara inmek gerekmektedir. Bu varsayımlar, benimsenen değerler temelli öğretilerin sonuçlarıdır. Değerler davranışlara yol gösterdikçe ve davranışlar da problemleri çözmede başarılı oldukça değerler zamanla temel varsayımlara dönüşmektedir. Varsayımlar sorgulanmadan kabul edilmeye başlandıkça, farkındalıktan çıkmakta ve bilinçaltına itilmektedir. Sorgulanmadan kabul edilen varsayımlar benimsenen değerlere göre çok daha az tartışmaya açıktır. Bu manada değerler, kültürün temeline ulaşmış, tartışılmaya kapalı, sorgulanmadan kabul edilen, varsayım formuna ulaşmış olanlar ile tartışılabilir ve açık olan benimsenmiş değerler olarak ikiye ayrılabilmektedir (Schein, 1984).



Şekil 2.1. Örgüt kültürünün katmanları ve katmanlar arası etkileşim (Schein, 1984)

Örgüt kültürünün en alt katmanında yer alan paylaşılan örtük varsayımlar, bireyleri günlük normal faaliyetlerin nasıl yürütüleceğine dair yönlendiren bir tür "filtre" görevi

üstlenmektedir. Varsayımlar ayrıca çalışanların örgüt politikalarını nasıl yorumladıklarını ve prosedürleri nasıl uyguladıklarını etkilemektedir. Bu politika ve prosedürler, orta katmanda yer alan benimsenen değerlerin bir parçasını oluşturmaktadır. Benimsenen değerler, örgüt yönetimine örgüt kültürünün üst katmanının, başka bir ifadeyle örgüt kültürünün "görünür" yanının anlaşılması açısından katkı sağlamaktadır. Bir dereceye kadar, benimsenen değerler kültürel yönü ortaya koymaktadır. Bununla birlikte bu "yön" ün yorumlanması, esas alınan paylaşılan örtük varsayımlara son derece bağlıdır. Bu üç örgüt kültürü katmanının, bilgi güvenliğinde "insan faktörünün" davranışsal yönleriyle yakından örtüştüğü görülmektedir (Niekerk ve Solms, 2010).

2.2.3. Örgüt kültürünün fonksiyonları

Gücün aynadaki yansıması kültürü ifade etmektedir. Güç, örgütü bir bütün olarak tutan ve onu bölümlere ayıran bir varlıktır. Bu manada örgüt kültürü, kendi çıkarlarına odaklanan farklı bireyleri ortak çıkarlara odaklanan örgüt adındaki bir oluşum içinde toplamaktadır. Aslında kültür yeni bir fikir değildir. Her çalışma alanının kendine has merkezî rol oynayan kavramları vardır. Nasıl ki ekonomide pazar, siyaset biliminde politika, stratejik yönetimde strateji kavramları araştırmalarda merkezî rol oynamaktaysa kültür de antropolojide uzun zamandır merkezî bir kavram olarak ele alınmaktadır. Antropolojinin bakış açısından değerlendirildiğinde kültür, yemekte içilen içecekten, dinlenilen müzikten nasıl iletişim kurduğumuza kadar çevremizdeki hemen her şeyi ifade etmektedir. Aynı zamanda kültür, tüm bunları yaparken kendine has benzersiz bir yol sunmaktadır. Bu anlamda kültür, bir örgütü bir başka örgütten, bir endüstriyi diğer bir endüstriden ve ulusları birbirinden ayıran farklılıkları ortaya koymaktadır. Örgüt kültürü ise bir örgütteki bireylerin toplu idrakı ve kavraması ile ilişkilendirilmektedir. Örgüt kültürü, gelenek ve alışkanlıkların yanı sıra hikâyeler, semboller, hatta binalar ve ürünler gibi daha somut tezahürlerde paylaşılan inançları "örgütsel zekâ" hâline getirmektedir. Bir bakıma örgüt kültürü, örgütün yaşama gücünü, fiziksel bedeninin ruhunu temsil etmektedir (Mintzberg ve diğerleri, 1998: 264-266).

Örgüt kültürü, örgütün iç ve dış çevresiyle uyum sorunlarının giderilmesine ilişkin öğrenilen çözümlerdir. Bu çözümler, benzer sorunların giderilmesinde de işe yaradıkça doğrular olarak kabul edilmekte, örgüt üyelerince paylaşılan normlara, değerlere ve inançlara dönüşmekte ve örgüte yeni katılanlara aktarılmak istenmektedir (Doğan, 2012:

109). Örgüt kültürü bir anlamda, tüm örgütte ve örgüt içerisindeki çeşitli birimlerde ne şekilde davranılması gerektiğini, neyin doğru ve neyin yanlış olduğunu belirleyen bir sosyal kontrol sistemi oluşturmaktadır (Erkmen, 2010: 3). Benzer bir yaklaşımla örgüt kültürü, grupların dış çevreyle uyum ve iç çevreyle bütünleşme süreçlerinde karşılaştıkları problemleri çözmeye çalışırken elde ettiği, keşfettiği ve geliştirdiği temel varsayımların bütünüdür. Bu varsayımlar, geçerlilikleri kabul edildiği ölçüde karşılaşılan problemlerin çözümünde kullanılmaya devam edilmekte ve gruba dâhil olan yeni bireylere bu problemlerle karşılaşması hâlinde nasıl algılanılması, düşünülmesi ve hissedilmesi gerektiğini gösteren doğru birer yol haritası olarak aktarılmakta ve öğretilmektedir (Schein, 1984).

Örgüt kültürü, bir grubun ya da topluluğun dünyadaki konumu ve işlevi hakkında varsayımların karmaşık bir kalıbıdır. Örgütler birçok değişkenden oluşan açık ve karmaşık bir sistemden oluşmaktadır ve bu sistemler çevresel faktörlerle yakından etkileşim hâlindedir. Herhangi bir örgüt, sağlamakta olduğu ürün ve servislerinin üretiminde verilimlik elde etmeye çalışır. Bu manada kullanılan temel kaynakların insan gücü, finans, hammadde, teknoloji ve bilgi olduğu bir ortamda örgüt kültürünün başlıca işlevi, dış çevreyle adaptasyonu ve örgüt içi entegrasyonu sağlamasıdır. Dolayısıyla örgüt kültürü, örgüt etkinliği ve performansıyla doğrudan bağlantılıdır. Örgüt kültürü ne kadar güçlü ise bir örgüt o kadar etkili ve verimli çalışır (Lapina ve diğerleri, 2015). Uzun bir paylaşılan geçmişi olan ya da önemli yoğun deneyimlerin paylaşıldığı örgütlerde "güçlü" kültürlerin varlığından bahsedilebilir (Schein, 1990). Uyumu ve değişimi teşvik eden güçlü bir kültür, çalışanları motive ederek, insanları paylaşılan hedefler ve yüksek bir misyon etrafında birleştirerek, eylemlerin stratejik önceliklerle uyumlu hâle getirilmesi adına kişilerin davranışlarını şekillendirerek ve yönlendirerek örgütsel performansı artırmaktadır (Daft, 2010: 387). Diğer bir ifadeyle örgüt kültürü, bir güdülenme veya güdüleme aracı olarak fonksiyon gerçekleştirmekte olup, örgüt üyelerini harekete geçiren ve örgüt üyelerinin paylaştıkları bazı kültürel ögelere bağlı olarak meydana gelen sosyal bir enerji olarak görülmektedir (Erkmen, 2010: 41).

Herhangi bir örgütte kültür, genel olarak o örgütün tüm üyeleri arasında paylaşılan inanç ve değerlerle tanımlanmaktadır. Paylaşılan inançlar, değerler, semboller, davranışlar ve ahlaki unsurlar bireyleri karar vermede bilinç dışı olarak yönlendirmektedir. Bir örgütün refahı üyelerinin refahına bağlı olduğundan, paylaşılan bu ideolojilerin örgütsel

performans üzerinde güçlü bir etkisi vardır (Gull ve Azam, 2012). Bu manada örgüt kültürü türünün anlaşılıyor olması, bir örgüt içinde etkin bir şekilde çalışmak adına yol gösterici olabilmektedir. İşlerin halledilmesi genel olarak birçok örgüt üyesinin hedefi olduğundan, dikkatli gözlemler yoluyla kültür türüne ilişkin verilecek bazı ön kararlar işlerin yapılması ile ilgili yeterli bilgiyi sağlayacaktır. Benzetimde bulunmak gerekirse araziyi geçmeye çalışmadan önce bölgeyi bilmek her zaman yarar sağlayacaktır (Harris, 1984).

Örgüt kültürü, çalışanların davranışlarını doğrudan etkilemekte ve bir kuruluşun gelişmesine yardımcı olmaktadır. Diğer bir ifadeyle örgüt kültürü, üst düzey yöneticilerin yeni stratejileri ve planları tasarlamalarında ve uygulamalarında kolaylaştırıcı rol oynamaktadır. Hatta insanların daha fazla çalışmasını veya daha yenilikçi olmasını sağlayabilmektedir. Resmî işleyen sistemler ve liderlik vasıtasıyla yapılamayan bazı işler dahi örgüt kültürü ile gerçekleştirilebilmektedir (Baker, 1980). Dolayısıyla üst yönetim, örgütün stratejik yönünü değiştirmeden önce, yeni stratejilere ayak uydurmak adına örgüt kültürünü yeniden şekillendirmeye hazır olmalıdır. Bu bağlamda örgüt kültürü, en üst düzeyde kullanılan kurumsal liderlik aracı olarak değerlendirilmelidir (Sayles ve Wright, 1985).

2.2.4. Örgüt kültürünün ölçümü

Araştırmacılar arasında örgüt kültürünün ölçümüyle ilgili net bir ortak düşünceye varılamadığı söylenebilir (O'Reilly ve diğerleri, 1991). Örgüt kültürü, bir örgütte yer alan alışılmış kılık kıyafet tarzı, kullanılan dil, davranışlar, inançlar, değerler, varsayımlar, statü ve otorite sembolleri, efsaneler, törenler, ritüeller, saygı ve saygısızlık biçimleri de dâhil olmak üzere çeşitli toplumsal olguları ifade etmektedir. Bunların hepsi bir örgütün karakterini ve normlarını tanımlamaya yardımcı olmaktadır. Bu çeşitli olgular göz önüne alındığında, örgüt kültürünün nasıl gözlemlenmesi ve ölçülmesi gerektiği hususunda veya rutin yönetim faaliyetlerinde ve örgütsel değişimde örgüt kültürüyle ilgili farklı metodolojilerin nasıl kullanılacağı konusunda bir fikir birliğinin sağlanamamış olması şaşırtıcı olmayacaktır (Scott ve diğerleri, 2003).

1980'lerden itibaren kültür kavramı, örgütsel çalışma alanlarında sıkça ele alınmaya başlanmış bir konu olup, alanyazına bu konuda çokça katkı sağlandığı görülmektedir.

Örgütsel kültür disiplininin geliştiği ilk aşamalarda kültür, örgütsel yaşamın sübjektif tarafını yansıtan bir kavram olarak algılanmakta ve nitel gözlem metotları ile ele alınmaktayken, 1990'lardan itibaren örgüt kültürü alanında yapılan çalışmalarda araştırmacıların nicel anket metotlarını uygulamakta ve karşılaştırılabilir kültür boyutlarını tanımlamakta oldukları görülmektedir (Denison, 1996).

Örgüt kültürü kavramı analiz edilirken üç önemli boyut özel olarak ele alınmalıdır. Örgüt kültürünün analiz edildiği birinci boyutu objektif / sübjektif boyuttur. Kültürün objektif yönleri örgüt üyelerinin zihinlerinin dışında kalanlardır. Bunlar kahramanların anıtları, resimleri, örgüt hikâyeleri, atalar, mitler, törenler ve ritüeller gibi yapay dokulardır. Sübjektif boyut ise örgütün bakış açısı, eğilimi ve varsayımları olup duyular tarafından doğrudan algılanamayan gerçekleri yansıtmaktadır. Sübjektif özelliklerin örnekleri arasında, düşüncelerden türemiş paylaşılan varsayımlar, inançlardan türemiş paylaşılan değerler, çevremizi nasıl yorumladığımızı gösteren paylaşılan manalar ve işlerin nasıl yapıldığını gösteren paylaşılan anlayışlar yer almaktadır. Örgüt kültürün analiz edildiği ikinci boyutu niteliksel / niceliksel boyuttur. Kültürün nitel yönleri insanların tanımlama, şifre çözme ve tercüme etmede kullandığı yorumlarıdır. Buna karşın, örgüt kültürünün niceliksel boyutu insanların bir kültür hakkında söylediği şeylerden ibarettir. Son olarak örgüt kültürünün analiz edildiği üçüncü boyut, gözlemci (dışarıdan) / yerli (içeriden) boyutudur. Örgüt kültürünün gözlemci yönü, örgüt üyelerinden toplanan yanıtlara yüklenen anlamlar veya örgüt dışındaki bir kişi tarafından gözlenen örgütsel davranışlardır. Dışarıdaki bir kişinin kültüre bakış açısını kazanmak önemlidir, çünkü bir gözlemci, örgüt içerisinde gözden kaçan bazı özellikleri tespit edebilmektedir. Bununla birlikte gözlemciler, kendi bakış açılarını olaylara katarak gözlemlenen kişinin ortaya koyduğu manayı yakalayamama sorununu da yaşayabilmektedir (Duncan, 1989).

Kültür, bir yabancı gözüyle örgüt dışından bakılarak veya örgütün bir üyesi gibi içeriden incelenebilir. Örgüt kültürüne dışarıdan bakılması, insanların neden süregelen şekilde davranış sergilediklerinin objektif bir biçimde ele alınmasını sağlar. Bu durum, dışarıdan bakanın örgüt içerisindekilerden farklı sosyal ve ekonomik ilişkilere sahip olması ile açıklanmaktadır. Örgüt kültürünün içeriden incelendiği ikinci durumda ise kültür, herhangi bir soyut, evrensel mantığa dayalı olmayan öznel bir yorum sürecinde değerlendirilmektedir (Mintzberg ve diğerleri, 1998: 265). Örgüt kültürünü tanımlayabilmek için, takip edilebilecek holistik (bütünselci), mecazi (dilsel) ve nicel

yaklaşımlar temelinde üç ayrı strateji mevcuttur. Holistik yaklaşım, araştırmacının örgüt içine girmesini, doğal bir örgüt üyesi gibi davranmasını ve böylelikle kültürün bir parçası olarak derinlemesine örgüt içinde gözlem yapabilmesini ifade etmektedir. Mecazi veya dilsel yaklaşımda araştırmacı, örgüt kültürünü tanımlamak için, tıpkı dedektiflerin bir kişinin kimliğini tespit etmede o kişiye özel parmak izini, ses kayıtlarını veya yazı sitilini kullanmaları gibi örgüt içi dokümanlarda, raporlarda, hikâyelerde ve diyaloglarda kullanılan dilin yapısını kullanmaktadır. Nicel yaklaşımda ise araştırmacı anket veya mülakat yöntemini kullanarak kültürün belirli boyutlarını değerlendirmektedir. Bu kapsamda nicel yaklaşım örgüt kültürü özelliklerinin değerlendirilmesinde birçok bakış açısına imkân sağlamaktadır (Cameron ve Quinn, 2006: 148).

Nitel metot savunucularından Schein'a (2009: 27-28) göre, bireylerin günlük davranışlarını şekillendiren, gözle görülemeyen, öğrenilmiş ve paylaşılan temel varsayımlar anlaşılabilirse bireylerin görülebilen davranışsal yaratılarını nasıl yönlendirdiği daha iyi kavranabilir. Fakat bunun tam tersi çok zordur. Diğer bir ifadeyle sadece davranışları gözlemleyerek varsayımlar anlaşılamamaktadır. Dolayısıyla kültürü tam manasıyla anlayabilmek için, sistematik gözlem sürecine dâhil olmak ve görülemeyen varsayımların açık hâle getirilmesinde örgüt üyelerine yardımcı olmak adına kendileriyle görüşmeler yapmak gerekmektedir. "Balıklar konuşabiliyor olsalardı, suyun ne olduğunu söyleyebilirlerdi" metaforunda olduğu gibi örgüt üyeleri, kültürlerinin ne olduğunu kolayca ifade edemeyebilirler. Buradan hareketle sadece davranışlar ve benimsenen değerlerle ilgili sorular yönelten anket ve benzeri tekniklerle örgüt kültürünün ölçülemeyeceği ve nicel olarak tanımlanamayacağı düşüncesi ortaya çıkmaktadır.

Belirli bir şekli olmayan ve kompleks bir olgu olarak görülen örgüt kültürünün ölçülmesi çok tartışmalı bir konu olarak süregelmiştir. Bu noktada bazı araştırmacılar, her bir kültürün kendine özgü olduğunu ve ölçülmesi yerine sezgisel olarak algılanması gerektiğini savunmaktayken diğerleri kültürün keşfedilmesinin en iyi yolunun, her örgütün âdetlerini oluşturan olayların hikâyelerini ve rivayetlerini analiz eden etnografik araştırmalar yürütmek olduğunu iddia etmektedirler. Örgüt kültürünün anket tekniği ile incelenmesinin hem avantajları hem de dezavantajları bulunmaktadır. Anket tekniğinin temel avantajı, aynı örgüt kültürü ölçme yönteminin birçok örgütte aynı şekilde uygulanabilmesi imkânını sağlıyor olmasıdır. Dolayısıyla anket sonuçları, daha sonra karşılaştırma ve genelleme yapabilmek adına bir dayanak noktası oluşturmaktadır. Örneğin

anketin iletişim endeksine eklenen birtakım maddeler, bir örgütün ilgili endekste daha düşük puan alan ikinci bir örgüte göre daha iyi bir iletişim kapasitesi olduğunu gösterebilmektedir. Benzer bir örnekte de iletişimin daha iyi olduğu örgütlerin daha iyi performans gösterdiğini gösteren bir bulgu, iletişim ile performans arasında yakın bir ilişki olduğunun kanıtı olarak değerlendirilebilir. Bununla birlikte anket yönteminin dezavantajı aşırı genellemeye karşı hiçbir koruma sağlamıyor olmasıdır. Bu noktada örneğin örgütlerde karar alma uygulamalarını karşılaştırmak bazen elma ile portakalı karşılaştırmak gibi olabilir (Denison, 1984).

Örgüt kültürü araştırmalarında kullanılacak en uygun metodun belirlenmesi noktasında bilim adamlarının yaşadıkları fikir ayrılıkları, nitel ve nicel çalışmalar arasındaki tartışmalara dayanmaktadır. Örgüt kültürü çalışmaları geleneksel olarak etnografik araştırmalar, derinlemesine ve açık uçlu görüşmeler gibi nitel metotlarla yürütülmektedir. Nitel metotlarla yürütülen çalışmalar, aşırı tanımlamayı amaç edinmekte ve sunmuş olduğu avantajlar çalışmanın maliyet unsurunu da beraberinde getirmektedir. Bununla birlikte nitel araştırma metotları örgütler arasında analitik karşılaştırma yapma olanağı sunmamaktadır. Sonuç olarak örgüt kültürü, örgüt kültürünün sistematik gözlemine olanak sağlayan güvenilir ve kolay yönetilebilir araçlar ile ölçülemedikçe birçok önemli teorik soru cevapsız kalacaktır (Quinn ve Spreitzer, 1991).

Her ne kadar nitel ve nicel yöntemlerde kullanılacak veri toplama teknikleri ile ilgili standart, ölçek ya da envanterlerin sayısı ve niteliği bakımından sınırlılıklar bulunsa da bu yöntemler örgüt kültürü hakkında betimleyici, sayısal ve somut verilere ulaşmayı kolaylaştırmaktadır (Erkmen, 2010: 133).

2.3. Rekabetçi Değerler Modeli

Son zamanlarda örgüt kültürü alanında yapılan çalışmalarda araştırmacılar nicel anket metotlarını uygulamakta ve karşılaştırılabilir kültür boyutlarını tanımlamaktadırlar (Denison, 1996). Nicel metot savunucularının başında gelen araştırmacılardan Robert E. Quinn ve John Rohrbaugh, örgüt kültürünü ölçümleyen Rekabetçi Değerler Modeli'ni geliştirmişlerdir (Quinn ve Rohrbaugh, 1981, 1983).

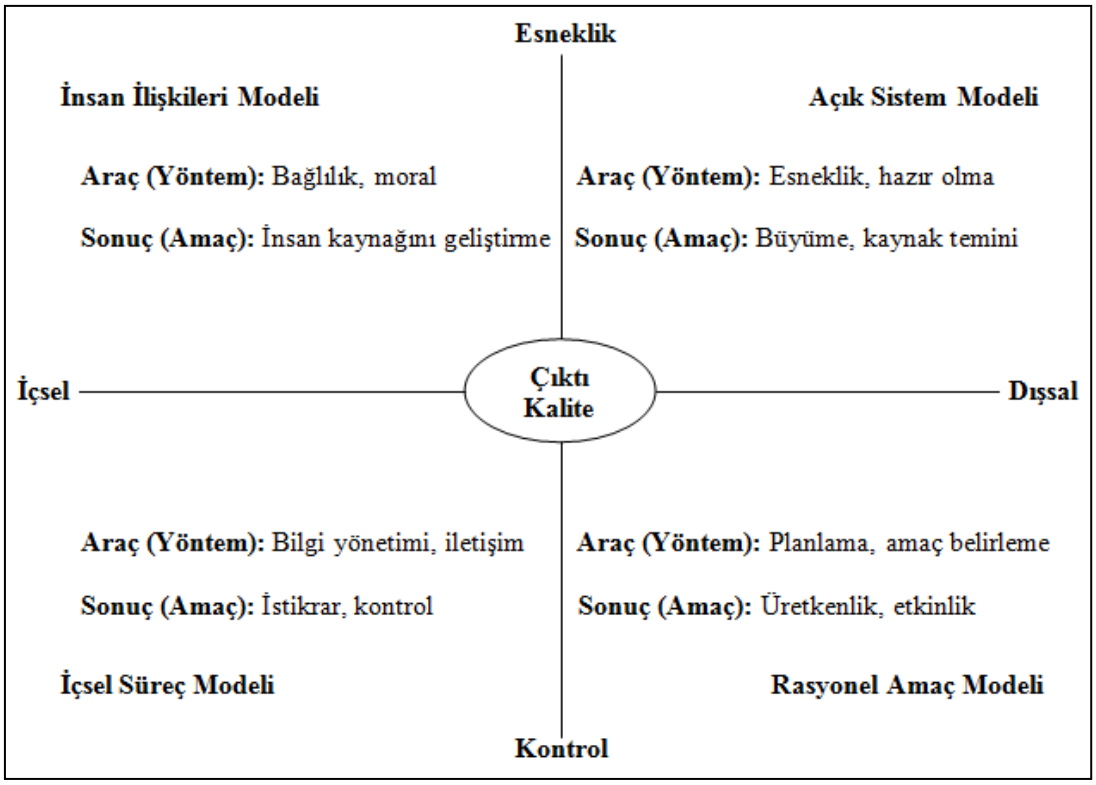
Örgüt kültürü, örgüt bireylerinin paylaştıkları ve sorgulamadan kabul ettikleri varsayımlar

üzerine kurulu olduğu için örgüt kültürünün objektif bir şekilde değerlendirilmesi zordur. Çünkü bu varsayımlar bireylerin bilinçaltında yatmaktadır. Bu varsayımlar, genellikle bireylerin ve örgütün davranışlarından ortaya çıkan hikâyeler, örgütte kullanılan dil yapısı, yaratılar ve normlar ile tanımlanmaktadır. Bilinçaltında yatan ve bireyler arası paylaşımda olan varsayımların doğası, örgüt bireylerinin gerçekle ilgili yorumlamalarını kategorilere ayrıştıran yargı eksenlerini (axes of bias) veya psikolojik ön-modelleri (psychological archetypes) çalışma konusu yapan başta filozof William T. Jones ve psikiyatr Carl G. Jung olmak üzere birçok araştırmacının ilgi odağı olmuştur. Çalışmalara konu olan bu kategoriler, bilinçaltı değerleri, varsayımları ve yorumlamaları kategorize etmede bireyler tarafından kullanılan farklı alanları ortaya çıkarmaktadır. Dolayısıyla bu kategoriler aynı zamanda örgütteki belirli kültür türlerini tanımlamada da kullanılabilir. Çünkü kültürler söz konusu değerler, varsayımlar ve yorumlamalar temelinde tanımlanmaktadır. Bu kategoriler daha sonraları 1981'de Quinn ve Rohrbaugh tarafından örgütsel etkinlik için deneysel olarak geliştirilen Rekabetçi Değerler Modeli'nin temelini teşkil etmiştir (Cameron ve Freeman, 1991). Rekabetçi Değerler Modeli'nin özünün psikolojik ön-modellerle uyumlu olmasından dolayı katılımcılar kültürel değerlendirmelerini yansıtırlarken Rekabetçi Değerler Modeli'ni kolaylıkla kullanabilmektedirler (Cameron ve Quinn, 2006: 151).

John Campbell ve arkadaşları 1974 yılında, örgütsel etkinliğin en geniş kapsamda ölçümüne olanak sağlayan 39 adet indikatör listesi tanımlamışlardır. Bu indikatörlerin kullanılabilirliğini ve kavranabilirliğini artırmak adına sayılarının azaltılması ve kümelenmesi yoluna gidilmiştir. Bu kapsamda Quinn ve Rohrbaugh tarafından yürütülen çalışmada, örgütsel etkinliğin ölçümünde kullanılacak indikatörler istatistiksel analize tabi tutulmuş ve 2 temel boyutta 4 ayrı kümede toplanmıştır. Örgütsel etkinlik kavramının birinci boyutu esneklik, sağduyululuk ve dinamizm kriterlerinden, istikrar, düzen ve kontrol kriterlerine doğru bir geçişi ifade etmektedir. İkinci boyut ise içsel oryantasyon, entegrasyon ve bütünlük kriterlerinden dışsal oryantasyon, farklılaşma ve rekabet kriterlerine doğru değişmektedir (Cameron ve Quinn, 2006: 34-35).

Şekil 2.2'de yer alan Quinn ve Rohrbaugh'un (1983) örgütsel etkinlik için geliştirmiş oldukları Rekabetçi Değerler Modeli'nde örgütsel etkinliğin kriterleri, içsel - dışsal, esneklik - kontrol ve araç (yöntem) - sonuç (amaç) olmak üzere üç ayrı rekabetçi değerler boyutunda sınıflandırılmıştır. İçsel - dışsal ve esneklik - kontrol eksenleri temel 2 boyutu

göstermekte ve bu boyutlar, İnsan İlişkileri Modeli, Açık Sistem Modeli, İçsel Süreç Modeli, Rasyonel Amaç Modeli olmak üzere 4 ayrı modeli ortaya koymaktadır. Diğer bir ifadeyle bu 4 modelin bütünleştirilmesi ile örgütsel etkinlik için Rekabetçi Değerler Modeli oluşmaktadır.



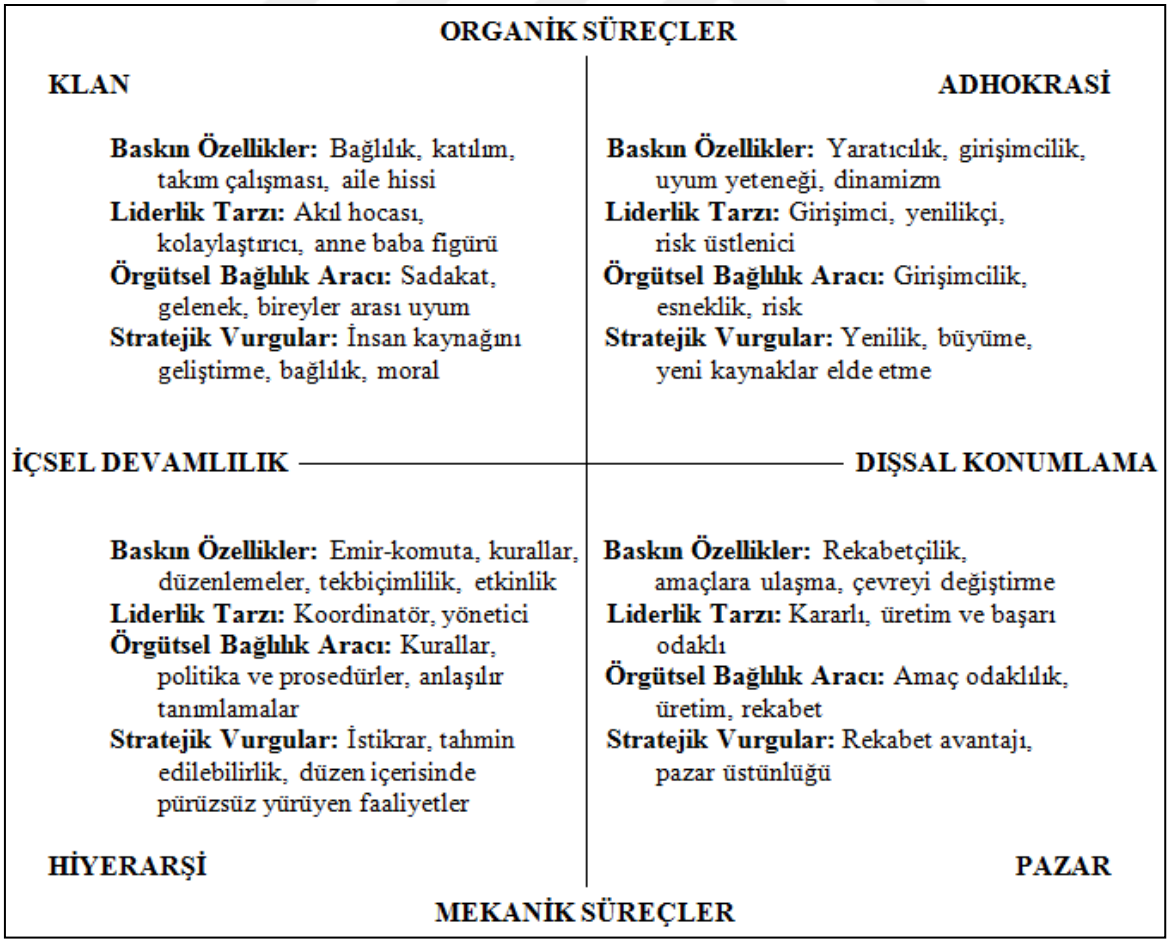
Şekil 2.2. Örgütsel etkinlik için Rekabetçi Değerler Modeli (Quinn ve Rohrbaugh, 1983)

Rekabetçi değer boyutlarının ilki içsel ve dışsal örgütsel odaklanma üzerine kuruludur. İçsel bakış açısında örgütteki bireylere odaklanılmakta, bireylerin refahı ve gelişimine vurgu yapılmaktadır. Dışsal bakış açısında ise örgütün kendisine odaklanılmakta, örgütün refahı ve başarısı vurgulanmaktadır. İkinci rekabetçi değerler boyutu, örgütün esnek veya kontrollü bir yapıya sahip olup olmadığını göstermektedir. Esnek örgüt yapısında bireysel girişkenliklerin ve örgütsel uyumun önünü açan yenilik ve değişimden yana bir örgütten bahsedilirken, kontrollü örgüt yapısında ise örgütün otoriter ve hiyerarşik bir yönetim tarzında düzenli bir örgüt yapısına sahip olduğu yansıtılmaktadır. Üçüncü boyutta ise planlama, hedef belirleme gibi önemli süreçlerde kullanılacak araçlara (yöntemlere) ve bu araçların kullanımı ile elde edilecek üretkenlik, kaynak temini gibi sonuçlara (amaçlara) odaklanılmaktadır. Şekil 2.2'nin sol üst çeyreğinde gösterilmekte olan İnsan İlişkileri Modeli'nde, esneklik ve içsel bakış açısı benimsenmektedir. Bu modelde, insan kaynağını geliştirme amacına ulaşmak için, bireylerin örgütsel bağlılığının ve moralinin yüksek

tutulması araç olarak kullanılmaktadır. Şekil 2.2'nin sağ üst çeyreğinde yer alan Açık Sistem Modeli'nde, esneklik ve dışsal bakış açısı benimsenmekte olup, büyüme ve kaynak temini amacına ulaşmada kullanılan araç, her duruma karşı esnek ve hazırlıklı olmadır. Şekil 2.2'nin sağ alt çeyreğinde gösterilmekte olan, kontrollü yapının ve dışsal bakış açısının benimsendiği Rasyonel Amaç Modeli'nde ise üretkenliği ve etkinliği elde etme amacına ulaşmak için, planlama ve amaç belirleme araç olarak kullanılmaktadır. Son olarak Şekil 2.2'nin sol alt çeyreğinde yer alan İçsel Süreç Modeli'nde, kontrollü yapı ve içsel bakış açısı benimsenmekte olup, istikrarı ve kontrolü sağlama amacına ulaşmada kullanılan araç, bilgi yönetimi ve iletişimdir (Quinn ve Rohrbaugh, 1981, 1983).

2.4. Cameron ve Freeman Örgüt Kültürü Türleri Modeli

Quinn ve Rohrbaugh'un örgütsel etkinlik için geliştirmiş oldukları Rekabetçi Değerler Modeli, Şekil 2.3'te görülen Örgüt Kültürü Türleri Modeli'nin temelini oluşturmaktadır.



Şekil 2.3. Cameron ve Freeman Örgüt Kültürü Türleri Modeli (Cameron ve Freeman, 1991)

Kültürün, örgüt üyelerinin değerleri, varsayımları ve yorumlamaları gibi faktörlerin ışığında tanımlanmasından dolayı örgüt kültürü türleri bu faktörlerin türetildiği psikolojik seviyelerde gruplandırılabilmektedir. Psikiyatr Jung'un oluşturmuş olduğu yapıdaki psikolojik modele benzer şekilde 4 örgüt kültürü türü de Rekabetçi Değerler Modeli'nde görülmektedir. Cameron ve Freeman'ın, Quinn ve Rohrbaugh'un örgütsel etkinlik için geliştirmiş oldukları Rekabetçi Değerler Modeli'ni referans alarak oluşturmuş oldukları Örgüt Kültürü Türleri Modeli'ndeki 4 örgüt kültürü türü hiyerarşi, pazar, klan ve adhokrasi olarak tanımlanmaktadır. Her bir 4 örgüt kültürü türü, 4 ana özellik çerçevesinde başlıca karakteristikler içermektedir. Örgüt kültürü türlerini yansıtan bu 4 ana özellik, baskın özellikler, örgütsel liderlik, örgüte bağlılık, stratejik vurgular olarak seçilmiştir (Cameron ve Freeman, 1991).

Cameron ve Freeman'ın Örgüt Kültürü Türleri Modeli'ne benzer şekilde Rekabetçi Değerler Modeli ile örtüşen içsel odak - dışsal odak ve istikrarlı - esnek boyutlarında yapılandırılan bir diğer model Denison Örgüt Kültürü Modeli'nde ise hiyerarşi için tutarlılık (consistency), pazar için misyon, klan için bağlılık (involvement) ve adhokrasi için uyarlanabilirlik (adaptability) kültür özellikleri kullanılmıştır (Denison, Haaland ve Goelzer, 2004). Denison Örgüt Kültürü Modeli'nin kültürel özelliklerine hiyerarşi, pazar, klan ve adhokrasi kültürlerinin tanımlamalarında yer verilecektir.

2.4.1. Hiyerarşi

Şekil 2.3'ün sol alt çeyreğinde yer alan hiyerarşi kültürü, içsel devamlılık ve mekanik süreçler üzerine kurulu, formel işleyiş süreçlerine hâkim resmî ve katı bir çalışma ortamını yansıtmaktadır. Resmî prosedürler, çalışanların ne yapacağına yön vermektedir. Liderler iyi birer yönetici ve organizatör olarak görülmektedir. Hiyerarşi kültüründe, durağanlık ve verimlilik temaları hâkim olup işlerin düzenli ve verimli bir şekilde yürütülmesi esastır. Resmî kural ve politikalar, örgüt bireylerini bir arada tutmaktadır. Hiyerarşi kültürünün tanımlanması, temel olarak 1900'lü yılların başlarında Avrupa'daki devlet kuruluşlarının yapıları hakkında çalışmalarda bulunmuş Alman sosyolog Max Weber'e dayanmaktadır. Hiyerarşinin Weber tarafından yapılan tanımında, kurallar, uzmanlık, yeteneğe göre mevki, emir-komuta yapısı içerisinde ast-üst ilişkisi, kamu ve bireysel mülkiyetin ayrımı, gayrişahsilik ve sorumluluk gibi yedi özellik yer almaktadır. Bu özelliklerin belirlenen bir amacı gerçekleştirmede son derece etkili olduğu düşünülmüştür. Ayrıca bu özellikler,

amacı verimli, güvenilir, kusursuz ve öngörülebilir çıktılar üretmek olan kuruluşlarda yaygın bir şekilde benimsenmiştir (Cameron ve Quinn, 2006: 38). Weber'in bürokrasi teorisine dayanan hiyerarşi kültüründe, örgüt içi etkinlik ve işbirliğine vurgu yapılmakta, tahakküm edici örgütsel özelliklere sıkı bir şekilde bağlanılmaktadır (Ahmadi ve diğerleri, 2012).

Hiyerarşi kültüründe kontrol ve istikrara özel önem verilerek örgüt içi süreçlerin devamlılığına vurgu yapılmaktadır (Ashraf, Kadir, Pihie ve Rashid, 2013). Okul sistemleri, polis kuvvetleri gibi benzeri yapılar gücün merkezî bir yerde toplanması eğilimi göstermektedir. Çünkü bu tarz örgütlerin işleyişi üzerinde örgüt dışı kaynaklı kontrol mekanizmaları uygulanmaktadır (Mintzberg, 1980).

Hiyerarşi kültüründe yapısal bir kültür vurgulanmakta olup, kurallara, normlara, prosedürlere ve geleneklere uyularak örgütsel amaçlara ulaşılmaktadır (Doğan, 2012: 129). Hiyerarşi kültürünün hâkim olduğu örgütlerde çevre, resmî ve yapısaldır. Liderler verimliliğe odaklanırlar. Resmî kural ve politikalar örgütü bir arada tutmaktadır. Hedefler, istikrar, tutarlılık ve sonuçların tekdüzeliği üzerine belirlenmektedir. Kalite, ölçme ve süreçlerin kontrolü ile geliştirilmektedir. Demiryolu veya yük nakliye şirketleri bu kültür türü ile uyumlu örgütlerdir (Polding, 2016).

Hiyerarşi kültüründe örgütü bir arada tutan temel bağ, kurallar, politikalar, prosedürler, anlaşılır tanımlamalar ve görevler temelli olup, stratejik vurgular arasında istikrar ve işlerin düzenli yürütülmesi yer almaktadır (Cameron ve Freeman, 1991). Hiyerarşi kültüründe yer alan rekabetçi değerler, düzeni, kuralları ve düzenlemeleri vurgulamaktadır. İşlemler, gözetim, değerlendirme ve yönlendirmeler altında gerçekleşmektedir. Açıkça tanımlanmış hedeflerin başarımı ve tutarlılık iş etkinliğini tanımlamaktadır (Deshpande, Farley ve Webster, 1993). Hiyerarşi kültüründe örgüt, yapısal ve kurallarla yönetilen resmî bir çalışma ortamına sahiptir. Liderler, iyi birer koordinatör veya organizatör olmaktan yana gurur duymaktadırlar. Uzun vadeli yaklaşımda, istikrarlı, verimli ve doğru bir şekilde yürütülen operasyonlar önem arz etmektedir. Güvenilirlik, doğru iş zamanlaması ve düşük maliyet sunma, başarının ana unsurlarıdır (Garcia ve diğerleri, 2012).

Hiyerarşi kültüründe karar verme, standartlaştırılmış kurallar, kontrol mekanizmaları ve denetim, başarının temel faktörleridir. Örgütün uzun vadeli hedefleri, istikrar,

öngörülebilirlik ve verimlilikten oluşmaktadır. İnsanların ne yapması gerektiği prosedürlerde tanımlanmaktadır. Resmî politikalar, örgüt üyelerini birbirine bağlar ve örgütün uzun vadeli hedefi, operasyonel verimlilik ile performans istikrarı sağlamaktır (Dadgar, Marzooghi, Torkzadeh, Mohammadi ve Barahouei, 2013).

Hiyerarşi kültürünün hâkim olduğu örgütlerde, kurallar, düzenlemeler, prosedürler ve yöntemler bağlamında görevler ve çalışma kriterleri tanımlanmaktadır. Tüm kural ve prosedürler, işin kim tarafından yapılacağını, kimin işten sorumlu olduğunu ve kimin kime rapor sunacağını belirlemektedir. Bu, her şeyin önceden planlandığı ve belgelendiği anlamına gelmektedir. Her şey, örgütü verimli hâle getirmek ve öngörülemeyen koşulları karşılayabilmek için yazılmakta ve koordine edilmektedir. Bu noktada örgütü bir arada tutan ana tema dokümante edilmiş kural ve prosedürlerdir. Dolayısıyla sorumluluk ve diğer koşullar açısından herhangi bir belirsizlik bulunmamaktadır (Gull ve Azam, 2012).

İçsel Süreç Modeli'ni yansıtan hiyerarşi kültürü öncelikle örgütün iç ortamıyla ilgilidir (Bkz. Şekil 2.2). Hiyerarşi kültüründe iç verimlilik, tekdüzelik, istikrar, kontrol, süreklilik, koordinasyon ve değerlendirme gibi hususlara odaklanılmakta, ölçüm, dokümantasyon ve bilgi yönetimi gibi süreçlere önem verilmektedir. Hiyerarşi kültürünün hâkim olduğu örgütler, konsolidasyon, denge ve 'sosyoteknik' sistemin idamesi doğrultusunda hareket etmektedir. Bu tür örgütler, güvenlik anlayışı, kural ve düzenlemeler tarafından motive edilmektedir. Hiyerarşi kültüründe liderler önem taşımaktadır. Liderler, muhafazakâr ve ihtiyatlı davranarak teknik konulara büyük önem atfetme eğilimindedirler ve ayrıca denetim, istikrar ve verimlilik gibi konularda örgüt etkinliğini değerlendirmektedirler. Etkinlik kriterleri, kontrol, istikrar ve verimlilik üzerine kuruludur (Denison ve Spreitzer, 1991).

Denison Örgüt Kültürü Modeli'ne göre hiyerarşi kültürünü yansıtan kültürel özellik tutarlılıktır. Bu özellikteki örgütler etkinliği, tutarlı, iyi koordine edilmiş ve iyi entegre olmuş güçlü kültürleri ile elde etmeye çalışmaktadır. Davranışlar, bir dizi temel değere dayalıdır. Liderler ve takipçileri, farklı görüş açılarında olsalar dahi anlaşmaya varma konusunda yeteneklidirler. Tutarlılık özelliği ortak bir zihniyet ve yüksek derecede uygunluk sonucu ortaya çıkan güçlü bir istikrar ve dâhili entegrasyon kaynağıdır (Denison ve diğerleri, 2004). Tutarlılık kültür özelliğine sahip bu örgütlerde hâkim olan hiyerarşi kültürü istikrarlı kültür olarak da adlandırılmakta olup, tekdüzelik, verimlilik, kural ve

düzenlemeler üzerinde durulmaktadır. Tutarlılığın vurgulandığı bu kültür türünde, örgüt tipik olarak resmî ve düzenli bir yeri yansıtmaktadır (Ebrahimi ve Naini, 2012).

Hiyerarşi kültürünü temsil eden bürokrasiler makine bürokrasisi ve profesyonel bürokrasi olarak ikiye ayrılmaktadır. Genellikle kitlesel üretim yapan örgütlerde görülen makine bürokrasisinde, üst kademeler ile operasyonel kısım arasında keskin bir ayrım bulunmakta, muhasebeciler, iş planlayıcıları ve iş analistleri gibi teknolojik yapı ve hukuk danışmanlığı, halkla ilişkiler gibi destek personeli örgütün büyük bir kısmını oluşturmakta, koordinasyon mekanizması olarak iş süreçlerinin standardizasyonu ve sınırlı yatay yerel yönetim uygulanmaktadır. Genellikle durgun çevrelerde, olgun örgütlerde ve sigorta kurumları, telefon şirketleri, posta müdürlükleri, vergi toplama daireleri gibi belirli kurumsal işleri yürüten devlet kuruluşlarında görülmektedir (Mintzberg, 1980). Makine bürokrasisinin hâkim olduğu hiyerarşi kültüründeki örgütlerin diğer örnekleri arasında otomobil üreticileri ve çelik üretim şirketleri bulunmaktadır. Yönetim genişliğinin dar olduğu ve üst yönetim ile alt seviyeler arasında sıralı kademelerin bulunduğu makine bürokrasisinde Max Weber'in ideal bürokrasisinin özelliklerinden birçoğuna rastlanmaktadır. Bununla birlikte bütün okulların tam manasıyla makine bürokrasisi kültürü ile uyumlu olduğunu söylemek mümkün olmamakla birlikte kamu okullarında makine bürokrasisinin birçok özelliği görülmektedir (Lunenburg, 2012). Hiyerarşi kültürünü temsil eden bir diğer bürokrasi türü de profesyonel bürokrasidir. Profesyonel bürokrasi yapısına sahip örgütler ise genellikle karmaşık ama durağan çevrelerde varlık göstermektedir. Karmaşıklık, ancak ileri eğitim programları ile öğrenilebilen bilgi ve yeteneklerin kullanımından kaynaklanmakta olup, durağanlık ise örgütte operasyonel manada işlerin belirli prosedürler çerçevesinde yürütüldüğünü göstermektedir. Dolayısıyla operasyonel manada profesyonel olarak işi yürütenlerin, örgütün genel prosedürleri çizgisinde kendi işlerinde özerkliğe sahip olmasından kaynaklı bu örgüt yapısında iş analistleri ve planlayıcıları düşük seviyede yer almaktadır. Bu tarz örgütler aynı zamanda işinde uzman yüksek eğitimli kişileri örgüte dâhil etmekte ve onlara özerklik sağlamaktadır. Profesyonel bürokrasi genellikle okul sistemlerinde, muhasebe şirketlerinde ve tekne imalat şirketlerinde görülmektedir (Mintzberg, 1980). Oldukça resmî bir yapı sunan, ancak alanında uzman operasyonel elemanlara özerklik sağlamak adına yerinden yönetim imkânı veren profesyonel bürokraside yüksek eğitimli profesyoneller örgüt müşterilerine uygun hizmetleri sunarlar. Üst düzey yönetim küçüktür ve az sayıda orta düzey yönetici vardır. İş analistlerini teşkil eden teknolojik yapı kısıtlıdır. Bununla birlikte profesyonel operasyonel kadronun büro ve

bakım desteğini sağlamak için çok sayıda destek personeli bulunmaktadır. Bu örgütlenme biçiminin örnekleri arasında üniversiteler, hastaneler ve büyük hukuk firmaları bulunmaktadır. Kamu okullarında profesyonel bürokrasinin birçok özelliği görülmektedir. Örneğin üniversite öğretim elemanları sınıf ortamlarında meslektaşları ve idari üstlerinden izole bir şekilde öğrencileri ile yakın temasta bulunurlar ve zorunlu kılınan müfredatın kısıtlamaları dâhilinde öğrencilerine kendi profesyonelliklerine ve stillerine uygun eğitim sunarlar (Lunenburg, 2012).

2.4.2. Pazar

Şekil 2.3'ün sağ alt çeyreğinde yer alan pazar kültürü, dışsal konumlama ve mekanik süreçlere yönelikliği ifade etmektedir. Tedarikçiler, müşteriler, yükleniciler, ruhsat sahipleri, birlikler ve düzenleyiciler gibi dışsal çevreyle olan işlemlere odaklanılmaktadır. Merkezî karar verme, uzmanlaşılmış işler ve kurallar ile içsel kontrolün sağlandığı hiyerarşi kültürünün aksine pazar kültüründe işlemler, öncelikle parasal işlemler gibi pazar mekanizmaları dikkate alınarak yürütülmektedir. Pazar kültürüne sahip örgütlerde rekabetçilik ve üretkenliğin elde edilmesinde, dışsal konumlamaya ve kontrole yüksek vurgu yapılmaktadır. Sonuç odaklı bir çalışma ortamının yansıtıldığı pazar kültüründe, liderler sağlam duruşlu ve titiz çalışan üretici ve rekabetçi birer yönetici olarak görülmektedir. Kazanmaya verilen önem, örgütü bir arada tutmaktadır. Rekabetçi faaliyetler ve ulaşılması zor hedefleri elde etme, uzun dönemli örgüt stratejisinde yer almaktadır. Pazar payı ve pazara girme başarı ölçütüdür. Rakipleri geçme ve pazar liderliği önemlidir (Cameron ve Quinn, 2006: 39-40).

Pazar kültüründe, kontrollü bir yapıya ve örgüt dışı konulara odaklanılmaktadır. Bu kültüre sahip örgütlerde, yüksek verimlilik ve rekabet edebilirliğe ulaşmak için dışsal gözlem ve değişime karşı direnç sergilenmektedir (Ahmadi ve diğerleri, 2012). Pazar kültüründe dışsal çevreye odaklanılmakla birlikte kontrol ve istikrara önem verilmektedir (Ashraf ve diğerleri, 2013).

Pazar kültüründe sonuçların önemli sayıldığı ve ödüllendirildiği bir kültür yapısına vurgu yapılmakta olup, örgütsel amaçlara pazar payı egemenliği elde etme inancıyla ulaşılmaktadır (Doğan, 2012: 129). Diğer bir ifadeyle pazar kültürü, rekabeti ve hedefleri vurgulayan sonuç odaklı bir örgütü yansıtmaktadır. Liderler, kazanma değerine odaklanan

kişilerdir. Başarı, pazar payı ve kârlılık üzerine kuruludur. Kalite, müşteri tercihleri ve pazar rekabet gücü ölçülerek geliştirilmektedir. Oto bayileri bu kültürle uyumlu örgütlerdir (Polding, 2016).

Pazar kültüründe örgütü bir arada tutan temel bağ, sonuç odaklılık, üretim ve rekabet temellidir. Stratejik vurgular arasında rekabet avantajı ve pazar üstünlüğü elde etme yer almaktadır (Cameron ve Freeman, 1991). İşlemler, pazar mekanizmaları tarafından yürütülmektedir. Örgütsel etkinliğin ölçümünde dikkate alınacak esas ölçüt, pazar koşullarında ulaşılan üretkenlik seviyesidir (Deshpande ve diğerleri, 1993). Pazar kültüründe sonuç odaklı bir örgüt kültürü söz konusudur. Liderler, zorlu mücadelelere giren, üretken ve rekabetçi karaktere sahiptirler. Örgüt, kazanma vurgusu ile bir arada tutulmaktadır. Kurumsal itibar ve başarı elde etme, sürekli olarak örgütün hedefinde yer almaktadır (Garcia ve diğerleri, 2012).

Kültürel manada kullanılan pazar teriminin, pazarlama işlevi veya piyasadaki tüketici kavramları ile benzerliği yoktur. Aksine pazar kültürü, bir pazarın kendisi olarak işlev gören bir örgüt türü anlamına gelmektedir. Pazar kültüründe örgüt içi işler yerine örgüt dışı ortama odaklanılması söz konusudur. Pazar, öncelikle para değişimi gibi ekonomik piyasa mekanizmalarıyla işlemektedir. Pazar kültürünün hâkim olduğu örgütlerin temel odağı, rekabet avantajı yaratmak için, diğer dış çevre unsurlarıyla alışveriş, satış ve sözleşme gibi işlemleri yürütmektir. Kârlılık, nihai sonuçlar, piyasa konumunda güç elde etme, zorlu hedefleri başarma ve müşteri tabanlarını koruma, pazar kültüründeki örgütlerin temel amaçları arasında yer almaktadır. Doğal olarak pazar kültürünün hâkim olduğu örgütlerde kabul edilen temel değerler, rekabet gücü ve üretkenliktir. Rekabet edebilirlik ve üretkenlik, dışsal konumlama ve kontrol vurgulanarak sağlanmaktadır (Shurbagi ve Zahari, 2012).

Pazar kültürünün baskın olduğu örgütler, verimlilik ve rekabet değerlerinden kazanç elde etmektedir. Rekabet başarısı, dışsal çevrenin kontrolüne ve başarıya vurgu yapılarak sağlanmaktadır. Pazar kültürünün temel varsayımları ve temel değerleri dinamik stratejilere, kârlılığı ve etkinliği elde etme amaçlarına dayanmaktadır. Bu kültürde, çalışmalar sonuç odaklı yürütülmektedir. Liderler ısrarcıdır ve örgüt üyelerini bir arada tutan bağ, rekabetçi çalışmalar, uzun vadeli başarılara ulaşılması ve amaçların yerine getirilmesi üzerine yapılan vurgular temelindedir. Pazar kültüründe başarı terimi, pazarın

içerisinde rekabetçi bir üye olmakla ifade edilmektedir (Dadgar ve diğerleri, 2013). Örgüt kültürünün, birbirinden ayırt edilebilir ancak birbiriyle ilişkili paylaşılan temel değerler, davranışsal normlar, yapay dokular ve davranış örüntüleri olmak üzere dört bileşenden oluştuğu dikkate alındığında, pazar kültüründe bu dört bileşenin tamamı pazar odaklılığı yansıtmaktadır (Homburg ve Pflesser, 2000).

Pazar kültürü, örgütsel başarının çıktıya dayandığı bir kültürdür. Örgüt ve paydaşları çok çalışma gerektiren bir çevrede birleşmekte ve üst yönetim istenilen sonuçların elde edilmesini ciddi derecede önemsemektedir. Üst yönetim her zaman başarıyı aramakta ve bütün örgüt bunun için birlikte çalışma sergilemektedir. Temel amaç, örgütün amaçlarına etkin ve verimli bir şekilde ulaşmak, pazar payı ve pazar liderliği açısından üstünlük elde etmektir. Pazar kültürüne sahip örgütler, rekabetin üstesinden gelmenin ve pazardan azami pay elde ederek sektörün en üst sıralarında yer almanın yollarını bulmaktadır (Gull ve Azam, 2012).

Rasyonel Amaç Modeli'ni yansıtan pazar kültüründe, verimlilik, performans, hedeflerin gerçekleştirilmesi ve başarı vurgulanmaktadır (Bkz. Şekil 2.2). Bu kültür türüne sahip örgütlerin amacı, iyi tanımlanmış hedeflerin peşinde koşmak ve gerçekleşmesini sağlamaktır. Motive edici faktörler, rekabeti ve önceden belirlenmiş sonuçların başarıyla elde edilmesini içermektedir. Liderler, hedefe odaklı, yönlendirici, üretken ve görevsel yaklaşımda bulunmakta, sürekli olarak örgütsel yapıyı kurmakta ve verimliliği teşvik etmektedirler. Etkinlik kriterleri, planlama, üretkenlik ve verimlilik üzerine kuruludur (Denison ve Spreitzer, 1991).

Pazar kültürü, çevreye uyumu, tutum ve davranışları pazara yönelik olan bir örgütün baskın ve dinamik bölümünü ifade etmektedir. Bu tanım dâhilinde öncelikli olarak pazar kültürü bileşenlerine (uyum, tutum ve davranışlara) atıfta bulunulmaktadır. Tanımda yer alan "dinamik" kavramı, bileşenleri birbirine bağlayan süreçleri ifade etmektedir. "Bölüm" tabiri ise kültürel çoğulculuğu ima etmektedir. Son olarak pazar odaklı bir kültürün örgüt çapında hâkim olduğu düşünüldüğünde, "baskın" ifadesi ile pazar odaklı kültürün alternatif diğer kültürlere nazaran baskın olduğu anlaşılmaktadır. Pazar odaklı kültürün gelişimi iki konuya bağlıdır. Bunlardan ilki, pazar odaklı kültürel varsayımların, yapıtların ve değerlerin varlığıdır. Diğeri ise pazar odaklı kültürün diğer kültürleri kontrol etme yeteneğini etkileyen faktörlerin analiz ediliyor olmasıdır. Pazar odaklı bir kültüre ilişkin

varsayımlar şunları içermektedir (Harris, 1998):

- Örgüt var olmak için çevreye bağımlıdır.
- Çevre örgütü etkilemektedir.
- Örgüt, çevresel etkileri analiz etme, öngörüde bulunma ve tepki verme yeteneğine sahiptir.
- Müşteri taleplerini, istek ve ihtiyaçlarını karşılamak mümkündür. Bu durum, uzun vadede kârlılık sağlamakta ve dolayısıyla örgüt hayatta kalma mücadelesinde başarılı olmaktadır.
- Örgütsel uyum, verimliliği ve etkinliği artırmaktadır.

Denison Örgüt Kültürü Modeli'ne göre pazar kültürünü yansıtan kültürel özellik misyondur. Bu özelliğe sahip başarılı örgütler, örgütsel stratejik hedefleri tanımlayan ve örgütün gelecekte nasıl görüneceğine dair vizyonunu ifade eden net bir amaç ve yön duygusuna sahiptir. Bir örgütün misyonu değiştiğinde, örgüt kültürü de değişmektedir (Denison ve diğerleri, 2004). Misyon kültür özelliğine sahip bu örgütlerde hâkim olan pazar kültürü hedef odaklı kültür olarak da adlandırılmakta olup, bu kültür türünde rekabete, hedeflere ulaşmaya, üretime, verimliliğe ve kâr odaklı önlemler almaya odaklanılmaktadır (Ebrahimi ve Naini, 2012).

Bölümlenmiş örgüt yapısına sahip bazı örgütlerde pazar temelli örgüt kültürü görülebilmektedir. Bu tarz örgütlerde üst yönetim, alt bölümlerin hedeflerini koordine eden mekanizmayı kurmaktadır. Her bir alt bölüm özerklik içinde dışsal kontrol mekanizmaları altında faaliyetlerini sürdürmektedir. Her bir bölüm, entegre bir sistem olarak örgütün genel hedefleri doğrultusunda birleşmektedir. Bölümlerin dışsal çevre ile ilgili kontrolleri merkezî bir şekilde yürütülmektedir. Bu örgütlenme biçimine örnek olarak ürün ve servis bazında pazar bölümlendirmelerine sahip örgütler verilebilir (Mintzberg, 1980).

2.4.3. Klan

Şekil 2.3'ün sol üst çeyreği klan kültürü olarak adlandırılmakta olup, bu kültür türünde içsel devamlılık ve organik süreçlere vurgu yapılmaktadır. Aile tipi örgüte olan benzerlikten dolayı bu kültür türüne klan denmektedir. Paylaşılan değerler ve hedefler,

bireyler arası bağlılık, bireysel katılımcılık ve biz olma duygusu klan kültürünü betimlemektedir. Klan kültüründe iktisadi bir teşekkülden ziyade geniş bir aile algısı hâkimdir. Takım çalışması, çalışanların katılımcılığı ve örgüte duydukları sadakat, klan kültürünün temel özellikleridir. Çalışanların kendilerinden çok şeyler paylaştığı, arkadaşça kurulu bir çalışma ortamını yansıtan klan kültürü geniş bir aile gibidir. Liderler, akıl hocası ve hatta anne baba figürü olarak görülmektedir. Sadakat ve gelenekler örgütü bir arada tutmakta olup, örgüte duyulan bağlılık yüksek seviyededir. Yüksek düzeyde örgüte duyulan bağlılık ve moral ile elde edilecek kişisel gelişimden uzun dönemli kazanç elde etme vurgusu vardır. Başarı, içsel örgüt iklimi ve insan odaklı olarak tanımlanmaktadır. Klan kültürüne sahip örgütler, takım çalışması, çalışan katılımcılığı ve fikir birliği temelinde kuruludur (Cameron ve Quinn, 2006: 41-43). Klan kültürü aile kültürü gibidir. Örgüt içi meselelere önem verilmekte ancak istikrardan ziyade esneklik üzerine odaklanılmaktadır. Ortaklık, ekip çalışması ve çalışanların örgütsel bağlılığı klan kültürünün temel özellikleri arasında yer almaktadır (Ahmadi ve diğerleri, 2012). Klan kültürü, esneklik hissi ile örgüt içinde yaşanan olaylara, insanlara ve müşterilere odaklanılmasını sağlamaktadır (Ashraf ve diğerleri, 2013).

Klan kültüründe işbirliğine, örgütsel bütünleşmeye ve uyuma vurgu yapılmakta olup, örgütsel amaçlara ortak değerlerin paylaşılması yoluyla ulaşılmaktadır (Doğan, 2012: 129). Klan kültürü dostça ve ailevi bir çalışma ortamını yansıtmaktadır. Liderler, ekip çalışmasını ve iletişimi teşvik eden mentorlar (rehberler) olarak görülmektedir. Personel, paylaşılan değerler boyutunda birbirine bağlılık hissetmektedir. İletişim, bir iyileştirme aracıdır. Sosyal hizmetler ya da inanç temelli örgütler bu kültürle uyumludur (Polding, 2016).

Klan kültüründe örgütü bir arada tutan temel bağ, gelenekler ve kişiler arası uyum temellidir. Stratejik vurgular arasında insan kaynakları gelişimi, yüksek seviyede moral ve örgüte duyulan bağlılık yer almaktadır (Cameron ve Freeman, 1991). Rekabetçi Değerler Modeli'ndeki pazar kültürünün karşıtı klan kültürüdür. Diğer bir ifadeyle rekabetçi değerler terminolojisinin manası gereğince klan kültürünün içerdiği değerler, pazar kültürününkilerle zıttır. Klan kültürü pazar kültürünün aksine, örgüte olan bağlılığı, çalışan katılımcılığını ve takım çalışmasını ifade etmektedir. Örgüt üyelerinin katılımcılığı ile sağlanan örgüte olan bağlılık ve çalışanların bireysel tatmini, pazar kültüründeki finansal ve pazar payı hedeflerine ulaşmaya kıyasla daha fazla önem taşımaktadır (Deshpande ve

diğerleri, 1993). Bir aile yapısını andıran klan kültüründe örgüt yöneticileri, lider ve rehber olarak görülmekte olup babacan yapıya sahiptirler. Örgütsel uyum ve ahlaki değerler çok önemlidir. Başarı, çalışanlara ilgi duyulması, müşteri ve tüketicilere karşı duyarlı davranış sergilenmesi ile tanımlanmaktadır (Garcia ve diğerleri, 2012).

Klan kültürünün temel özellikleri arasında, ekip çalışması, çalışanların katılımı ve örgütsel bağlılık yer almaktadır. Çalışma grupları, grup performansına dayalı olarak ödüllendirilmekte olup, ödüller kişisel değildir. Çalışanlar, çalışmalarının ve örgütlerinin iyileştirilmesi yönünde teşvik edilir. Klan kültüründe, çevre arkadaş ortamı olarak görülmekte, insanlar işleri paylaşmakta ve örgüt geniş bir aileye benzemektedir. Örgüt liderleri ve yöneticileri, örgüt üyelerini sadakate, ritüellere ve inançlara bağlayan hususları gözlemlemektedirler. Örgütsel bağlılık, örgüt çalışanlarında yaygın olan bir kavramdır. Diğer bir ifadeyle klan kültürünün hâkim olduğu örgütler, insan kaynaklarının geliştirilmesi ve insanların morali ile ilişkili olan kavramlar üzerinde durmaktadır. Bu bağlamda klan kültürünün temel varsayımları şunlardır (Dadgar ve diğerleri, 2013):

- Çevre, grup kültürü ve insan kaynakları ile iyi yönetilmektedir.
- Müşteriler iş ortağı olarak kabul edilmektedir.
- Üst yönetim, çalışanlara güç vermekten ve çalışanların katılımını, bağlılık ve sadakatini artırmaktan sorumludur.

Klan kültürü, çalışanların kendilerini rahat hissettikleri ve tereddüt etmeden diğer çalışanlarla kolayca paylaşımda bulunabilecekleri bir ortam sunmaktadır. Çalışma ortamı arkadaşça kurulu, keyifli ve sosyal bir çevre olarak algılanmaktadır. Örgütün üst kademesi kanaat önderleri olarak değerlendirilmektedir. Bu tür örgütlerde, samimi bir ortam oluşumu için gerekli bazı faktörler takip edilmektedir. Bu faktörler, güvenilirlik, gelenekler, inançlar ve örgüt içi işbirliği niteliğindedir. Örgütler, çalışanların uzmanlıklarını, deneyimlerini, güvenlerini, aralarındaki koordinasyonu artırmak, kariyerlerini ilerletmek ve çalışanlarla uzun vadeli bir ilişki kurmak için ortam sağlamaya çalışmaktadır. Çünkü günümüzde, örgütlerin yetenekli çalışanları örgütte tutmaları çok zordur. Bu nedenle bu faktörler, örgütlerin hedeflerini etkin ve verimli bir şekilde karşılamasına yardımcı olabilmektedir. Klan kültüründe başarı açısından değer, örgütün çalışanlarına sağladığı çevreye bağlıdır. Örgütsel başarı, örgütteki çalışanların

koordinasyonuna ve güvenilirliğine bağlıdır. Klan kültürüne sahip örgütlerde, bu özellikleri elde etmek için büyük bütçeler ayrılmaktadır (Gull ve Azam, 2012).

Klan kültür ilkeleri, örgütlerin çalkantılı bir ortamda stratejik olarak yönetilebilmesi için kullanılacak yönergeleri ortaya koyabilmektedir. Çalkantılı koşullar altında örgütler, belirsizlikleri savuşturabilmek için kendi yapısal konsolidasyonunu sağlamak durumundadır. Böyle bir yapısal konsolidasyon, toplumsal özel bölgelerin veya klanların oluşmasıyla sağlanabilir. Klan kültürüne sahip bir örgütün yapısal özellikleri, örgütün bir işte büyümesi ve gelişmesi ile ortaya çıkmaktadır. Klan kültürünü benimseyen bir örgüt, kendisini koruyacak ve iç istikrarı sağlayacak fazlasıyla yönetilebilir bir sosyal ortam elde etme eğilimindedir. Klan kültürünün hâkim olduğu örgütlerin bugüne kadar belirlenmiş olan başlıca özellikleri şunlardır (Chan, 1997):

- Bireysel klan üyesinin önemine inanılmaktadır.
- İç istikrarın sağlanmasına önem verilmektedir.
- Örgütsel kaynaşmaya vurgu yapılmakta ve bu çerçevede biz zihniyetin içselleştirilmesi sağlanmaktadır.
- Örgütü dış çevresinden güçlü bir şekilde ayırmaya ve kendi kendine yeterlik seviyesine ulaşmak için dış istikrarsızlığa karşı savunma duvarının oluşturulmasına çalışılmaktadır.
- Kültürün zayıflatılmasını engellemek için, bilişsel kontrol mekanizmaları, sosyokültürel inançlar ve bireylerin kendilerini tanıtmasında kullanılan davranış biçimleri gibi sosyokültürel bariyerler kullanılmaktadır.
- Klan kimliğinin ve kültürün önemine inanılmaktadır. Bu uğurda her ne pahasına olursa olsun gelenekler, ritüeller, ayinler ve kahramanlar korunmaktadır. Klanın sembollerine saldırmak, örgüte saldırmakla aynı şeydir.
- Klan üyelerinin yabancılara oranla daha büyük bir güven derecesi ve esneme kabiliyeti vardır. Ciddi cezaların kullanımıyla örgütsel onur ve örgütün varlığı korunmaktadır.
- Kuralların yorumlanması ve cezalandırmalara karar verilmesi klanın yaşlı üyeleri tarafından gerçekleştirilmektedir.

Klan kültürü, kültürel açıdan homojen bir örgütü yansıtmaktadır. Klan üyelerinin birçoğu

ortak hedeflere ulaşma yolunda ortak değerler, hedefler seti ve inançları paylaşmaktadırlar. Klan kültürü, her bir örgüt üyesini sosyalleşme ile birbirine bağlayarak bireysel amaçları örgütsel amaçlar ile birleştiren işlev üstlenmektedir. Böylelikle örgüt üyelerinin örgüte hizmet etme motivasyonu sağlanmaktadır. Ortak hedefler, bireyleri tamamen sosyalleştirmekte ve onlara işleri gerçekleştirmenin en iyi yolu hakkında bilgi vermektedir. Dolayısıyla karar verme süreci neredeyse içgüdüsel bir hâl almaktadır. Bununla birlikte bu sosyalleşme, ancak yeni üyelerin örgüt kültürüyle benzer değerleri paylaşmasıyla mümkün olmaktadır. Örgüt üyeleri kendilerini tamamen örgüte entegre ederek bireysel yaklaşımdan daha fazla kazanç elde edeceklerini bilmektedirler (Ouchi ve Price, 1993).

Denison Örgüt Kültürü Modeli'ne göre klan kültürünü yansıtan kültürel özellik bağlılıktır. Bu özelliğe sahip örgütler etkinliği elde etmek için, personelini güçlendirmekte, örgüt yapısını takımlardan kurmakta ve her kademede insan gücünün kabiliyetini geliştirmektedir. Yöneticiler ve çalışanlar, işlerine sıkı sıkıya bağlıdırlar ve örgütün bir kısmının dahi olsa sahibi olduğunu hissetmektedirler. Bireyler, çalışmalarını etkileyecek kararlara katılabileceklerini bilmektedirler. Çalışmalar, doğrudan örgüt hedeflerine bağlı olarak yürütülmektedir (Denison ve diğerleri, 2004). Bağlılık kültür özelliğine sahip bu örgütlerde hâkim olan klan kültürü işbirliği kültürü olarak da adlandırılmakta olup, bu kültür türünde yardımlaşma, bağlılık, bilgi paylaşımı, güven, personel güçlendirme ve takım çalışması üzerinde durulmaktadır (Ebrahimi ve Naini, 2012).

Grup kültürü olarak da adlandırılan klan kültüründe öncelikli olarak insan ilişkileri dikkate alınmaktadır. İnsan İlişkileri Modeli'ni yansıtan bu kültür türünde, esneklik vurgulanmakta ve örgüt içine odaklanılmaktadır (Bkz. Şekil 2.2). Grupların devamlılığı esastır. Bir gruba ait olmak, güven ve katılımcılık temel değerlerdir ve birincil motivasyon faktörleri bağlanma, kaynaşma ve üyeliktir. Liderler, katılımcı, düşünceli ve destekleyici olma eğiliminde olup takım çalışması yoluyla etkileşimi kolaylaştırmaktadırlar. Etkinlik kriterleri, insan potansiyelinin geliştirilmesi ve grup üyelerinin örgüte bağlılığı üzerine kuruludur (Denison ve Spreitzer, 1991).

2.4.4. Adhokrasi

Şekil 2.3'ün sağ üst çeyreğinde yer alan, dışsal konumlama ve organik süreçler üzerine kurulu dördüncü kültür türü de adhokrasi olarak adlandırılmaktadır. Adhokrasi kelimesinin

kökü, İngilizce "ad hoc"a dayanmakta olup geçici, özel amaçlı ve dinamik anlamlarına sahiptir. Adhokrasi kültürü, genellikle uzay, yazılım geliştirme, danışmanlık ve film yapımcılığı gibi endüstrilerde faaliyet gösteren örgütlerde görülmektedir. Bu tür örgütler, yaratıcı ve yenilikçi olmaya ve doğan yeni fırsatlara çabuk uyum sağlamaya çalışır. Pazar ve hiyerarşi kültürlerinin aksine, adhokrasi kültüründe merkezî güç veya otorite ilişkileri bulunmamaktadır. Güç, sorunlarla karşılaşıldığı ana dayalı olarak bireyler veya görev takımları arasında iletilmektedir. Adhokrasi kültürü, dinamizm, girişimcilik ve yaratıcı çalışma alanlarıyla tanımlanmaktadır. Çalışanlar, ellerini taşın altına koymaya ve risk almaya isteklidirler. Adhokrasi kültürünün hâkim olduğu örgütlerde liderler, vizyon sahibi, yaratıcı ve risk odaklı olarak görülmektedir. Örgütü bir arada tutan bağ, tecrübeye ve yenilikçiliğe olan bağlılıktır. Stratejik odak noktası, yeni bilgi, ürün ve servislere sahip olmada lider olabilmektir. Değişime ve karşılaşılabilecek yeni zorluklara hazır olmak önemlidir. Adhokrasi kültürünün uzun dönemli stratejileri arasında hızlı büyüme ve yeni kaynaklar elde etme yer almaktadır. Başarı, kendine özgü, orijinal ürün ve servisler üretmek ile tanımlanmaktadır (Cameron ve Quinn, 2006: 43-45). Adhokrasi kültüründe örgütler dışsal çevreye yönelmekte, esneklik ve değişimi vurgulamaktadır (Ahmadi ve diğerleri, 2012). Diğer bir ifadeyle adhokrasi kültürünün odağı, bireysellik, esneklik ve dışsal çevre üzerinedir (Ashraf ve diğerleri, 2013).

Adhokrasi kültüründe girişimciliğe vurgu yapılmakta olup, örgütsel amaçlara belirsizlikle başa çıkma, esneklik, yenilik yapma ve yaratıcılıkla ulaşılmaktadır (Doğan, 2012: 129). Örgüt ortamı yaratıcılık ile tanımlanmaktadır. Çalışanlar risk almaktadırlar. Liderler yenilikçi ve vizyoner (ileri görüşlü) olarak görülmektedir. Örgütü bir arada tutan bağ yeniliktir. Öne çıkan yeni ürünler başarıyı tanımlamaktadır. Bireysel girişkenlik değer ifade etmektedir. Kalite, ihtiyaçların önceden tahmin edilmesi ve yeni ürün standartlarının oluşturulması ile geliştirilmektedir. Apple gibi teknoloji odaklı şirketler bu kültür türü ile uyumlu örgütlere örnek olarak verilebilir (Polding, 2016).

Hiyerarşi kültürünün aksine adhokrasi kültüründe örgütü bir arada tutan temel bağ, girişimciliğe, esnekliğe ve risk almaya olan bağlılık temelli olup, stratejik vurgular arasında yenilikçilik, büyüme ve yeni kaynaklar elde etme yer almaktadır (Cameron ve Freeman, 1991). Rekabetçi değerler terminolojisinin manası gereğince adhokrasi kültürünün taşıdığı değerler, hiyerarşi kültürününkilerle zıttır. Adhokrasi kültüründe hiyerarşi kültürünün aksine, girişimciliğe, yenilikçiliğe ve çevresel uyuma vurgu

yapılmaktadır. Örgüt genelinde esnek ve hoşgörülü bir ortam kanısı hâkimdir. Örgütsel etkinlik, örgütün büyümesi için yeni pazarlar ve yönler bulunması ile tanımlanmaktadır (Deshpande ve diğerleri, 1993). Adhokrasi kültürüne sahip bir şirket, dinamik, girişimci ve yaratıcı bir iş yeridir. Liderler, yenilikçi ve risk alma sorumluluğunu üstlenenler olarak görülmektedir. Örgüt, deneyler ve yenilikçilik ile bir arada tutulmaktadır. Başarının kaynağı, yeni, benzersiz ürün ve hizmetler üretmektir (Garcia ve diğerleri, 2012).

Adhokrasi kültürü, yeni yüzyılın karmaşık ortamları ve hızlı değişen koşulları ile izah edilebilmektedir. Örgütler yenilikçilik, yaratıcılık ve öncülük varsayımlarından hareketle başarıya ulaşmaktadır. Adhokrasi kültüründe, yönetimin girişimcilik ve yaratıcılık alanındaki eğitimleri dikkate alınmakta, yaratıcılık vasıtasıyla üstünlük ve kazanç elde etme vurgusu yapılmaktadır. Bu bağlamda adhokrasi kültürünün temel özellikleri şunlardır (Dadgar ve diğerleri, 2013):

- Örgütler, sabit bir örgütsel yapı çizelgesine sahip değildir. Organizasyon şeması, görev misyonu için hızlı ve geçici olarak oluşturulmaktadır.
- Çalışma ortamı geçicidir. Yöneticinin sabit bir görev yeri yoktur ve gerekli olduğu durumda çalışma ortamı geçici olarak oluşturulmaktadır.
- Roller geçici olarak oluşturulmaktadır. Çalışma üyeleri geçici olarak belirlenmekte ve sorumluluklar geçici olarak devredilmektedir.
- Yaratıcılık ve yenilik teşvik edilmektedir. Geçici olarak oluşturulan adhokrasi kültürü, hiyerarşi kültürünün genellikle hâkim olduğu büyük devlet ortamları için uyumsuzdur.

Adhokrasi kültürü, enerjik, kendi kendine düzen kuran, çalışanların ve yönetimin yaratıcı işler konusunda istekli oldukları ve tüketicilerin değişen ihtiyaçlarına göre yeni teklifler geliştirdikleri bir kültürü ifade etmektedir. Bütün örgüt, farklı ve yeni bir şekilde teklif geliştirmeye ve yenilikçi fikirler bulmaya çalışmaktadır. Önderler, yeni deneyimler ışığında yaratıcılıkla fikirler geliştirmektedirler. Bu durum, çalışanlara bilgi, deneyim ve fikirlerini geliştirmede yardımcı olmaktadır. Böylelikle çalışanlar tekliflerini tüketicilerin değişen istek ve ihtiyaçlarına göre yapabilmektedirler. Günümüzde örgütler arası sektörel manada büyük bir rekabet vardır ve bütün örgütler kendi sektörlerinde lider olma yarışındadır. Bu senaryoda, örgütler her zaman kendilerini değişime ayak uydurmaya ve

rakiplerine nazaran en üst sıralara yerleşmeye çalışmaktadır. Bu manada örgütsel başarı, yeni fikirler geliştirmek ve bu fikirleri tüketicilerin gözünde benzersiz kılmak ile tanımlanmaktadır. Adhokrasi kültürünün hâkim olduğu örgütler için ana tema, tüketiciler tarafından kolayca fark edilebilecek sunumlara sahip olmaktır (Gull ve Azam, 2012).

Denison Örgüt Kültürü Modeli'ne göre adhokrasi kültürünü yansıtan kültürel özellik uyarlanabilirliktir. Uyarlanabilir örgütler, müşterileri tarafından yönlendirilen, risk alan, hatalarından öğrenen ve değişim yaratmada yetenek ve tecrübeye sahip olan öğrenen örgütlerdir. Uyarlanabilir özellikteki örgütler müşterilerine değer sağlamak adına yeteneklerini geliştirmek için sürekli olarak sistemlerini değiştirmektedir (Denison ve diğerleri, 2004). Uyarlanabilir kültür özelliğine sahip bu örgütlerde hâkim olan adhokrasi kültürü yenilikçi kültür olarak da adlandırılmakta olup, bu kültür türünde yaratıcılığa, girişimciliğe, uyarlanabilir olmaya, dinamizme vurgu yapılmakta ve tamamen yaratıcı, dinamik bir çalışma ortamı desteklenmektedir (Ebrahimi ve Naini, 2012).

Açık Sistem Modeli'ni yansıtan adhokrasi kültürü, biçim ve işleyiş açısından hiyerarşi kültürü ile taban tabana zıttır (Bkz. Şekil 2.2). Adhokrasi kültürü tipik olarak genişleme ve dönüşüm yolunda ilerlemektedir. Ayrıca kavrayış, değişim ve adaptasyonu vurgulayarak genel sistemin rekabetçi konumuna odaklanmaktadır. Adhokrasi kültüründe esneklik ve değişim örgüt varlığının temelini oluşturmaktadır ve örgütün ana odak noktası dış çevredir. Bu kültürün diğer önemli özellikleri arasında büyüme eğilimi, kaynak arayışı, yaratıcılık ve dış çevreye uyum yer almaktadır. Örgüt üyelerini motive eden kavramlar, büyüme, teşvik, yaratıcılık ve çeşitliliktir. Adhokrasi kültüründe liderler, risk alma, girişimci ve idealist olma eğiliminde olup örgüt vizyonunu geliştirmeye yatkındırlar. Liderler ayrıca sürekli olarak ek kaynaklar edinmeye, görünürlük ve meşruiyet kazanmaya ve dışardan destek almaya çalışmaktadırlar. Adhokrasi kültüründe etkinlik kriterleri, büyümeyi, yeni pazarların oluşturulmasını ve kaynak teminini hedef koymaktadır. (Denison ve Spreitzer, 1991).

Adhokrasi kültürü, davranış kalıplarının çok az seviyede resmî hâle getirildiği, merkeziyetçiliğin olmadığı ve iş uzmanlıklarının yatayda genişlediği organik bir örgüt yapısını yansıtmaktadır. Bu kültür türüne sahip örgütler, dinamik, karmaşık çevrelerde var olmakta ve sofistike yenilikleri talep etmektedir. Adhokrasiler, işletimsel adhokrasi ve yönetimsel adhokrasi olmak üzere iki temel yapıda ele alınabilir. İşletimsel adhokraside

yaratıcılık doğrudan danışmanlık firması, reklam ajansı ve film şirketi gibi dış kaynakların tasarrufunda ortaya çıkmaktadır. Yönetimsel adhokraside ise yaratıcı proje çalışmaları, kimya ve uzay bilimleri gibi alanlarda faaliyet gösteren örgütlerin kendi bünyesinde gerçekleştirilmektedir (Mintzberg, 1980). Adhokrasi kültüründe koordinasyon aracı olarak bireyler arası karşılıklı uyumlaştırma kullanılır. İş analistlerini teşkil eden teknolojik yapı küçüktür, çünkü teknik uzmanlar örgütün operasyonel çekirdeğinde yer almaktadır. Bu tarz örgüt kültüründe, rutin olmayan görevler yerine getirilmekte ve sofistike teknolojiler kullanılmaktadır. Birincil hedef, yenilik yapmak ve değişen ortamlara hızlı uyum sağlamaktır. Adhokrasi kültürünün hâkim olduğu örgütlere örnek olarak havacılık ve elektronik endüstrilerinde faaliyet gösteren ve ar-ge yapan firmalar verilebilir. Hiçbir okul saf adhokrasi kültüründe değildir, ancak çok zengin bölgelerin orta ölçekli okullarında, adhokrasi kültür özelliklerinden bazılarına rastlanılabilmektedir (Lunenburg, 2012).

2.5. Rekabetçi Değerler Modeli Boyutunda Kültür Yaşam Döngüsü

Belirli bir grupta kültürün oluşması için, öncelikle yeterli seviyede istikrarlı bir ortak tarihin yaşanmış olması gerekmektedir. Benzer bir ifadeyle tarihsel geçmişi olmayan veya üyelerinin sıklıkla değiştiği bazı örgütlerde kapsayıcı bir örgüt kültürü olamayacaktır (Schein, 1990).

Her grup veya örgüt, birden fazla farklı çevrede varlık gösterebilen açık bir sistemdir. Çevrede meydana gelen değişiklikler grupların içinde stres ve gerginlik oluşturarak yeni öğrenmeleri ve adaptasyonu zorunlu kılmaktadır. Aynı zamanda gruba katılan yeni üyeler, mevcut varsayımları etkileyecek yeni inanç ve varsayımları beraberlerinde getirmektedirler. Bununla birlikte kültürün gelişmesine ve büyümesine yönelik devam eden sürekli bir baskı söz konusu olmaktadır. Örneğin esnek çalışma saatlerine, kendi kendini izleyen, kontrol eden sistemlere sahip, katı mesai saatlerinin olmadığı ve çalışanlara yüksek güveninin duyulduğu uzay endüstrisi şirketlerinde evrimsel gelişmenin zorunlu olarak yaşandığı görülebilir (Schein, 1990).

Adhokrasi kültürü örgütün genç olması ile yakından ilişkilidir. İlerleyen zaman, bir örgütü bürokratikleşmeye ve hiyerarşi kültürüne doğru itmektedir. Örneğin yaratıcılıkta en iyi performansı yerine getiren yeteneklerin zamanla standartlaşması işletimsel adhokrasiden profesyonel bürokrasiye dönüşümü sağlamaktadır. Çünkü işletimsel adhokrasinin en büyük

zayıflığı yaratıcılık gerektiren yeni projelerin nereden geleceğinin bilinmemesidir. Bu belirsizliğin ortadan kaldırılması için, bürokratik konfigürasyona doğru bir eğilim başlamaktadır. Bir örgüt büyüdükçe daha bürokratik hâle gelmektedir. Aynı zamanda hiyerarşi kültürünü temsil eden bürokrasilerin de kendi içinde büyüme eğilimi vardır (Mintzberg, 1980).

Rekabetçi Değerler Modeli'ne göre yeni kurulmuş olan veya küçük hacimli örgütlerde örgüt kültüründe değişim yaşanmakta ve kültür türleri arasında ilerleme kaydedilmektedir. Yeni kurulmuş olan herhangi bir örgüt, yaşamaya başladıktan sonra zamanla büyümektedir. Örgütsel yaşam döngüsünün en erken safhalarında, örgütler, resmî yapıya sahip olmayan ve girişimcilik ile karakterize edilen adhokrasi kültüründe egemen olma eğilimindedir. Resmî politikalar ve yapılardan büyük oranda yoksun olunan bu aşamada örgütler genellikle tek, güçlü, vizyon sahibi bir lider tarafından yönlendirilmektedir. Örgütün zamanla gelişmesiyle birlikte örgüt kültüründe aile hissinin, güçlü aidiyet duygusunun ve kişilerin örgütle bütünleşmesinin vurgulandığı klan kültürüne yönelim gerçekleşmektedir. Toplumsal ve kişisel dostluğun hâkim olduğu klan kültüründe örgüt üyeleri, sosyal ve duygusal ihtiyaçlarının birçoğunu örgütte karşılamaktadırlar. Bununla birlikte örgüt büyümeye devam ettikçe potansiyel krizler sıklıkla ortaya çıkmaktadır. Neticede genişleyen sorumlulukları kontrol altına alabilmek için, örgüt yapısını ve standart prosedürleri vurgulama ihtiyacı ile karşı karşıya kalınmaktadır. Zamanla düzen ve öngörülebilirlik gerekli olmaya başlamakta ve hiyerarşi kültürüne geçiş eğilimine girilmektedir. Hiyerarşi kültürü ile birlikte örgüt üyelerinin iş yerleri ile ilgili daha önceleri hissettikleri dostça bir ortam olma duygusu kaybolmakta ve kişisel memnuniyetler azalmaktadır. Hiyerarşi kültürü yönelimine zamanla rekabet gücünü, sonuçlara ulaşmayı ve dış çevre ile ilişkileri vurgulayan pazar kültür özellikleri eklenmeye başlanmaktadır. Pazar kültürüne geçişle birlikte örgütün odak noktası, kişisel olmayan yaklaşımlardan ve resmî kontrollerden, müşteri yönelimine ve örgüt dışındaki rekabete kaymaktadır. Şüphesiz ki olgunluğa erişmiş ve yüksek etkinlikte çalışan örgütler, bu dört kültürün her birini temsil eden alt birimler veya bölümleri geliştirme eğilimi göstermektedir. Örneğin bir örgütün ar-ge bölümünde adhokrasi kültürü baskınken, muhasebe bölümünde hiyerarşi kültürü baskın olabilir. Bununla birlikte genellikle bir veya daha fazla kültür türü bir örgütte hâkim olabilmektedir (Cameron ve Quinn, 2006: 53-54). Birçok büyük işletme, baskın bir kültüre ve çeşitli alt kültürlere sahiptir. Örgüte kişiliğini kazandıran baskın kültür, makro bir yaklaşım içermektedir. Bununla birlikte alt kültürler, her bölümde fonsiyonel işlerin yapılış

şekillerine göre ortaya çıkabilmektedir. Örneğin bir işletmede pazarlama bölümünde daha rekabete yönelik bir kültür hissedilirken, muhasebe ve finans bölümü hiyerarşi kültürüne yakın özellikler gösterebilmektedir (Erkmen, 2010: 16).

Apple şirketinde yaşanan kültür yaşam döngüsü, örgüt kültürünün zamanla değişim göstermesine örnek olarak verilebilir. Apple şirketinin ilk kuruluş yıllarında girişimcilik, yenilikçilik ve adhokrasi kültürü hâkimdi. Birkaç yıl sonra Apple, Macintosh Takımı olarak adlandırılan "korsan" grubu ile birlikte sektörde yaşanan en başarılı girişimlerden birini kurmuş oldu. Çalışanlardan seçilerek oluşturulan bu takım, insanların evlerinde kullanmak üzere satın almak isteyeceği bir bilgisayar geliştirmekle görevlendirildi. O zamana kadar bilgisayarlar, mühendisler ve matematikçilerin kullandığı, odaları dolduracak büyüklükte korkutucu donanım parçalarıydı. Kişisel veya aile uygulamalarında bilgisayarların kullanılabileceğini düşünen çok az insan vardı. Bununla birlikte bu küçük Apple korsan grubu, eğlenceli, yaklaşılabilir, hepsi bir arada (all-in-one) türünde bir makine olarak Macintosh bilgisayarını tasarladı ve geliştirdi. İlk başlarda sadece hesaplama aracı olarak kullanılan bilgisayar artık fare, simgeler, açılan pencereler ve resim boyayabilen bir yazılım (Mac-Paint) içerir hâle gelmişti. Bu süreçte grubun çabaları o kadar başarılıydı ki tüm örgütte klan kültürü benimsenmiş vaziyetteydi. Bununla birlikte şirketin muazzam başarısı örgütü üçüncü bir kültür türüne yöneltti. Dünya çapında yaygınlaşan dağıtım kanallarıyla yüz binlerce bilgisayarın satıldığı, IBM, Compaq ve Wang gibi güçlü rakiplerin varlık gösterdiği rekabetçi ortamın oluşmasıyla birlikte kontrol ve standart prosedürlerine ihtiyaç duyulmaya başlandı. Sonuç olarak hiyerarşi kültürüne uyumlu bir yönetim anlayışı geliştirme yoluna gidildi. Adhokrasi ve klan kültürlerinin Apple şirketinde egemen olduğu zamanlarda şirketin CEO'su olan Jobs, çalışanlarını rahatlatıcı ve yenilikçiliği destekleyen başarılı bir takım lideriydi. Kendisi bir verimlilik uzmanı ve yöneticisi olmamakla birlikte hiyerarşi kültürünü yönetmeye eğilimli biri de değildi. Bu nedenle PepsiCo'dan John Scully, Apple'da istikrar ve kontrolü sağlamak için işe alındı. Tahmin edilebileceği gibi, klan ve adhokrasi kültürlerinin hiyerarşi kültürü ile değişimi, örgüt genelinde kriz meydana getirdi ve Apple kurucusu Jobs sonuç olarak şirketten ayrılmak zorunda kaldı. Nitekim yeni kültürün yansıtmış olduğu değerler ve öncelikler, mevcut taleplerle Jobs'un yönlendirmelerini senkronize etmemeye başlamıştı. Hiyerarşi kültürüne geçiş genellikle tutukluluk hissi, çekirdek değerleri terk etme, aile duygularını kural ve politikalarla değiştirme hissi üretmekteydi. Ancak, Scully usta bir verimlilik ve pazarlama uzmanıydı ve becerileri Apple şirketinin değişen kültürüne daha

yakından uyum sağladı. Apple, Scully yönetiminde büyük ve olgun bir örgüt hâline geldiğinde, örgüt kültüründe dördüncü aşamaya geçiş sağlanmaya başlandı. İlk yıllardaki genç ayrılıkçı bir grubu karakterize eden yenilikçi bir şirket durumundan pazar kültürü ile uyumlu, verimlilik ve pazarlama anlayışının hâkim olduğu bir yapıya doğru geçiş tamamlanmış oldu. Kültür değişiminde gelinen son aşamayla birlikte elde edilen genel örgüt kültürü profilinde, bugün birçok olgun örgütte olduğu üzere klan ve adhokrasi kültür boyutlarının en aza indirildiği, hiyerarşi ve pazar kültürlerinin ise vurgulanarak bir norm hâline dönüştürüldüğü görülmektedir (Cameron ve Quinn, 2006: 54-57).

2.6. Bilgi Güvenliği

Bilgi, kâğıt üzerinde yazılı olabileceği gibi, elektronik ortamda depolanmış, elektronik veya normal posta yolu ile iletilmiş, filmlerde gösterimde ve konuşmalarda sözlü olmak üzere birçok formda bulunabilir. Paylaşılırken ve depolanırken hangi formda veya manada olursa olsun, bilgi uygun bir şekilde korunmalıdır. Bilgi ve bilgiyi destekleyen süreçler, sistemler ve bilgisayar ağları önemli iş varlıklarıdır. Örgütlerin bilgi sistemleri ve bilgisayar ağları artan bir şekilde, bilgisayar destekli dolandırıcılık, casusluk, sabotaj, vandalizm, yangın ve sel baskını gibi birçok kaynaktan gelebilecek güvenlik tehditleriyle karşılaşmaktadır. Bilgisayar virüsleri, bilgisayar korsanlarının faaliyetleri ve servis reddi (denial of service) saldırıları gibi birçok bilgi güvenliğini tehdit edici kaynaklar günümüzde gittikçe yaygınlaşmakta, saldırılar hırslı ve karmaşık bir hâl almaktadır. Bilgi sistemlerine ve servislerine bağımlılık, örgütleri güvenlik tehditlerine maruz bırakmaktadır (British Standard [BS], 1999: 1).

Bilgiyle yakalanan rekabet avantajının korunması ve daha ileriye götürülmesi, örgütlerin bilgiyi doğru ve etkin bir şekilde yönetebilmesi ile doğru orantılı olacaktır. Doğru ve etkin bir bilgi yönetimi ise bilginin güvenliğinin sağlanmasıyla bir bütünlük sergilemektedir. Dolayısıyla bilgi yönetimi süreçlerinde bilgi güvenliğinin sağlanıyor olması, örgütlerin rakiplerine karşı elde ettikleri rekabet avantajının korunmasında ön koşul niteliği taşımaktadır. Bu bağlamda bilginin, yasal ve uygun olmayan kullanımdan, çalınmaktan ve taklit edilmekten korunması gerekmektedir. Bilginin korunması sürecinde başarısız olan örgütler, elde edilen bilgiler ile verimli sonuçlar alabilir, ancak bu bilgiler, aynı zamanda başka örgütler tarafından da kullanılabileceğinden rekabet avantajını sağlama özelliğini kaybedebilir (Çakar, Yıldız ve Dur, 2010).

Teknoloji ilerledikçe ve herkes bilgi güvenliğine dâhil olmaya başladıkça bilgi güvenliği tehditleri ve saldırılarında çeşitlilik artmakta ve yeni saldırı türleri gelmeye devam etmektedir (Kim, 2013). Federal Soruşturma Bürosu (Federal Bureau of Investigation) bünyesinde kurulmuş olan İnternet Suçları Şikâyet Merkezi'nin (Internet Crime Complaint Center) kurulduğu tarih Mayıs 2000'den 2015'e kadar geçen süre zarfında 3 463 620 adet şikâyet kayıt edilmiştir. 2010 ile 2015 yılları arasında ise yıl başına ortalama 300 000 adet şikâyet yer almıştır. Şikâyetlerin çoğu İnternet dolandırıcılığını adreslemektedir. 2015 yılı itibarıyla kaydedilen şikâyetlerden kaynaklı toplam 1 070 711 522 ABD Dolar değerinde kayıp yaşandığı rapor edilmiştir (Internet Crime Complaint Center [IC3], 2015: 4, 12).

Bilgi güvenliği yönetimi ile örgütün bilgi varlıklarının güvenliğini kontrol eden, tehditlerin tespit edilmesi, örgütteki mevcut bilgi güvenliği seviyesinin gözlemlenmesi, bilgi güvenliği prosedürleri gibi yönetimsel güvenlik kontrollerinin tasarlanması ve uygulanması, erişim kontrol sistemleri gibi teknik kontrollerin takip edilmesi ve bilgi güvenliğinin idamesi için dokümante etme, bilgi güvenliği olaylarına cevap verme, çalışanların eğitimi gibi günlük eylemlerin yürütülmesi sağlanmaktadır (Ebrahimi ve Naini, 2012).

Doğru güvenlik kontrollerinin tanımlanıp uygulanmasıyla bilgi güvenliğinde istenilen seviyeler elde edilebilir. Uygun güvenlik kontrollerinin tanımlanması ise karmaşık olabilmektedir. Ayrıca kontrollerin tanımlanmasında birçok kuruluşun sahip olmadığı uzmanlık ve özel kaynaklara ihtiyaç duyulabilmektedir. Dolayısıyla bilgi kaynaklarının istenilen seviyede korunmasını sağlayan güvenlik kontrollerin tanımlanmasında örgütlerin kullanabileceği BGYS standartlarına ihtiyaç duyulmaktadır (Chang ve Lin, 2007). BGYS, "kurumun hassas bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşımdır" (Önel ve Dinçkan, 2007). Örgüt genelinde bilgi güvenliğinin temin edilmesi için, teknolojik çözümlerle birlikte bilgi güvenliğinin insan yönünü de dikkate alan BGYS yapılandırılmalı ve bu kapsamda uygun güvenlik politikaları, kontroller, prosedürler belirlenmeli ve uygulanmalıdır. BGYS, bilgi güvenliği teknolojilerini ve yönetim süreçlerini uygulayarak tüm değerli bilgi varlıklarının korunmasında, örgütün iç ve dış tüm çevresinden bilgiye karşı doğabilecek çeşitli risklerin azaltılmasında kullanılmaktadır (Chang ve Lin, 2007). BGYS'nin örgüt genelinde uygulanması için oluşturulmuş standartların başında ISO/IEC 27001 gelmektedir (Mataracıoğlu ve Özkan, 2011). ISO/IEC 27001 standardının tarihsel gelişim süreci, BGYS'lerin yaratıcısı olarak tanınan

Prof. Edward Humphreys'in BGYS standardı geliştirme çalışmalarına dayanmaktadır. Daha sonra bu çalışmalardan yararlanılarak İngiliz Standartlar Enstitüsü (BSI - British Standards Institute) tarafından 1995 yılında BS-7799 standardının ilk kısmı olan BS7799-1 oluşturulmuştur (Humphreys, 2011). 1998 yılında ise aynı standardın ikinci kısmı, BS7799-2 olarak yayınlanmıştır. 2000 yılında BS7799-1 standardı temel alınarak Uluslararası Standartlar Teşkilâtı (ISO - International Organization for Standardization) tarafından ISO/IEC 17799 standardı geliştirilmiştir. Daha sonra bu standart, 11 Kasım 2002 tarihinde Türk Standardları Enstitüsü (TSE) tarafından TS ISO/IEC 17799 olarak kabul edilmiştir. BS7799-2 standardı ise yine, TSE tarafından 17 Şubat 2005 tarihinde TS 17799-2 standardı olarak kabul edilmiştir. 2 Mart 2006 tarihinde, TS 17799-2'nin yerini TS ISO/IEC 27001:2005 standardı almıştır (Ersoy, 2012: 11-13). 18 Aralık 2013 tarihinde ise TS ISO/IEC 27001:2005, yerini TS ISO/IEC 27001:2013 standardına bırakmıştır (Türk Standardları Enstitüsü [TSE], 2017). ISO/IEC 27001'den başka, bilgi teknolojileri alanında uluslararası alanda tanınmış bir diğer yönetim sistemi ise Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA - Information Systems Audit and Control Association) tarafından geliştirilmiş ve ülkemizde de ağırlıklı olarak bankacılık sektöründe kullanılan Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri (COBIT - Control Objectives for Information and Related Technology) rehberidir (Ersoy, 2012: 14).

BGYS standartlarında geçen en genel tanım itibarıyla bilgi güvenliği, bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunmasıdır (BS, 1999: 1; TS, 2006: 4). Bilgi Teknolojileri Altyapı Kütüphanesi'nin (Information Technology Infrastructure Library) üçüncü versiyonunda da benzer bir ifadeyle bilgi güvenliği, bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması olarak tanımlanmaktadır. Ayrıca kimlik doğrulama, sorumluluk, inkâr edilemezlik ve güvenilirlik gibi diğer özellikler de bilgi güvenliği kapsamında korumaya dâhil edilebilmektedir (Clinch, 2009). Fussell'e (2005) göre de bilgi güvenliği modeli gizlilik, bütünlük ve erişilebilirlikten oluşmaktadır. Benzer bir ifadeyle bilgi güvenliği, "elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür" (Canbek ve Sağıroğlu, 2006). Bilgi güvenliği ile bilgiye ve bilgi işleme kaynaklarına erişimin sağlanmasına paralel olarak sistem içerisinde bilginin gizliliğinin ve bütünlüğünün temin edilmesi hedeflenmektedir (Ryan ve Bordoloi, 1997). Bilgisayar güvenliği kavramı ise donanım, yazılım, bilgi, veri ve telekomünikasyon gibi bilgi sistemleri kaynaklarının gizlilik,

bütünlük ve erişilebilirliğinin sağlanması için bilgisayar ağlarının korunmasıdır (Guttman ve Roback, 1995: 5; Onwubiko ve Lenaghan, 2007).

Gizlilik, bütünlük ve erişilebilirlik, korunan bilgi varlıklarının güvenlik boyutlarını temsil ederken; insanlar, süreçler ve teknoloji bu korumanın nasıl gerçekleştiğini açıklamaktadır. İnsanlar, süreçler ve teknoloji, bilgi güvenliğinin tesisinde aynı derecede önemli bir rol oynamaktadır. Bununla birlikte insanlara ve süreçlere, tamamen göz ardı edilmemekle birlikte düşük seviyede önem verilirken güvenlik duvarları gibi teknolojik çözümlere çoğunlukla gerekenden fazla ilgi gösterilmektedir. Güvenlik duvarları ve diğer teknoloji bileşenleri gerekli temel korumayı sağlamaya yardımcı olurken, bir kullanıcının kasten veya yanlışlıkla erişim yetkilerini kötüye kullanması ya da kontrolündeki kaynakları korumaması durumunda tüm bu teknolojik güvenlik bileşenleri işe yaramaz hâle gelebilir. İnsanları hedef alan bilgisayar korsanlığı saldırıları ne yazık ki sürekli yükseliş sergilemekte ve tek başına teknolojik çözümler vasıtasıyla bu tarz saldırılar engellenememektedir. İnsanları hedef alan saldırıların kolay uygulanabilir olması, kurumsal güvenlik için büyük bir tehdit olarak kabul edilmektedir (Okenyi ve Owens, 2007).

Bir örgüt bilgi sistemlerini korumak istediğinde, öncelikle bilgi güvenliğinde hangi gereksinimlerin karşılanması gerektiğini belirlemelidir. Örneğin bir üniversite, bilgi sistemlerinde var olan öğrenci notları gibi verilerin bütünlüğünü ve gizliliğini korumalıdır. Aynı zamanda sistemlerin İnternet üzerinden öğrencilerin, personelin, diğer araştırmacı ve eğitmenlerin erişimine açık olması beklenebilir (Bishop, 2003).

2.7. Bilgi Güvenliği Boyutları

İşletme bilgi güvenliğinin etkin bir şekilde sağlanmasının yolu, iyi tanımlanmış iş süreçleri doğrultusunda bilgi güvenliğinin iş stratejisi ile uyumlu hâle getirilmesidir. İş stratejisi, süreçler içerisinde bilgi güvenliği risklerinin, gizliliğin, bütünlüğün ve erişilebilirliğin tanımlamasını, ölçülmesini, yönetilmesini ve hatta sorumluluğun sağlanmasını gerektirmektedir (Istikoma ve diğerleri, 2015). Bilgi güvenliği hakkında yürütülen birçok araştırma, bilgi güvenliğinin gizlilik, bütünlük ve erişilebilirlik olmak üzere üç temel prensibini destekleyen algoritmalar, yöntemler ve standartlar üzerine odaklanmaktadır (Stanton, Stam, Mastrangelo ve Jolton, 2005). Bilgi güvenliği çok boyutlu olmasına karşın,

temel olarak üç prensipten söz edilmektedir: Gizlilik, bütünlük, erişilebilirlik (Chou, Yen, Lin ve Cheng, 1999; Harris, 2013: 22; Jones, 2004). Temel bilgi güvenliği prensiplerine ek olarak sorumluluk (izlenebilirlik), kimlik sınaması, güvenilirlik ve inkâr edememe gibi diğer kavramlar da bilgi güvenliği kapsamında ele alınmaktadır (Canbek ve Sağıroğlu, 2006; Ebrahimi ve Naini, 2012; Harris, 2013: 298; TBD, 2006: 3; TS, 2006: 4). Bilgi güvenliği konusunda üç temel prensip gizlilik, bütünlük ve erişilebilirliğe ek olarak sorumluluk kavramını da diğer bir önemli bilgi güvenliği prensibi olarak ele alan çalışmalar mevcuttur (Chang ve Lin, 2007).

Bu tez çalışmasında, bilgi güvenliği algısının belirlenmesinde bilgi güvenliğinin gizlilik, bütünlük, erişilebilirlik ve sorumluluk prensipleri temel alınmış olup, alt bölümlerde bu dört prensibin anlatımına yer verilmiştir.

2.7.1. Gizlilik

Gizlilik, bilginin sadece yetkilendirilmiş kişilerin erişimine açılmasıdır (BS, 1999: 1). Benzer bir ifadeyle gizlilik prensibi, gizli olanların gizli kalması gerektiğine işaret etmektedir (Chou ve diğerleri, 1999). Bir başka deyişle gizlilik, bilginin yetkisiz kişiler, programlar veya süreçler tarafından erişilemiyor olmasının garantisini sunmaktadır (Harris, 2013: 160). Bilgi sistemlerinin ve iletişiminin kasıtlı veya yanlışlıkla yetkisiz kişilere erişime açılmasının engellenmesi için gizliliğin korunması gerekmektedir (Onwubiko ve Lenaghan, 2007). Gizlilik ile "sadece siz görebilirsiniz" prensibine vurgu yapılmakta ve erişim hakkının sadece yetkisi olanlarla sınırlandırılması ifade edilmektedir (Jones, 2004).

Gizlilik, yalnızca yetkili hesaplar veya sistemler tarafından bilgiye erişim olduğunu güvence altına almaktadır. Bir başkasının e-postalarını okumak, gizli bilgi elde etmek için çöpleri incelemek ve şifre bilgilerini not etmek gizliliğin ihlaline örnek olaylar olarak verilebilir. Mayıs 2008'de İngiltere'de yaşanan ve yetkisizce gizli bilginin ifşasına neden olan fotoğraf skandalı gizliliğin ihlaline verilebilecek örnek bir olaydır. İngiliz Hükümeti'ni zor duruma sokan söz konusu olayda zamanın bakanı Caroline Flint'in, İngiltere konut piyasası hakkında hazırlanmış bir belge ile fotoğrafı çekilmişti. Fakat çekilen fotoğrafta belge metninin okunabiliyor olması ve metinde hükümetin kamuya açıklamayı düşünmediği endişelerinin yer alıyor olması İngiliz Hükümeti'ni zora sokmuştu (Clinch, 2009). Bu olayda konu olan belge gibi bazı bilgilerin gizliliğinin korunması gerekmektedir.

Örneğin öğrencilerin notları, finansal işlemler, tıbbi kayıtlar ve vergi beyannameleri korunmayı gerektirecek hassaslıkta bilgiler içermektedir. Diplomatik ve askerî sırlar, şirketlerin pazarlama ve ürün geliştirme planları ve eğitimcilerin sınav soruları gibi diğer bilgilerin de gizliliğinin korunmasına gerek duyulmaktadır. Bilgi işleme alanındaki gizlilik kavramı, korunmakta olan verilere yalnızca yetkili kişiler veya sistemler tarafından erişilebiliyor olmasını ifade etmektedir. Veri gizliliğinin korunması aşağıdaki olayların olması durumunda başarısızlığa uğrayacaktır (Pfleeger, Pfleeger ve Margulies, 2015: 8-9):

- Yetkisiz bir kişinin korunmakta olan veriye erişmesi,
- Yetkisiz bir süreç veya programın korunmakta olan veriye erişmesi,
- Belirli verilere erişmeye yetkili olan bir kişinin yetkili olmadığı diğer verilere de erişmesi,
- Yetkisiz bir kişinin korunmakta olan bir verinin yaklaşık değerine erişmesi (örneğin birinin maaşını tam olarak bilmemekle birlikte maaşın belirli bir aralıkta olduğunun veya belirli bir miktarı aştığının biliniyor olması),
- Yetkisiz bir kişinin korunmakta olan bir verinin varlığını öğrenmesi (örneğin bir şirketin yeni bir ürün geliştirdiğinin ya da iki şirketin birleşmesi konusunda görüşmelere devam edildiğinin yetkisiz taraflarca bilinmesi).

Gizlilik prensibinin ihlaliyle bilgiye yetkisiz erişim riskinin doğması söz konusu olmaktadır. Kimlik bilgileri, bireysel kullanıcıların tercih bilgileri, gizli kurumsal veriler (ar-ge bilgileri, müşteri kayıtları gibi önemli iş verileri) veya iletişim verileri yetkisiz erişimlere veya çalınmaya karşı korunmalıdır. Gizliliğe karşı gerçekleştirilen saldırılar, genelde pasif atak türünde olup bilgiyi değiştirmeden ele geçirme amacı taşımaktadır. Özel bilgisayar korsanlığı saldırıları hariç bu tarz pasif saldırılar, veri iletimi esnasında şifrelenmemiş mesaj içeriğini dinleyebilen paket algılayıcılarını (packet sniffers) kullanmaktadır (Grzebiela, 2002). Bununla birlikte saldırganlar, ağ izleme (network monitoring), omuz üzerinden gözetleme (shoulder surfing), şifre dosyalarının çalınması, şifreleme mekanizmalarının kırılması ve sosyal mühendislik (social engineering) saldırıları ile gizlilik mekanizmalarını bozmaya çalışmaktadır. Omuz üzerinden gözetleme saldırısı, kötü niyetli bir kişi tarafından diğer kişilerin omuz üzerlerinden klavyedeki tuş vuruşlarının ve bilgisayar ekranında görülen bilgilerin gözetlenmesidir. Sosyal mühendislik saldırısında ise kötü niyetli bir kişi diğer kişileri kandırmakta ve bu yolla gizli

bilginin paylaşımı sağlanmaktadır. Örneğin bilgiye erişim yetkisi olan kullanıcılara e-posta atılarak kandırma girişiminde bulunulabilir. Bununla birlikte sosyal mühendislik saldırıları birçok formda olabilmektedir. Birebir iletişim ortamları, sosyal mühendislik saldırılarının gerçekleştirilmesi için kullanılabilir. Kullanıcılar, bilgiyi şifrelemeden farklı bir kişiye göndererek, sosyal mühendislik saldırısı neticesinde kandırılarak, şirketin ticari sırlarını paylaşarak veya yürütülen işlemler esnasında gizli bilgiyi korumak adına yeterince özeni göstermeyerek gizlilik değeri taşıyan bilgiyi bilerek ya da bilmeyerek açık edebilirler. Gizlilik, depolanan ve iletilen verinin şifrelenmesi, verilerin sınıflanması, erişim kontrol mekanizmaları ve bilgi güvenliği prosedürleri hakkında çalışanların eğitilmesi ile sağlanabilir (Harris, 2013: 24). Sosyal mühendislik, insan ve teknoloji temelli teknikler ile gerçekleştiren insanları hedef alan saldırıların bir parçasıdır. İnsan temelli sosyal mühendislik saldırılarında telefonla ya da şahsen gerçekleştirilecek etkileşimler temel alınmaktadır. Teknoloji temelli sosyal mühendislik saldırılarında ise bir kişiden istenen bilgiyi kimlik avı (phishing) vb. saldırılar ile almaya çalışan zararlı yazılımlar kullanılmaktadır. Hassas bilgi, ağ içinde veya ağlar arasında iletilirken, yetkisiz kişilerin bilgiye erişiminin engellenmesi ve iletimin kesintiye uğramaması için bilgi şifrelenmelidir. Bilginin gizliliğini daha da artırmak için, saldırıları engelleyemese de zorlaştıran savunma amaçlı stratejilerin bir parçası olarak saldırı tespit sistemleri, saldırı engelleme sistemleri, güvenlik duvarları ve benzeri teknolojiler kullanılabilir (Okenyi ve Owens, 2007).

2.7.2. Bütünlük

Bilginin bütünlüğü ile bilginin içeriğinde yasal olmayan yollarla meydana gelebilecek değişikliklerin tespiti ve içeriğinin değişmediğinin doğrulanması sağlanmaktadır. Bütünlük, bilginin ve bilgi işleme metotlarının doğruluğunun ve tamlığının korunmasıdır (BS, 1999: 1). Bilgisayar ağlarının sunmuş olduğu servislerin tam, eksiksiz, tutarlı, güvenilir ve güncel olduğundan emin olabilmek, bütünlüğün korunmasıyla sağlanır (Onwubiko ve Lenaghan, 2007). Bilgi, yetkisiz modifikasyonlardan korunmalı, tam ve eksiksiz olmalıdır. Bütünlüğü sağlayan güvenlik mekanizmalarında bilginin tamlığı ve yetkisiz değiştirilmediği teyit edilmektedir. Örneğin bir kişi çevrimiçi (online) bankacılık sistemine bağlanarak su faturası ödemek isteyebilir. Bu durumda bankanın fatura için hesaptan ödenecek miktarın bütünlüğü konusunda emin olması gerekir. Bütünlüğün korunmadığı aksi durumda banka su faturası için yanlış ödeme yapabilir (Harris, 2013: 159). Veri ve ağ güvenliği anlamında bütünlük prensibi ile bilgide sadece yetkili kişilerce

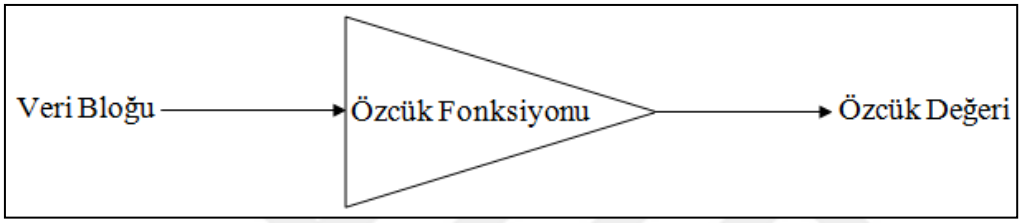
değişiklik yapılabilmesinin garantisi sunulmaktadır (Kanday, 2012).

Bütünlük, bilginin yetkili kişiler veya işlemler haricinde depolama veya iletim anında değiştirilmediğini güvence altına almakta, yetkisiz bir biçimde kasıtlı ya da bilinçsizce değiştirilmediğinin de garantisini sunmaktadır. Bir bilgisayarda depolanmış verinin bilgisayar virüsü eylemiyle değiştirilmesi, bilgi bütünlüğünün bozulmasına sebep olabilir (Clinch, 2009). Bütünlük ile ilgili birkaç yıl öncesinde yaşanan ihlal olayına, Word belgesindeki kötü amaçlı bir makro yazılımı örnek olarak verilebilir. Bu yazılım, metin içerisindeki İngilizce "is" sözcüklerinin ardından olumsuzluk manası veren "not" kelimesini eklemiş ve bu durum cümlelerin genelinde istenenin tam tersi anlamı ortaya çıkarmıştı. Bu örnek olayda, belge söz dizimi olarak doğru gözüktüğü için insanlar tarafından değişiklikler hemen algılanamamıştı. Bütünlük ihlaline bir başka örnek olarak da nümerik verilerin Roma rakamına çevrildiği durum verilebilir. Her ne kadar "IV" Roma rakamı anlam itibarıyla nümerik karakter "4" ün yerine geçiyor olsa da "IV" çoğu uygulamada rakam karakteri olarak algılanılmayacak ve yanıtın açıkça 4 olarak beklendiği bir durumda bütünlük ihlali oluşturacaktır. Bu ve benzeri örnekler, yaşanmakta olan bütünlük ihlallerinin bazılarını göstermektedir. Bütünlüğün muhafaza edildiği durumda, bilginin tamlığının, kesinliğinin, değiştirilmemiş olduğunun, iç tutarlığının, anlamlı ve kullanışlı olduğunun, sadece kabul edilebilir yollarla yetkili kişiler ve süreçlerle değiştirildiğinin anlamı çıkmaktadır. Bu manada bütünlük, bu özelliklerin iki veya daha fazlasının sağlandığı anlamına gelmektedir (Pfleeger ve diğerleri, 2015: 10-11).

Bütünlük prensibinin ihlali, bilgi veya veri üzerinde yetkisiz değişiklik yapılması riskini doğurmaktadır. Örneğin teklif ve siparişler gibi önemli mesaj içerikleri ortadaki adam saldırısı (man in the middle attack) gerçekleştirilerek taklit edilebilmekte ve bütünlük prensibi ihlal edilebilmektedir. Bu atak modelinde saldırgan, iki tarafın iletişimi esnasında tarafların yerine geçerek iletişimin kendi üzerinden gerçekleşmesini sağlamaktadır. Saldırganın üzerinden geçen mesaj içeriğinde yetkisiz değişiklik yapması bütünlük prensibini zafiyete uğratmaktadır (Grzebiela, 2002).

Elektronik ortamda tutulan bilginin tahrif edilmediğinin ispatlanması için sayısal imza teknolojisi kullanılmaktadır. Sayısal imza teknolojisinde, bilginin doğruluğunun ve tamlığının teyidi “özcük fonksiyonları” (hash algoritmaları) ile sağlanır. İletişim veya depolama hataları gibi doğal nedenlerden veya yetkisiz bir işlem sonucu oluşmuş

hatalardan dolayı içeriği değişmiş bir veri setinin doğrulaması, önceden ve sonradan alınacak özcük değerlerinin karşılaştırılması ile yapılabilir (Aydın ve İnce, 2005). Örneğin elektronik ortamda mesajın iletimi esnasında, mesaj içeriği Şekil 2.4'te de görüldüğü üzere özcük fonksiyonundan geçirilerek "özcük değeri" (mesaj özeti) oluşturulur ve mesajla birlikte alıcı tarafına iletilir. Alıcı tarafında da ulaşan mesaj aynı özcük fonksiyonundan geçirilir ve tekrar özcük değeri oluşturulur. Alıcının üretmiş olduğu özcük değeri ile göndericiden gelen özcük değeri karşılaştırılır. Şayet her iki özcük değeri arasında bir değişiklik varsa mesaj içeriği iletim esnasında değiştirilmiş demektir (Information Systems Audit and Control Association [ISACA], 2006: 406).



Şekil 2. 4. Veri bloklarının özcük fonksiyonuna tabi tutulması işlemi (Aydın ve İnce, 2005)

Ülkemizde de 5070 sayılı "Elektronik İmza Kanunu" ile imzalanmış elektronik veride, sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imzaya tanımlama getirilmiştir (Resmî Gazete, 2004).

2.7.3. Erişilebilirlik

Erişilebilirlik, yetkili kişilerin bilgi ve varlıklarına erişiminin korunmasıdır (BS, 1999: 1). Diğer bir ifadeyle erişilebilirlik, bilgisayar ağ ve servislerinin içeriğine, tanımlanan yetki seviyelerinde erişim sağlanabilmesinin korunmasıdır (Onwubiko ve Lenaghan, 2007). Erişilebilirlik sayesinde kullanıcılar erişim yetkileri dâhilinde bilgilere zamanında ve güvenilir bir şekilde ulaşabilirler. Burada önem verilmesi gereken nokta, bilginin gizliliğini ve bütünlüğünü sağlamak amaçlı uygulanan şifreleme ve sayısal imza benzeri teknolojiler, bilgiye zamanında erişimi zedeleyecek boyutta olmamalıdır. Örneğin doğru zamanda ve doğru fiyattan hisse senedi satmak isteyen bir borsacı için bilginin doğruluğu ve bilgiye zamanında erişim bilginin gizliliğinden çok daha önemlidir (Harris, 2013: 159). Şayet servis veya bileşenler erişilemez durumda ise gizlilik ve bütünlük bir mana ifade etmeyecektir (Fussell, 2005). Erişilebilirlik, iş sürekliliği planlamasının ana temalarından biridir. Ayrıca işin devam ettirilmesi için gerekli olan kaynakların, kaynaklara bağlı olarak

çalışan insanlara ve sistemlere sunulmaya devam edilmesini sağlar. Bu durum, yedeklemelerin ciddiyetle yapılması ve sistemlerin, ağların ve operasyonların mimarisine yedekliliğin dâhil edilmesi gerektiği anlamına gelmektedir. Şayet önemli bir zaman dilimi için iletişim hatlarının hizmet dışı kalması veya servislerin kullanılmaz durumda olması söz konusu olacaksa yedekliliği sağlamak adına alternatif iletişim hatları ve servisleri kurmanın hızlı ve test edilmiş bir yolu olmalıdır (Harris, 2013: 888).

Bir bilgisayar kullanıcısının başına gelebilecek en kötü olay, açma düğmesine basıldığında bilgisayarın açılmaması, verilere ve programlara erişememe durumunun yaşanmasıdır. Bununla birlikte bilgisayarlarda çoğunlukla yaşanmakta olan aşırı yüklenme sorunu da erişilebilirliği kısıtlamaktadır. Aşırı yüklenme durumunda verilere ve programlara erişim gittikçe yavaşlamakta ve bilgisayarın cevap verme hızı normal veya kabul edilebilir seviyenin altına inmektedir. Erişilebilirlik hem veri hem de hizmetler için geçerlidir. Bir nesne veya hizmet kullanılabilir bir formdaysa, servis gereksinimlerini karşılayacak kapasiteye sahipse, bekleme modunda sınırlı bir bekleme süresine ihtiyaç duyuyorsa ve servisler kabul edilebilir bir süre zarfında tamamlanıyorsa erişilebilirlik kriterlerinin sağlandığı düşünülebilir. Erişilebilirliğin tanımlanabilmesi için gerekli bazı ölçütler şunlardır (Pfleeger ve diğerleri, 2015: 11-12):

- Taleplere zamanında cevap veriliyor olmalıdır.
- Kaynaklar kullanıcılara eşit dağıtılmalı ve bazı talep sahiplerinin diğerlerine nazaran kaynak kullanımında üstünlüğü olmamalıdır.
- Kaynaklara erişimde eşzamanlılık kontrollerinin gerçekleştiriliyor olması gerekmektedir. Bu kapsamda kullanıcılara eşzamanlı erişim hakkı sağlanıyorken istenildiğinde erişimin kilitlenebiliyor olması veya gerektiğinde bazı kullanıcılara özel erişim yetkilerinin tanımlanabiliyor olması desteklenmelidir.
- İlgili hizmet veya sistemler hata tolerans seviyelerinde sunuluyor olmalıdır. Donanım veya yazılım hataları ani bilgi kaybı yaşatmamalı, bunun yerine olası kesintilerde geçici çözümlere gidilmesi imkânı sağlanmalıdır. Bu noktada sistemin duracağına ilişkin yapılacak uyarılar kullanıcıya başka bir sisteme geçme şansı tanıyabilir.
- Servis veya sistemler kolaylıkla amacına uygun olarak kullanılabilmelidir. Bu erişilebilirliğin bir özelliğidir. Kullanılamaz durumda olan bir sistem erişilebilirlik

ihlalinin temel nedenidir.

Erişilebilirlik prensibinin ihlali, işlevselliğin yetkisiz bir şekilde bozulması riskini doğurmaktadır. Tüm yetkili tarafların her zaman iletişim hâlinde olmasını ve bilgiye erişimi mümkün kılan kurumsal çevrimiçi görünümün erişilebilirliğinin kaybolması iş süreçlerine zarar verecektir. Dağıtık servis reddi (distributed denial of service) atakları gerçekleştirilerek erişilebilirlik prensibine karşı saldırılar oluşturulabilmektedir. Dağıtık servis reddi saldırıları farklı birçok bilgisayardan eş zamanlı olarak başlatılmakta ve hedef bilgisayar aşırı trafik yoğunluğundan dolayı hizmet verememeye başlamaktadır. Bu durum, hedef bilgisayarın vermesi gereken hizmetinin erişilebilirliğini zafiyete uğratmaktadır (Grzebiela, 2002). Bu bağlamda erişilebilirlik, kullanıcıların ya da sistemlerin yetkili oldukları zaman diliminde erişecekleri bilginin mevcut olduğuna dair güvence sağlamaktadır. İnternet tabanlı servis reddi saldırısı nedeniyle yetkili kişilerin kurumsal verilere erişmesi kısıtlanmaktadır. Bununla birlikte kullanıcı hatasıyla da erişilebilirlik zarar görebilmektedir. Veri dosyasının yanlışlıkla silinmesi nedeniyle bir personelin bordro programını çalıştıramıyor olması, kullanıcı hatasıyla oluşabilecek erişilebilirlik ihlaline verilebilecek bir örnektir (Clinch, 2009).

2.7.4. Sorumluluk

Sorumluluk, bilgisayar ve ağ sistemleri için çok önemli bir konudur. "Ne yapıldı?", "kim yaptı?" gibi soruların cevaplandırılması sorumluluk prensibi ile sağlanmaktadır. Bu iki soru aynı zamanda adli bilişim ile alakalıdır. Adli bilişim, bu sorulara erişilebilir sistemler altında yer alan insan faktörünü dâhil ederek cevap arar (Xiao, Meng ve Takahashi, 2012). Bu manada sorumluluk prensibi ile olay kayıt (log) dosyalarının korunarak kullanıcı verilerinin denetiminin gerçekleştirilmesi amaçlanmaktadır. Örneğin bir kullanıcının veri üzerinde bazı eylemler gerçekleştiriyor olması durumunda, veri üzerinde yanlış bir şey yapılıp yapılmadığının denetlenmesine gerek duyulmaktadır. Bu kontrol, olay kayıtlarının gözden geçirilmesiyle gerçekleştirilebilir (Hande ve Mane, 2015). Aynı zamanda sorumluluk prensibi ile çalışanların bilgi güvenliği politikalarını ihlal etmesi durumunda örgütün ne yanıt vereceğine ve hangi eylemleri gerçekleştireceğine gönderme yapılmaktadır (Tang ve diğerleri, 2016). Sorumluluk prensibi, örgütün bilgi güvenliği uygulamalarına bağlı kalınmayı ve bireylerin eylemlerinden dolayı sorumlu tutulmasını içermektedir (Ebrahimi ve Naini, 2012).

Sorumluluk kelimesinin tanımlanmasında sorumluluk süreçleri altı farklı boyutta ele alınabilir (Meijer, 2001):

1. Sorumluluk sürecine neden olan bir olayın varlığı süreci başlatır.
2. Sürecin başlamasını müteakip meydana gelen olay hakkında sorumluluğu olan ya da sorumlu tutulan kişilerin tespiti gerekecektir.
3. Sorumluluk sürecinin devamı için bir kişi veya örgütün sorumlu tutulduğu bir durumun varlığı söz konusu olmalıdır.
4. Sorumluluk sürecinde, bahse konu durumun varlığından sorumlu olanların tartışılması ve yargılanması sürecine geçilir.
5. Sorumluların yargılanması sürecinde kullanılacak kriterler belirlenmelidir.
6. Bazı durumlarda kişi veya örgütlere sorumluluklarından kaynaklı cezai işlemler ve yaptırımların uygulanması gündeme gelebilir.

Yukarıdaki boyutlar ışığında sorumluluk süreçleri kendi içinde üç fazda değerlendirilmektedir: Birinci faz bilgi fazı olup, sorgulama için çeşitli kaynaklardan verilerin toplanması bu aşamada yapılmaktadır. İkinci fazda, belirli norm ve kriterlere göre vuku bulan eylemlerin tartışılması ve yargılanması yürütülmektedir. Yaptırımların uygulanması ise üçüncü ve son fazda gerçekleşmektedir (Meijer, 2001).

Sorumluluk sürecinin bilgi fazındaki sorumluluk kavramı, "izlenebilirlik" olarak da Türkçeye çevrilebilen bilgi güvenliği prensibidir. İzlenebilirlik, bir bilgisayar sistemi ya da ağı üzerinde bilgiye erişimden sonra gerçekleşecek herhangi bir olayın, sonradan analiz edilebilmesi için kayıt altına alınmasını ifade etmektedir. İzlenebilirliğin tam manasıyla yerine getirilebilmesi için, olay kayıtlarını tutacak bir kayıt tutma (logging) sistemine ve bu kayıtları araştıracak bir hesap inceleme (auditing) sistemine ihtiyaç duyulur (Canbek ve Sağıroğlu, 2006). FISMA, HIPAA, SOX, PCI DSS gibi uluslararası yasalar ve standartlar da kayıt tutma sistemi (log yönetimi) kullanımını mecbur kılmaktadır (Kent ve Souppaya, 2006: 2.7-2.8). Ayrıca ülkemizde de 23 Mayıs 2007 tarih ve 26530 sayılı Resmî Gazete'de (2007a) yayımlanan 5651 Sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki Kanun” ve bu kanunu dayanak alan 1 Kasım 2007 tarih ve 26687 sayılı Resmî Gazete'de (2007b) yayımlanan “İnternet Toplu Kullanım Sağlayıcıları Hakkındaki Yönetmelik”, kurumların olay kayıt yönetimi ile ilgili yükümlülüklerini belirlemiştir.

İzlenebilirlik sayesinde, bir kişi bir eylem gerçekleştirdiğinde, kişinin yanlış bir şey yapıp yapmadığını görebilmek için, eylem dikkatlice incelenebilir ve belki de kişi eyleminden dolayı sorumlu tutulabilir (Kanday, 2012). Borglund (2008), polislerin faaliyetleri üzerine yürüttüğü çalışmasında, eylemlerinden dolayı sorumlu tutulan kişi veya kişilerin bulunmasında elektronik kayıtlardan yararlanıldığı ve bu yöntemde sorumluluk kriterinin etkili olduğunu ifade etmektedir.

Şayet bilgi sahiplikleri açıkça tanımlanmış değilse ve bilgi sahipleri bilgi güvenliğinden sorumlu tutulmazlarsa ciddi güvenlik riskleri ortaya çıkacaktır. Bilgi güvenliği için sorumluluk, sadece bilgi güvenliği yöneticisine verilmemeli, diğer tüm çalışanlar arasında da paylaştırılmalıdır. Bu hesap verilebilirlik açıkça tanımlanmış olmalı ve doğru örgüt yapılarıyla güçlendirilmelidir (Solms ve Solms, 2004).

Andriole (2014), elektronik tıbbi kayıtların güvenliğini konu alan çalışmasında, mahremiyet içerikli elektronik hasta bilgilerinin güvenliğinin sağlanmasında üç temel güvenlik boyutunu ele almaktadır: Birinci boyut olan "fiziksel güvenlik", cihazların doğrudan sadece yetkili kişilerin erişimine açık olması, beklenmeyen acil durum protokollerinin tesis edilmesi, veri yedekleme, veri kopyalarının tutulması ve kullanım dışı kalan cihazların düzgün bir şekilde yok edilmesi süreçlerini kapsamaktadır. İkinci boyut olan "teknik güvenlik" boyutu, güvenlik duvarlarının kurulu olmasını, güvenli iletişim için SSL teknolojisinin veya sanal özel ağların (virtual private network) kullanılmasını ve şifreleme tekniklerini içermektedir. Üçüncü boyut olan "yönetimsel güvenlik" çerçevesinde ise güvenlik politikalarının dokümante edilmesi ve çalışanların bu politika içeriği kapsamında eğitilmesi vurgulanmaktadır. Kullanıcıların bilgi sistemlerine erişimleri ve erişim sonrası yaptıkları faaliyetleri kullanıcı kimlik bilgileri, tarih ve zaman bilgisiyle birlikte kayıt altına alınmalıdır. Politikaların elektronik veri depolama ve tüm sistemlerin yedeklenmesi süreçlerinde uygulanması, bilgi sistemleri olaylarının raporlanması ve güvenlik olaylarının çözümlenmesi için özel metotların geliştirilmesi gerekmektedir. Politika ve prosedürleri ihlalde bulunanlar için ele alınacak sorumluluk, yaptırım ve disiplin faaliyetleri anlaşılır bir şekilde dokümante edilmelidir. Gaunt da (2000) Andriole'ye benzer şekilde hasta bilgilerinin güvenliğinin sağlanması için, sorumluluk prensibi kapsamında güvenlik politikalarının yaygınlaşması ve ayrıca mahremiyet içerikli bilgileri paylaşan kuruluşlar arasında bilgi güvenliği anlaşmalarının kabul edilmesi gerektiğini vurgulamaktadır. Bununla birlikte sorumluluk ve izlenebilirlik çatısı anlaşılır

bir şekilde oluşturulmadıysa kabul edilecek güvenlik anlaşmalarından beklenen sonuç elde edilemez. Bilgi güvenliği için sorumluluk çatısının tanımlanmaması durumunda bilgi güvenliği politikalarının gerekliliklerinin yerine getirilmesinde zorluklar yaşanacağı aşikârdır.

Bilgi sorumluluğu, ölçülebilir bir insan faktörü olarak bilgi güvenliği ihlal olaylarını azaltmakta ve ortadan kaldırmaktadır. Yasal gereklilikler olduğu müddetçe bilgi sorumluluğu ölçümleri uygulanabilir olmaktadır (Gajanayake, Sahama ve Lane, 2013). Örgütler, çalışanlarına bilgi güvenliği politikaları hakkında eğitimler vererek ve disiplin prosedürlerini oluşturarak sorumluluk kriterini güçlendirebilir (Chang ve Lin, 2007). Bu bağlamda bilgisayar güvenlik programlarında başarıyı elde etmenin anahtarlarından biri eğitimlerle kullanıcılarda güvenlik farkındalığının oluşturulmasıdır. Çalışanlar kurumsal politika ve prosedürlerden haberdar edilmezlerse çalışanların bilgisayar kaynaklarını güvence altına almak için etkili bir şekilde hareket etmeleri beklenemez. Politikaların yaygınlaştırılması ve uygulanması ancak eğitim programları aracılığıyla güçlendirilebilir (Guttman ve Roback, 1995: 144).

Sorumluluk prensibinin ihlali, sorumsuzluk riskini doğurmaktadır. Örneğin sorumluluk prensibine yönelik gerçekleştirilen bir saldırı türü olan maskeleme saldırısında (masquerade attack) IP yanıltma (IP spoofing) gibi teknikler kullanılarak sahte kimlikler taklit edilebilmektedir. IP yanıltma ile saldırgan kişi, bir başka bilgisayardan geliyormuş gibi sahte IP adresleri alarak gerçek kimliğini saklayabilmekte ve sorumluluktan uzak bir şekilde paketler üretebilmektedir (Grzebiela, 2002).

2.8. Örgüt Kültürü ve Bilgi Güvenliği İlişkisi

Dijital çağla birlikte yeni örgütsel yapılar ortaya çıkmakta ve örgüt yapıları yoğun bilgi paylaşımını destekler niteliğe kavuşmaktadır. Dolayısıyla örgüt yapıları, yüksek düzeyde kişiler ve örgütler arası iletişimi kolaylaştırır bir hâle dönüşmektedir. İş süreçlerinde daha verimli, etkili ve duyarlı olabilmek için örgütler, bilgisayar ağlarının ve bilgisayar temelli bilgi sistemlerinin kullanımına önem vermektedir. Bununla birlikte bilgi ve iletişim teknolojilerinin kullanımı bilgisayar istismarı olaylarını da beraberinde getirmektedir (Dhillon ve Backhouse, 2000). Diğer bir ifadeyle büyük miktarda verinin elektronik ortamda depolanıyor ve işleniyor olması, bilgi teknolojilerinin doğasında yer alan

zayıflıklardan kaynaklı bilgi güvenliği kuşkularının oluşmasına neden olmaktadır (Chiu ve Chen, 2005).

Bilgisayar Güvenliği Enstitüsü (Computer Security Institute) ve Federal Soruşturma Bürosu tarafından yürütülen, 2004 yılında bilgisayar suçları ve güvenliği konulu araştırmanın sonuçlarına göre, yıllar içerisinde bilgisayar sistemlerine yapılan saldırılarda veya sistemlerin kötü niyetli kullanımında sabit ve yavaş bir azalış sergilendiği görülürken, ortalama olarak firmaların bildirdiği yıllık kayıplarda ve her bir saldırı olayı başına düşen zararlarda bir yükseliş olduğu görülmüştür. Bu ters yönlü eğilim, örgütlerin son yıllarda şifreleme, erişim kontrolü ve saldırı tespit sistemleri gibi daha çok teknik konulardaki bilgisayar güvenliği uygulamalarına odaklanmalarından kaynaklanmaktadır. Bilgi güvenliği sistemlerine yatırım yapılması kadar çalışanların bilgi güvenliği hususundaki örgütsel bağlılıkları ve herkesçe bilgi güvenliği amaçlarının anlaşılıyor olması gittikçe önemli bir hâl almaktadır (Chang ve Lin, 2007).

Bilgi güvenliğinin amacı bilgi, donanım, yazılım ve çalışanlar gibi değerli varlıkların korunmasıdır. Bunun etkin bir şekilde tesis edilmesi için, güvenlikle alakalı risklerin anlaşılması, bu kapsamda uygun kontrollerin geliştirilmesi ve uygulanması gerekmektedir. Çalışanlar tarafından kontroller ne derece uygulayabiliyorsa örgüt güvenlik seviyesi de o derece artacaktır. Şayet kontrol ve prosedürlerin neden uygulandığı ve neyi hedeflediği tam manasıyla anlaşılmıyor ise en iyi şekilde tasarlanmış olsalar dahi teknik kontrol ve prosedürlerden beklenen fayda elde edilemeyecektir. Bilgisayar Güvenliği Enstitüsü tarafından tüm bilgisayar ağlarının kötüye kullanılma eylemlerinin %60 ile %80 arasındaki büyük çoğunluğunun örgüt içindeki insanlardan kaynaklı olduğu tahmin edilmektedir (Woodhouse, 2007). Nitekim 874 bilgi sistemleri güvenlik uzmanına (CISSP - Certified Information Systems Security Professional) yöneltilen bir anket çalışmasında da bilgi güvenliğini etkileyen 25 adet konuya ulaşılmış ve yüksek puanlı ilk 18 konunun 10'u teknik konulardan ziyade yönetimsel faaliyetlerle alakalı çıkmıştır. İlk 2'de yer alan güvenlik konusu da sırasıyla üst yönetimin desteği ve kullanıcı farkındalık eğitimleri olarak tespit edilmiştir (Knapp, Marshall, Rainer ve Morrow, 2006).

Çalışanların örgüt başarısında kritik öneme sahip olduğu yadsınamaz bir gerçektir, fakat hâlâ bilgi güvenliği konusundaki en zayıf halkayı çalışanlar teşkil etmektedir. Örgüt içi kaynaklı güvenlik olayları sayıca örgüt dışı kaynaklı olanları geçmekte ve bu durum,

örgütlerin çalışmasına karşı en büyük tehdit olarak algılanmaktadır (Vroom ve Solms, 2004). Danışmanlık şirketi PricewaterhouseCoopers tarafından 2004'te yürütülmüş bilgi güvenliği ihlallerini konu alan anket çalışmasında da birçok güvenlik ihlalinin teknolojik eksikliklerden ziyade insan hatalarından kaynaklandığı sonucuna ulaşılmıştır (Veiga ve Eloff, 2007). Bilgi güvenliği alanında fiziksel ve teknolojik manada yapılan harcamalar artmasına rağmen, personel hataları ve aldatılmalarının sonucu olarak bir dizi güvenlik olayıyla karşılaşılmaya devam edilmektedir (Chan ve diğerleri, 2005).

Bilgi güvenliği tehditleri ve zayıflıkları sürekli değişim içinde olduğundan bilgi güvenliği risklerinin azaltılmasında çözümlerin kusursuz oluşturulması kolay olmamaktadır. Bilgisayar ağının bir bileşeninin kasıtlı ya da hatayla riske atılmasından ağa bağlı herkes olumsuz yönde etkilenebilir. Bu durum, iş süreçlerinde bilgisayar ağlarına bağımlı olmanın beraberinde getirdiği bir tehlikedir. Peki bu tehlikeyi bertaraf etmek için ne yapılmalıdır? Bu soruya cevap olarak akıllara, öncelikle daha fazla teknolojik yatırımın yapılması gerekliliği gelebilir. Fakat esas olan çalışanların bilgi güvenliği algısının oluşturulması olmalıdır. Kültürel değişim yoluyla grupların bilgi teknolojileri güvenliğini nasıl algılaması gerektiği sağlanabilir. Diğer bir ifadeyle bilgi güvenliği algısının oluşmasında, kültürel değişime ihtiyaç duyulmaktadır (Carblanc ve Moers, 2003).

Bilgi güvenliği konusu genellikle teknolojik konularla alakalı olarak gözükse de güvenliğin insanlarla da ilişkili olduğu sıklıkla gözlemlenmektedir. Bilgi güvenliğinin sağlanmasındaki en önemli husus, insanlarda doğru zihniyetin kurulması ve insanların güvenliği sağlamak adına veya en azından güvenlik bakış açısıyla çalışmalarını yürütüyor olmasıdır. Ne yazık ki insanlar bu konuda bir varlık olmaktan çok bir engel olarak algılanılmaktadır (Furnell ve Thomson, 2009). Bu bağlamda insan faktörünün bilgi güvenliği yapısı içerisindeki yerinin anlaşılıyor olması önem arz etmektedir. Kişilerin bilgi güvenliği yönetimi uygulamalarına yönelik uyumlarındaki algı ve güdüleri, güvenlik olaylarıyla alakalı teknolojik çözümlerin azaltılmasında faydalı olmakta olup hangi tür koruyucu önlemlerin alınması gerektiği hususunda yol gösterici olabilmektedir (Ahlan ve diğerleri, 2015).

Bilgi güvenliği, teknolojiyi, süreçleri ve insanları kapsamaktadır. Şifreleme sistemleri, anti virüs yazılımları, kimlik doğrulama mekanizmaları ve güvenlik duvarları gibi teknolojik çözümler, bilgiye karşı oluşabilecek tehditlerin azaltılmasında tek başına yetersiz

kalmaktadır. Bilgi güvenliği ilk aşamalarda, bilgi teknolojileri ortamının korunmasında daha çok teknik bir yaklaşım olarak nitelendirilmekteydi. Örgütlerdeki teknik vasıflı kişiler zamanla bilgi güvenliğinde yönetimin önemli bir rol oynadığının ve üst yönetimin de bilgi güvenliği süreçlerine dâhil edilmesi gerektiğinin farkına vardılar. Bu durum, bilgi güvenliğinin örgütsel yapı ile bütünleşmesi aşamasına geçişi sağlamış oldu. Bu aşamayla birlikte daha önceleri ihmal edilen insan faktörü, öncelikle adreslenmesi gereken büyük bir bilgi güvenliği tehdit kaynağı olarak algılanmaya başlandı. Bilgi güvenliğinde gelinen son aşamada ise bilgi güvenliğinin, günlük faaliyetlerle ve çalışanların iş yapış şekilleriyle bütünleşmesinin gerekli olduğu vurgulanmaktadır (Veiga ve Eloff, 2007).

Hem bireysel hem de örgütsel açıdan bilgi güvenliği önemli bir konudur. Bu konuda uzmanların genel düşüncesi, bilgi için güvenli bir ortamın yalnızca teknolojik çözümlerle garanti edilemeyeceği yönündedir. Bilgi güvenliği alanında teknolojik çözümlerin yanı sıra kullanıcı davranışları önemli bir faktör olarak değerlendirilmelidir. Kullanıcılar tarafından kasıtlı ya da ihmalkârlıkla bilgi güvenliğini tehdit eden davranışlar sergilenmesi, bilgisayar korsanlarının bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini kendi çıkarları doğrultusunda değiştirmeye yönelik saldırılarına fırsat vermektedir. Hesap bilgilerini paylaşma, İnternet'ten yazılım indirme, parolaları not kağıtlarında yazılı hâlde bulundurma, sosyal güvenlik numaralarını kullanıcı adı veya parolası olarak belirleme kullanıcı hatalarının başlıcaları arasında yer almaktadır. Güvenlik ihlalleri genellikle kullanıcıların ihmalkârlığı, bilgisizliği, ilgisizliği, disiplinsiz hareketleri, direnç göstermeleri ve farkındalık eksikliğinden kaynaklanmaktadır. Bu bağlamda bilgi güvenliğinin tesisinde karşılaşılan ana sorun, kullanıcılar tarafından sergilenen bilgi güvenliğine aykırı davranışlardır (Safa ve diğerleri, 2015). Örgütlerde bilgi güvenliği kültürü, çalışanların algısını ve bilgi güvenliği ile alakalı davranışlarını etkilemektedir. Örgüt içindeki kişiler tarafından kaynaklanabilecek birçok bilgi güvenliği tehdidi çalışanların bilgi güvenliği algısı ile engellenebilir (Alhogail, 2015). Diğer bir ifadeyle bilgi güvenliği, bilgi güvenliğinin önemi hususundaki kullanıcı algısı olarak tanımlanmaktadır (Kruger ve Kearney, 2006).

Solms ve Solms (2004) çalışmalarında örgüt bünyesinde bilgi güvenliği planlarının uygulanmasını olumsuz yönde etkileyecek 10 büyük temel yanlışı şu şekilde sınıflandırmışlardır:

1. Bilgi güvenliğinin örgüt yönetiminin sorumluluğunda olarak algılanmaması,
2. Bilgi güvenliğinin teknik boyutta ele alınıp yönetimsel boyutta ele alınmaması,
3. Bilgi güvenliği yönetiminin çok boyutlu bir disiplin olduğunun göz ardı edilmesi,
4. Bilgi güvenliği planlarının tanımlanan riskler temelinde oluşturulması gerekliliğinin kavranamaması,
5. Bilgi güvenliği yönetiminde uluslararası kabul görmüş uygulamaların dikkate alınmaması,
6. Bilgi güvenliği politikalarının mutlak surette gerekli olduğu algısının oluşmaması,
7. Bilgi güvenliğine uyum sağlanmasının ve bu manada izlenebilirliğin (sorumluluğun) gerekli olduğu düşüncesinin hâkim olmaması,
8. Uygun bilgi güvenliği yönetim yapısının kesinlikle gerekli olduğunun farkına varılamaması,
9. Kullanıcılar arasında bilgi güvenliği farkındalığının kritik öneme sahip olduğunun anlaşılamaması,
10. Bilgi güvenliği yöneticilerinin, sorumluluklarını düzgün bir şekilde yerine getirmelerine yardımcı olacak altyapı ve araçlar ile desteklenmemesi.

Yukarıda sınıflandırılan bu 10 temel yanlış doğrultusunda bireylerin davranışlarını şekillendiren örgüt kültüründe, bilgi güvenliği ile alakalı önemli değişiklikler olmadığı müddetçe, teknik düzeyde temin edilen çözümlerden istenilen düzeyde bilgi güvenliği performansının elde edilemeyeceği söylenebilir (Solms ve Solms, 2004). Örgüt kültürü genel olarak bireylerin tutum ve davranışlarını yöneten ve şekillendiren paylaşılan değerler, inançlar, varsayımlar ve uygulamalar bütünü olarak tanımlandığından, çalışan davranışlarının güvenlik faaliyetleri üzerinde nasıl bir etkiye sahip olabileceğinin araştırılmasında örgüt kültürünü anlamak faydalı olacaktır (Lim, Chang, Maynard ve Ahmad, 2009).

Bilgi güvenliği örgüt misyonunu desteklemeli, uygun maliyetlerle tesis edilmeli ve örgüt kültürüyle uyum içerisinde yürütülmelidir. Ayrıca bilgi güvenliği, teknolojiyi, süreçleri ve insanları bir bütün olarak kapsamalıdır. Örgüt kültürü, son kullanıcı farkındalığının seviyesini yansıtan öğrenilen davranışlar sistemi olup bilgi güvenliği süreçlerinin başarı veya başarısızlığı üzerinde etkiye sahip olabilmektedir. Güvenlik kültürü, bireylerin örgüt içinde güvenliği nasıl algıladıklarını tanımlamak için kullanılmaktadır. Bilgi güvenliğinin etkin ve proaktif olarak sağlanabilmesi için, tüm çalışanlar pasif birer gözlemci olmaktansa

aktif birer katılımcı olmalıdır. Bunu yaparken çalışanlar, bilgi güvenliği algısı açısından örgüt kültürünün norm ve değerlerini kuvvetle muhafaza etmeli ve yaygın bir şekilde paylaşıyor olmalıdırlar (Koskosas ve diğerleri, 2011). Bununla birlikte örgüt kültürü örgüt stratejisi ile uyumlu olmadıkça, herhangi bir iş sürecinde olumlu değişikliklerin elde edilemeyeceği açıktır. Dolayısıyla bilgi güvenliğinde başarılı sonuçlar elde etmek için, örgüt kültürünün stratejik hedefler ile uyumlu hâle getirilmesi gerekmektedir (Kannan ve Sivasubramanian, 2016).

İnsan unsuruna dayanan ve insanları hedef alan bilgisayar korsanlığı saldırıları diğer saldırı türlerine göre daha kolay gerçekleştirilebildiğinden önlenmesi en zor bilgi güvenliği tehditlerinden sayılmaktadır. İnsanların kendilerine özgü ifadeler ile kolaylıkla kandırılma eğilimi içinde olmalarından dolayı sosyal mühendislik saldırılarına karşı savunmasız kalınmaya devam edilmektedir. Bu tür saldırılara karşı alınacak en iyi önlem, kişilere bilgi varlıklarının değerinin farkında olmaları hususunda eğitim verilmesidir. İnsanları kandırmaya yönelik gerçekleştirilen bu tür saldırılar hakkında farkındalık yaratmak, sosyal mühendislik faaliyetlerinin teşhis edilmesini kolaylaştırmaktadır. Sosyal mühendislik riskini azaltmak için, kullanıcılara eğitimlerin verilmesi ve bilgi güvenliği farkındalığının oluşturulması, kendisini saldırılara karşı savunmak zorunda kalan bir örgüt veya kişi için zorunlu hâle gelmektedir. Bu nedenle bir örgütün, tüm çalışanlarında güvenlik farkındalığı oluşturma amaçlı eğitim programları hazırlaması gerekmektedir. Bu eğitim programları, çeşitli sosyal mühendislik saldırı tekniklerini ve bu tür saldırılara karşı nasıl mücadele edileceğini vurgulamalıdır. İnsanlar sosyal mühendislik saldırılarına maruz kaldıklarında ilk olarak savunma mekanizması olarak soğukkanlı ve bilinçli davranış sergilemelidir. Örneğin kimlik avı saldırılarını bilen bilinçli bir kişinin, hesap bilgilerinin güncellenmesini isteyen bir e-posta alması durumunda, istenilen güncellemeleri yapma olasılığı düşük olacaktır. İnsanlar sahip oldukları bilginin değerini daha iyi kavradıkça, bilginin nasıl ele alınacağı konusunda daha dikkatli davranırlar. Örneğin çöpe atılması gereken bilgisayardaki verilerin veya kâğıt formatında değerli bilgiler içeren dokümanların imha edilmesi esnasında gereken özeni gösterirler. Etkili bir güvenlik farkındalığı, davranışların güvenilir ve sezgisel hâle geldiği bir durumda ortaya çıkmakta ve böylece çalışanların bilgiyi güvenli bir şekilde ele almalarını sağlayan otomatik bir refleks oluşturmaktadır. Etkili bir bilgi güvenliği farkındalığı neticesinde örgüt genelinde olumlu bir davranışsal ve kültürel değişiklik olmalıdır. Bilgi güvenliği farkındalığı oluşturma stratejisi güvenlik üzerine odaklı olmayı ve çalışanların tutumlarını değiştirmeyi amaçlamalıdır. Güvenlik

hataları, bireylerin çalışmalarını başarıyla tamamlamalarına engel olabilir ve örgütün varlığını tehdit edebilir. Bu noktada, örgütlerin güvenlik farkındalık programlarının değerini anlaması ve çalışanlardaki farkındalık açığını kapatmaya kararlı olması kritik önem taşımaktadır. İyi tasarlanan ve sürekli olarak geliştirilen bir güvenlik farkındalığı programı, çalışanların güvenlik bilincinin güçlendirilmesi üzerinde büyük bir etkiye sahip olabilmektedir. Güvenlik farkındalık programlarının nihai amacı, kullanıcıları bilgi varlıklarının korunması gerekliliği hususunda bilinçlendirmek ve bu çerçevede davranış değişiklikleri oluşturmaktır. Farkındalık eğitimleri ile güvenliğin kritikliği hususunda çalışanlarda algı oluşturulabilir (Okenyi ve Owens, 2007).

Çalışanlarda bilgi güvenliği farkındalığının oluşturulması, örgütlerin güvenlik risklerinden korunmasında büyük rol oynamaktadır. Çalışanlarda bilgi güvenliği farkındalığının eksikliği, önemli bilgilerin paylaşılması, sistemlere yetkisiz erişilmesi ve belgelerin uygunsuz kullanılması gibi ihmalkârlık kaynaklı olumsuz sonuçları doğurabilir (Dahbur, Bashabsheh ve Bashabsheh, 2017). Bilgi güvenliği farkındalığını oluşturma, güvenlik risklerinin sürekli değişiyor olmasından kaynaklı zorlu ve dinamik bir süreci yansıtmaktadır. Dolayısıyla sürekli olarak farkındalık programlarının ölçülüyor ve risk profillerinde meydana gelen değişikliklerin takip ediliyor olması önem arz etmektedir (Kruger ve Kearney, 2006). Bilgi güvenliği farkındalığı, bilgi güvenliği davranışları açısından dikkatli bir tavır takınılmasına yönelik çalışanların tutumunu etkilemektedir. Kültürel normlar, bireyler üzerinde davranışları gerçekleştirme ya da gerçekleştirmeme noktasında toplumsal baskıya yol açmakta ve insanların ne düşündüğünün önemli olduğu algısına işaret etmektedir. Bu bağlamda farkındalık programları, örgüt kültürünün ayrılmaz bir parçası olmalıdır (Safa ve diğerleri, 2015).

Örgütsel bilgi varlıklarının korunması temelde insani bir sorundur. Bir kuruluşun çalışanlarının, kurumun bilgi varlıklarının korunmasında en zayıf halka olduğu yaygın olarak bilinmektedir. Çalışanlar sıklıkla bilgi varlıklarının korunması konusunda kayıtsız kalmakta ve güvenlik tehditlerine tepki göstermemektedirler. Bu nedenle çalışan davranışlarının yönetimin bilgi güvenliği hedefleriyle uyumunu sağlamak ve hedeflerin iletilmemesini veya yanlış iletilmesini önlemek için, bilgi güvenliği temelli örgüt kültürünün geliştirilmesi gerekmektedir. Bununla birlikte çalışanların bilgi güvenliği acil durumlarını veya tehditlerini belirleyebiliyor olmaları önem arz etmektedir. Bu sebeple açıkça yazılı bir şekilde bilgi güvenliği politika ve prosedürlerinin olması hayati önem

taşımaktadır. Ayrıca bu politika ve prosedürlerin içeriği, kapsamlı bilgi güvenliği farkındalığı ve eğitim programları vasıtasıyla çalışanlara iletilmeli ve güvenlik tehditlerinin nasıl tespit edileceği konusunda çalışanlara yol gösterici olmalıdır (Thomson ve Niekerk, 2012). Etkin güvenlik politikalarının geliştirilmesi ve çalışanlara düzenli olarak farkındalık eğitimlerinin verilmesi için, öncelikle çalışanların çevrimiçi davranışlarının anlaşılıyor olması gerekmektedir (Li ve diğerleri, 2014). Çalışanlar arasında paylaşılan örtük varsayımların ve bunlara karşılık gelen inanç ve değerlerin güvenlik politikalarına uygun olması, çalışanların bilgi güvenliği davranışlarında önemli bir rol oynamaktadır (Safa ve diğerleri, 2015).

Etkin bir bilgi güvenliği yönetiminin, bilgi güvenliği politikalarının oluşturulması ve uygulanmasıyla tesis edileceği konusunda yüksek bir fikir birliği söz konusudur (Fulford ve Doherty, 2003). Nasıl ki resmî sistemler yasalar ile kurulmakta ise güvenlik ile alakalı çevreyi de güvenlik politikaları düzene sokmaktadır. Bilgi güvenliği politikalarının olmadığı durumda, güvenlik uygulamaları, hedefler ve sorumluluklar ile sınırlandırılamamakta ve bu durum bilgi güvenliğinde zayıflıklarının artmasına yol açmaktadır. Güvenlik politikaları, bilgi güvenliği yönetiminin başlangıç noktası olup bilgi işlem birimlerinin ve yetkili kullanıcıların birlikteliği ile yürütülmelidir (Higgins, 1999). Çalışanların gizlilik gereksinimlerine uygun olarak bilgileri işlemeleri için, örgütlerde bilgi güvenliği açısından olumlu bir kültürün varlığı gereklidir. Bilgi güvenliği politikaları, bilginin korunması adına çalışanların davranışlarını yönlendirmede kritik bir öneme sahiptir. Bu bağlamda çalışanlar, bilgi güvenliği politikalarının gerekliliklerinden haberdar olmalı ve bunları anlamalıdır. Çalışanların bilgiyi güvenli bir şekilde işleyebilmeleri adına bilgi güvenliği politikalarına uyulması önem arz etmektedir. Bilgi güvenliği politikaları, insan, süreç ve teknoloji kontrollerinin bir kombinasyonu aracılığıyla uygulanmaktadır. İnsan perspektifinden bakıldığında, politikalar bilgiyi işleyen çalışanları yönlendirmekte ve örgütsel bilgi ile uğraşırken etik kararların alınmasını sağlamaktadır. Politikalar ayrıca çalışanların bilgi varlıklarını kullanım biçimini etkilediğinden, insan davranışları yasal, düzenleyici ve sözleşmeye dayalı gerekliliklere uygun olarak yönlendirilebilmektedir. Bir bilgi güvenliği politikasının bilgi güvenliği kültürü üzerinde nasıl bir etkiye sahip olduğunu anlamak için, öncelikle nasıl bir kültürün geliştirileceğinin anlaşılması gerekmektedir. Bilgi güvenliği kültürünün nasıl geliştirileceğinin anlaşılmasında da örgüt kültürü yol gösterici olmaktadır (Veiga, 2015). Bununla birlikte politikalara uyumlulukta genel olarak örgüt kültürünün etkisi mevcuttur. Örgüt kültürü, bilgi güvenliği

politikalarının etkili bir şekilde uygulanmasını sağlamaktadır (Knapp ve diğerleri, 2009).

Örgüt yönetimi, çalışanların güvenlik politikalarına hemen uymalarını beklememeli, bunun yerine öncelikli olarak çalışanların uyması gereken politikaları bir ölçüde sınırlandırmalı, böylelikle davranışların bilgi güvenliğine uygun olarak şekillenmesine olanak sağlamalıdır. Çalışanlar bilgi güvenliği politikalarını öğrendikçe ve politikalara uymaya başladıkça yönetim yavaşça ek politikalar getirerek sonunda tüm politikaların örgüt kültürünün ayrılmaz bir unsuru hâline gelmesini sağlayabilir. Politikalar takip edildikçe çalışanların davranışları değişmektedir. Bu durum aynı zamanda zihniyeti değiştirmekte ve zamanla örgüt kültürü, çalışanların sadece güvenlik kurallarını yerine getirmesini değil, aynı zamanda bilgi güvenliği uyum sürecinin otomatik olmasını ve davranışların, örgüt kültürünün bir parçası olarak bilinç dışı sergilenmesini sağlamaktadır. Örgütsel verilerin korunması ve güvenlik politikalarına uyumun sağlanması için en etkili yol, yönetimin günlük faaliyetlerde güvenliği artırmasıdır. Bunu başarmak için, örgütün tüm üyelerinin farkındalık düzeylerinin yükseltilmesi gerekmektedir. Böylece güvenlik, örgütün diğer bir tabirle örgüt kültürünün ayrılmaz bir parçası hâline gelmektedir. Bu bağlamda yönetim ve güvenlik uzmanlarının bilmesi gereken 3 temel nokta vardır (Corriss, 2010):

1. Güvenliğin örgüt kültürünün ayrılmaz bir unsuru hâline getirilmesi gerekmektedir. Bunun için, öncelikle tüm personel için geçerli olabilecek uygulanabilir ve çalışan verimliliğini engellemeyen güvenlik politikalarının bir alt kümesi belirlenmelidir. Bilgi güvenliği farkındalığı ve uyumu, eğitim, teşvik ve politikalara yukarıdan aşağıya herkesin bağlılık hissetmesi yoluyla sağlanabilir. Politikalara uyum sürecinde yönetim, günlük davranışları etkileyen tüm politikalar norm olarak kabul edilene kadar politikalara aşamalı olarak eklemelerde bulunabilir.
2. Güvenliği kurum kültürüne entegre etmek yukarıdan aşağıya doğru olmalıdır. Bununla birlikte orta düzey yönetimin güvenlik konusunda sürece dâhil edilmesi kritik önem taşımaktadır. Bilgi güvenliği yetkilileri ise değişikliği teşvik etmeye yardımcı olabilir.
3. Bilgi güvenliği ile bütünleşik bir örgüt kültürü, verimlilik artışı gibi diğer yararlar da sağlayacaktır. Uygulamaların yüksek seviyede güvenlikli olması yaşam döngüsü maliyetlerini azaltmakta ve verimliliği artırmaktadır. Ayrıca gelişmiş bir itibarın, kârlılığı artırıcı ve koruyucu ilave yararları olacaktır. Bilgi güvenliğine

uyumun örgüt kültürünün bir parçası hâline gelmesi, bilgi güvenliği risklerini azaltmakta ve bu da sigorta ve denetim maliyetlerinin düşmesine neden olmaktadır. Bununla birlikte iyi bir güvenlik düzeyi, maliyetlerin düşmesini ve etkinliğin artmasını sağlamaktadır.

Bilgi güvenliği uygulamalarının ve prosedürlerinin başarıyla tatbik edilmesinin önündeki en yaygın engellerden biri insan unsurudur. Bilgi varlıklarına en büyük tehdidi genellikle bilinçsiz ve ilgisiz son kullanıcılar oluşturmaktadır. Dolayısıyla güvenlik uygulamalarının davranışların doğal bir parçası hâline gelmesini sağlamak için, örgütlerde bilgi güvenliği kültürünün geliştirilmesi gerekmektedir. Bununla birlikte kültürün değiştirme gücü büyük ölçüde yönetimin elindedir. Yönetimin, bilgi güvenliği kültürünün değişiminde ve geliştirilmesinde başlangıç noktası olarak çalışanların mevcut güvenlik kabul seviyelerini, görüş ve uygulamalarını dikkate alması önemlidir (Furnell ve Thomson, 2009). Üst yönetim desteğinin olmaması durumunda, tüm bilgi güvenliği programları başarısızlıkla sonuçlanmaktadır. Güvenlik çözümleri ve yönetimin desteğiyle bütünleşen bir kültürel değişim olmadığı müddetçe teknolojik çözümlerden beklenen fayda elde edilememektedir. Üst yönetim desteğinin azalmasıyla birlikte güvenlik politikalarının uygulama seviyesinde de düşüş görülmektedir (Knapp ve Ford, 2006). Nitekim Al-Izki ve Weir (2016) tarafından yürütülen çalışmada da üst yönetimin tutumu ile bilgi güvenliği politikalarına uyum arasında güçlü bir ilişkinin varlığı tespit edilmiştir.

Çalışanların iş süreçlerine tabi tuttuğu bilginin risk boyutunu anlıyor olmaları, bilgiyi korumak ve kendi faaliyetlerinde sorumluluk almak adına bilgi güvenliği kontrollerini uygulamaları gerekmektedir. Örgüt genelinde kişisel içerikli gibi tüm hassas ve gizli bilgiler için, bilgi güvenliği ile uyumlu davranışların sergilendiği kültür türünün telkin edilmesi gerekmektedir. Bu açıdan bilginin güvenlik risklerinden korunduğu ve bilginin gizliliğinin sağlandığı bir kültür yapısının oluşturulması zorunludur (Veiga ve Martins, 2015).

Güvenlik kültürü, üst yönetimin güvenliğe bağlılığı, güvenlik konusunda iletişimin varlığı ve bilgisayar sistemlerinin izlenmesi olmak üzere üç temel boyutta oluşmaktadır (D'Arcy ve Greene, 2014). Güçlü bir bilgi güvenliği ortamı, ancak tüm kademe yönetimlerin ve çalışanların katılımıyla sağlanabilir. Bu manada Chan ve diğerleri (2005) tarafından yürütülen çalışmada, üst yönetim uygulamalarının, doğrudan denetleyici uygulamaların ve

çalışma arkadaşları ile sosyalleşmenin, çalışanların bilgi güvenliği algısı ile doğrudan ilişkili olduğu sonucuna ulaşılmıştır.

Pek çok bilgi sistemi doğası gereği güvensiz olduğu için, ekonomik değer açısından bilgiye bağlı olarak faaliyet gösteren her örgütte bilgi varlıklarının korunması adına BGYS'nin tasarlamasına gerek duyulmaktadır. Etkili bir BGYS oluşturmanın önemi dikkate alındığında, öncelikle bu sistemi etkileyen faktörler tanımlanmalıdır. Bilgi güvenliği yönetimi esas olarak teknik ve teknik olmayan faktörlerden etkilenmektedir. Teknik faktörler, farklı donanım ve yazılımları içermektedir. Bununla birlikte bilgi güvenliği yönetimini etkileyen teknik olmayan faktörler arasında bilgi güvenliği farkındalığı, güvenlik politikaları, örgüt boyutu, çalışanların katılımı ve eğitimi, bütçe, yöneticilerin bilgi teknolojileri ile uyumu, yönetim desteği, örgüt kültürü, çevresel belirsizlikler ve çalışılan endüstri türü yer almaktadır. Bu nedenle teknik çözümlerin bilgi güvenliği adına oluşturulan bütüncül bir yöntemin yalnızca bir parçası olduğu ve teknik çözümler hariç diğer çeşitli faktörlerin bilgi güvenliği yönetimini etkilediği görülmektedir. Örgüt kültürünün, örgüt performansı ve örgüt bünyesinde yürütülen bilgi güvenliği faaliyetleri üzerinde etkiye sahip olmasından dolayı yöneticilerin, güvenlik hedeflerini ilerletmek adına örgüt kültürünü önemli bir faktör olarak değerlendirmeleri gerekmektedir. Ne yazık ki örgütlerin çoğunda teknik çözümlerin güvenlik sorunlarına hızlı ve anlık cevap verdiği düşünülmektedir. Bununla birlikte her ne kadar en iyi donanım veya yazılım sistemleri kullanılıyor olsa da kullanıcıların güvenlik parametrelerini takip etmemeleri, güvenlik farkındalığının oluşmaması veya genel manada örgütün güvenlik çözümlerinin örgüt kültürüyle uyuşmaması doğru bilgi güvenliği yapısına ulaşmada sorun oluşturacaktır. Bilgi güvenliğine ilişkin kullanılan teknolojik güvenlik ürünlerinin insanlar tarafından işletilmesi ve yönetilmesi gerektiği için, teknolojik güvenlik çözümleri tek başına iyi bir güvenlik yönetimi politikası ve uygulaması olmaksızın bir örgütü bilgi güvenliği tehditlerine karşı koruyamaz. Bu nedenle örgütler, hem bilgi güvenliği hem de örgüt kültürü yönlerini birleştiren, sadece görünür ve sesli formdaki yapay dokulara, davranış kalıplarına değil aynı zamanda insanın iç doğasına, aktivitelerine, saklı ve bilinçaltı ilişkilerine odaklanan entegre bir stratejiyi benimsemelidir. Örgüt kültürü her seviyedeki örgütsel davranışlardan etkilendiği için, bilgi güvenliği ile ilgili örgütsel davranışları anlamak ve geliştirmek adına örgüt kültürünün bilgi güvenliği yönetim uygulanmalarını nasıl etkilediği incelenebilir. Ayrıca bilgi güvenliği amacı doğrultusunda örgüt liderleri, örgüt kültürünü şekillendirmek için uygun seçimler yaparak ve değişik yaklaşımlara ayak uydurarak bilgi güvenliği

girişimlerinin başarısını artırmak adına elverişli bir ortam yaratabilirler (Ebrahimi ve Naini, 2012).

Her örgütün, birtakım varsayımlar, değerler, normlar içeren ve örgüt içindeki faaliyetleri yönlendiren belirli bir kültürü vardır. Örgüt kültürü, çeşitli şekillerde tanımlanmakta ve örgütün karakter ve normlarının tanımlanmasına yardımcı olan yönetim tarzları, ödül sistemleri, iletişim şekilleri ve karar verme tarzları gibi birçok tanımlanabilir değer setleriyle ifade edilmektedir. Örgüt kültürü kuşkusuz çalışanların davranışlarını ve tüm örgütün faaliyetlerini etkilemektedir. Bu açıdan değerlendirildiğinde bir örgütün BGYS uygulamalarının örgüt kültürü tarafından desteklenmesi ve yönlendirilmesi gerekmektedir. Birçok araştırmacı tarafından da bilgi güvenliğinin teknik bir konu olmaktan çok yönetimi ilgilendiren bir husus olduğu vurgusu yapılmaktadır. Örgütteki güvenlik kültüründe köklü değişiklikler yapılmadıkça bilgi güvenliği yönetiminde istenilen düzeyde etkinlik elde edilemeyecektir (Tang ve diğerleri, 2016).

Örgüt kültürü, en temel ifadeyle öğrenilen davranışlar sistemidir. Öğrenilen davranışlar, bilgi güvenliği süreçlerinin başarısını önemli ölçüde etkileyen son kullanıcı farkındalık seviyesini yansıtmaktadır. Son zamanlarda bilgi güvenliği bilgi teknolojileri konusu olmaktan çıkıp ağırlıklı olarak yönetimi ilgilendiren bir konu olmaya başlamıştır (Woodhouse, 2007). Çalışanlar üzerinde çevre baskısı uygulayan kültürel normlar, paydaşların bilgiye ve bilgi güvenliğine değer verme düzeylerini de etkilemektedir (Tajuddin ve diğerleri, 2015).

Bilgi güvenliğinin insan boyutu, örgüt içindeki bilgi varlıkları ile doğrudan temas hâlindeki her bir bireyin davranışıyla alakalıdır. Bilgi güvenliği kültürü, bilgi güvenliğinin herkesin sorumluluğunda olmasını sağlamayı amaçlamaktadır (Alhogail, 2015). Bilgi güvenliği kültürünün oluşturulması için, iki temel hususun gerçekleşmesi gerekmektedir. İlk olarak davranışları etkileyen, çalışanları ve yöneticileri politikalarda var olan doğru şeyleri yapmaları hususunda teşvik eden veya yanlış eylemler hususunda da engelleyen çevresel faktörler tanımlanmalıdır. İkinci olarak da bilgi güvenliği için kritik olan hem iç hem de dış faktörleri idare eden etkili bir yönetim stratejisi uygulanmalıdır. Bireysel bilgi ve beceriler önemli olmakla birlikte çalışanların davranışlarına bağlı şekillenen bilgi güvenliği kültürünün oluşumunda tek başına yeterli olamamaktadır. Kişilerin inanç seti ya da kişisel kültürü, güvenlik davranışlarına yönelik kişisel tutumların etkilenmesinde büyük

rol oynamaktadır. Dolayısıyla davranışsal değişim sürecinde temel inançları anlamak çok önemlidir (Alfawaz ve diğerleri, 2010). Bilgi güvenliği kültürünün oluşturulması ve yönetilmesinde başarının elde edilmesi, bilgi ile etkileşimde bulunan üst yönetimden örgütün tüm kademelerine kadar herkesi içeren takım çalışmasını gerektirmektedir (Alhogail ve Mirza, 2014b). Bilgi güvenliği kültürü, bilgi varlıklarını korumak ve bilgi güvenliğini alışkanlık hâline getirmek amacıyla bilgi güvenliği gereksinimleri ile tutarlı olmak adına nasıl davranılması gerektiğini gösteren algıların, tutumların, değerlerin ve varsayımların bir bütünüdür (Alhogail ve Mirza, 2014a). Benzer bir ifadeyle bilgi güvenliği kültürü, bilginin korunduğu ve gizliliğin örgüt içindeki tüm iş yapış şekillerinin bir parçası olduğu kültür yapısıdır. Bu kültür yapısında çalışanlar, bilginin yaşam döngüsünün tüm zaman dilimlerinde, bilginin gizliliğine ve korunmasına katkıda bulunmakta ve bu doğrultuda tutum, varsayım, inanç, değer ve algılarını sergilemektedirler (Veiga ve Martins, 2015). Bilgi güvenliği kültürü aynı zamanda bilgi ve iletişim teknolojileriyle etkileşimde bulunulduğunda, bilgi varlıklarının güvenliğini tehlikeye atabilecek eylemlerden korunmak adına insan davranışına rehberlik eden bir yapı sağlamaktadır. Algılar, yapay dokular, değerler ve varsayımlar doğrultusunda güvenlikle alakalı doğru davranış modellerini destekleyen kültür yapısı, çalışanların davranışları üzerinde emirle kısıtlamalarda bulunan yasal düzenlemelerden çok daha etkilidir. Bilgi güvenliğinin etkin bir şekilde tesis edilmesinin, ancak çalışanların güvenlik önlemlerini biliyor, anlıyor ve kabul ediyor olmaları durumunda mümkün olacağı aşikârdır (Alhogail, 2015).

Bilgi güvenliği politika ve prosedürleri ile ilgili olarak çalışanların düşünceleri, inançları ve davranışları örgütün bilgi güvenliği kültürü veya iklimi ile daha da geliştirilebilir. Örgütsel bilgi güvenliği kültürü ve bilgi güvenliği farkındalığı seviyesi arasındaki ilişki, çalışanların çoğunluğunun bilgi güvenliği politika ve prosedürlerini yorumlama ve bunlara tepki verme biçimlerinin örgütsel norm hâline gelebileceğini ima etmektedir. Bu manada örgütsel güvenlik kültürü ve normları, çalışanların bilgi güvenliği politika ve prosedürleri bağlamında düşünce, inanç ve davranış biçimlerini etkilemelidir (Parsons ve diğerleri, 2015). Çeşitli teorilere, modellere ve farklı yaklaşımlara rağmen bilgi güvenliğindeki değişimi başarmak, temel varsayımlar, zımnî kanaatler, değerler ve inançlarla uğraşmayı gerektirdiğinden genellikle kolay olmamaktadır (Alhogail ve Mirza, 2014b).

Bilgi güvenliğinin örgüt kültürüyle bütünleşmesi ve kültür ile bir uyum içerisinde

sağlanması için, bilgi güvenliği, örgütteki günlük faaliyetlerin bir parçası olmalı ve çalışanların davranışlarında alışkanlık hâline gelmelidir. Eğer örgüt çalışanları bilgi güvenliği konusundaki rol ve sorumluluklarını bilmiyorlarsa örgütler, bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini korumada zorluk yaşayacaktır (Thomson, Solms ve Louw, 2006). Bu açıdan bilgi güvenliği yönetimi, teknolojide, politikalarda, prosedürlerde, çalışanların günlük faaliyetlerinde ve çalışanların bilgi varlıkları ile etkileşiminde değişikliklere neden olmaktadır (Alhogail ve Mirza, 2014b). Örgüt kültürünün davranışları ve örgütsel yaratıları etkileyen değerlere ve bilinçaltı varsayımlara sahip olması sebebiyle bilgi güvenliği ile örgüt kültürü arasında iç içe geçmiş bir ilişkinin varlığından söz edilebilir (Lim ve diğerleri, 2009).

Schein'in örgüt kültürü katmanları modeline (Bkz. Şekil 2.1) bilgi güvenliği açısından bakıldığında başlangıç katmanı olan görülebilir dokular (yaratılar), örgütte bilgi güvenliği uygulamalarının neler olduğunun ve bilgi güvenliği temelli iş yapış şekillerinin bir göstergesidir. Gerekli beceri ve yeterlilikler olmaksızın, çalışanların bilgi ile ilişkili görevleri güvenli bir şekilde yürütmeleri imkânsız olmaktadır. Gündelik görevlerin güvenli bir şekilde gerçekleşmesi için, çalışanların görevlerin nasıl güvenli bir şekilde yerine getirileceği konusunda yeterli bilgiye sahip olmaları gerekmektedir. Bilgi sistemlerine ve kaynaklarına yetkisiz erişimi engelleyen kilitli kapılar gibi fiziksel güvenlik önlemleri ve çalışanların iş yapış şekillerini bilgi güvenliği perspektifinde düzenleyen bilgi güvenliği politikaları görülebilir dokulara örnek olarak verilebilir. Bilgi güvenliği politikalarının oluşturulmasına temel teşkil eden ve yöneticiler tarafından vurgulanan bilgi güvenliği stratejisi de ikinci katmandaki benimsenen ve paylaşılan değerleri ifade edebilir. Bu manada benimsenen değerler, bilgi güvenliği politikalarının oluşturulmasından sorumlu olan kişilere, politikalara güvenlikle ilgili nelerin dâhil edilmesi gerektiği hususunda yol gösterici olmaktadır. En son katman bilinçaltı varsayımlarda da bilgi güvenliğinin önemine duyulan inançlar yer almaktadır. Örneğin spesifik bir kontrole neden ihtiyaç duyulduğunun çalışanlar tarafından biliniyor olması, bilgi güvenliğinin sağlanmasında temel bir rol oynamaktadır. Özetle örgüt kültürünün, bilgi güvenliği üzerine pozitif veya negatif manada çok büyük etkisi olmaktadır (Niekerk ve Solms, 2010; Vroom ve Solms, 2004).

Bilgi güvenliği kültürü oluşumunda, örgüt kültürünün yapay dokular (yaratılar) katmanı ile diğer katmanları arasında nedensel bir ilişki vardır. Başka bir deyişle görünür dokular ya da "çalışanların bilgi güvenliğine yönelik sergiledikleri davranış biçimleri", benimsenen

değerlerin, gömülü varsayımların ve altta yatan bilgi güvenliği algısının bütünleşik etkisinde kalmaktadır. Etkili bir bilgi güvenliği kültürü oluşumu için gerekli olan bilgi güvenliği algısı, Schein'in örgüt kültürü katmanları modelinde en alta eklenecek dördüncü yeni bir katman olarak da değerlendirilebilir (Niekerk ve Solms, 2010).

3. KAVRAMSAL ÇERÇEVE İLE İLGİLİ ARAŞTIRMALAR

Bu bölümde, kavramsal çerçeve ile ilgili yürütülmüş başlıca çalışmalar beş alt bölümde ele alınmıştır. Birinci alt bölümde, örgüt kültürünü ölçümlemek amacıyla kullanılan Rekabetçi Değerler Modeli'nin farklı uygulama yöntemleri anlatılmıştır. Rekabetçi Değerler Modeli kullanılarak örgüt kültürününün ölçümlendiği, üniversiteler dışındaki örgütlerde yürütülen başlıca çalışmalar ikinci alt bölümde, yurt dışı üniversitelerde yürütülen başlıca çalışmalar üçüncü alt bölümde ve Türkiye'deki üniversitelerde yürütülen başlıca çalışmalar da dördüncü alt bölümde sunulmuştur. Beşinci ve son alt bölümde ise Rekabetçi Değerler Modeli ile ölçümlenen örgüt kültürü ile bilgi güvenliği ilişkisini incelemek amacıyla yürütülmüş çalışmalara yer verilmiştir.

3.1. Rekabetçi Değerler Modeli Uygulama Yöntemleri

Bu alt bölümde, Rekabetçi Değerler Modeli referans alınarak Cameron ve Freeman tarafından geliştirilmiş olan 16 sorulu Örgüt Kültürü Türleri Modeli ve bu modelin daha sonra Cameron ve Quinn tarafından genişletilmesi ile elde edilen 24 sorulu Örgüt Kültürü Değerlendirme Aracı'nın (OCAI - Organizational Culture Assessment Instrument) uygulama yöntemleri anlatılmıştır.

Cameron ve Freeman'ın (1991) Rekabetçi Değerler Modeli'nden yararlanarak geliştirmiş oldukları Örgüt Kültürü Türleri Modeli'nde hiyerarşi, pazar, klan ve adhokrasi olarak sınıflandırılan örgüt kültürü türleri, baskın özellikler, örgütsel liderlik, örgüte bağlılık ve stratejik vurgular olarak belirlenen 4 ayrı boyutta ele alınmaktadır. Örgüt kültürü türleri, her bir boyut altında 4'er soru olmak üzere toplam 16 soru ile betimlenmektedir. Bu ölçeğin işletilmesinde denekler örgüt kültürünün söz konusu 4 boyut altında yer alan sorularına 100 puanı paylaştırmaktadırlar. Başka bir ifadeyle her bir boyutta yer alan 4 soruya verilen cevapların puanları toplamı boyut içerisinde 100'e tamamlanmaktadır.

Cameron ve Freeman'ın geliştirmiş oldukları örgüt kültürünü nicel olarak tanımlayan bu ölçeğe daha sonraları "çalışanların yönetimi" ve "başarı kriteri" olmak üzere 2 yeni boyut daha eklenerek OCAI geliştirilmiştir. Sonuç olarak OCAI ile örgüt kültürü, baskın özellikler, örgütsel liderlik, çalışanların yönetimi, örgüte bağlılık, stratejik vurgular ve

başarı kriteri olmak üzere 6 farklı boyutta değerlendirilmektedir. Bu boyutlar bir bütün olarak örgüt fonksiyonlarının temel kültürel değerlerini ve görülmeyen varsayımlarını yansıtmaktadır. OCAI'da yer alan her bir boyutta da Cameron ve Freeman'ın ölçeğinde olduğu gibi 4 soru yer almakta ve sorulara verilen cevapların puanları toplamı her bir boyut içerisinde 100'e tamamlanmaktadır (Cameron ve Quinn, 2006: 25-29, 151).

Cameron ve Freeman'ın 16 sorulu Örgüt Kültürü Türleri Modeli ve 24 sorulu OCAI ölçeklerinde, her bir boyut içerisinde yer alan 4 soru sırasıyla klan, adhokrasi, pazar ve hiyerarşi örgüt kültürü türlerini temsil etmektedir. Sonuç olarak her bir boyuttaki 1. sorulara verilen cevapların puanlarının ortalaması klan kültürünün, 2. sorulara verilen cevapların puanlarının ortalaması adhokrasi kültürünün, 3. sorulara verilen cevapların puanlarının ortalaması pazar kültürünün ve 4. sorulara verilen cevapların puanlarının ortalaması da hiyerarşi kültürünün örgütün genel örgüt kültürü profilindeki ağırlığını ortaya koymaktadır (Cameron ve Freeman, 1991; Cameron ve Quinn, 2006: 63-65).

Yürütülen örgüt kültürü çalışmalarına bakıldığında, Rekabetçi Değerler Modeli'nin uygulanmasında 100 puanın paylaştırılması yönteminin yanı sıra Likert ölçeğinin kullanıldığı çalışmalara da rastlanılmaktadır. Rekabetçi Değerler Modeli'nin uygulanmasında kullanılan 100 puan paylaştırma yönteminde, her bir örgüt kültürü türüne verilen puan miktarı diğer örgüt kültürü türlerine verilen puan miktarlarına bağlıyken, Likert ölçeğinin kullanımında örgüt kültürü türleri birbirlerinden bağımsız olarak ölçümlenmektedir. 100 puan paylaştırma yönteminde bir örgüt kültürü türü yüksek puan alırken diğer örgüt kültürü türlerinin daha az puan alması gerekmektedir. Buna karşın, Likert ölçeği örgüt kültürü türleri arasında daha gerçekçi ilişkileri ortaya koymaktadır. Likert ölçeğinin kullanımında örgüt kültürü türleri bağımsız olarak değerlendirildiğinden aynı anda birden fazla örgüt kültürü türü yüksek veya az değerler alabilmektedir. Örgüt kültürü ölçümleme çalışmalarında, 4 örgüt kültürü türü arasındaki farklılıkların vurgulanmasının amaçlandığı durumlarda 100 puan paylaştırma yöntemi kullanılabilirken, verilerin karmaşık istatistiki analizlere tabi tutulmasının gerektiği durumlarda ise Likert ölçeği kullanılmaktadır. Rekabetçi Değerler Modeli'nde Likert ölçeğinin kullanılmasının sunduğu avantajlardan biri de genel örgüt kültürü profilinin tanımlanabiliyor olmasıdır. Ayrıca bir örgütün genel kültür profili, sadece bir örgüt kültürü türüyle tanımlanamamakta ve hatta birçok örgütte birden fazla örgüt kültürü türünün özellikleri mevcut olabilmektedir (Quinn ve Spreitzer, 1991).

Quinn ve Spreitzer (1991), 4 boyutlu, toplam 16 sorulu Rekabetçi Değerler Modeli ölçeğini Amerika'daki 86 ayrı firmadan toplam 796 yöneticiye 100 puan paylaştırmalı ve Likert ölçekli olmak üzere 2 ayrı yöntemle uygulayarak söz konusu yöntemlerin karşılaştırmasını yapmışlardır. Çalışmada, hiyerarşi kültürü haricindeki örgüt kültürü türlerinden pazar "rasyonel kültür", klan "grup kültürü" ve adhokrasi "gelişimsel kültür" olarak adlandırılmıştır. Ankete katılanların %13'ü üst düzey yöneticilerden, %45'i orta üstü düzey yöneticilerden, %39'u orta düzey yöneticilerden ve %2'lik kısmı da çalışanlardan oluşmaktadır. Elde edilen sonuçlar incelendiğinde, Likert ölçekli anket sonuçlarının güvenirlik düzeyini temsil eden Cronbach Alpha değerlerinin hiyerarşi kültürü için 0,77, pazar kültürü için 0,78, klan kültürü için 0,84, adhokrasi kültürü için 0,81 olduğu ve 100 puan paylaştırma yöntemiyle elde edilen alpha değerlerine göre daha yüksek çıktığı görülmüştür.

3.2. Rekabetçi Değerler Modeli'nin Üniversiteler Dışında Uygulandığı Başlıca Çalışmalar

Bu alt bölümde, yapılan alanyazın taramasında karşılaşılan, üniversiteler dışında diğer örgütlerde Rekabetçi Değerler Modeli'nin uygulanmasıyla örgüt kültürünün konu alındığı çalışmalara yer verilmiştir.

Libya Ulusal Petrol Şirketi'nde örgüt kültürünün iş tatmini üzerine etkisinin incelendiği bir çalışmada 5'li Likert ölçekli 24 sorulu OCAI anketi, şirket çalışanlarından 280 kişiye uygulanmış ve veri analizine tabi tutulabilecek 227 adet geri dönüş elde edilmiştir. Anketin güvenirlik düzeyini temsil eden Cronbach Alpha değerleri sırasıyla hiyerarşi kültürü için 0,952, pazar kültürü için 0,840, klan kültürü için 0,855 ve adhokrasi kültürü için 0,856 çıkmıştır. Çalışmanın sonucunda, şirket genelinde hiyerarşi kültürünün diğer örgüt kültürü türlerine nazaran baskın olduğu görülmüş ve 4 örgüt kültürü türüyle iş tatmini arasında pozitif bir ilişkinin varlığı tespit edilmiştir (Shurbagi ve Zahari, 2012).

Boggs ve Fields (2010), Kuzey Carolina'daki kiliselerde örgüt kültürüyle kilise performansı arasındaki ilişkiyi araştıran çalışmalarında 7'li Likert ölçekli 24 sorulu OCAI anketini 205 kiliseye uygulamışlardır. 53 kiliseden, %5,6'sı kilise çalışanı olmak üzere toplam 299 katılımcıdan anket sorularına eksiksiz bir şekilde cevap elde edilmiştir. Güvenirlik düzeyini temsil eden Cronbach Alpha değerleri sırasıyla hiyerarşi kültürü için

0,85, pazar kültürü için 0,87, klan kültürü için 0,87 ve adhokrasi kültürü için 0,83 çıkmıştır. Çalışmanın sonucunda, kiliselerin 48'inde klan, 3'ünde hiyerarşi, 2'sinde de adhokrasi kültürünün baskın olduğu, pazar kültürünün ise herhangi bir kilisede baskın olmadığı görülmüştür.

İran Karafarin Bankası'nda örgüt kültürü türleri ve boyutlarıyla strateji uygulama boyutları arasındaki ilişkinin incelendiği bir başka çalışmada banka merkezlerindeki müdür ve uzmanlardan oluşan 136 kişiye 5'li Likert ölçekli 24 sorulu OCAI anketi uygulanmış olup, 101 katılımcı anket sorularına eksiksiz bir şekilde cevap vermiştir. Örgüt kültürü ve strateji uygulama önermelerini içeren anketin güvenirlik düzeyini temsil eden Cronbach Alpha değeri 0,957 çıkmıştır. Çalışmanın sonucunda, örgüt kültürü türleri ve boyutlarıyla strateji uygulama boyutları arasında pozitif ilişkinin varlığı tespit edilmiştir. Özellikle örgüt kültürünün stratejik vurgular boyutunun ve esneklik odaklı klan ve adhokrasi kültürlerinin strateji uygulama üzerindeki etkisinin diğer örgüt kültürü türleri ve boyutlarının etkisine göre yüksek çıktığı görülmüştür (Ahmadi ve diğerleri, 2012).

Türkiye'de inşaat endüstrisinde faaliyet gösteren örgütlerin genel örgüt kültürü profilini ortaya çıkarmaya yönelik yürütülen çalışmada da 5'li Likert ölçekli 24 sorulu OCAI anketi kullanılmıştır. Bu çalışma kapsamında 351 firma ile irtibata geçilmiş ve ankete dönüş veren 134 firmadan toplam 826 adet cevap elde edilmiştir. Güvenirlik düzeyini temsil eden Cronbach Alpha değerleri sırasıyla hiyerarşi ve pazar kültürleri için 0,86, klan ve adhokrasi kültürleri için 0,89 çıkmış olup, Türkiye'deki inşaat sektörünün genel örgüt kültürü profilinde klan kültürünün diğer örgüt kültürü türlerine nazaran baskın olduğu sonucuna ulaşılmıştır (Yazıcı, Giritli, Oraz ve Acar, 2007).

Türkiye'de, Ankara'da bulunan ihtisaslaşmış iki hastanede ve Edirne'nin Uzunköprü ilçesinde bulunan genel hizmet hastanesinde yürütülen bir diğer çalışmada da Cameron ve Freeman'ın 16 sorulu Örgüt Kültürü Türleri Modeli anketi 100 puan paylaştırma cevaplama yöntemiyle uygulanmıştır. 367 hastane çalışanına uygulanmış ankete veri analizine tabi tutulabilecek 343 katılımcıdan geri dönüş elde edilmiştir. İhtisas hastanelerinde adhokrasi, genel hizmet hastanesinde hiyerarşi ve çalışmaya dâhil edilen hastanelerde genel örgüt kültürü profili olarak hiyerarşi kültürünün baskın olduğu görülmüştür. Ayrıca çalışmada hiyerarşi kültürünün hâkim olduğu hastanelerin idari tutum ve sahip oldukları değerler setinin çalışanları motive etmediği sonucuna ulaşılmıştır

(Aydıntan ve Göksel, 2012).

Türkiye'de, Elazığ il merkezinde bir üniversite hastanesi, üç devlet hastanesi ve iki tane de özel sağlık kuruluşu olmak üzere toplam altı hastanede, örgüt kültürüyle örgütsel bağlılık arasındaki ilişkiyi araştıran bir diğer çalışmada da Cameron ve Freeman'ın 16 sorulu Örgüt Kültürü Türleri Modeli anketi 100 puan paylaştırma cevaplama yöntemiyle uygulanmıştır. Araştırmanın örneklemi hekim, hemşire, idari personel ve diğer sağlık personeli olmak üzere toplam 256 çalışandan oluşmuştur. Araştırmanın bulgularına göre, verilerin toplanmış olduğu tüm hastanelerin genel örgüt kültürü profilinde hiyerarşi kültürünün baskın çıktığı ve hiyerarşi kültürünü sırasıyla pazar, adhokrasi ve klan kültürlerinin takip ettiği sonucuna ulaşılmış; çalışanların hastanelerini daha çok kontrollü bir yapıya sahip mekanik süreçler boyutundaki hiyerarşi ve pazar kültürleri ile tanımladıkları görülmüştür. Bununla birlikte hiyerarşi kültürünün baskınlık düzeyinin, en fazla üniversite hastanesinde olmak üzere kamu hastaneleri genelinde daha yüksek çıktığı gözlemlenmiştir. Ayrıca örgütsel bağlılık ile klan ve adhokrasi kültürleri arasında pozitif, hiyerarşi ve pazar kültürleri arasında da negatif ilişkinin varlığı tespit edilmiş; önem sırasıyla örgütsel bağlılık üzerinde klan kültürünün pozitif, pazar kültürünün de negatif yönde etkiye sahip olduğu sonucuna ulaşılmıştır (Erdem, 2007).

Türkiye'de, İstanbul'un farklı ilçelerinde bulunan üç farklı zincir hastanenin merkez hastanelerinde, örgütsel sessizlik ile algılanan bireysel performans, örgüt kültürü ve demografik değişkenler arasındaki etkileşimi sorgulayan bir başka çalışmada da örgüt kültürü ölçeği için 24 sorulu OCAI anketi kullanılmıştır. Katılımcılardan 100 puan paylaştırma cevaplama yöntemiyle örgüt kültürünün mevcut ve arzulanan durumlarını ortaya koymaları istenmiştir. Araştırmanın örneklemi hastanelerde çalışan hemşirelerden oluşmuş olup, eksik veriler ve uç değer analizlerinin ayıklanması sonucunda 102 bireyin verisi analize dâhil edilmiştir. Güvenirlik düzeyini temsil eden Cronbach Alpha değerleri hiyerarşi kültürü için 0,823, pazar kültürü için 0,618, klan kültürü için 0,764 ve adhokrasi kültürü için 0,594 olarak hesaplanmıştır. Araştırmanın bulgularına göre, çalışmaya konu olan hastanelerin genel örgüt kültürü profilinde hiyerarşi kültürünün 27,98 ortalama ile diğer örgüt kültürü türlerine nazaran baskın olduğu sonucuna ulaşılmıştır. Ayrıca arzulanan örgüt kültürü türleri incelendiğinde ise klan kültürünün 30,36 ortalama ile en yüksek puanı aldığı görülmüştür (Aktaş ve Şimşek, 2014).

Malezya'nın Kedah Eyaleti'nde ilkokul seviyesindeki yüksek performanslı ve düşük performanslı okulların örgüt kültürünün mevcut ve arzulanan durumlarının tanımlanması amacıyla yürütülen bir başka çalışmada da ölçek olarak 24 sorulu OCAI anketi 100 puan paylaştırma cevaplama yöntemiyle uygulanmıştır. Basit tesadüfi örnekleme ile Kedah Eyaleti'ndeki iki yüksek performanslı okul için 129, iki düşük performanslı okul için de 100 ilkokul öğretmeninden veriler elde edilmiştir. Araştırmanın bulgularına göre, hem yüksek performanslı hem de düşük performanslı ilkokullarda mevcut baskın örgüt kültürünün hiyerarşi olduğu ve bunu sırasıyla pazar, klan ve adhokrasi kültürlerinin takip ettiği ortaya konmuştur. Ayrıca verilerin toplanmış olduğu 4 okulun tamamında, arzulanan örgüt kültürü türleri incelendiğinde ise en yüksek puanı klan kültürünün aldığı görülmüştür (Daud, Raman, Don, Sofian ve Hussin, 2015).

Filipinler'de yer alan Buhatan Ulusal Lisesi'nde çalışan personel üzerinde yürütülen çalışmada da OCAI ölçeğine göre mevcut ve arzulanan kültür türlerinin tespit edilmesi ve etkinlik düzeyinin müdür, öğretmenler ve görevliler düzeyinde değerlendirilmesi amaçlanmıştır. OCAI anketi, 0-4 arası puanlamalı 5'li Likert ölçeği ile uygulanmıştır. Toplam 34 kişiden elde edilen sonuçlara göre, okulda öğretmenlerin akademik ve idari roller üstlendikleri görülmüş olup, baskın mevcut örgüt kültürünün 3,27 ile klan ve arzulanan örgüt kültürünün de 3,00 ile yine klan olduğu sonucuna ulaşılmıştır (Ocbian ve Dichoso, 2015).

Rawalpindi ve Islamabad'da faaliyet gösteren girişimci örgütlerde, örgüt kültürü türlerinin çalışanların iş doyumu üzerine etkisini araştıran bir diğer çalışmada da 24 sorulu OCAI anketi 5'li Likert ölçeği kullanılarak uygulanmıştır. Anket formlarının gönderilmiş olduğu 25 örgütün 11'inden toplam 120 adet geri dönüş elde edilmiştir. Güvenirlik düzeyini temsil eden Cronbach Alpha değerleri hiyerarşi kültürü için 0,713, pazar kültürü için 0,827, klan kültürü için 0,710 ve adhokrasi kültürü için 0,812 olarak hesaplanmıştır. Çalışmaya konu olan girişimci örgütlerin genel örgüt kültürü profilinde klan kültürünün diğer örgüt kültürü türlerine nazaran baskın olduğu, klan kültürünü de adhokrasi kültürünün takip ettiği sonucuna ulaşılmıştır. Klan ve adhokrasi kültürlerine dayalı çalışanların işlerinden memnun olduğu, hiyerarşi ve pazar kültürleri altında çalışanların iş doyumlarının ise düşük olduğu sonucu elde edilmiştir (Fatima, 2016).

Türkiye İş Kurumu'nda (İŞKUR) örgüt kültürü profilini araştıran bir diğer çalışmada da 16

maddeden oluşan Rekabetçi Değerler Modeli ölçeğinin öngörülen kuramsal modele uyumu doğrulayıcı faktör analiziyle tespit edilmiş ve modelin örgüt kültürünü incelemek için kullanılabileceği görülmüştür. Ankara'da bulunan İŞKUR Genel Merkezi'ne bağlı 11 farklı daire başkanlığında çalışan toplam 502 kişiye uygulanmış olan ankete veri analizine tabi tutulabilecek 161 katılımcıdan geri dönüş elde edilmiştir. Katılımcılar, ölçeği 5'li Likert ölçeği üzerinden cevaplamışlardır. Anketin güvenirlik düzeyini temsil eden Cronbach Alpha değerleri örgüt kültürünü ölçümleyen tüm maddeler dikkate alındığında hiyerarşi kültürü (bürokrasi kültürü) için 0,75, pazar kültürü için 0,865, klan kültürü için 0,82 ve adhokrasi kültürü (girişimci kültür) için 0,86 çıkmıştır. En yüksek skor değeri klan kültürü için elde edilmişken, en düşük skor değerini adhokrasi kültürünün aldığı sonucuna ulaşılmıştır. Her ne kadar klan kültürünün skor değeri, diğer örgüt kültürü türlerine kıyasla daha yüksek hesaplanmış olsa da klan kültürünün, genel örgüt kültürü profilinde kurumu tanımlayacak seviyede yer almadığı ve çalışanlar tarafından güçlü bir şekilde paylaşılan bir kültür türü olmadığı yorumu yapılmıştır (Özdemir, 2015).

3.3. Rekabetçi Değerler Modeli'nin Yurt Dışı Üniversitelerde Uygulandığı Başlıca Çalışmalar

Bu alt bölümde, yapılan alanyazın taramasında karşılaşılan, yurt dışı üniversitelerde Rekabetçi Değerler Modeli'nin uygulanmasıyla örgüt kültürünün konu alındığı çalışmalara yer verilmiştir. Bu çalışmaların en başında, üniversiteler dışında diğer örgütlerde yürütülen Rekabetçi Değerler Modeli uygulamalarına da temel teşkil etmiş olan, Cameron ve Freeman'ın Örgüt Kültürü Türleri Modeli'ni oluşturdukları çalışma gelmektedir.

Cameron ve Freeman (1991), çalışmalarında örgüt kültürü türleri, rekabetçi değerler boyutları dâhilinde örgüt kültürü uyumlulukları ve kültür türlerinin baskınlık seviyeleri ile örgütsel etkinlik arasındaki ilişkilerin varlığını araştırmışlar ve bu kapsamda Rekabetçi Değerler Modeli'nden yararlanarak geliştirmiş oldukları 16 sorulu Örgüt Kültürü Türleri Modeli ölçeğini 100 puan paylaştırma cevaplama yöntemiyle Amerika'daki 4 yıllık yüksek eğitim veren yüksekokul ve üniversitelerden 334'üne uygulamışlardır. Bu okulların 29'u (%9'u) doktora seviyesinde yüksek eğitim veren okuldan, 127'si (%38'i) sanat okulundan, 157'si (%47'si) dört yıllık özgür sanatlar enstitüsünden ve 21'i de (%6'sı) işletme, sağlık veya askerî gibi özel alanlarda eğitim veren okullardan oluşmaktadır. Her bir okuldan 12 ile 20 arasında dönüş elde edilmiş olup, toplamda 3406 kişi anket sorularına eksiksiz bir

şekilde cevap vermiştir. Cevap verenlerin 1317'si yönetimde yer alanlardan, 1162'si fakülte ve bölüm yöneticilerinden ve 927'si de mütevelli heyet üyelerinden oluşmaktadır. Çalışma sonunda hiçbir okulun sadece 1 örgüt kültürü ile tanımlanamadığı, fakat birçok okulda baskın örgüt kültürü türlerinin mevcut olduğu görülmüştür. Okullar genelinde örgüt kültürü olarak en çok klan kültürü görülmüşken, en az görülen örgüt kültürü ise pazar kültürü olarak ortaya çıkmıştır. Sonuç olarak bu çalışmada, örgüt kültürü türlerinin uyumlulukları ve baskınlık seviyeleriyle örgütsel etkinlik arasında önemli derecede ilişki olmadığı, fakat örgüt kültürü türleriyle örgütsel etkinlik arasında önemli bir ilişkinin olduğu tespit edilmiştir.

Dadgar ve diğerleri (2013), İran'daki Şiraz Üniversitesi'nin örgüt kültürünü, öğretim elemanları, çalışanlar ve öğrencilerin algıları çerçevesinde 5'li Likert ölçekli 24 sorulu OCAI anketi kullanarak ortaya koymaya çalışmışlardır. Şiraz Üniversitesi genelinde uygulanan ankete veri analizine tabi tutulabilecek 803 adet geri dönüş elde edilmiştir. Dönüş yapan bu katılımcıların 226'sı öğretim elemanı, 261'i idari personel ve 375'i de öğrencilerden oluşmaktadır. Anketin güvenirlik düzeyini temsil eden genel Cronbach Alpha değeri de 0,75 çıkmıştır. Çalışmanın sonucunda, Şiraz Üniversitesi'ndeki baskın örgüt kültürünün klan olduğu görülmüştür.

Ashraf ve diğerleri (2013), İran'daki özel üniversitelerde örgüt kültürüyle örgütsel yenilikçilik arasındaki ilişkiyi araştıran çalışmalarında örgüt kültürü önermeleri için 5'li Likert ölçekli 24 sorulu OCAI anketini İran'daki 5 özel üniversitenin öğretim elemanlarına uygulamış olup, ulaşılan 485 öğretim elemanının 369'u anket sorularına eksiksiz bir şekilde cevap vermiştir. Anket öncesinde 50 kişiye uygulanan pilot test sonuçlarına göre, güvenirlik düzeyini temsil eden Cronbach Alpha değerleri sırasıyla hiyerarşi kültürü için 0,750, pazar kültürü için 0,763, klan kültürü için 0,715 ve adhokrasi kültürü için 0,775 çıkmıştır. Çalışmanın sonucunda, seçilen 5 özel üniversite genelinde klan kültürünün diğer örgüt kültürü türlerine nazaran baskın olduğu tespit edilmiştir. Bununla birlikte örgütsel yenilikçilik ile klan, adhokrasi ve pazar kültürleri arasında pozitif ilişkinin olduğu, hiyerarşi kültürü ile örgütsel yenilikçilik arasında ise kayda değer bir ilişkinin olmadığı görülmüştür.

Çin'deki bir üniversitede yürütülen, örgüt kültürüyle öğretim elemanlarının psikolojik güçlendirilmeleri ve örgütsel vatandaşlık davranışları arasındaki ilişkinin incelendiği bir

başka çalışmada da örgüt kültürü önermeleri için Likert ölçekli 24 sorulu OCAI anketi kullanılmıştır. 64 öğretim elemanına uygulanan ankete 42 katılımcı eksiksiz bir şekilde cevap vermiştir. Anketin güvenirlik düzeyini temsil eden Cronbach Alpha değerleri sırasıyla hiyerarşi kültürü için 0,85, pazar kültürü için 0,78, klan kültürü için 0,86 ve adhokrasi kültürü için 0,71 çıkmıştır. Sonuç olarak çalışmanın yürütüldüğü üniversitenin baskın örgüt kültürünün pazar olduğu görülmüştür (Jiang ve Fu, 2011).

Fralinger ve Olson (2007), Amerika'daki Rowan Üniversitesi'nde sağlık ve uygulama bilimleri bölümündeki mevcut örgüt kültürünü ve örgüt kültürü değiştirme stratejisini tanımlamayı amaç edinen çalışmalarında 100 puan paylaştırma cevaplama yöntemiyle 24 sorulu OCAI anketini 50 lisans öğrencisine uygulamışlardır. Çalışmanın sonucunda, anketin uygulandığı ilgili bölümdeki mevcut örgüt kültürünün klan olduğu ve takip eden 5 yıl içerisinde de öğrencilerin klan kültürünü daha güçlü bir şekilde görmek istedikleri anlaşılmıştır.

Letonya'nın başkenti Riga'da kurulu olan Riga Teknik Üniversitesi'nde yürütülen bir diğer çalışmada da üniversitede örgüt kültürünün mevcut ve arzulanan durumlarının tespit edilmesi ve örgüt kültürünün üniversite yönetiminin kalitesi üzerindeki rolünün incelenmesi amaçlanmıştır. 2014 yılında üniversitenin yönetimine ve çalışanlarına uygulanan 24 sorulu OCAI anketinin sonuçlarına göre, üniversitedeki baskın mevcut örgüt kültürünün hiyerarşi olduğu sonucu elde edilmiştir. Bununla birlikte arzulanan kültür türlerinin ise klan ve adhokrasi olduğu belirlenmiştir. Ayrıca üniversitedeki örgüt kültürünün kalite yönetimi için zemin oluşturduğu ve doğrudan gelişime katkı sağladığı sonucuna ulaşılmıştır (Lapina ve diğerleri, 2015).

Meksika'da kuruluşları eski ve yeni olan iki üniversitenin mevcut ve arzulanan örgüt kültürleri üzerine yürütülen bir diğer çalışmada da 24 sorulu OCAI anketi, kuruluşu eski olan üniversiteden 254 ve kuruluşu yeni olandan da 239 kişiden olmak üzere toplam 493 akademik personel ve öğrenciye 100 puan paylaştırma cevaplama yöntemiyle uygulanmıştır. Üniversitelerin ikisinde de mevcut örgüt kültüründe pazar kültürünün baskın olduğu, gelecekte ise kuruluşu eski olan üniversitede klan kültürünün, yeni olanda ise adhokrasi kültürünün arzulandığı görülmüştür. Güvenirlik düzeyini temsil eden Cronbach Alpha değerleri, kuruluşu eski olan üniversitenin mevcut örgüt kültüründe 0,66, arzulanan örgüt kültüründe 0,75; kuruluşu yeni olan üniversitenin mevcut örgüt kültüründe

0,667, arzulanan örgüt kültüründe ise 0,618 olarak elde edilmiştir (Garcia ve diğerleri, 2012).

3.4. Rekabetçi Değerler Modeli'nin Türkiye'deki Üniversitelerde Uygulandığı Başlıca Çalışmalar

Bu alt bölümde, yapılan alanyazın taramasında karşılaşılan, Türkiye'deki üniversitelerde Rekabetçi Değerler Modeli'nin uygulanmasıyla örgüt kültürünün konu alındığı çalışmalara yer verilmiştir.

Karşılaşılan çalışmaların ilki Fırat Üniversitesi bünyesinde gerçekleştirilmiştir. Bu çalışmada, üniversitede örgüt kültürünün mevcut ve arzulanan durumlarının tanımlanması amaçlanmıştır. Araştırmanın evreni olarak Fırat Üniversitesi'nde çalışmakta olan akademik personel seçilmiştir. Veriler kolayda örnekleme yöntemiyle 2009 yılı Kasım ve Aralık aylarında 150 akademik personelden toplanmıştır. Cameron ve Freeman'ın 4 boyutlu 16 sorulu Örgüt Kültürü Türleri Modeli anketi 100 puan paylaştırma cevaplama yöntemiyle uygulanmıştır. Akademik personelin üniversiteyi ilişkilendirdiği mevcut örgüt kültürüne bakıldığında, üniversitede hiyerarşi kültürünün öne çıktığı ve hiyerarşi kültürünü sırasıyla pazar, klan ve adhokrasi kültürlerinin izlediği sonucuna ulaşılmıştır. Üniversitede arzulanan örgüt kültürü incelendiğinde ise en yüksek puanı klan kültürünün aldığı görülmüştür (Erdem, Adıgüzel ve Kaya, 2010).

Örgüt kültürünü konu alan çalışmaların bir diğeri de çalışmanın yürütüldüğü zamanki adı Zonguldak Karaelmas Üniversitesi olan Bülent Ecevit Üniversitesi'nde gerçekleştirilmiştir (Murat ve Açıkgöz, 2007). Bu çalışma, 2005-2006 eğitim ve öğretim yılında Zonguldak Karaelmas Üniversitesi'ndeki yöneticilerin rekabetçi değerler yaklaşımı açısından örgüt kültürüne ilişkin algılamalarını ortaya koymaya çalışan Açıkgöz'ün (2006) yüksek lisans tezinden türetilmiştir. Çalışmada, veri toplama aracı olarak 5'li Likert ölçekli 32 soruluk anket kullanılmıştır. Ankette yer alan 32 sorunun 25'inde tezin bir diğer araştırma konusu olan pozitif örgüt kültürünün varlığı sorgulanmaktadır. OCAI anketinden uyarlanmış olan kalan 7 soruyla ise hiyerarşi, pazar, klan ve adhokrasi kültürleri değerlendirilmeye çalışılmıştır. Örgüt kültürünü ölçen sorular hiyerarşi kültürü için 2, pazar kültürü için 3, klan kültürü için 1 ve adhokrasi kültürü için 1 soru olacak şekilde dağılım göstermiştir. Zonguldak Karaelmas Üniversitesi'nin akademik ve idari birimlerinde çalışan toplam 134

yöneticiye uygulanmış olan ankete veri analizine tabi tutulabilecek 131 katılımcıdan geri dönüş elde edilmiştir. Veriler tamsayım yöntemi kullanılarak toplanmıştır. Anketin pozitif örgüt kültürü ile örgüt kültürü türlerine yönelik önermelerini içeren toplam 32 sorusunun güvenirlik düzeyini temsil eden Cronbach Alpha değeri 0,93 çıkmıştır. Örgüt kültürü türlerinin ölçümünde Cameron ve Freeman'ın 4 boyutlu 16 sorulu Örgüt Kültürü Türleri Modeli veya Cameron ve Quinn'in 6 boyutlu 24 sorulu OCAI ölçeklerinin kullanılmadığı bu çalışmada, örgüt kültürü önermelerini içeren OCAI'dan uyarlanmış toplam 7 sorunun her biri kendi özelinde değerlendirilmiş ve üniversitede genel olarak bir örgüt kültürü türünün baskın olduğu vurgusu yapılmamıştır.

Türkiye'de üniversitelerdeki örgüt kültürünü Rekabetçi Değerler Modeli ekseninde konu alan bir diğer çalışma ise Ege Üniversitesi bünyesinde gerçekleştirilmiştir. Ege Üniversitesi'nin mevcut örgüt kültürünün, üniversitenin öz değerlendirme raporunda yer alan misyon, vizyon ve stratejik hedefleriyle ne derece uyumlu olduğunun tespitini konu alan bu çalışmada, örgüt kültürünün tanımlanmasında Açıkgöz'ün (2006) yüksek lisans tezinde kullanılmış olan anketten yararlanılmıştır. Anket, 2009-2010 eğitim ve öğretim yılında tesadüfi seçilen 136 üniversite öğretim elemanına uygulanmış ve veri analizine tabi tutulabilecek 126 adet geri dönüş elde edilmiştir. Yapılan analiz sonucunda, Ege Üniversitesi'nin genel örgüt kültürü profilinde hiyerarşi kültürünün diğer örgüt kültürü türlerine nazaran baskın olduğu açıklanmıştır (Beytekin, Yalçınkaya, Doğan ve Karakoç, 2010).

3.5. Örgüt Kültürü ile Bilgi Güvenliği İlişkisini İnceleyen Çalışmalar

Bu alt bölümde, yapılan alanyazın taramasında karşılaşılan, Rekabetçi Değerler Modeli ile ölçümlenmiş olan örgüt kültürünün, çalışanların bilgi güvenliği davranışları ve bilgi güvenliği yönetimi üzerine etkisini incelemek amacıyla yürütülmüş çalışmalara yer verilmiştir.

Örgüt kültürünün çalışanların bilgi güvenliği politikası uygulamalarına karşı sergiledikleri davranışları üzerine etkisini araştıran bir çalışmada, örgüt kültürü ölçümünde 24 sorulu OCAI ölçeği, bilgi güvenliği davranışlarının ölçümünde ise örgüt bilgi güvenliği politikasının 5 boyutu dikkate alınarak hazırlanmış olan toplam 16 sorulu ölçek kullanılmıştır. Davranış odaklı soru seti 7'li Likert, örgüt kültürünü ölçümleyen OCAI

ölçeği ise 100 puan paylaştırma cevaplama yöntemiyle birçok alt şirketten oluşan 100 binin üzerinde toplam çalışana sahip üretim şirketinde uygulanmış ve tesadüfi seçilen 1000 kişiye ulaştırılan ankete 109 kişiden eksiksiz dönüş elde edilmiştir. Bu 109 katılımcının 35'i (%32,1'i) ticari, 19'u (%17,4'ü) bilgi teknolojileri ve 11'i de (%10,1'i) güvenlik alanlarında faaliyet gösteren alt şirketlerde çalışmaktadır. Çalışmada, örgüt kültürü türlerinden hiyerarşi "istikrarlılık", pazar "etkinlik", klan "işbirliği", adhokrasi "yaratıcılık" olarak adlandırılmıştır. Veri analizinden sonra güvenirlik düzeyini temsil eden Cronbach Alpha değerleri sırasıyla hiyerarşi kültürü için 0,81, pazar kültürü için 0,84, klan kültürü için 0,85 ve adhokrasi kültürü için 0,85 olarak elde edilmiştir. Çalışmanın sonucunda şirketin genel örgüt kültürü profilinde hiyerarşi kültürü baskın çıkmış olup, bilgi güvenliği politikası uygulamalarındaki çalışanların davranışları üzerinde klan kültürünün negatif ve pazar kültürünün ise pozitif etkiye sahip olduğu, adhokrasi ve hiyerarşi kültürlerinin ise çalışanların davranışları üzerinde pozitif veya negatif manada herhangi bir etkiye sahip olmadığı görülmüştür (Shaw, 2012: 47-48, 50, 58, 70, 74, 94-95, 102).

İran'da mühendislik ve inşaat şirketi olarak faaliyet gösteren Tam Iran Khodro'da yürütülmüş olan bir başka çalışmada da örgüt kültürü ile bilgi güvenliği yönetimi arasındaki ilişki konu alınmıştır. Örgüt kültürü ölçümünde Rekabetçi Değerler Modeli boyutlarında istikrarlı, hedef odaklı, işbirliği ve yenilikçi kültür türlerinde yapılandırılan Denison Örgüt Kültürü Modeli'nden yararlanılmıştır. Örgüt kültürü ölçümü için Denison Örgüt Kültürü Modeli'nden türetilen 30 sorulu ölçek kullanılmıştır. Bilgi güvenliği yönetimi ise bilgi güvenliği prensiplerinden gizlilik, bütünlük, erişilebilirlik, sorumluluk, kimlik doğrulama, inkâr edilemezlik ve güvenilirlik boyutlarında hazırlanmış olan 35 sorulu ölçek ile değerlendirilmiştir. Çalışmanın anketi, 5'li Likert ölçek kullanılarak şirketin yazılım, donanım ve ağ bölümlerinde çalışmakta olan yönetici ve uzmanlardan oluşan toplam 30 kişiye uygulanmıştır. Cronbach Alpha değerlerinin anketin veri analizinde kullanılabilmesini sağlayacak güvenirlikte çıktığı belirtilmiştir. Kültür türleri ile bilgi güvenliği bağımlı değişkeni arasındaki ilişkinin incelendiği korelasyon analizi sonuçlarına göre, klan kültürünü temsil eden işbirliği kültürü ve adhokrasi kültürünü temsil eden yenilikçi kültür ile bilgi güvenliği yönetimi arasında anlamlı düzeyde ilişkinin var olduğu, pazar kültürünü temsil eden hedef odaklı kültür ve hiyerarşi kültürünü temsil eden istikrarlı kültür ile bilgi güvenliği yönetimi arasında anlamlı bir ilişkiye rastlanılmadığı ifade edilmiştir. Daha sonra kültür türlerinin bilgi güvenliği bağımlı değişkeni üzerindeki etkisi regresyon analizi ile incelenmiş olup, klan, adhokrasi ve pazar kültürlerinin bilgi

güvenliğini pozitif yönde etkilediği, bunun yanı sıra hiyerarşi kültürünün bilgi güvenliğini etkilemediği sonucuna ulaşılmıştır (Ebrahimi ve Naini, 2012).

Chang ve Lin (2007) de örgüt kültürünün bilgi güvenliği yönetimi üzerine olan etkisini araştıran çalışmalarında, örgüt kültürü ölçümü için Rekabetçi Değerler Modeli boyutlarında kültürün örgüt özellikleri, liderlik özellikleri, örgütsel iklim ve yönetim şekli karakteristiklerini dikkate alarak hazırlamış oldukları 26 sorulu ölçeği, bilgi güvenliği yönetiminin ölçümü için ise BS7799-1 standardını dikkate alarak bilgi güvenliğinin gizlilik, bütünlük, erişilebilirlik ve sorumluluk boyutlarında hazırlamış oldukları 19 sorulu ölçeği kullanmışlardır. Çalışmada, örgüt kültürü türlerinden hiyerarşi "istikrarlılık", pazar "etkinlik", klan "işbirliği", adhokrasi "yaratıcılık" olarak adlandırılmış ve bilgi güvenliği yönetim uygulamalarının etkinliği de bilgi güvenliği prensiplerinden gizlilik, bütünlük, erişilebilirlik ve sorumluluk boyutlarında değerlendirilmiştir. Kullanılan ölçekte istikrarlılık kültürü 6, etkinlik kültürü 6, işbirliği kültürü 8, yaratıcılık kültürü 6, gizlilik prensibi 5, bütünlük prensibi 5, erişilebilirlik prensibi 3 ve sorumluluk prensibi 6 soru ile ölçülmüştür. 7'li Likert ölçeği kullanılarak hazırlanan anket formu Tayvan'daki 196 şirkete ulaştırılmış ve veri analizinde kullanılabilir 87 kişiden geri dönüş elde edilmiştir. Dönüş yapan katılımcıların %33,3'ü finansal sektörde, %20,6'sı elektrik elektronik veya bilgisayar endüstrisinde, %20,7'si hizmet sektöründe ve %25,5'i de üretim, sağlık ve yemek endüstrisi gibi diğer alanlarda çalışmakta olup, toplam katılımcıların %40,2'si üst düzey yöneticilerden geriye kalan %59,8'i de bilgi teknolojileri alanında bilgi ve tecrübeye sahip uzman personelden oluşmaktadır. Anketin güvenirlik düzeyini temsil eden Cronbach Alpha değerleri sırasıyla istikrarlılık kültürü (hiyerarşi kültürü) için 0,885, etkinlik kültürü (pazar kültürü) için 0,848, işbirliği kültürü (klan kültürü) için 0,903, yaratıcılık kültürü (adhokrasi kültürü) için 0,892, gizlilik için 0,875, bütünlük için 0,717, erişilebilirlik için 0,673 ve sorumluluk için 0,865 olarak elde edilmiştir. Çalışmanın sonucunda, bilgi güvenliği yönetimi üzerinde Rekabetçi Değerler Modeli'ndeki kontrol odaklı hiyerarşi ve pazar kültürlerinin pozitif etkisi olduğu görülmüştür. Buna karşıt olarak esneklik odaklı klan ve adhokrasi kültürlerinin bilgi güvenliği yönetimi üzerinde herhangi bir etkisinin olmadığı, yalnızca bir istisna olarak klan kültürünün bilgi güvenliği prensiplerinden gizliliğin üzerinde negatif etkisi olduğu sonucuna ulaşılmıştır.

4. MATERYAL VE METOT

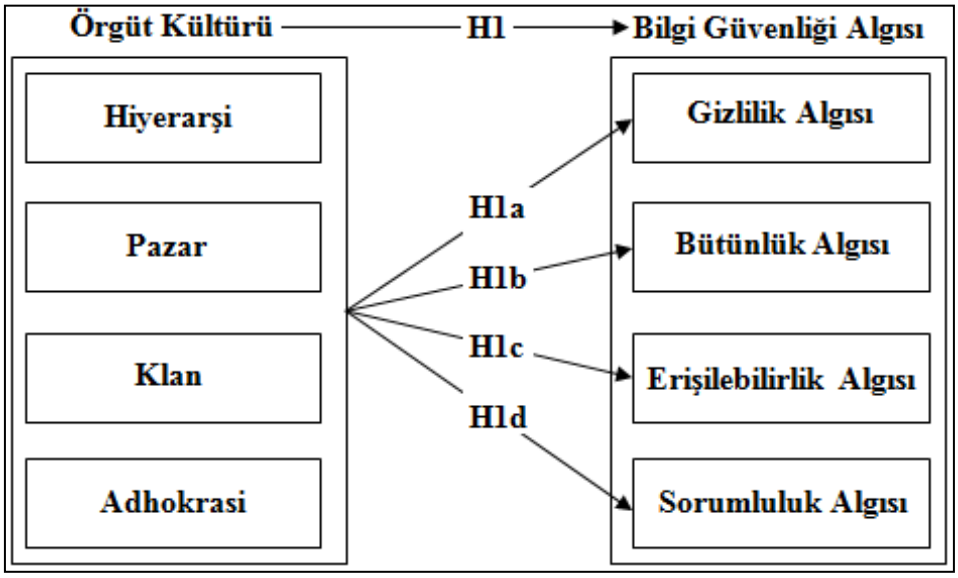
Bu bölümde, tez çalışması kapsamında uygulanan materyal ve metot beş alt bölümde ele alınmıştır. Birinci alt bölümde araştırmanın amacı, ikinci alt bölümde araştırmanın hipotezleri, üçüncü alt bölümde araştırmada kullanılan yöntem ve teknikler, dördüncü alt bölümde araştırmanın evreni ve örneklemi, beşinci ve son alt bölümde ise araştırmanın sınırları yer almaktadır.

4.1. Araştırmanın Amacı

Araştırmada, Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profilinin Cameron ve Freeman Örgüt Kültürü Türleri Modeli'ne göre örgüt kültürü türleri hiyerarşi, pazar, klan ve adhokrasi temelinde tanımlanması, üniversitelerde çalışan akademik personelin bilgi güvenliği algısı profilinin, bilgi güvenliği prensiplerinden gizlilik, bütünlük, erişilebilirlik ve sorumluluk boyutlarında değerlendirilmesi ve örgüt kültürünün akademik personelin bilgi güvenliği, gizlilik, bütünlük, erişilebilirlik ve sorumluluk algıları üzerine etkisinin incelenmesi amaçlanmaktadır.

4.2. Araştırmanın Hipotezleri

Araştırmanın hipotez çatısı Şekil 4.1'de verilmiştir.



Şekil 4.1. Araştırmanın hipotez çatısı

Hipotez çatısına göre, bağımsız değişkenler Cameron ve Freeman örgüt kültürü türleri hiyerarşi, pazar, klan ve adhokrasi olup, bağımlı değişkenler ise akademik personelin bilgi güvenliği prensiplerinden gizlilik, bütünlük, erişilebilirlik, sorumluluk üzerine algıları ve bu 4 prensip algısını ölçümleyen anket sorularının ortalama puanına sahip bilgi güvenliği algısıdır.

Örgüt kültürünün, bilgi güvenliği ve bilgi güvenliği prensipleri algıları üzerine etkisi aşağıdaki hipotezler ile sorgulanmıştır:

H1: Örgüt kültürü bilgi güvenliği algısını etkiler.
H1a: Örgüt kültürü bilgi güvenliğinin gizlilik prensibi algısını etkiler.
H1b: Örgüt kültürü bilgi güvenliğinin bütünlük prensibi algısını etkiler.
H1c: Örgüt kültürü bilgi güvenliğinin erişilebilirlik prensibi algısını etkiler.
H1d: Örgüt kültürü bilgi güvenliğinin sorumluluk prensibi algısını etkiler.

4.3. Araştırmada Kullanılan Yöntem ve Teknikler

Araştırmada veri toplama aracı olarak anket kullanılmıştır. Anketin hiyerarşi, pazar, klan ve adhokrasi örgüt kültürü türlerine ilişkin soruları, Cameron ve Quinn (2006: 26-28) tarafından geliştirilmiş, geçerliği ve güvenirliği sağlanmış olan 24 sorulu OCAI ölçeği dikkate alınarak hazırlanmıştır. OCAI ölçeği ile örgüt kültürü, baskın özellikler, örgütsel liderlik, çalışanların yönetimi, örgüte bağlılık, stratejik vurgular ve başarı kriteri olmak üzere 6 farklı boyutta değerlendirilmektedir (Cameron ve Quinn, 2006: 151). Anketin bilgi güvenliği algısına ilişkin sorularının hazırlanmasında da Chang ve Lin'in (2007) bilgi güvenliği yönetim standardı BS7799-1'den uyarlayarak hazırlamış oldukları, geçerliği ve güvenirliği sağlanmış; bilgi güvenliğinin gizlilik, bütünlük, erişilebilirlik ve sorumluluk prensipleri ile tanımlandığı 19 sorulu ölçekten yararlanılmıştır.

Ölçeğinin hazırlanmasında yararlanılan 24 sorulu OCAI ve 19 sorulu bilgi güvenliği yönetimi ölçekleri, üniversitelerdeki iş yapış şekilleri dikkate alınarak Türkçeye tercüme edilmiştir. Bu esnada ölçeğin kapsam geçerliğinin sağlanması adına ifade, imlâ ve anlam açısından bilişim uzmanlarının ve akademik personelin değerlendirmelerinden yararlanılmıştır. Bu süre zarfında ölçeğin bilgi güvenliği algısını betimleyen sorularının bilişim alanı dışında üniversitelerin farklı bölümlerinde çalışan akademik personelin

tamamı tarafından da anlaşılabilir olması amacıyla hazırlanan ölçek, deneklere uygulanmadan önce anlam açısından değerlendirilmek üzere tarih, işletme ve tıp alanlarında çalışan akademik personelin yorumuna sunulmuştur. Bilişim uzmanlarının ve akademik personelin değerlendirmeleri doğrultusunda, anlaşılmasında zorluk yaşanan veya yanlış anlaşılan sorular anlamı kolaylaştıran ifadelerle güncellenmiş ve bazı sorularda ise anlatımı kolaylaştıran parantez içerisinde örnek tanımlamalar yapılmıştır. Araştırmanın ölçeği, kapsam, ifade, imlâ ve anlam açısından değerlendirildikten sonra deneklere uygulanmıştır.

Araştırma ölçeğinin hazırlanmasında yararlanılan ölçeklerin kullanıldığı çalışmalara tezin 3. Bölüm'ünde yer verilmiştir. Söz konusu çalışmalarda, yararlanılan ölçeklerin Cronbach Alpha değerlerinin, veri analizinde kullanılabilmesini sağlayacak kabul edilebilir güvenirlikte çıktığı görülmüş ve dolayısıyla araştırma ölçeğinin güvenirlik analizinde ön test uygulamasına gerek duyulmamıştır.

Örgüt kültürü türünü ve bilgi güvenliği algısını ölçümleyen anket bağlamında 5'li Likert ölçeği kullanılmış olup, 1=Kesinlikle katılmıyorum, 5= Kesinlikle katılıyorum düzeylerini temsil etmekte ve 1'den 5'e doğru puanlamada katılım düzeyi artmaktadır.

Üç bölümden oluşan ölçeğin 1. kısmındaki 24 soru (1-24. sorular) ile çalışılmakta olunan üniversitenin örgüt kültürü türü, 2. kısmındaki 19 soru (25-43. sorular) ile akademik personelin bilgi güvenliği algısı betimlenmekte ve 3. kısmında da katılımcıların demografik bilgilerini içeren 5 soru yer almaktadır (Ek-1).

Ölçeğin 1. kısmında yer alan 1-4. sorular baskın özellikler, 5-8. sorular örgütsel liderlik, 9-12. sorular çalışanların yönetimi, 13-16. sorular örgüte bağlılık, 17-20. sorular stratejik vurgular ve 21-24. sorular ise başarı kriteri boyutlarında örgüt kültürünü betimlemektedir. Her bir boyutu temsil eden dörderli grup soruların kendi içindeki ilk sorusu klan kültürünü, ikinci sorusu adhokrasi kültürünü, üçüncü sorusu pazar kültürünü ve dördüncü sorusu da hiyerarşi kültürünü tanımlamaktadır. Diğer bir ifadeyle 1., 5., 9., 13., 17. ve 21. soruların aldığı puanların aritmetik ortalaması klan kültürünü, 2., 6., 10., 14., 18. ve 22. soruların aldığı puanların aritmetik ortalaması adhokrasi kültürünü, 3., 7., 11., 15., 19. ve 23. soruların aldığı puanların aritmetik ortalaması pazar kültürünü ve 4., 8., 12., 16., 20. ve 24. soruların aldığı puanların aritmetik ortalaması ise hiyerarşi kültürünü betimlemektedir.

Ölçeğin 2. kısmında yer alan 25-29. sorular (5 soru) ile bilgi güvenliğinin gizlilik prensibi algısı, 30-34. sorular (5 soru) ile bilgi güvenliğinin bütünlük prensibi algısı, 35-37. sorular (3 soru) ile bilgi güvenliğinin erişilebilirlik prensibi algısı ve 38-43. sorular (6 soru) ile de bilgi güvenliğinin sorumluluk prensibi algısı betimlenmektedir. Her bir bilgi güvenliği prensibinin ilgili sorularının aldığı puanların aritmetik ortalaması, o prensip algısını betimlemektedir. Gizlilik algısı, bütünlük algısı, erişilebilirlik algısı ve sorumluluk algısı boyutlarından oluşan bilgi güvenliği algısının puanı ise bilgi güvenliği prensipleri algılarını betimleyen toplam 19 sorunun aldığı puanların aritmetik ortalaması ile elde edilmektedir.

Bağımsız değişkenler örgüt kültürü türleri hiyerarşi, pazar, klan ve adhokrasi ile bağımlı değişkenler bilgi güvenliği algısı, gizlilik algısı, bütünlük algısı, erişilebilirlik algısı ve sorumluluk algısı arasındaki ilişkinin varlığı Pearson kolerasyon analizi ile sorgulanmıştır. Daha sonra veriler doğrusal regresyon analizine tabi tutularak bağımsız değişkenlerin bağımlı değişkenler üzerindeki etkisi test edilmiştir.

4.4. Araştırmanın Evreni ve Örneklemi

Araştırmanın evrenini Türkiye'deki devlet üniversitelerinde çalışmakta olan profesör, doçent, yardımcı doçent, öğretim görevlisi, okutman, uzman, araştırma görevlisi ve çevirici unvanlarındaki akademik personel (öğretim elemanı) oluşturmaktadır. Yükseköğretim Kurulu'nun (YÖK) yayınlamış olduğu öğretim elemanı istatistiklerinde, araştırmanın yürütüldüğü 2015-2016 eğitim öğretim yılı için, devlet üniversitelerinde 76751'i erkek, 55615'i kadın olmak üzere toplam 132366 akademik personelin bulunduğu belirtilmektedir (Yükseköğretim Kurulu [YÖK], 2017). Evrendeki akademik personelin tamamına ulaşılmaya çalışılmıştır. Veri toplama yöntemi olarak tesadüfi olmayan örnekleme yöntemlerinden kolayda örnekleme yöntemi kullanılmıştır.

Anket formunun Google Formlar İnternet bağlantı linki, Türkiye'deki 106 devlet üniversitesindeki akademik personele e-posta ile ulaştırılmıştır. Personelin e-posta adresleri üniversite web sitelerinden temin edilmiştir. Ayrıca Gazi Üniversitesi İşletme Bölümü, Nevşehir Hacı Bektaş Veli Üniversitesi İşletme Bölümü ve Erciyes Üniversitesi Tıp Fakültesi'nde çalışmakta olan akademik personele anket formları elle teslim edilmiş ve toplanmıştır. Sonuç olarak korelasyon ve regresyon analizlerine, kullanılabilir durumda

olan 118'i elden, 2905'i de e-posta yolu ile toplanmış toplam 3023 anket formu dâhil edilmiştir. Anket verilerinin analizinde IBM SPSS 21 paket programından yararlanılmıştır.

4.5. Araştırmanın Sınırları

Araştırmada veri toplamada YÖK'ün web sitesinde listelenen devlet üniversiteleri ile sınırlı kalınmıştır (YÖK, 2016). Vakıf üniversitelerinin yapısı, yönetim şekli ve işleyişi devlet üniversitelerinden farklı olduğu için vakıf üniversiteleri bu araştırmaya dâhil edilmemiş ve vakıf üniversitelerindeki akademik personelden veri toplanmamıştır.

Türkiye'de devlet üniversitelerindeki idari personel ve öğrencilerin geneline ulaşmada karşılaşılacak zaman, mekân ve maliyet kısıtlarından dolayı araştırmanın evrenine sadece akademik personel dâhil edilmiştir.

Zaman kısıtının doğal bir sonucu olarak araştırma belirli bir zaman diliminde yürütülmüş ve veriler 19.01.2016 - 21.04.2016 tarihleri arasında toplanabilmiştir.

Verilerin toplanmış olduğu tarihlerde, YÖK'ün web sitesinde yer alan 109 devlet üniversitesinden 106'sındaki akademik personele anket formları e-posta yoluyla iletilebilmiştir. Verilerin toplandığı tarih aralığında İskenderun Teknik Üniversitesi ve Sağlık Bilimleri Üniversitesi'nin web sitelerindeki akademik birimler sayfasının henüz yapım aşamasında olmasından ve Türkiye Uluslararası İslam, Bilim ve Teknoloji Üniversitesi'nin web sitesinin ise mevcut olmamasından kaynaklı bu üniversitelerde çalışan akademik personelin e-posta adreslerine ulaşılamamış ve bu 3 üniversiteden veri toplanamamıştır.

Bilgi güvenliği algısı ile ilgili elde edilen bilgiler, Chang ve Lin'in (2007) oluşturmuş oldukları ölçekteki bilgi güvenliği prensiplerinden gizlilik, bütünlük, erişilebilirlik ve sorumluluk boyutlarının sorularıyla sınırlıdır. Bilgi güvenliğinin temel 3 ana prensibi gizlilik, bütünlük ve erişilebilirliğin yanı sıra sorumluluk haricinde de kimlik doğrulaması, güvenilirlik ve inkâr edememe gibi bilgi güvenliği prensipleri mevcuttur. Bu araştırmada gizlilik, bütünlük, erişilebilirlik ve sorumluluk hariç söz konusu diğer bilgi güvenliği prensipleri, bilgi güvenliği algısı ölçümünde dikkate alınmamıştır.

Anket formlarının e-posta ile gönderiminde alıcı adreslerin e-posta kutusu kotasının dolmuş olması, verilerin toplanmış olduğu tarihlerde sıkça e-posta gönderimi yapıldığı için anket e-postalarının üniversite e-posta sunucularında spam e-posta olarak algılanılması ve üniversite web sitelerinde yer alan akademik personelin e-posta adreslerinin güncel olmaması gibi bazı teknik sorunlar nadiren de olsa yaşanmıştır. Bu sorunlardan kaynaklı bazı e-postaların iletilemediğine dair geri bildirim e-postaları alınmıştır. Bu durum, anket formunun bazı akademik personele ulaştırılmasında sınırlılık oluşturmuştur.

5. BULGULAR

Araştırma verilerinin analiz ve değerlendirilmesinde öncelikle araştırmada kullanılan ölçeğin güvenirliğini test etmek için Cronbach Alpha güvenirlik analizinden yararlanılmıştır. Daha sonra örneklemin demografik değişkenlere göre dağılımlarına, ölçekteki maddelere ilişkin tanımlayıcı istatistiklere ve verilerin frekans analizi sonuçlarına yer verilmiştir. Frekans analizi sonuçlarına göre, Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profili ve akademik personelin bilgi güvenliği algısı değerlendirilmiştir. Daha sonra hipotezlerin test edilmesine geçilmiştir. Hipotezlerin test edilmesi sürecinde öncelikle bağımsız değişkenler örgüt kültürü türleri hiyerarşi, pazar, klan ve adhokrasi ile bağımlı değişkenler bilgi güvenliği algısı, gizlilik algısı, bütünlük algısı, erişilebilirlik algısı ve sorumluluk algısı arasındaki anlamlı bir ilişkinin varlığını sorgulayan Pearson kolerasyon analizinin sonuçlarına yer verilmiştir. Son olarak da doğrusal regresyon analizi ile örgüt kültürünün, bilgi güvenliği algısı, gizlilik algısı, bütünlük algısı, erişilebilirlik algısı ve sorumluluk algısı üzerindeki etkisini sorgulayan hipotezlerin testleri gerçekleştirilmiştir.

5.1. Güvenirlik Analizi

Anketin uygulamaya tabi tutulabilmesi için, öncelikle güvenirlik testlerini geçmiş olması gerekmektedir. Güvenirlik katsayısı hesaplama tekniklerinden Cronbach Alpha iç güvenirlik katsayısı yöntemi kullanılmıştır. Cronbach Alpha iç güvenirlik katsayısının 0,7'den büyük olması ölçeği güvenilir kılmaktadır (Field, 2009: 675).

Çizelge 5.1'de yer alan güvenirlik istatistikleri incelendiğinde, değişkenler için hesaplanan Cronbach Alpha iç güvenirlik katsayılarının tamamının 0,7 değerinden, erişilebilirlik hariç diğer tüm değişkenlerde de 0,8 değerinden büyük çıktığı görülmektedir. Erişilebilirlik değişkeninin güvenirlik katsayısının 0,7'den büyük olmakla birlikte 0,8'den düşük çıkması, erişilebilirliğin diğer değişkenlere nazaran daha az soruyla - 3 madde ile ölçülmesinden kaynaklanmaktadır. Sonuç olarak kullanılan ankette her bir değişken için iç güvenirlik katsayılarının 0,7 değerinden büyük olduğu görülmekte olup, ölçeğin bütünü itibarıyla güvenilir olduğu ve verilerin analize tabi tutulmasında bir sorun olmadığı sonucuna ulaşılmıştır.

Çizelge 5.1. Kullanılan anketin güvenirlik istatistikleri

Değişkenler	Madde Sayısı	Cronbach Alpha
Hiyerarşi	6	0,856
Pazar	6	0,890
Klan	6	0,880
Adhokrasi	6	0,887
Gizlilik Algısı	5	0,846
Bütünlük Algısı	5	0,870
Erişilebilirlik Algısı	3	0,718
Sorumluluk Algısı	6	0,890
Bilgi Güvenliği Algısı	19	0,942

N=3023

5.2. Örneklemin Demografik Değişkenlere Göre Dağılımı

Ankete katılanların cinsiyet, yaş grupları, mesleki deneyim ve idari görev itibarıyla dağılımları Çizelge 5.2'de verilmektedir. Ayrıca bir diğer demografik değişken olan çalışılan üniversiteye göre dağılımlar da Ek-2'de yer almaktadır.

Çizelge 5.2. Örneklemin cinsiyet, yaş grupları, mesleki deneyim ve idari görev itibarıyla dağılımları

Demografik Özellikler		Frekans	Yüzde
Cinsiyet	Kadın	1272	42,1
	Erkek	1751	57,9
	Toplam	3023	100,0
Yaş	25'ten küçük	55	1,8
	25-34 arası	1291	42,7
	35-44 arası	934	30,9
	45-54 arası	541	17,9
	55 veya 55'ten büyük	202	6,7
	Toplam	3023	100,0
Mesleki Deneyim	1-5 yıl	1149	38,0
	6-10 yıl	639	21,1
	11-15 yıl	368	12,2
	16-20 yıl	354	11,7
	21 veya üzeri yıl	513	17,0
	Toplam	3023	100,0
İdari Görev	Var	832	27,5
	Yok	2191	72,5
	Toplam	3023	100,0

Çizelge 5.2'deki demografik özelliklere ait frekans ve yüzde dağılımlarına bakıldığında en çok yüzde dağılım değerlerinin, %57,9 ile erkek, %42,7 ile 25-34 yaş aralığında, %38,0 ile 1-5 yıl arası mesleki deneyime sahip ve %72,5 ile idari görevi olmayan akademik personele ait olduğu görülmektedir.

5.3. Ölçekteki Maddelere İlişkin Tanımlayıcı İstatistikler

Örgüt kültürü ve bilgi güvenliği algısını ölçmeye yönelik toplam 43 anket sorusuna ilişkin katılım, ortalama ve standart sapma değerleri Çizelge 5.3'te verilmiştir.

Çizelge 5.3. Anket sorularının ortalama ve standart sapma değerleri

Soru		N	Ort.	Std. Sapma
1	Üniversitede, kişisel ilişkiler iyi seviyededir. Çalışma ortamı geniş bir aile gibidir. Çalışanlar kendilerinden çok şey paylaşmaktadırlar.	3023	2,84	1,175
2	Üniversite, çok dinamik ve girişimci bir yerdir. Çalışanlar, ellerini taşın altına koymaya ve risk almaya isteklidirler.	3023	**2,51**	**1,093**
3	Üniversite, sonuç odaklı bir yapıya sahiptir. İşin yapılması vurgusu vardır. Çalışanlar, kurumsal hedeflere ulaşmada rekabetçi ve başarı odaklıdırlar.	3023	3,02	1,132
4	Üniversite, çok kontrollü ve planlı bir yerdir. Genellikle resmî prosedürler, çalışanların ne yapacağına yön vermektedir.	3023	3,13	1,149
5	Üniversiteyi yönetenler, genellikle akıl hocası, yardım edici veya eğitici olarak görülmektedir.	3023	2,75	1,217
6	Üniversiteyi yönetenler, genellikle girişimci, yenilikçi veya risk alan kişiler olarak görülmektedir.	3023	2,69	**1,219**
7	Üniversiteyi yönetenler, genellikle rekabetçi, üretken veya sonuç odaklı kişiler olarak görülmektedir.	3023	2,86	1,200
8	Üniversiteyi yönetenler, genellikle işlerin düzenli ve verimli bir şekilde yürütülmesinden sorumlu yöneticiler olarak görülmektedir.	3023	**3,33**	1,182
9	Üniversitedeki yönetim tarzı; takım çalışması, fikir birliği ve çalışan katılımcılığı ile nitelendirilmektedir.	3023	2,70	1,199
10	Üniversitedeki yönetim tarzı; bireysel risk alma, yeniliği araştırma, çalışanların bağımsızlığı ve bireyselliği ile nitelendirilmektedir.	3023	2,71	1,166
11	Üniversitedeki yönetim tarzı; üniversiteler arası rekabet, akademik talepleri karşılama ve başarıyı elde etme ile nitelendirilmektedir.	3023	2,99	1,166
12	Üniversitedeki yönetim tarzı; iş güvenliği, kural ve düzenlemelere uygunluk, istikrarlı ilişkiler ile nitelendirilmektedir.	3023	3,02	1,110

Çizelge 5.3. (devam) Anket sorularının ortalama ve standart sapma değerleri

13	Üniversiteyi bir arada tutan bağ, sadakat ve karşılıklı güvendir. Üniversiteye bağlılık yüksek düzeydedir.	3023	2,64	1,211
14	Üniversiteyi bir arada tutan bağ, yenilik ve araştırma geliştirmeye olan bağlılıktır. Üniversitede, önde gelen yenilikçi bir eğitim kuruluşu olma vurgusu vardır.	3023	2,91	1,215
15	Üniversiteyi bir arada tutan bağ, kurumsal hedefleri gerçekleştirmeye ve başarıyı elde etmeye verilen önemdir.	3023	2,99	1,179
16	Üniversiteyi bir arada tutan bağ, resmî kurallar ve politikalar doğrultusunda kusursuz çalışan bir örgütün devamlılığına verilen önemdir.	3023	3,10	1,135
17	Üniversitede, kişinin gelişimine vurgu vardır. Örgüt içinde yüksek güven, şeffaflık ve katılımcılık süregelmektedir.	3023	2,67	1,201
18	Üniversitede, yeni kaynaklar elde etme ve zorlu mücadelelere girme vurgusu vardır. Yeni şeyler denemek ve yeni fırsatlar aramak değer ifade etmektedir.	3023	3,03	1,192
19	Üniversitede, kurumsal rekabet ve başarı vurgusu vardır. Kurumsal hedeflere ulaşmak ve eğitim-öğretimde başarılı olmak baskındır.	3023	3,13	1,155
20	Üniversitede, süreklilik ve istikrarlı olma vurgusu vardır. Verimliliğin, kontrolün sağlanması ve faaliyetlerin kusursuz yürütülmesi önemlidir.	3023	3,22	1,136
21	Üniversite başarıyı; insan kaynakları gelişimi, takım çalışması ve çalışanların kurumsal bağlılığı temelinde tanımlamaktadır.	3023	2,92	1,185
22	Üniversite başarıyı; benzersiz, lider ve en yenilikçi üniversiteye sahip olma temelinde tanımlamaktadır.	3023	2,96	1,184
23	Üniversite başarıyı; eğitim-öğretimde kazanma ve diğer üniversitelerden daha başarılı olma temelinde tanımlamaktadır. Rekabetçi liderlik, anahtar kelimedir.	3023	3,10	1,151
24	Üniversite başarıyı; verimlilik temelinde tanımlamaktadır. Güvenilirlik, kusursuz iş planlaması ve kaynakların etkin kullanımı kritik öneme sahiptir.	3023	3,07	1,159
25	Üniversitede, kişisel ve işle alakalı önemli bilgilerin korunmasını sağlamak amacıyla güvenlik kontrollerinin (şifreleme sistemleri gibi) uygulandığını düşünüyorum.	3023	3,40	1,115
26	Erişim yetkisi olmayan kullanıcıların, üniversite bilgi kaynaklarına erişiminin engellendiğini düşünüyorum.	3023	3,45	1,075
27	Çalışanların, bilginin yayınlanmasında ve transferinde üniversite politika ve düzenlemelerine uymak zorunda olduğunu düşünüyorum.	3023	3,81	1,013
28	Üniversitede, önemli bilgilerin, kötü niyetli müdahaleler (bilgi sistemlerine zorla girme ve casus yazılımlar gibi) tarafından çalınmasına karşı korunduğunu düşünüyorum.	3023	3,41	1,077
29	Üniversitede, önemli bilgilerin, yetkisiz ifşadan korunması için bilgi güvenliği ölçümlerinin uygulandığını düşünüyorum.	3023	3,28	1,040
30	Üniversitede, bilgi kaynaklarının sürekli olarak güncellendiğini ve düzenli olarak bilgi yedeklerinin oluşturulduğunu düşünüyorum.	3023	3,20	1,062

Çizelge 5.3. (devam) Anket sorularının ortalama ve standart sapma değerleri

31	Üniversitede, düzenli olarak risk değerlendirmesinin yapıldığını ve bilgi kaybı olasılığının azaltılması için güvenlik planlarının güncellendiğini düşünüyorum.	3023	3,03	1,058
32	Çalışanların, üniversite bilgi sistemleri veritabanlarına (web sitesi, elektronik belge yönetim sistemi, öğrenci ve personel bilgi sistemi veritabanları gibi) önemli bilgileri koyduklarını düşünüyorum.	3023	3,44	1,066
33	Üniversitede, yetkisiz kullanıcılar tarafından bilgi değişikliği (bilginin oluşturulması, değiştirilmesi ve silinmesi gibi) yapılmasının engellenmesi için güvenlik kontrollerinin (değişim yönetimi prosedürleri gibi) tesis edildiğini düşünüyorum.	3023	3,39	1,010
34	Üniversitede, bilginin doğruluğunun ve güvenilirliğinin artırılması amacıyla veritabanlarının düzenli olarak bakımının yapıldığını düşünüyorum.	3023	3,33	1,037
35	Üniversitede, bilgi sistemlerinin bozulması ve bilgi servislerinin kesintiye uğrama olasılığının azaltılmasına önem verildiğini düşünüyorum.	3023	3,37	1,052
36	Üniversitede, özel bilgi kaynaklarına sadece yetkili kullanıcılara sağlanmış olan haklar çerçevesinde erişilebilmesini sağlayan erişim kontrol prosedürlerinin var olduğunu düşünüyorum.	3023	3,52	**0,994**
37	Kullanıcıların, erişim yetkileri dâhilinde üniversite bilgi sistemlerine (e-posta, öğrenci ve personel bilgi sistemi gibi) herhangi bir zamanda ve herhangi bir yerden erişebildiğini düşünüyorum.	3023	**3,86**	1,052
38	Üniversitede, örgütsel bilgi güvenliği politika ve düzenlemelerine aykırı davrananlara yaptırım uygulayan prosedürlerin var olduğunu düşünüyorum.	3023	3,14	1,023
39	Üniversitede, bilgi güvenliği hakkında yararlı eğitim ve öğretimlerin verildiğini düşünüyorum.	3023	2,63	1,114
40	Üniversitede, bilgi güvenliği ile alakalı etiketlerin ve uyarıcı işaretlerin bilgisayarlara ve iletişim cihazlarına görünecek bir şekilde yapıştırıldığını düşünüyorum.	3023	**2,56**	**1,122**
41	Üniversitede, bilgi güvenliği faaliyetlerini sağlamlaştırmak ve bilgi güvenliği sorunlarına müdahale edebilmek için yönetim yapısının, rol ve sorumluluklarla uyumlu bir şekilde kurulduğunu düşünüyorum.	3023	2,98	1,019
42	Üniversitede, bilgi güvenliği kontrollerinin uygun bir şekilde oluşturulduğunu ve çalışanların bu kontrollerle alakalı bilgi güvenliği protokollerini, normlarını ve düzenlemelerini takip ettiklerini düşünüyorum.	3023	2,96	1,018
43	Üniversitede, rutin olarak bilgi güvenliği denetimlerinin yönetildiğini ve bilgi suistimaline veya bilgi sistemlerine girme teşebbüslerine ait geçmiş kayıt ve verilerin muhafaza edildiğini düşünüyorum.	3023	3,10	1,023

Anketin örgüt kültürünü ölçen ilk 24 sorusu analiz edildiğinde, en küçük ortalama değeri 2,51 ile adhokrasi kültürünü baskın özellikler boyutunda betimleyen 2. sorunun, en büyük değeri de 3,33 ile hiyerarşi kültürünü örgütsel liderlik boyutunda betimleyen 8. sorunun aldığı sonucuna ulaşılmıştır. Örgüt kültürünü baskın özellikler, örgütsel liderlik, çalışanların yönetimi, örgüte bağlılık, stratejik vurgular ve başarı kriteri olmak üzere toplam 6 farklı boyutta betimleyen dörderli soru grupları kendi içinde değerlendirildiğinde, boyutların tamamında mekanik süreçleri yansıtan hiyerarşi ve pazar kültürlerini betimleyen soruların, organik süreçleri yansıtan klan ve adhokrasi kültürlerini betimleyen sorulardan yüksek değerler aldığı görülmüştür. Başarı kriteri boyutundaki 24. soru hariç diğer tüm boyutlarda da en yüksek puanı hiyerarşi kültürünü betimleyen sorular almıştır.

Anketin bilgi güvenliği algısını ölçen sonraki 19 sorusu analiz edildiğinde ise en küçük ortalama değeri 2,56 ile sorumluluk algısını betimleyen 40. sorunun, en büyük ortalama değeri de 3,86 ile erişilebilirlik algısını betimleyen 37. sorunun aldığı görülmüştür.

Örgüt kültürünü ölçen soruların standart sapma değerleri incelendiğinde, adhokrasi kültürünü baskın özellikler boyutunda betimleyen 2. sorunun 1,093 değeri ile en homojen dağılımı gösterdiği, adhokrasi kültürünü örgütsel liderlik boyutunda betimleyen 6. sorunun ise 1,219 değeri ile en yüksek standart sapmaya sahip olduğu görülmüştür. Bilgi güvenliği algısını ölçen soruların standart sapma değerleri incelendiğinde de erişilebilirlik algısını betimleyen 36. sorunun 0,994 değeri ile en homojen dağılımı gösterdiği, sorumluluk algısını betimleyen 40. sorunun ise 1,122 değeri ile en yüksek standart sapmaya sahip olduğu sonucuna ulaşılmıştır.

5.4. Verilerin Frekans Analizi

Bağımlı ve bağımsız değişkenlerin frekans analizi sonuçları Çizelge 5.4'te, cinsiyet, yaş grupları, mesleki deneyim ve idari görev itibarıyla aldığı ortalama değerler de Çizelge 5.5'te verilmiştir. Çizelge 5.4'te frekans analizi sonuçları verilen değişkenlerden bilgi güvenliği, gizlilik, bütünlük, erişilebilirlik ve sorumluluk algılarının ortalama değerleri dikkate alınarak hazırlanmış olan Türkiye'deki devlet üniversitelerinde çalışan akademik personelin bilgi güvenliği algısı profili Şekil 5.1'de, örgüt kültürü türlerinin ortalama değerleri dikkate alınarak hazırlanmış olan Türkiye'deki devlet üniversitelerinin Cameron

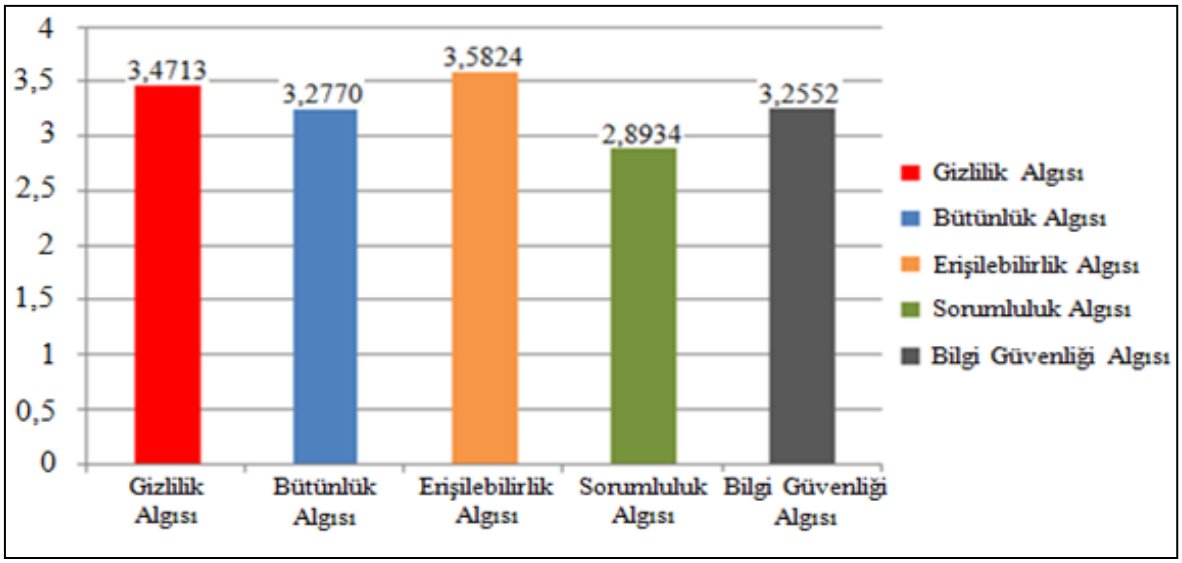
ve Freeman Örgüt Kültürü Türleri Modeli'ne göre genel örgüt kültürü profili de Şekil 5.2'de verilmiştir.

Çizelge 5.4. Verilerin değişkenlere göre frekans analizi

Değişkenler	Ortalama Değer	Standart Sapma	Varyans	Minimum	Maksimum
Hiyerarşi	3,1465	0,87366	0,763	1	5
Pazar	3,0163	0,93496	0,874	1	5
Klan	2,7548	0,94670	0,896	1	5
Adhokrasi	2,8019	0,94154	0,886	1	5
Gizlilik Algısı	3,4713	0,83761	0,702	1	5
Bütünlük Algısı	3,2770	0,84874	0,720	1	5
Erişilebilirlik Algısı	3,5824	0,82596	0,682	1	5
Sorumluluk Algısı	2,8934	0,84622	0,716	1	5
Bilgi Güvenliği Algısı	3,2552	0,73639	0,542	1	5

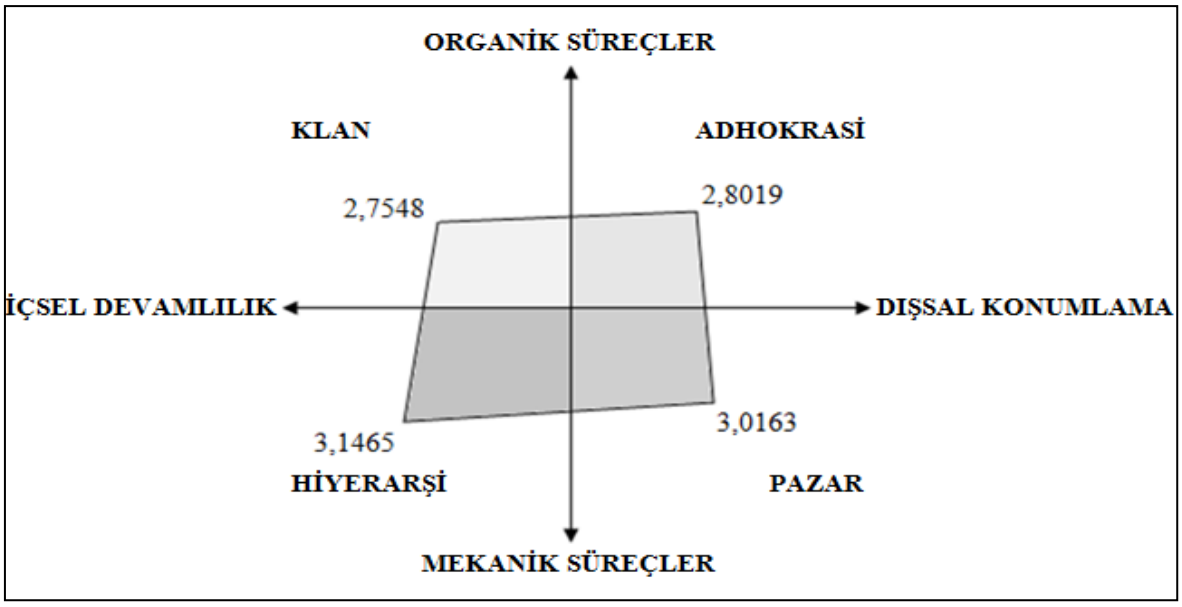
Çizelge 5.5. Değişkenlerin cinsiyet, yaş grupları, mesleki deneyim ve idari görev itibarıyla aldığı ortalama değerler

		Hiyerarşi	Pazar	Klan	Adhokrasi	Gizlilik Algısı	Bütünlük Algısı	Erişilebilirlik Algısı	Sorumluluk Algısı	Bilgi Güvenliği Algısı
Cinsiyet	Kadın	3,2550	3,1693	2,8217	2,9092	3,5473	3,3211	3,6250	2,9534	3,3125
	Erkek	3,0678	2,9052	2,7063	2,7239	3,4160	3,2450	3,5515	2,8499	3,2136
Yaş	<25	3,5879	3,4576	3,1697	3,2061	3,7091	3,4291	3,6970	3,0697	3,4316
	25-34 arası	3,1521	3,0143	2,7547	2,7779	3,4575	3,2163	3,5432	2,8459	3,2144
	35-44 arası	3,1535	3,0273	2,7457	2,8267	3,5079	3,3323	3,6231	2,8945	3,2862
	45-54 arası	3,1023	2,9769	2,7354	2,7726	3,4340	3,2913	3,5958	2,9433	3,2670
	≥55	3,0776	2,9637	2,7368	2,8078	3,4248	3,3297	3,5776	3,0107	3,2931
Mesleki Deneyim	1-5 yıl	3,2636	3,1214	2,8676	2,8803	3,5278	3,2752	3,5851	2,9125	3,2761
	6-10 yıl	3,0198	2,8871	2,6158	2,6792	3,3956	3,2200	3,5456	2,8125	3,1889
	11-15 yıl	3,0815	2,9629	2,6916	2,7672	3,4500	3,2804	3,5824	2,8469	3,2358
	16-20 yıl	3,1234	2,9779	2,7095	2,7980	3,5390	3,3175	3,5904	2,9421	3,3003
	≥ 21 yıl	3,1049	3,0068	2,7521	2,8064	3,4074	3,3216	3,6166	2,9513	3,2738
İdari Görev	Var	3,2364	3,0992	2,8764	2,9161	3,5135	3,3745	3,6502	2,9543	3,3219
	Yok	3,1124	2,9849	2,7087	2,7585	3,4552	3,2400	3,5567	2,8703	3,2299



Şekil 5.1. Türkiye'de devlet üniversitelerindeki akademik personelin bilgi güvenliği algısı profili

Şekil 5.1'de görüldüğü üzere Türkiye'de devlet üniversitelerindeki akademik personelin erişilebilirlik algısının 3,5824 ortalama değeri ile en yüksek puana sahip olduğu, erişilebilirlik algısını sırasıyla 3,4713 ortalama değeri ile gizlilik algısının ve 3,2770 ortalama değeri ile bütünlük algısının takip ettiği, sorumluluk algısının da 2,8934'lük puanla en az ortalama değere sahip olduğu anlaşılmaktadır. Akademik personelin bilgi güvenliği algısını bilgi güvenliği prensipleri temelinde betimleyen toplam 19 sorunun aritmetik ortalaması olarak genel bilgi güvenliği algısı puanının ise 3,2552 çıktığı görülmektedir.



Şekil 5.2. Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profili

Şekil 5.2'de de görüldüğü üzere örgüt kültürünü ölçümleyen tüm gözlem verileri bir bütün olarak ele alındığında, Türkiye'deki devlet üniversiteleri genelinde hiyerarşi kültürünün 3,1465 ortalama değeri ile baskın olduğu ve hiyerarşi kültürünü 3,0163 ortalama değeri ile pazar kültürünün takip ettiği anlaşılmaktadır. Hiyerarşi ve pazar kültürlerinden sonra, sırasıyla 2,8019 ortalama değeri ile adhokrasi kültürü ve 2,7548 ortalama değeri ile de klan kültürü gelmektedir. Diğer bir yaklaşımla Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profilinde hiyerarşi ve pazar kültürlerinin temsil ettiği mekanik süreçlerin, klan ve adhokrasi kültürlerinin temsil ettiği organik süreçlere göre baskın olduğu görülmektedir.

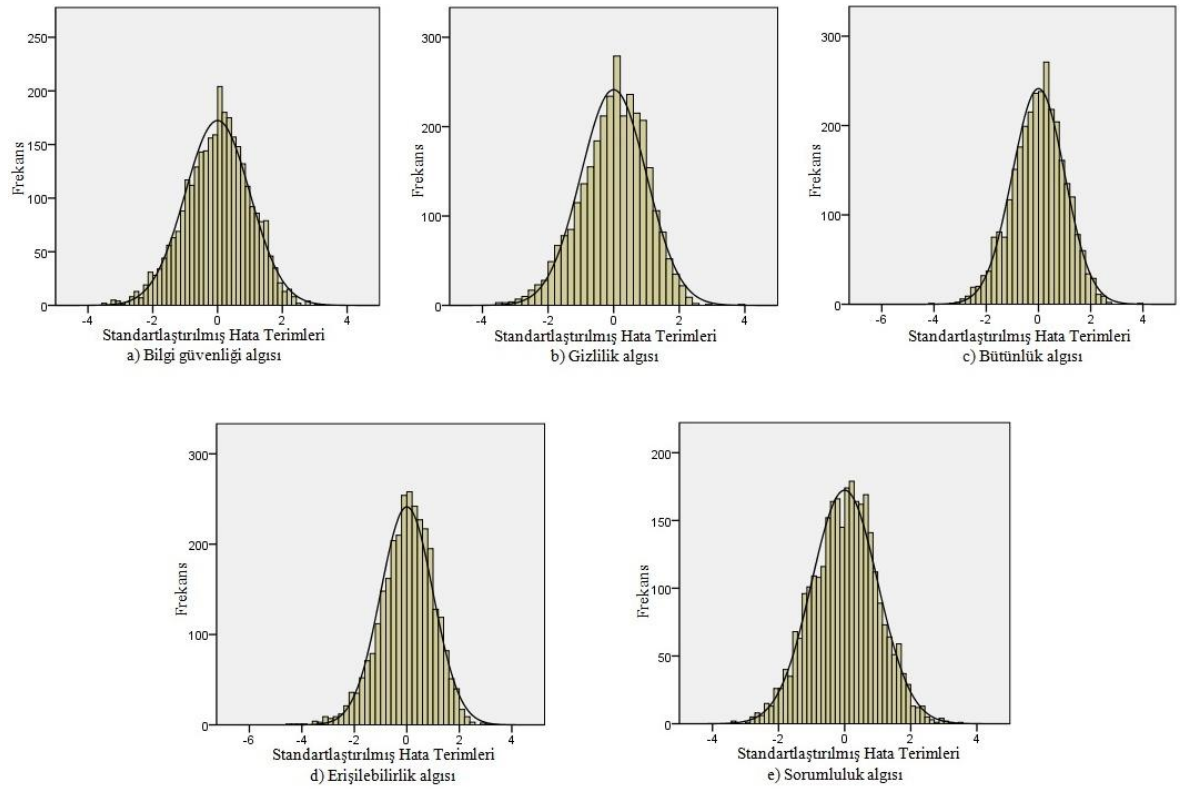
Bağımlı ve bağımsız değişkenlerin cinsiyet, yaş grupları, mesleki deneyim ve idari görev itibarıyla aldığı ortalama değerler (Bkz. Çizelge 5.5) incelendiğinde, örgüt kültürü türleri, bilgi güvenliği algısı ve bilgi güvenliği prensipleri algıları değişkenlerinin tümünde en yüksek puanların cinsiyet açısından kadın, yaş grupları açısından 25'ten küçük yaş dilimindeki ve idari görev açısından ise idari görevi olan akademik personele ait olduğu görülmektedir. Mesleki deneyim açısından bakıldığında da 1-5 yıl arası mesleki deneyime sahip akademik personel için örgüt kültürü türlerinin tamamının en yüksek puanı aldığı, bununla birlikte bilgi güvenliği algısının 16-20 yıl arası mesleki deneyime sahip akademik personelde daha yüksek çıktığı, bilgi güvenliği algısı boyutları özelinde ise gizlilik algısı hariç diğer tüm bilgi güvenliği prensipleri algılarında en yüksek puanların 21 ve üzeri yıl mesleki deneyime sahip akademik personele ait olduğu görülmektedir.

5.5. Korelasyon Analizi

Değişkenlerin arasındaki ilişkinin derecesini ve yönünü belirlemek için en sık kullanılan istatistiki yöntem, korelasyon analizidir. Pearson korelasyon katsayısı, aralıklı ölçekte ölçülmüş olan değişkenlerin arasındaki doğrusal ilişkinin derecesine ve yönüne bakılmak istendiğinde en sık kullanılan bir katsayı olup 'r' harfiyle gösterilir ve -1 ile +1 arasında bir değer almaktadır. Katsayı pozitif ise değişkenlerin biri artarken diğeri de artıyor; negatif ise değişkenlerin biri artarken diğeri azalıyor anlamına gelmektedir (Durmuş, Yurtkoru ve Çinko, 2013: 143-144).

Değişkenler arası Pearson korelasyon analizi yapabilmek için, öncelikle değişkenlerin normal dağıldığı varsayımının sağlanması gerekmektedir (Hauke ve Kossowski, 2011). Normallik varsayımının sağlanması için, bağımlı değişkenlerin hata terimleri (gözlemlenen

ve beklenen değerler farkı) normal dağılmış olmalıdır (Durmuş ve diğerleri, 2013: 157). Şekil 5.3'te yer alan histogramlarda bağımlı değişkenler bilgi güvenliği algısı, gizlilik algısı, bütünlük algısı, erişilebilirlik algısı ve sorumluluk algısının hata terimlerinin normal dağıldığı görülmektedir.



Şekil 5.3. Bağımlı değişkenlerin hata terimlerinin dağılımı

Korelasyon katsayısının (r), mutlak değer olarak 0,70-1,00 arasında olması yüksek; 0,30-0,70 arasında olması orta; 0-0,30 arasında olması ise düşük düzeyde bir ilişki olarak tanımlanabilir (Büyüköztürk, 2015: 32).

Çizelge 5.6'da yer alan Pearson korelasyon matrisindeki r katsayıları değerlendirildiğinde, örgüt kültürü türleri hiyerarşi, pazar, klan ve adhokrasi ile akademik personelin gizlilik, bütünlük, erişilebilirlik, sorumluluk ve bilgi güvenliği algıları arasında istatistiki olarak p=0,000 (p<0,01) anlamlılık düzeyinde, pozitif ve orta düzeyde doğrusal bir ilişkinin var olduğu sonucuna ulaşılmıştır. Korelasyon katsayısı değerleri incelendiğinde bağımsız değişkenler örgüt kültürü türleri hiyerarşi, pazar, klan ve adhokrasinin, sırasıyla bağımlı değişkenlerden gizlilik algısı ile 0,542, 0,524, 0,494, 0,507 değerlerinde, bütünlük algısı ile 0,561, 0,559, 0,533, 0,546 değerlerinde, erişilebilirlik algısı ile 0,509, 0,493, 0,450, 0,467

değerlerinde, sorumluluk algısı ile 0,550, 0,549, 0,561, 0,558 değerlerinde ve bilgi güvenliği algısı ile de 0,622, 0,613, 0,593, 0,602 değerlerinde doğrusal anlamlı bir ilişki içinde olduğu görülmektedir.

Çizelge 5.6. Değişkenler arası korelasyon matrisi

Pearson Korelasyon	Hiyerarşi	Pazar	Klan	Adhokrasi	Gizlilik Algısı	Bütünlük Algısı	Erişilebilirlik Algısı	Sorumluluk Algısı	Bilgi Güvenliği Algısı
Hiyerarşi	1								
Pazar	0,845*	1							
Klan	0,782*	0,816*	1						
Adhokrasi	0,795*	0,883*	0,876*	1					
Gizlilik Algısı	0,542*	0,524*	0,494*	0,507*	1				
Bütünlük Algısı	0,561*	0,559*	0,533*	0,546*	0,742*	1			
Erişilebilirlik Algısı	0,509*	0,493*	0,450*	0,467*	0,665*	0,750*	1		
Sorumluluk Algısı	0,550*	0,549*	0,561*	0,558*	0,623*	0,715*	0,598*	1	
Bilgi Güvenliği Algısı	0,622*	0,613*	0,593*	0,602*	0,868*	0,918*	0,821*	0,872*	1

* p=0,000 (p<0,01) düzeyinde anlamlıdır (2 yönlü)

5.6. Doğrusal Regresyon Analizi

Korelasyon analizi herhangi iki değişken arasında bir ilişki olup olmadığını istatistiki olarak test ederken, regresyon analizi ise bir bağımlı değişkenin diğer değişken(ler) tarafından bir matematiksel eşitlik ile nasıl açıklandığını belirlemeye çalışır. Değişkenler arasında doğrusal ilişkinin olduğu ve bir bağımlı değişkenin birden fazla bağımsız değişken tarafından açıklandığı durumlarda çoklu doğrusal regresyon analizi kullanılır (Büyüköztürk, 2015: 91; Durmuş ve diğerleri, 2013: 154).

Çoklu doğrusal bağıntı varsayımı (multicollinearity)

Doğrusal regresyon analizinin doğru sonuçlar vermesi için, bağımsız değişkenlerin birbiriyle ilişkili olmaması varsayımının gerçekleşmesi gerekmektedir. Bağımsız değişkenlerden biri diğer bağımsız değişken veya değişkenlerin bir doğrusal fonksiyonu olarak ifade ediliyorsa bağımsız değişkenler arasında doğrusal ilişkinin varlığından söz edilir. Bu duruma çoklu doğrusal bağıntı problemi (multicollinearity) adı verilmektedir

(Albayrak, 2005; Topal, Eyduran ve Yağanoğlu, 2010). Korelasyon matirisinde bağımsız değişkenlerin korelasyon katsayılarının mutlak değerlerinin büyük olması (1'e yakın olması), çoklu doğrusal bağıntının varlığına işaret edebilir. Çoklu doğrusal bağıntının olmaması için bağımsız değişkenler arasında önemli bir korelasyonun (r>0,9) olmaması gerekmektedir (Field, 2009: 233). Fakat bununla birlikte yüksek korelasyon katsayıları mutlaka çoklu doğrusal bağıntının varlığı anlamına da gelmemektedir (Büyüköztürk, 2015: 100; Jeeshim ve Kucc, 2002; Vupa ve Alma, 2008).

Çoklu doğrusal bağıntının saptanmasında korelasyon matris katsayılarının incelenmesinin yanı sıra kullanılan birkaç yaklaşım bulunmaktadır. Çoklu doğrusal bağıntı probleminin saptanmasında kullanılan yöntemlerin başında varyans büyütme faktörü VIF (Variance Inflation Factor) değerinin $VIF=1/(1-R^2)$ eşitliği ile hesaplanması gelmektedir. Bağımsız değişkenler arasında ilişki yoksa determinasyon katsayısı $R^2=0$ olacağından VIF değeri 1'e eşit olacaktır. Şayet bağımsız değişkenler arasında tam bir ilişki varsa determinasyon katsayısı $R^2=1$ olacağından VIF sonsuz değere ulaşacaktır. Bununla birlikte çoklu doğrusal bağıntı probleminin saptanmasında kullanılan bir diğer yöntem, bağımsız değişkenler için tolerans değeri TV'nin (Tolerance Value) $TV=(1-R^2)$ eşitliği ile hesaplanmasıdır. Bu eşitlikten de anlaşılacağı üzere TV=1/VIF olmakta ve daha küçük TV değeri daha büyük VIF değeri anlamına gelmektedir (Vupa ve Alma, 2008). VIF değerinin 10'dan büyük veya TV değerinin 0,1'den küçük olması durumunda anlamlı bir çoklu doğrusal bağıntı probleminden şüphe edilebilir (Büyüköztürk, 2015: 100; Jeeshim ve Kucc, 2002).

Regresyon katsayılarının t istatistiği değerlerinin hiçbiri anlamlı olmadığı hâlde regresyon modeline ait olan F istatistiğinin anlamlı olması, veri setinde çoklu doğrusal bağlantının varlığının bir göstergesidir (Topal ve diğerleri, 2010). Başka bir ifadeyle çoklu doğrusal bağıntı probleminin varlığı söz konusu olduğunda, modelin determinasyon katsayısı R^2 değeri yüksek, ancak bağımsız değişkenlerden hiçbiri veya çok azı t testine göre anlamlı olmaktadır (Vupa ve Alma, 2008).

Bağımsız değişkenlerin korelasyon matrisinin determinant değerinden yararlanarak da çoklu doğrusal bağıntı problemi saptanabilmektedir. Söz konusu determinant değerinin 0,00001'den büyük olması çoklu doğrusal bağıntı probleminin olmadığı anlamına gelmektedir (Field, 2009: 660).

Çoklu doğrusal bağıntının saptanmasında kullanılan bir diğer yöntem ise koşul indeksi CI'nın (Condition Index) kontrol edilmesidir. Koşul indeksi, $CI = (\lambda max/\lambda i)^{0,5}$ formülü ile hesaplanmaktadır. Burada λmax, bağımsız değişkenlerin korelasyon matrisindeki en büyük özdeğeri (eigenvalue), λi ise matristeki i'nci özdeğeri ifade etmektedir. CI değerinin 30'dan büyük olduğu durumlar çoklu doğrusal bağıntının varlığına işaret etmektedir (Büyüköztürk, 2015: 100; Coenders ve Saez, 2000; Saikia ve Singh, 2014).

Bağımsız değişkenler örgüt kültürü türleri hiyerarşi, pazar, klan ve adhokrasi arasında çoklu doğrusal bağıntının olmaması varsayımı H1 hipotezinde kontrol edilmiştir.

5.6.1. Hipotez testleri

Hipotezler için çoklu doğrusal regresyon modelleri oluşturulurken bağımsız değişkenleri temsil eden örgüt kültürü türleri hiyerarşi, pazar, klan ve adhokrasi, SPSS'de "enter" metoduyla analize sokulmuştur.

H1 hipotez testi

H1: Örgüt kültürü bilgi güvenliği algısını etkiler.

H1 hipotezinde bağımlı değişken gizlilik algısı, bütünlük algısı, erişilebilirlik algısı ve sorumluluk algısı boyutlarından oluşan bilgi güvenliği algısıdır. Çizelge 5.7'de regresyon modelinin düzeltilmiş R^2 istatistiği değerinin 0,426 çıktığı görülmektedir. Buna göre, bağımsız değişkenler örgüt kültürü türlerinin bilgi güvenliği algısını açıklama oranı %42,6'dır. Diğer bir ifadeyle bilgi güvenliği algısına ilişkin toplam varyansın %42,6'sı örgüt kültürü türleri ile açıklanmaktadır.

Çizelge 5.7. Bilgi güvenliği algısı için regresyon modelinin açıklama gücü

Model	R	R^2	Düzeltilmiş R^2	Standart Hata
1	0,654[a]	0,427	0,426	0,55772

a. Yordayıcılar: (Sabit), Hiyerarşi, Pazar, Klan, Adhokrasi

Regresyon analizinde hipotez testi, F istatistiği ile gerçekleştirilir (Durmuş ve diğerleri, 2013: 159). Çizelge 5.8'de yer alan bilgi güvenliği algısı için oluşturulmuş regresyon

modelinin ANOVA tablosunda görüldüğü üzere modelin F istatistiğinin p değeri 0,000 (p<0,01) çıkmış olup, H1 hipotezi kabul edilmiştir. Bunun anlamı bilgi güvenliği algısının örgüt kültürü türleri ile tahmin edilmesinin istatistiki olarak mümkün olduğudur.

Çizelge 5.8. Bilgi güvenliği algısı için regresyon analizinin ANOVA[a] tablosu

Model		Kareler Toplamı	df	Ortalama Kareler	F	Anlamlılık (p)
1	Regresyon	699,994	4	174,999	562,608	0,000[b]
	Hata terimleri	938,746	3018	0,311		
	Toplam	1638,740	3022			

a. Bağımlı Değişken: Bilgi Güvenliği Algısı
b. Yordayıcılar: (Sabit), Hiyerarşi, Pazar, Klan, Adhokrasi

Regresyon modelinin genel bir sınaması F istatistiği ile yapıldıktan sonra modeli oluşturan standartlaştırılmamış katsayıların her biri için anlamlılık testi t istatistiği ile uygulanır (Durmuş ve diğerleri, 2013: 159). Bu aşamada test edilecek katsayıların t istatistiklerinin p değerlerine bakılacak olup, anlamlılık düzeyinde olan (p<0,01 veya p<0,05) standartlaştırılmamış katsayılar tahmin edilecek matematiksel modeli oluşturacaktır (Durmuş ve diğerleri, 2013: 164). Bağımsız değişkenlerin bağımlı değişkene ilişkin önem sıralarını yorumlamada ise regresyon modelindeki katsayılar kullanılmaz. Bu amaçla standartlaştırılmış katsayılar (β) dikkate alınacak olup, en yüksek β değerine sahip olan bağımsız değişken, bağımlı değişken üzerinde göreli olarak en önemli yordayıcı olacaktır (Büyüköztürk, 2015: 99).

Çizelge 5.9. Bilgi güvenliği algısı için regresyon modeli katsayıları ve doğrusal bağıntı istatistikleri

Model		Standartlaştırılmamış Katsayılar		Standartlaştırılmış Katsayılar	t	Anlamlılık (p)	Doğrusal Bağıntı İstatistikleri	
		Katsayı	Standart Hata	Katsayı(β)			Tolerans	VIF
1	(Sabit)	1,565	0,038		41,104	0,000		
	Hiyerarşi	0,254	0,023	0,301	11,153	0,000	0,261	3,833
	Pazar	0,114	0,027	0,144	4,251	0,000	0,165	6,058
	Klan	0,111	0,023	0,143	4,792	0,000	0,212	4,706
	Adhokrasi	0,087	0,028	0,111	3,093	0,002	0,148	6,745

Çizelge 5.9'da yer alan modelin standartlaştırılmış katsayılarının (β), hiyerarşi için 0,301, pazar için 0,144, klan için 0,143 ve adhokrasi için 0,111 çıktığı, diğer bir ifadeyle bilgi güvenliği algısı üzerinde göreli olarak önem sırasıyla hiyerarşi, pazar, klan ve adhokrasi

kültürlerinin etkili olduğu görülmektedir. Bununla birlikte modeli oluşturacak standartlaştırılmamış katsayıların t istatistiklerinin p değerleri, sabit değer, hiyeraşi, pazar ve klan için 0,000 ($p<0,01$), adhokrasi için 0,002 ($p<0,01$) anlamlılık düzeyinde çıkmıştır. Bu bağlamda bilgi güvenliği algısının yordamlanmasına ilişkin oluşturulan regresyon eşitliği (matematiksel model) aşağıda verilmiştir:

Bilgi Güvenliği Algısı

= 1,565 + 0,254 x Hiyerarşi + 0,114 x Pazar + 0,111 x Klan + 0,087 x Adhokrasi

Bağımsız değişkenlerde doğrusal bağıntı olmaması varsayımı ise Çizelge 5.9'daki doğrusal bağıntı istatistikleri, Çizelge 5.10'daki bağımsız değişkenlerin korelasyon matrisi ve Çizelge 5.11'de yer alan doğrusal bağıntı diyagnostik tablosu kullanılarak sınanmıştır.

Çizelge 5.10. Bağımsız değişkenlerin korelasyon matrisi

Korelasyon Matrisi	Hiyerarşi	Pazar	Klan	Adhokrasi
Hiyerarşi	1	0,845	0,782	0,795
Pazar	0,845	1	0,816	0,883
Klan	0,782	0,816	1	0,876
Adhokrasi	0,795	0,883	0,876	1

Determinant = 0,013

Çizelge 5.11. Doğrusal bağıntı diyagnostik tablosu

Boyut	Özdeğer (λ)	Koşul İndeksi (CI)	Varyans Oranları				
			(Sabit)	Hiyeraşi	Pazar	Klan	Adhokrasi
1	4,887	1,000	0,00	0,00	0,00	0,00	0,00
2	0,069	8,415	0,77	0,00	0,01	0,04	0,02
3	0,020	15,495	0,16	0,30	0,13	0,45	0,02
4	0,015	18,227	0,06	0,45	0,15	0,30	0,29
5	0,009	23,817	0,00	0,25	0,71	0,21	0,67

Çizelge 5.9'da görüldüğü üzere modelin F istatistiğinin anlamlı olduğu durumda (Bkz. Çizelge 5.8) bağımsız değişkenlerin tamamı t testine göre anlamlı çıkmıştır. Ayrıca bağımsız değişkenlerin tamamının VIF değerlerinin 10'dan küçük ve tolerans değerlerinin 0,1'den büyük olduğu görülmektedir. Bununla birlikte Çizelge 5.10'da yer alan bağımsız değişkenlerin korelasyon matrisinin determinant değeri 0,013 olup 0,00001'den büyük olma şartını da sağlamaktadır. Ayrıca Çizelge 5.11'de yer alan doğrusal bağıntı diyagnostik

tablosundan da CI değerlerinin tamamının 30'dan küçük çıktığı görülmektedir. Bu bilgiler ışığında bağımsız değişkenler örgüt kültürü türleri hiyerarşi, pazar, klan ve adhokrasi arasında çoklu doğrusal bağıntı probleminin olmadığı sonucuna ulaşılmıştır.

H1a hipotez testi

H1a: Örgüt kültürü bilgi güvenliğinin gizlilik prensibi algısını etkiler.

H1a hipotezinde bağımlı değişken gizlilik algısıdır. Çizelge 5.12'de yer alan 1. regresyon modelinde düzeltilmiş R^2 istatistiği değerinin 0,313 çıktığı görülmektedir. Bu modele göre, bağımsız değişkenler örgüt kültürü türlerinin gizlilik algısını açıklama oranı %31,3'tür. Çizelge 5.13'te yer alan modelin ANOVA tablosunda görüldüğü üzere modelin F istatistiğinin p değeri 0,000 ($p<0,01$) anlamlılık düzeyinde çıkmıştır. Çizelge 5.14'te de görüldüğü üzere modeli oluşturan katsayıların t istatistiklerinin p değerleri, sabit değer, hiyerarşi ve pazar için 0,000 ($p<0,01$), klan için 0,016 ($p<0,05$) anlamlılık düzeyinde çıkmıştır. Adhokrasi katsayısı için p değeri 0,055 ($p>0,05$) anlamlılık düzeyinde olup, adhokrasinin gizlilik algısı üzerinde anlamlı bir etkiye sahip olmadığı görülmüştür.

Çizelge 5.12. Gizlilik algısı için regresyon modelinin açıklama gücü (model 1)

Model	R	R^2	Düzeltilmiş R^2	Standart Hata
1	0,560[a]	0,314	0,313	0,69427

a. Yordayıcılar: (Sabit), Hiyerarşi, Pazar, Klan, Adhokrasi

Çizelge 5.13. Gizlilik algısı için regresyon analizinin ANOVA[a] tablosu (model 1)

Model		Kareler Toplamı	df	Ortalama Kareler	F	Anlamlılık (p)
1	Regresyon	665,522	4	166,380	345,184	0,000[b]
	Hata terimleri	1454,690	3018	0,482		
	Toplam	2120,212	3022			

a. Bağımlı değişken: Gizlilik Algısı
b. Yordayıcılar: (Sabit), Hiyerarşi, Pazar, Klan, Adhokrasi

Bağımsız değişken adhokrasinin gizlilik algısı üzerinde anlamlı bir etkiye sahip olmamasından dolayı 1. modelde yer alan adhokrasi doğrusal regresyon analizinden çıkarılmış, sadece hiyerarşi, pazar ve klan bağımsız değişkenlerinin analize tabi

tutulmasıyla 2. model elde edilmiştir. Elde edilen yeni doğrusal regresyon modelinin tabloları Çizelge 5.15, 5.16 ve 5.17'de verilmiştir.

Çizelge 5.14. Gizlilik algısı için regresyon modeli katsayıları (model 1)

Model		Standartlaştırılmamış Katsayılar		Standartlaştırılmış Katsayılar	t	Anlamlılık (p)
		Katsayı	Standart Hata	Katsayı (β)		
1	(Sabit)	1,802	0,047		38,011	0,000
	Hiyerarşi	0,295	0,028	0,308	10,438	0,000
	Pazar	0,119	0,033	0,133	3,593	0,000
	Klan	0,070	0,029	0,079	2,404	0,016
	Adhokrasi	0,067	0,035	0,075	1,922	0,055

Çizelge 5.15. Gizlilik algısı için regresyon modelinin açıklama gücü (model 2)

Model	R	R^2	Düzeltilmiş R^2	Standart Hata
2	0,560[a]	0,313	0,312	0,69458

a. Yordayıcılar: (Sabit), Hiyerarşi, Pazar, Klan

Çizelge 5.16. Gizlilik algısı için regresyon analizinin ANOVA[a] tablosu (model 2)

Model		Kareler Toplamı	df	Ortalama Kareler	F	Anlamlılık (p)
2	Regresyon	663,741	3	221,247	458,605	0,000[b]
	Hata terimleri	1456,471	3019	0,482		
	Toplam	2120,212	3022			

a. Bağımlı değişken: Gizlilik Algısı
b. Yordayıcılar: (Sabit), Hiyerarşi, Pazar, Klan

Çizelge 5.17. Gizlilik algısı için regresyon modeli katsayıları (model 2)

Model		Standartlaştırılmamış Katsayılar		Standartlaştırılmış Katsayılar	t	Anlamlılık (p)
		Katsayı	Standart Hata	Katsayı (β)		
2	(Sabit)	1,801	0,047		37,971	0,000
	Hiyerarşi	0,297	0,028	0,310	10,499	0,000
	Pazar	0,152	0,029	0,170	5,342	0,000
	Klan	0,100	0,024	0,113	4,144	0,000

Çizelge 5.15'te yer alan 2. ve nihai regresyon modeline göre, bağımsız değişkenler örgüt kültürü türlerinin gizlilik algısını açıklama oranı olarak düzeltmiş R^2 istatistiği değerinin 0,312 çıktığı görülmektedir. Diğer bir ifadeyle gizlilik algısına ilişkin toplam varyansın

%31,2'si örgüt kültürü türleri ile açıklanmaktadır. Çizelge 5.16'da yer alan gizlilik algısı için oluşturulmuş regresyon modelinin ANOVA tablosunda görüldüğü üzere modelin F istatistiğinin p değeri 0,000 ($p<0,01$) düzeyinde çıkmış olup, H1a hipotezi kabul edilmiştir. Bunun anlamı gizlilik algısının örgüt kültürü türleri ile tahmin edilmesinin istatistiki olarak mümkün olduğudur.

Çizelge 5.17'de yer alan modelin standartlaştırılmış katsayılarının (β), hiyerarşi için 0,310, pazar için 0,170 ve klan için 0,113 çıktığı, diğer bir ifadeyle gizlilik algısı üzerinde göreli olarak önem sırasıyla hiyerarşi, pazar ve klan kültürlerinin etkili olduğu görülmektedir. Bununla birlikte modeli oluşturacak standartlaştırılmamış katsayıların t istatistiklerinin p değerleri, sabit değer, hiyerarşi, pazar ve klan için 0,000 ($p<0,01$) anlamlılık düzeyinde çıkmıştır. Bu bağlamda gizlilik algısının yordamlanmasına ilişkin oluşturulan regresyon eşitliği (matematiksel model) aşağıda verilmiştir:

Gizlilik Algısı = 1,801 + 0,297 x Hiyerarşi + 0,152 x Pazar + 0,100 x Klan

H1b hipotez testi

H1b: Örgüt kültürü bilgi güvenliğinin bütünlük prensibi algısını etkiler.

H1b hipotezinde bağımlı değişken bütünlük algısıdır. Çizelge 5.18'de yer alan regresyon modeline göre, bağımsız değişkenler örgüt kültürü türlerinin bütünlük algısını açıklama oranı olarak düzeltmiş R^2 istatistiği değerinin 0,348 çıktığı görülmektedir. Diğer bir ifadeyle bütünlük algısına ilişkin toplam varyansın %34,8'i örgüt kültürü türleri ile açıklanmaktadır. Çizelge 5.19'da yer alan bütünlük algısı için oluşturulmuş regresyon modelinin ANOVA tablosunda görüldüğü üzere modelin F istatistiğinin p değeri 0,000 ($p<0,01$) düzeyinde çıkmış olup, H1b hipotezi kabul edilmiştir. Bunun anlamı bütünlük algısının örgüt kültürü türleri ile tahmin edilmesinin istatistiki olarak mümkün olduğudur.

Çizelge 5.18. Bütünlük algısı için regresyon modelinin açıklama gücü

Model	R	R^2	Düzeltilmiş R^2	Standart Hata
1	0,591[a]	0,349	0,348	0,68508

a. Yordayıcılar: (Sabit), Hiyerarşi, Pazar, Klan, Adhokrasi

Çizelge 5.19. Bütünlük algısı için regresyon analizinin ANOVA[a] tablosu

Model		Kareler Toplamı	df	Ortalama Kareler	F	Anlamlılık (p)
1	Regresyon	760,509	4	190,127	405,102	0,000[b]
	Hata terimleri	1416,443	3018	0,469		
	Toplam	2176,952	3022			

a. Bağımlı değişken: Bütünlük Algısı
b. Yordayıcılar: (Sabit), Hiyerarşi, Pazar, Klan, Adhokrasi

Çizelge 5.20. Bütünlük algısı için regresyon modeli katsayıları

Model		Standartlaştırılmamış Katsayılar		Standartlaştırılmış Katsayılar	t	Anlamlılık (p)
		Katsayı	Standart Hata	Katsayı (β)		
1	(Sabit)	1,517	0,047		32,430	0,000
	Hiyerarşi	0,251	0,028	0,259	8,997	0,000
	Pazar	0,144	0,033	0,159	4,387	0,000
	Klan	0,102	0,029	0,113	3,558	0,000
	Adhokrasi	0,091	0,034	0,101	2,649	0,008

Çizelge 5.20'de yer alan modelin standartlaştırılmış katsayılarının (β), hiyerarşi için 0,259, pazar için 0,159, klan için 0,113 ve adhokrasi için 0,101 çıktığı, diğer bir ifadeyle bütünlük algısı üzerinde göreli olarak önem sırasıyla hiyerarşi, pazar, klan ve adhokrasi kültürlerinin etkili olduğu görülmektedir. Bununla birlikte modeli oluşturacak standartlaştırılmamış katsayıların t istatistiklerinin p değerleri, sabit değer, hiyeraşi, pazar ve klan için 0,000 ($p<0,01$), adhokrasi için 0,008 ($p<0,01$) anlamlılık düzeyinde çıkmıştır. Bu bağlamda bütünlük algısının yordamlanmasına ilişkin oluşturulan regresyon eşitliği (matematiksel model) aşağıda verilmiştir:

Bütünlük Algısı

$$= 1,517 + 0,251 \text{ x Hiyerarşi} + 0,144 \text{ x Pazar} + 0,102 \text{ x Klan} + 0,091 \text{ x Adhokrasi}$$

H1c hipotez testi

H1c: Örgüt kültürü bilgi güvenliğinin erişilebilirlik prensibi algısını etkiler.

H1c hipotezinde bağımlı değişken erişilebilirlik algısıdır. Çizelge 5.21'de yer alan 1. regresyon modelinde düzeltilmiş R^2 istatistiği değerinin 0,274 çıktığı görülmektedir. Bu

modele göre, bağımsız değişkenler örgüt kültürü türlerinin erişilebilirlik algısını açıklama oranı %27,4'tür. Çizelge 5.22'de yer alan modelin ANOVA tablosunda görüldüğü üzere modelin F istatistiğinin p değeri 0,000 ($p<0,01$) anlamlılık düzeyinde çıkmıştır. Çizelge 5.23'te de görüldüğü üzere modeli oluşturan katsayıların t istatistiklerinin p değerleri, sabit değer, hiyerarşi ve pazar için 0,000 ($p<0,01$) anlamlılık düzeyinde çıkmıştır. Klan katsayısı için p değeri 0,313 ($p>0,05$) ve adhokrasi katsayısı için p değeri 0,194 ($p>0,05$) anlamlılık düzeyinde olup, klan ve adhokrasinin erişilebilirlik algısı üzerinde anlamlı bir etkiye sahip olmadığı görülmüştür.

Çizelge 5.21. Erişilebilirlik algısı için regresyon modelinin açıklama gücü (model 1)

Model	R	R^2	Düzeltilmiş R^2	Standart Hata
1	0,524[a]	0,275	0,274	0,70391

a. Yordayıcılar: (Sabit), Hiyerarşi, Pazar, Klan, Adhokrasi

Çizelge 5.22. Erişilebilirlik algısı için regresyon analizinin ANOVA[a] tablosu (model 1)

Model		Kareler Toplamı	df	Ortalama Kareler	F	Anlamlılık (p)
1	Regresyon	566,264	4	141,566	285,708	0,000[b]
	Hata terimleri	1495,393	3018	0,495		
	Toplam	2061,657	3022			

a. Bağımlı değişken: Erişilebilirlik Algısı
b. Yordayıcılar: (Sabit), Hiyerarşi, Pazar, Klan, Adhokrasi

Çizelge 5.23. Erişilebilirlik algısı için regresyon modeli katsayıları (model 1)

Model		Standartlaştırılmamış Katsayılar		Standartlaştırılmış Katsayılar	t	Anlamlılık (p)
		Katsayı	Standart Hata	Katsayı (β)		
1	(Sabit)	2,035	0,048		42,333	0,000
	Hiyerarşi	0,287	0,029	0,304	10,017	0,000
	Pazar	0,144	0,034	0,162	4,258	0,000
	Klan	0,030	0,029	0,034	1,008	0,313
	Adhokrasi	0,046	0,035	0,052	1,300	0,194

Bağımsız değişkenler klan ve adhokrasinin erişilebilirlik algısı üzerinde anlamlı bir etkiye sahip olmamasından dolayı 1. modelde yer alan klan ve adhokrasi doğrusal regresyon analizinden çıkarılmış, sadece hiyerarşi ve pazar bağımsız değişkenlerinin analize tabi tutulmasıyla 2. model elde edilmiştir. Elde edilen yeni doğrusal regresyon modelinin tabloları Çizelge 5.24, 5.25 ve 5.26'da verilmiştir.

Çizelge 5.24. Erişilebilirlik algısı için regresyon modelinin açıklama gücü (model 2)

Model	R	R^2	Düzeltilmiş R^2	Standart Hata
2	0,523[a]	0,273	0,273	0,70437

a. Yordayıcılar: (Sabit), Hiyerarşi, Pazar

Çizelge 5.25. Erişilebilirlik algısı için regresyon analizinin ANOVA[a] tablosu (model 2)

Model		Kareler Toplamı	df	Ortalama Kareler	F	Anlamlılık (p)
2	Regresyon	563,315	2	281,658	567,698	0,000[b]
	Hata terimleri	1498,342	3020	0,496		
	Toplam	2061,657	3022			

a. Bağımlı değişken: Erişilebilirlik Algısı
b. Yordayıcılar: (Sabit), Hiyerarşi, Pazar

Çizelge 5.26. Erişilebilirlik algısı için regresyon modeli katsayıları (model 2)

Model		Standartlaştırılmamış Katsayılar		Standartlaştırılmış Katsayılar	t	Anlamlılık (p)
		Katsayı	Standart Hata	Katsayı (β)		
2	(Sabit)	2,034	0,048		42,287	0,000
	Hiyerarşi	0,306	0,027	0,324	11,185	0,000
	Pazar	0,194	0,026	0,219	7,576	0,000

Çizelge 5.24'te yer alan 2. ve nihai regresyon modeline göre, bağımsız değişkenler örgüt kültürü türlerinin erişilebilirlik algısını açıklama oranı olarak düzeltmiş R^2 istatistiği değerinin 0,273 çıktığı görülmektedir. Diğer bir ifadeyle erişilebilirlik algısına ilişkin toplam varyansın %27,3'ü örgüt kültürü türleri ile açıklanmaktadır. Çizelge 5.25'te yer alan erişilebilirlik algısı için oluşturulmuş regresyon modelinin ANOVA tablosunda görüldüğü üzere modelin F istatistiğinin p değeri 0,000 ($p<0,01$) düzeyinde çıkmış olup, H1c hipotezi kabul edilmiştir. Bunun anlamı erişilebilirlik algısının örgüt kültürü türleri ile tahmin edilmesinin istatistiki olarak mümkün olduğudur.

Çizelge 5.26'da yer alan modelin standartlaştırılmış katsayılarının (β), hiyerarşi için 0,324 ve pazar için 0,219 çıktığı, diğer bir ifadeyle erişilebilirlik algısı üzerinde göreli olarak önem sırasıyla hiyerarşi ve pazar kültürlerinin etkili olduğu görülmektedir. Bununla birlikte modeli oluşturacak standartlaştırılmamış katsayıların t istatistiklerinin p değerleri, sabit değer, hiyerarşi ve pazar için 0,000 ($p<0,01$) anlamlılık düzeyinde çıkmıştır. Bu

bağlamda erişilebilirlik algısının yordamlanmasına ilişkin oluşturulan regresyon eşitliği (matematiksel model) aşağıda verilmiştir:

Erişilebilirlik Algısı = 2,034 + 0,306 x Hiyerarşi + 0,194 x Pazar

H1d hipotez testi

H1d: Örgüt kültürü bilgi güvenliğinin sorumluluk prensibi algısını etkiler.

H1d hipotezinde bağımlı değişken sorumluluk algısıdır. Çizelge 5.27'de yer alan regresyon modeline göre, bağımsız değişkenler örgüt kültürü türlerinin sorumluluk algısını açıklama oranı olarak düzeltmiş R^2 istatistiği değerinin 0,353 çıktığı görülmektedir. Diğer bir ifadeyle sorumluluk algısına ilişkin toplam varyansın %35,3'ü örgüt kültürü türleri ile açıklanmaktadır. Çizelge 5.28'de yer alan sorumluluk algısı için oluşturulmuş regresyon modelinin ANOVA tablosunda görüldüğü üzere modelin F istatistiğinin p değeri 0,000 ($p<0,01$) düzeyinde çıkmış olup, H1d hipotezi kabul edilmiştir. Bunun anlamı sorumluluk algısının örgüt kültürü türleri ile tahmin edilmesinin istatistiki olarak mümkün olduğudur.

Çizelge 5.27. Sorumluluk algısı için regresyon modelinin açıklama gücü

Model	R	R^2	Düzeltilmiş R^2	Standart Hata
1	0,595[a]	0,354	0,353	0,68068

a. Yordayıcılar: (Sabit), Hiyerarşi, Pazar, Klan, Adhokrasi

Çizelge 5.28. Sorumluluk algısı için regresyon analizinin ANOVA[a] tablosu

Model		Kareler Toplamı	df	Ortalama Kareler	F	Anlamlılık (p)
1	Regresyon	765,696	4	191,424	413,148	0,000[b]
	Hata terimleri	1398,331	3018	0,463		
	Toplam	2164,027	3022			

a. Bağımlı değişken: Sorumluluk Algısı
b. Yordayıcılar: (Sabit), Hiyerarşi, Pazar, Klan, Adhokrasi

Çizelge 5.29'da yer alan modelin standartlaştırılmış katsayılarının (β), hiyerarşi için 0,210 pazar için 0,075, klan için 0,219 ve adhokrasi için 0,133 çıktığı, diğer bir ifadeyle sorumluluk algısı üzerinde göreli olarak önem sırasıyla klan, hiyerarşi, adhokrasi ve pazar kültürlerinin etkili olduğu görülmektedir. Bununla birlikte modeli oluşturacak

standartlaştırılmamış katsayıların t istatistiklerinin p değerleri, sabit değer, hiyeraşi, klan ve adhokrasi için 0,000 ($p<0,01$), pazar için 0,036 ($p<0,05$) anlamlılık düzeyinde çıkmıştır.

Çizelge 5.29. Sorumluluk algısı için regresyon modeli katsayıları

Model		Standartlaştırılmamış Katsayılar		Standartlaştırılmış Katsayılar	t	Anlamlılık (p)
		Katsayı	Standart Hata	Katsayı (β)		
1	(Sabit)	1,174	0,046		25,253	0,000
	Hiyerarşi	0,204	0,028	0,210	7,339	0,000
	Pazar	0,068	0,033	0,075	2,094	0,036
	Klan	0,195	0,028	0,219	6,885	0,000
	Adhokrasi	0,119	0,034	0,133	3,498	0,000

Çizelge 5.29'un değerlendirilmesi neticesinde sorumluluk algısının yordamlanmasına ilişkin oluşturulan regresyon eşitliği (matematiksel model) aşağıda verilmiştir:

Sorumluluk Algısı

= 1,174 + 0,204 x Hiyerarşi + 0,068 x Pazar + 0,195 x Klan + 0,119 x Adhokrasi

5.6.2. Hipotez test sonuçlarının genel değerlendirilmesi

Örgüt kültürünün, bilgi güvenliği algısı, gizlilik algısı, bütünlük algısı, erişilebilirlik algısı ve sorumluluk algısı üzerindeki etkisini sorgulayan hipotezlerin, çoklu doğrusal regresyon analizleri ile gerçekleştirilmiş test sonuçları Çizelge 5.30'da özetlenmiştir.

Çizelge 5.30. Hipotez testlerinin sonuç tablosu

Araştırmanın Hipotezleri		Düzeltilmiş R^2	p	Sonuç
H1	Örgüt kültürü bilgi güvenliği algısını etkiler.	0,426	0,000	Kabul
H1a	Örgüt kültürü bilgi güvenliğinin gizlilik prensibi algısını etkiler.	0,312	0,000	Kabul
H1b	Örgüt kültürü bilgi güvenliğinin bütünlük prensibi algısını etkiler.	0,348	0,000	Kabul
H1c	Örgüt kültürü bilgi güvenliğinin erişilebilirlik prensibi algısını etkiler.	0,273	0,000	Kabul
H1d	Örgüt kültürü bilgi güvenliğinin sorumluluk prensibi algısını etkiler.	0,353	0,000	Kabul

Çizelge 5.30'da görüldüğü üzere araştırmada test edilen tüm hipotezler kabul edilmiştir. Diğer bir ifadeyle örgüt kültürünün, bilgi güvenliği prensipleri temelinde bilgi güvenliği algısı ile birlikte gizlilik algısı, bütünlük algısı, erişilebilirlik algısı ve sorumluluk algısı üzerinde etkiye sahip olduğu sonucuna ulaşılmıştır. Çoklu doğrusal regresyon analizi sonuçlarına göre, önem sırasıyla bilgi güvenliği algısı üzerinde hiyerarşi, pazar, klan ve adhokrasinin; gizlilik algısı üzerinde hiyerarşi, pazar ve klanın; bütünlük algısı üzerinde hiyerarşi, pazar, klan ve adhokrasinin; erişilebilirlik algısı üzerinde hiyerarşi ve pazarın; sorumluluk algısı üzerinde de klan, hiyerarşi, adhokrasi ve pazarın olumlu yönde etkiye sahip olduğu görülmüştür. Analiz sonuçları bir bütün olarak ele alındığında ise bilgi güvenliği algısı, gizlilik algısı, bütünlük algısı, erişilebilirlik algısı ve sorumluluk algısından oluşan bağımlı değişkenlerin tümü üzerinde olumlu yönde etkiye sahip olan ortak örgüt kültürü türlerinin hiyerarşi ve pazar olduğu sonucuna ulaşılmıştır.

6. SONUÇ VE ÖNERİLER

Bu tez çalışmasında, Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profilinin ve üniversitelerde çalışan akademik personelin bilgi güvenliği algısının belirlenmesi ve örgüt kültürünün bilgi güvenliği algısı üzerine etkisinin incelenmesi amaçlanmıştır. Bu amaç doğrultusunda genel örgüt kültürü profilinin tanımlanmasında Cameron ve Freeman Örgüt Kültürü Türleri Modeli ve bilgi güvenliği algısının belirlenmesinde de bilgi güvenliğinin gizlilik, bütünlük, erişilebilirlik ve sorumluluk prensipleri temel alınmıştır. Araştırmanın yürütülmesinde kullanılan ölçeğin örgüt kültürü türlerine ilişkin soruları, Cameron ve Freeman Örgüt Kültürü Türleri Modeli'nde tanımlanan örgüt kültürleri hiyerarşi, pazar, klan ve adhokrasi için Cameron ve Quinn (2006: 26-28) tarafından geliştirilmiş 24 sorulu OCAI ölçeği dikkate alınarak hazırlanmıştır. Araştırma ölçeğinin bilgi güvenliği algısına ilişkin 19 sorusunun hazırlanmasında ise Chang ve Lin'in (2007) BGYS standardı BS7799-1 doğrultusunda geliştirmiş oldukları ölçek referans alınmıştır. Çalışmaya özgü ölçeğin hazırlanmasında yararlanılan, geçerliği ve güvenirliğinin önceki çalışmalarda sağlandığı görülen bu iki ölçeğin Türkçeye tercümesi esnasında, kapsam geçerliğinin sağlanması adına bilişim uzmanlarının ve akademik personelin değerlendirmelerinden yararlanılmıştır. Ölçeğin uygulanmasında 5'li Likert ölçeği kullanılmış olup, araştırmanın örneklemi 3023 akademik personelden oluşmuştur. Anketin hesaplanan Cronbach Alpha iç güvenirlik katsayılarının her bir değişken için 0,7 değerinden büyük ve dolayısıyla ölçeğin bütünü itibarıyla güvenilir olduğu sonucuna ulaşılmıştır.

Araştırmanın Problemleri ile İlgili Sonuçlar

Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profili değerlendirildiğinde hiyerarşi kültürünün, diğer örgüt kültürü türlerine kıyasla 3,1465 ortalama değeri ile baskın çıktığı sonucuna ulaşılmıştır. Bunun yanı sıra pazar kültürünün de örgüt kültürü profilinde hiyerarşi kültüründen sonra 3,0163 ortalama değeri ile yer aldığı görülmüştür. Hiyerarşi ve pazar kültürlerinden sonra adhokrasi kültürü 2,8019 ortalama değerini almış, en düşük değere sahip örgüt kültürü ise 2,7548 ortalama değeri ile klan olmuştur. Araştırmanın evrenindeki akademik personelin çalışmakta olduğu üniversitelerin, kurallar, politikalar, prosedürler, anlaşılır tanımlamalar ve görevler temelli resmî işleyiş süreçlerine hâkim birer devlet kuruluşu olduğu düşünüldüğünde, hiyerarşi kültürünün baskın çıkması anlamlı

karşılanmıştır. Nitekim Mintzberg'e (1980) göre, gücün merkezî bir yerde toplanması eğilimi gösteren, operasyonel manada profesyonel olarak işleri yürütenlerin belirli prosedürler çerçevesinde kendi özerkliklerine sahip olduğu okul sistemlerinde, hiyerarşi kültürünü temsil eden bürokrasilerden profesyonel bürokrasi hâkimdir. Lunenburg'a (2012) göre de kamu okullarında profesyonel bürokrasinin birçok özelliği görülmektedir. Tezin 3. Bölüm'ünde sunulmuş olan alanyazın taramasına bakıldığında da bu durumu destekler nitelikte, Türkiye'deki devlet üniversitelerinden Ege Üniversitesi ve Fırat Üniversitesi bünyesinde örgüt kültürü konusu üzerine Rekabetçi Değerler Modeli'nden yararlanılarak yürütülmüş çalışmalarda, üniversitelerin genel örgüt kültürü profilinde hiyerarşi kültürünün diğer örgüt kültürü türlerine nazaran baskın çıktığı görülmüştür (Beytekin ve diğerleri, 2010; Erdem ve diğerleri, 2010). Benzer şekilde, Rekabetçi Değerler Modeli'nin kullanılmasıyla yürütülmüş bir başka çalışmada da devlet üniversitesiyle ilişkili olarak Fırat Üniversitesi Hastanesi'nin örgüt kültürü profilinde hiyerarşi kültürünün yüksek düzeyde baskın çıktığı sonucuna ulaşılmıştır (Erdem, 2007).

Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profilinde pazar kültürünün de hiyerarşi kültüründen sonra önemli ölçüde yer aldığının gözlemlenmiş olmasının, yüksek öğretim alanında üniversitelerarası yaşanan rekabet ortamında, üniversitelerin ortaya koyduğu rekabet avantajı elde etme stratejisinin yanı sıra, başarı ve sonuç odaklılık anlayışıyla açıklanması mümkündür. Cameron ve Freeman Örgüt Kültürü Türleri Modeli boyutlarında hiyerarşi ve pazar kültürlerinin ortak yönü değerlendirildiğinde ise Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profilinde kontrollü bir yapıya sahip mekanik süreçlerin baskın olduğu sonucuna ulaşılmıştır. Araştırmanın evrenini temsil eden devlet üniversitelerinin çoğunun köklü bir geçmişe sahip olduğu, yeni olanlarının ise genellikle köklü olanlardan ayrılarak kurulmuş olduğu dikkate alındığında, devlet üniversitelerinin genel örgüt kültürü profilinde elde edilen sonuçların, kültür yaşam döngüsüne göre de tutarlı olduğu görülmektedir. Nitekim Rekabetçi Değerler Modeli boyutunda kültür yaşam döngüsü kapsamında birçok örgütte, ilerleyen zamanla birlikte klan ve adhokrasi kültürlerinin etkisi azalmakta, mekanik süreçleri yansıtan hiyerarşi ve pazar kültürleri ise baskın hâle gelmektedir (Cameron ve Quinn, 2006: 57). Alanyazına bakıldığında da bu durumu destekler nitelikte, Türkiye'deki devlet üniversitelerinden Selçuk Üniversitesi'nde yürütülmüş bir çalışmada, üniversitedeki akademik personelin genel olarak mekanik örgüt yapısı anlayışını, organik örgüt yapısına göre daha fazla benimsediği sonucu elde edilmiştir (Gülnar, 2009). Benzer şekilde, Fırat Üniversitesi'nde

örgüt kültürünü konu alan, Rekabetçi Değerler Modeli'nden yararlanılarak yürütülmüş bir çalışmada, üniversitenin örgüt kültürü profilinde sırasıyla hiyerarşi ve pazar kültürlerinin diğer örgüt kültürü türlerine göre baskın çıktığı, akademik personelin üniversiteye ait kültürel özellikleri daha çok mekanik süreçler boyutunda tanımladığı görülmüştür (Erdem ve diğerleri, 2010). Rekabetçi Değerler Modeli'nin kullanılmasıyla yürütülmüş farklı bir çalışmada da devlet üniversitesiyle ilişkili olarak Fırat Üniversitesi Hastanesi'nin örgüt kültürü profili, hastane çalışanları tarafından mekanik süreçler boyutunda tanımlanmıştır (Erdem, 2007).

Türkiye'de devlet üniversitelerindeki akademik personelin bilgi güvenliği algısı değerlendirildiğinde, bilgi güvenliği algısını bilgi güvenliği prensipleri temelinde betimleyen toplam 19 sorunun aritmetik ortalaması olarak genel bilgi güvenliği algısının 3,2552 değerini aldığı sonucuna ulaşılmıştır. Bilgi güvenliği algısına bilgi güvenliği prensipleri algıları boyutlarında bakıldığında ise erişilebilirlik algısının 3,5824 ortalama değeri ile diğer bilgi güvenliği prensipleri algılarına nazaran yüksek çıktığı, erişilebilirlik algısını sırasıyla 3,4713 ortalama değeri ile gizlilik ve 3,2770 ortalama değeri ile bütünlük algılarının takip ettiği, sorumluluk algısının ise 2,8934 ile en az ortalama değere sahip, genel bilgi güvenliği algısı puanının altında değer alan tek bilgi güvenliği prensibi algısı olduğu görülmüştür. Erişilebilirlik prensibi algısının yüksek çıkması, Türkiye'deki devlet üniversitelerinde bilgi sistemlerinin bozulması ve bilgi servislerinin kesintiye uğraması olasılığının azaltılmasına önem verildiği, bilgi sistemlerinin herhangi bir zamanda ve herhangi bir yerden (İnternet veya İntranet üzerinden) öğrencilerin, personelin, diğer araştırmacı ve eğitmenlerin yetkileri dâhilinde erişimine açık olduğu algısının genel bir göstergesidir. Sorumluluk algısının ise genel bilgi güvenliği algısına ve diğer bilgi güvenliği prensipleri algılarına göre düşük çıkmasının, üniversitelerde bilgi güvenliği hakkında yararlı eğitimlerin verilmesi, bilgi güvenliği ile ilgili uyarıcı işaretlerin görünür yerlerde bulunması, bilgi güvenliği yönetim yapısının rol ve sorumluluklarla uyumlu bir şekilde kurulması, bilgi güvenliği kontrolleriyle alakalı bilgi güvenliği protokollerinin, normlarının ve düzenlemelerinin takip edilmesi hususlarında akademik personelin olumsuz yönde algıya sahip olmasından kaynaklandığı görülmüştür.

Örgütteki davranışları yönlendiren paylaşılmış değerlerin ve inançların örüntüsü olan örgüt kültürü, bireylerin bilinçaltı varsayımları temelinde şekillenmekte ve algılama yoluyla kurumsallaşmış gelenekleri sonraki nesillere ve dönemlere aktarma işlevini üstlenmektedir.

Örgüt kültürünün görünür dokularını oluşturan davranış biçimleri, değerlerin, varsayımların ve varsayımları anlamlı bir bütüne dönüştüren algıların etkisi altında kalmaktadır. Varsayımlarda meydana gelecek değişimler, algıyı değiştirmekte, bu durum da benimsenen değerlere ve insan davranışlarına yansımaktadır. Çalışanların bilgi güvenliği ile alakalı davranışlarını pozitif yönde etkileyen bilgi güvenliği algısının örgüt kültürünün temelinde yatan varsayımlar doğrultusunda değişime uğrayacağı vurgusundan hareketle, bilgi güvenliği algısının oluşmasında kültürel değişime ihtiyaç duyulmaktadır. Kültürel değişim yoluyla çalışanların bilgi güvenliğini istenilen şekilde algılaması sağlanabilir. Bu manada örgüt kültürü, çalışanların bilgi güvenliği algısını ve bilgi güvenliği ile alakalı sergileyecekleri davranışları etkilemektedir. Çalışanların bilgi güvenliği yönetimi uygulamalarına uyumlarındaki algı ve güdüleri, bilgi güvenliği ekseninde oluşturulacak örgüt kültürünün temelini teşkil edecektir. Diğer bir ifadeyle örgüt kültürü, bilgi güvenliği gereksinimleri ile uyumlu olmak adına nasıl davranılması gerektiğini gösteren değerlerin ve varsayımların bir bütünü olarak karşımıza çıkmakta ve örgüt üyelerinin bilgi güvenliği algısını şekillendirmektedir. Nitekim bu tez çalışmasında da Pearson korelasyon analizi sonuçlarına göre, Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profilinde yer alan örgüt kültürü türleri hiyerarşi, pazar, klan ve adhokrasi ile akademik personelin bilgi güvenliği, gizlilik, bütünlük, erişilebilirlik ve sorumluluk algıları arasında istatistiki olarak $p<0,01$ anlamlılık düzeyinde, pozitif doğrusal bir ilişkinin var olduğu ve korelasyon katsayılarının 0,450 ile 0,622 arasında değerler aldığı görülmüştür. Bununla birlikte çoklu doğrusal regresyon analizi sonuçlarına göre de örgüt kültürünün akademik personelin bilgi güvenliği, gizlilik, bütünlük, erişilebilirlik ve sorumluluk algıları üzerine olan etkisini sorgulayan hipotezlerin tamamı kabul edilmiştir. Bu bağlamda bilgi güvenliği prensipleri algıları boyutlarından oluşan ana bağımlı değişken bilgi güvenliği algısının örgüt kültürü türleri ile $p<0,01$ anlamlılık düzeyinde istatistiki olarak tahmin edilmesinin mümkün olduğu ve bilgi güvenliği algısına ilişkin toplam varyansın %42,6'sının örgüt kültürü türleri ile açıklanabildiği sonucuna ulaşılmıştır. Buna göre, bilgi güvenliği algısı üzerinde önem sırasıyla hiyerarşi, pazar, klan ve adhokrasi kültürlerinin olumlu yönde etkili olduğu, bu noktada göreli olarak klan kültürünün etkisinin pazar kültürünün etkisine yakın değerde çıktığı görülmüştür. Bilgi güvenliği algısına bilgi güvenliği prensipleri boyutlarında bakıldığında da önem sırasıyla, gizlilik algısı üzerinde hiyerarşi, pazar ve klanın; bütünlük algısı üzerinde hiyerarşi, pazar, klan ve adhokrasinin; erişilebilirlik algısı üzerinde hiyerarşi ve pazarın; sorumluluk algısı üzerinde ise klan, hiyerarşi, adhokrasi ve pazarın olumlu yönde etkili olduğu sonucuna ulaşılmıştır. Burada

dikkat edilmesi gereken husus, klan kültürünün bilgi güvenliği algısı boyutlarından sorumluluk algısı üzerindeki etkisinin, gizlilik, bütünlük ve erişilebilirlik algıları üzerindeki etkisine kıyasla en yüksek düzeyde çıkmış olmasıdır. Nitekim klan kültürünün sorumluluk algısı üzerindeki yüksek etkisinin bir yansıması olarak da ana bağımlı değişken bilgi güvenliği algısı üzerinde klan kültürünün pazar kültürüyle yaklaşık aynı düzeyde etkiye sahip olduğu görülmüştür.

Regresyon analiz sonuçları bir bütün olarak ele alındığında, akademik personelin bilgi güvenliği, gizlilik, bütünlük, erişilebilirlik ve sorumluluk algılarının tümü üzerinde olumlu yönde etkiye sahip olan ortak örgüt kültürü türlerinin, mekanik süreçleri yansıtan hiyerarşi ve pazar olduğu sonucuna ulaşılmıştır. Ayrıca sorumluluk hariç diğer bilgi güvenliği prensipleri algılarının tamamında en etkili örgüt kültürünün de hiyerarşi olduğu görülmüştür. Sorumluluk algısı üzerinde ise öncelikli olarak klan kültürü etkili olmakla birlikte ikinci ve en yakın etkiye sahip örgüt kültürü yine hiyerarşi çıkmıştır. Nitekim uluslararası arenada yaygın olarak kabul gören bilgi sistemleri yönetim yaklaşımları hiyerarşi kültürüne dayanmaktadır (Eloff ve Solms, 2000). Diğer bir ifadeyle hiyerarşi kültüründe istikrara ve kontrol amaçlarına ulaşmada bilgi yönetimi araç olarak kullanılmaktadır (Quinn ve Rohrbaugh, 1983). Benzer bir ifadeyle de hiyerarşi kültürünün hâkim olduğu örgütlerde bilgi yönetimi süreçlerine önem verilmektedir (Denison ve Spreitzer, 1991). Bununla birlikte bilginin korunması süreci, bilgi yönetimi süreçleri içerisinde yer almaktadır (Lee ve Yang, 2000). Dolayısıyla bilginin korunması kapsamında ele alınacak bilgi güvenliğinin, bilgi yönetiminin bir alt süreci olmasından hareketle, hiyerarşi kültürünün bilgi güvenliği algısı ve bilgi güvenliği prensipleri algıları üzerinde olumlu yönde yüksek etkiye sahip olması anlamlı karşılanmıştır.

Chang ve Lin (2007) tarafından yürütülen, Rekabetçi Değerler Modeli'ne göre tanımlanan örgüt kültürü türlerinin, bilgi güvenliği prensiplerinden gizlilik, bütünlük, erişilebilirlik ve sorumluluk boyutlarında değerlendirilen bilgi güvenliği yönetimi üzerine etkisinin incelendiği çalışmada, kontrol odaklı istikrarlılık (hiyerarşi) ve etkinlik (pazar) kültürlerinin bilgi güvenliği yönetimi üzerinde pozitif etkisi olduğu, işbirliği (klan) kültürünün gizlilik üzerinde negatif etkisinin olması dışında esneklik odaklı işbirliği (klan) ve yaratıcılık (adhokrasi) kültürlerinin bilgi güvenliği yönetimi üzerinde herhangi bir etkisinin olmadığı sonucuna ulaşılmıştır. Bu sonuç, tez çalışmamızda elde edilen, bilgi güvenliği, gizlilik, bütünlük, erişilebilirlik ve sorumluluk algılarının tümü üzerinde pozitif

etkiye sahip ortak örgüt kültürü türlerinin hiyerarşi ve pazar olduğu sonucunu destekler niteliktedir.

Örgüt kültürü ile bilgi güvenliği ilişkisini inceleyen tezin 3. Bölüm'ünde sunulmuş diğer çalışmalara bakıldığında, Rekabetçi Değerler Modeli'ne göre tanımlanan örgüt kültürü türleri ile bilgi güvenliği prensiplerinden gizlilik, bütünlük, erişilebilirlik, sorumluluk, kimlik doğrulama, inkâr edilemezlik ve güvenilirlik boyutlarında değerlendirilen bilgi güvenliği yönetimi arasındaki ilişkinin incelendiği bir diğer çalışmada da klan, adhokrasi ve pazar kültürlerinin bilgi güvenliğini pozitif yönde etkilediği, buna karşılık hiyerarşi kültürünün bilgi güvenliğini etkilemediği görülmüştür (Ebrahimi ve Naini, 2012). Ayrıca benzer bir konu olarak örgüt kültürü türlerinin, çalışanların bilgi güvenliği politikası uygulamalarına karşı sergiledikleri davranışları üzerine etkisini araştıran bir başka çalışmada ise klan kültürünün, çalışanların bilgi güvenliği ile alakalı davranışları üzerinde negatif, pazar kültürünün ise pozitif etkiye sahip olduğu, adhokrasi ve hiyerarşi kültürlerinin ise çalışanların davranışları üzerinde pozitif veya negatif manada herhangi bir etkiye sahip olmadığı sonucuna ulaşılmıştır (Shaw, 2012: 102). Sonuç olarak alanyazın taramasında karşılaşılan örgüt kültürü ile bilgi güvenliği ilişkisini inceleyen çalışmalarda ve bu tez çalışmasında elde edilen bulgular bir bütün olarak değerlendirildiğinde, Rekabetçi Değerler Modeli boyutlarındaki örgüt kültürü türlerinin, bilgi güvenliği prensipleri temelinde bilgi güvenliği algısı, bilgi güvenliği yönetimi ve bilgi güvenliği politikası uygulamalarındaki çalışanların davranışları üzerinde etkiye sahip olduğu görülmektedir.

Öneriler

Bilgiden üst düzey katma değer elde edebilmek için, öncelikle örgütlerin, tüm iş süreçlerinde bilgi yönetimi uygulamalarından maksimum ölçüde yararlanıyor olması gerekmektedir. Bilgi yönetiminin tüm alt süreçlerinde olması gereken en önemli unsuru ise bilginin korunmasıdır. Bilgiye dayalı elde edilmiş olan rekabet avantajının yitirilmemesi için, bilgi güvenliği sağlanmalı ve bu kapsamda teknik düzeyde yönetimsel faaliyetlerin ele alınmasının yanı sıra, bilgi güvenliğinin en zayıf halkası olan insan profilinin bilgi güvenliği perspektifinde algısı geliştirilmelidir. Teknolojik gelişmelerin hızla yaşandığı günümüzde bilgiye bağımlı örgütlerin çevreden etkilenmemesi mümkün değildir. Çevreye ayak uydurma gereksinimi tabiî olarak örgütlerde dün var olan varsayımları ve inançları

geçersiz kılmaktadır. Bilgi güvenliği uygulama alanlarında da benzeri durum yaşanmaktadır. Bilgi güvenliğinin etkin bir şekilde sağlanabilmesi için, yeni tip saldırılarla mücadelenin sağlanabilmesi gerekmektedir. Bu bağlamda yeni güvenlik metodolojilerine uyumluluğun sağlanması adına çalışanlar bilgi güvenliği ile alakalı yeni varsayımlara ve inançlara hızla uyum göstermeli, çalışanların davranışları ve algıları bilgi güvenliği ile uyumlu hâle getirilmelidir.

Örgütlerde bilgi güvenliği riskini azaltmak için, bilgi güvenliği prensipleri temelinde alınan teknolojik önlemlerin yanı sıra bilgi güvenliğinin insan yönü de dikkate alınmalıdır. İstenilen düzeyde bilgi güvenliği seviyesine ulaşılabilmesi için, çalışanlarda güvenlik farkındalığının oluşmasına, güvenlik kontrollerine ve yönetim desteğine gereksinim duyulmaktadır. Bu nedenle örgüt genelinde bilgi güvenliğinin tesis edilmesi için, uluslararası geçerlilikteki standartlar rehberliğinde teknolojik çözümlerle birlikte insan faktörünü de dikkate alan BGYS yapılandırılmalı, bu kapsamda oluşturulacak uygun güvenlik politikaları, prosedürleri ve kontrolleri tüm örgüt birimlerinin ve çalışanlarının katılımıyla uygulanmalıdır. Boss, Kirsch, Angermeier, Shingler ve Boss'a (2009) göre de bilgi güvenliği politikalarının belirlenmesi ve davranışların değerlendirilmesi, bireyleri güvenlik politikalarına uyumun zorunlu olduğuna inandırmada etkili olmaktadır. Zorunluluk algısı, bireyleri güvenlik önlemleri almaya yönlendirmektedir. Bu nedenle bireylerin yönetim tarafından izlenildiklerine inanmaları, davranışların bilgi güvenliği yaptırımlarına uyumunu artıracaktır.

Bilgi güvenliğinin sadece bilgi teknolojileriyle ilgili bölümlerin değil, tüm örgüt birimlerinin sorumluluğunda olduğu bilinci hâkim olmalıdır. Çünkü bilgi güvenliği uygulamalarında başarının elde edilmesi, çalışanların tamamında bilgi güvenliğinin gerekliliği algısının oluşturulmasına bağlıdır. Ayrıca üst yönetim desteği ve çalışma arkadaşları ile sosyalleşme, çalışanların bilgi güvenliği algısını doğrudan etkilemektedir. Bilgi güvenliği algısı açısından, öğrenilen davranışların bütünü olan örgüt kültürünün norm, değer ve inançları örgüt içerisinde yaygın bir şekilde paylaşılıyor ve düzenli olarak verilecek farkındalık eğitimleri ile güvenliğin kritikliği hususunda çalışanlarda algı oluşturuluyor olmalıdır.

Örgüt kültürünün temelinde yatan varsayımların algılama sürecini etkilediği sonucundan hareketle, davranışların temelinde yatan bilgi güvenliği algısının şekillendirilmesinde örgüt

kültürü bir araç olarak kullanılmalıdır. Cameron ve Freeman Örgüt Kültürü Türleri Modeli'ne göre örgütlerde genellikle bir örgüt kültürü türü baskın olmakla birlikte, diğer örgüt kültürü türlerinin de çalışanların davranışları üzerinde, baskın örgüt kültürü türüne nazaran az da olsa etkisi olmaktadır. Bu durum, örgüt kültürünün bilgi güvenliği algısı üzerindeki etkisi için de geçerlidir. Çünkü farklı örgüt kültürü türlerinin farklı bilgi güvenliği prensipleri algıları üzerindeki etki düzeyleri de farklı olmaktadır. Bilgi güvenliği algısı, bilgi güvenliği prensipleri temelinde şekillenmektedir. Bilgi güvenliği prensiplerinden gizlilik, bütünlük ve erişilebilirlik bir denge içerisindedir. Gizlilik ve bütünlüğü artırmak adına atılacak adımlar, erişilebilirliğin belirli sınırlamalar altında tutulmasını sağlayacaktır. Bunun tam tersi olarak erişilebilirliği artırmak da gizlilik ve bütünlükten ödün vermek anlamına gelecektir. Bu prensipler arasında nasıl bir dengenin kurulacağı örgüt misyonuna göre değişecektir. Nasıl ki sır niteliği taşıyan bilgileri bulunduran örgütlerde gizlilik ve bütünlük prensipleri, erişilebilirlik prensibine göre daha önemli olabilecekken, gizlilik değeri taşımayan kamuya açık bilgileri sunan örgütlerde de erişilebilirlik daha önem verilen bir bilgi güvenliği prensibi olacaktır. Bu bağlamda çalışanlarda örgüt stratejisi ve misyonuyla uyumlu bilgi güvenliği algısının geliştirilmesinde, farklı örgüt kültürü türlerinin özellikleri önem sırasıyla bir bütün olarak dikkate alınmalıdır.

Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profilinin baskın olarak mekanik süreçleri yansıtan hiyerarşi ve pazar kültürlerinden oluşması ve bu iki örgüt kültürü türünün, gizlilik, bütünlük ve erişilebilirlik algısı üzerinde en yüksek etki düzeylerine sahip olması ışığında, öncelikle hiyerarşi ve pazar kültür özellikleri üzerinden akademik personelin gizlilik, bütünlük ve erişilebilirlik algılarında istenilen denge elde edilebilir. Bununla birlikte hiyerarşi ve pazar kültürlerinin yanı sıra az da olsa gizlilik algısı üzerinde klan kültürünün, bütünlük algısı üzerinde de klan ve adhokrasi kültürlerinin etkisi dikkate alınmalıdır.

Gizlilik, bütünlük ve erişilebilirliğin yanı sıra bilgi güvenliğinde sorumluluk prensibi ayrı bir önem taşımaktadır. Sorumluluk prensibi ile kullanıcıların bilgi kaynaklarına erişimleri sırasında sergileyecekleri davranışların bilgi güvenliği politika ve prosedürleri ölçüsünde kontrol altına alınması sağlanmakta, kullanıcılar bilgi sistemleri üzerinde yürüttükleri faaliyetlerinin takip edildiğini ve faaliyetlerinden dolayı sorumlu tutulabileceklerini bilmektedirler. Bu tez çalışmasının sonuçları çerçevesinde, Türkiye'de devlet

üniversitelerindeki akademik personelin sorumluluk algısının diğer bilgi güvenliği prensipleri algılarına nazaran düşük çıktığı görülmüştür. Bu sonuçtan hareketle, üniversitelerde bilgi güvenliği hakkında eğitimlerin verilme sıklığı artırılmalı, bilgi güvenliği ile alakalı hatırlatıcı uyarılar görünür yerlerde bulundurulmalı, bilgi güvenliği yönetim yapısı rol ve sorumluluklarla uyumlu bir şekilde kurulmalı ve bilgi güvenliği kontrolleriyle alakalı oluşturulacak bilgi güvenliği protokolleri takip edilmelidir. Bununla birlikte sorumluluk algısı üzerinde, önem sırasıyla klan, hiyerarşi, adhokrasi ve pazar kültürlerinin olumlu yönde etkiye sahip olduğu görülmüş; içsel devamlılık üzerine kurulu olan klan ve hiyerarşi kültürlerinin etki düzeyleri, dışsal konumlama üzerine kurulu olan adhokrasi ve pazar kültürlerine göre oldukça yüksek çıkmıştır. Bu sonuç, insan faktörünün sorumluluk algısı üzerinde diğer bilgi güvenliği prensipleri algılarındakine kıyasla daha fazla etkili olduğunu göstermektedir. İnsan faktörünün örgüt içi bilgi güvenliği yaptırımlarına uyumunun sorumluluk çatısını oluşturduğu, bu manada bilgi sorumluluğunun ölçülebilir bir insan faktörü olduğu, Cameron ve Freeman Örgüt Kültürü Türleri Modeli'nin içsel devamlılık boyutunda da örgütteki bireylere odaklanıldığı düşünüldüğünde, içsel devamlılık üzerine kurulu olan klan ve hiyerarşi kültürlerinin sorumluluk algısı üzerinde en yüksek etkiye sahip olması anlamlı karşılanmıştır. Dolayısıyla akademik personelin sorumluluk algısının artırılmasında, öncelikle içsel devamlılık üzerine kurulu olan klan ve hiyerarşi kültür özelliklerinin yaygınlaştırılması daha etkili olacaktır. Bunun yanı sıra sorumluluk algısı üzerinde, az da olsa var olan adhokrasi ve pazar kültürlerinin etkisi göz ardı edilmemelidir.

Türkiye'de devlet üniversitelerindeki akademik personelin bilgi güvenliği algısı, bilgi güvenliği prensiplerinden gizlilik, bütünlük, erişilebilirlik ve sorumluluk boyutlarında değerlendirilmiştir. Bu çalışmanın devamı olarak gizlilik, bütünlük, erişilebilirlik ve sorumluluk haricinde kimlik doğrulama, inkâr edilemezlik ve güvenilirlik gibi diğer bilgi güvenliği prensipleri boyutları da araştırmalara dâhil edilerek, bilgi güvenliği algısının ölçümlenmesinde bakış açısı genişletilebilir.

Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profilinin tanımlanmasında araştırmanın evreni olarak akademik personel seçilmiştir. Bununla birlikte üniversitelerde akademik personelin yanı sıra idari personel de çalışmaktadır. Nitekim Mintzberg'e (1980) göre de profesyonel bürokrasi yapısındaki devlet okullarında operasyonel manada profesyonel olarak işi yürüten yüksek eğitimli kişilerin büro ve bakım desteğini sağlamak

adına çok sayıda destek personeli istihdam edilmektedir. Bu bağlamda gelecekte yürütülecek çalışmalarda, akademik personel dışında üniversitelerde görev yapan idari personel de araştırma evrenine dâhil edilerek, akademik ve idari personelin kültürel özellikleri değerlendirme farklılıkları ele alınabilir ve Türkiye'deki devlet üniversitelerinin çalışanlar nezdinde genel örgüt kültürü profilinin tanımlanmasında daha bütüncül bir bakış açısı kazandırılabilir. Ayrıca örgüt kültürünün üniversitelerde çalışan personelin dışında üniversitelerin hizmet sunmakta olduğu öğrencilerin de algı ve davranışlarını etkilemesinden dolayı Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profilinin ölçümlenmesinde öğrencilerin değerlendirmelerinden de yararlanılabilir.

Cameron ve Freeman Örgüt Kültürü Türleri Modeli'ne göre Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profilinin mevcut görünümüne OCAI ölçeği uygulanarak ulaşılmıştır. OCAI ölçeği, aynı zamanda çalışanların gelecekte arzuladıkları örgüt kültürünü de ölçümleyebilmekte ve böylelikle mevcut ve arzulanan örgüt kültürü profillerinin karşılaştırılması olanağını sunmaktadır. Mevcut ile arzulanan örgüt kültürü profilleri arasındaki tutarsızlık alanlarının gözlemlenmesi ile kültürel değişim için bir yol haritası belirlenebilir (Cameron ve Quinn, 2006: 23-24, 71-72). Bu bağlamda çalışmanın devamı olarak Türkiye'de devlet üniversitelerindeki akademik personelin, gelecekte üniversitelerde olmasını istedikleri örgüt kültürü ölçümlenebilir ve elde edilecek arzulanan örgüt kültürü profili ile bu tez çalışmasında elde edilen mevcut örgüt kültürü profilinin karşılaştırması yapılarak üniversiteler genelinde kültürel özelliklerde izlenecek değişim adımları değerlendirilebilir.

Bu tez çalışmasında elde edilen bulgular, Türkiye'deki devlet üniversitelerinin genel örgüt kültürü profilinin tanımlanması, akademik personelin bilgi güvenliği prensipleri temelinde algı düzeylerinin ortaya konması ve örgüt kültürünün bilgi güvenliği algısı üzerindeki etkisinin tespit edilmesi açısından anlamlıdır. Bu sonuçların, araştırmanın evrenini temsil eden devlet üniversitelerinin yanı sıra diğer örgüt türleri için de anlam ifade edeceği öngörülmektedir. Gelecekte, Türkiye'deki devlet üniversiteleri hariç diğer örgüt türlerinde örgüt kültürünün bilgi güvenliği algısı üzerindeki etkisini konu alan araştırmalar yürütülerek konuya farklı sonuç setleri ışığında değerlendirmeler getirilebilir. Bu bağlamda örgüt kültürü profilinin, çalışanların bilgi güvenliği algısının ve örgüt kültürü türlerinin bilgi güvenliği algısını etkileme düzeylerinin, örgütlerin uzun dönemli bilgi güvenliği stratejileri doğrultusunda kültür türleri özelliklerinden hareketle bilgi güvenliği prensipleri

temelinde çalışanlarda örgüt misyonuyla uyumlu, istenilen düzeyde bilgi güvenliği algısının oluşturulmasına ve teknolojik çözümlerin yanı sıra insan faktörünü de dikkate alan bilgi güvenliği yönetiminin sağlanmasına katkı sağlayacağı değerlendirilmektedir.

KAYNAKLAR

Açıkgöz, B. (2006). *Rekabetçi Değerler Yaklaşımı Açısından Yöneticilerin Örgüt Kültürüne İlişkin Algılamaları: Zonguldak Karaelmas Üniversitesi Örneği*. Yayımlanmamış Yüksek Lisans Tezi, Zonguldak Karaelmas Üniversitesi Sosyal Bilimleri Enstitüsü, Zonguldak.

Ahlan, A. R., Lubis, M. and Lubis, A. R. (2015). Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science*, 72, 361-373.

Ahmadi, S. A. A., Salamzadeh, Y., Daraei, M. and Akbari, J. (2012). Relationship between Organizational Culture and Strategy Implementation: Typologies and Dimensions. *Global Business and Management Research: An International Journal*, 4(3-4), 286-299.

Aktaş, H. ve Şimşek, E. (2014). Örgütsel Sessizlik ile Algılanan Bireysel Performans, Örgüt Kültürü ve Demografik Değişkenler Arasındaki Etkileşim. *Akdeniz Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 14(28), 24-52.

Albayrak, A. S. (2005). Çoklu Doğrusal Bağlantı Halinde Enküçük Kareler Tekniğinin Alternatifi Yanlı Tahmin Teknikleri ve Bir Uygulama. *Zonguldak Karaelmas Üniversitesi Sosyal Bilimler Dergisi*, 1(1), 105-126.

Albrechtsen, E. and Hovden, J. (2010). Improving Information Security Awareness and Behaviour through Dialogue, Participation and Collective Reflection. An Intervention Study. *Computers & Security*, 29(4), 432-445.

Alfawaz, S., Nelson, K. and Mohannak, K. (2010). Information Security Culture: A Behaviour Compliance Conceptual Framework. *Conferences in Research and Practice in Information Technology Series*, 105, 47-55.

Alhogail, A. (2015). Design and Validation of Information Security Culture Framework. *Computers in Human Behavior*, 49, 567-575.

Alhogail, A. and Mirza, A. (2014a). Information Security Culture: A Definition and a Literature Review. *IEEE Conference Publications, 2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, 1-7.

Alhogail, A. and Mirza, A. (2014b). A Framework of Information Security Culture Change. *Journal of Theoretical and Applied Information Technology*, 64(2), 540-549.

Al-Izki, F. and Weir, G. R. S. (2016). Management Attitudes toward Information Security in Omani Public Sector Organisations. *IEEE Conference Publications, 2016 Cybersecurity and Cyberforensics Conference (CCC)*, 107-112.

Andriole, K. P. (2014). Security of Electronic Medical Information and Patient Privacy: What You Need to Know. *Journal of the American College of Radiology*, 11(12), 1212-1216.

Ashraf, G., Kadir, S. A., Pihie, Z. A. L. and Rashid, A. M. (2013). Relationship between Organizational Culture and Organizational Innovativeness in Private Universities in Iran. *World Applied Sciences Journal*, 22(6), 882-885.

Aydın, H. ve İnce, F. (2005). Bilgi Güvenliği ve Özcük Fonksiyonları Uygulamaları. *Havacılık ve Uzay Teknolojileri Dergisi*, 2(1), 65-70.

Aydıntan, B. (2009). *Örgüt Zekâsı ve Yönetimi Kavramlar - Modeller - Uygulama*. Ankara: Gazi Kitabevi, 130.

Aydıntan, B. ve Göksel, A. (2012). Cameron-Freeman-Quinn Örgüt Kültürü Tipolojileri Ekseninde Örgüt Kültürü Farklılaşma Dinamikleri. *Niğde Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 5(2), 53-62.

Baker, E. L. (1980). Managing Organizational Culture. *McKinsey Quarterly*, Autumn 1980 (4), 51-61.

Balogh, A., Gaal, Z. and Szabo, L. (2011). Relationship between Organizational Culture and Cultural Intelligence. *Management & Marketing Challenges for the Knowledge Society*, 6(1), 95-110.

Beytekin, O. F., Yalçınkaya, M., Doğan, M. and Karakoç, N. (2010). The Organizational Culture at the University (Öğretmenlerin Profesyonel Öğrenmesini Etkileyen Faktörlerin İncelenmesi). *The International Journal of Educational Researchers*, 2(1), 1-13.

Bishop, M. (2003). What is Computer Security?. *IEEE Journals & Magazines*, 1(1), 67-69.

Boggs, W. B. and Fields, D. L. (2010). Exploring Organizational Culture and Performance of Christian Churches. *International Journal of Organization Theory and Behaviour*, 13(3), 305-334.

Borglund, E. A. M. (2008). Electronic Records Use Changes through Temporal Structures and Rhythms. *Archives & Social Studies: A Journal of Interdisciplinary Research*, 2(1), 103-134.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A. and Boss, R. W. (2009). If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security. *European Journal of Information Systems*, 18(2), 151-164.

British Standard. (1999). *BS 7799-1:1999 Information Security Management - Part1: Code of Practice for Information Security Management*. London: British Standards Institution, 1.

Büyüköztürk, Ş. (2015). *Sosyal Bilimler için Veri Analizi El Kitabı*. Ankara: Pegem Akademi, 32, 91, 99, 100.

Cameron, K. S. and Freeman, S. J. (1991). Cultural Congruence, Strength, and Type: Relationships to Effectiveness. *Research in Organizational Change and Development*, 5, 23-58.

Cameron, K. S. and Quinn, R. E. (2006). *Diagnosing and Changing Organizational Culture*. (Revised Edition). San Francisco: Jossey-Bass, 17, 23-29, 34-35, 38-45, 53-57, 63-65, 71-72, 148, 151.

Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi*, 9(3), 165-174.

Carblanc, A. and Moers, S. (2003). Towards a Culture of Online Security. *OECD Observer*, 240/241, 30-31.

Cavallari, M. (2011). The Organizational Relationship between Compliance and Information Security. *International Journal of the Academic Business World*, 5(2), 63-76.

Chan, A. (1997). Corporate Culture of a Clan Organization. *Management Decision*, 35(2), 94-99.

Chan, M., Woon, I. and Kankanhalli, A. (2005). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy & Security*, 1(3), 18-41.

Chang, S. E. and Lin, C. S. (2007). Exploring Organizational Culture for Information Security Management. *Industrial Management & Data Systems*, 107(3), 438-458.

Chiu, R. K. and Chen, J. C. H. (2005). A Generic Service Model for Secure Data Interchange. *Industrial Management & Data Systems*, 105(5), 662-681.

Chou, D. C., Yen, D. C., Lin, B. and Cheng, P. H. L. (1999). Cyberspace Security Management. *Industrial Management & Data Systems*, 99(8), 353-361.

Clinch, J. (2009). ITIL V3 and Information Security. *Clinch Consulting, White Paper*, 1-40.

Coenders, G. and Saez, M. (2000). Collinearity, Heteroscedasticity and Outlier Diagnostics in Regression. Do They Always Offer What They Claim?. *Metodoloski Zvezki*, 16, 79-94.

Corriss, L. (2010). Information Security Governance: Integrating Security into the Organizational Culture. *GTIP'10 Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies*, 35-41.

Çağlayan, S., Korkmaz, M. ve Öktem, G. (2014). Sanatta Görsel Algının Literatür Açısından Değerlendirilmesi. *Eğitim ve Öğretim Araştırmaları Dergisi*, 3(1), 160-173.

Çakar, N. D., Yıldız, S. ve Dur, S. (2010). Bilgi Yönetimi ve Örgütsel Etkinlik İlişkisi: Örgüt Kültürü ve Örgüt Yapısının Temel Etkileri. *Ege Akademik Bakış*, 10(1), 71-93.

Dadgar, H., Marzooghi, R., Torkzadeh, J., Mohammadi, M. and Barahouei, F. (2013). A Comparative Evaluation of the Perception of Lecturers, Employees and Students about the Organizational Culture of Shiraz University. *Life Science Journal*, 10(1), 441-448.

Daft, R. L. (2010). *Organization Theory and Design*. (Tenth Edition). Ohio: South-Western Cengage Learning, 374-375, 387.

Dahbur, K., Bashabsheh, Z. and Bashabsheh, D. (2017). Assessment of Security Awareness: A Qualitative and Quantitative Study. *International Management Review*, 13(1), 37-58.

Daud, Y., Raman, A., Don, Y., Sofian M. O. F. and Hussin, F. (2015). The Type of Culture at a High Performance Schools and Low Performance School in the State of Kedah. *International Education Studies*, 8(2), 21-31.

Davenport, T. H., Long, D. W. and Beers, M. C. (1998). Successful Knowledge Management Projects. *Sloan Management Review*, 39(2), 43-57.

Denison, D. R. (1984). Bringing Corporate Culture to the Bottom Line. *Organizational Dynamics*, 13(2), 5-22.

Denison, D. R. (1996). What is the Difference between Organizational Culture and Organizational Climate? A Native's Point of View on a Decade of Paradigm Wars. *Academy of Management Review*, 21(3), 619-654.

Denison, D. R., Haaland, S. and Goelzer, P. (2004). Corporate Culture and Organizational Effectiveness: Is Asia Different from the Rest of the World?. *Organizational Dynamics*, 33(1), 98-109.

Denison, D. R. and Spreitzer, G. M. (1991). Organizational Culture and Organizational Development: A Competing Values Approach. *Organizational Change and Development*, 5, 1-21.

Deshpande, R., Farley, J. U. and Webster, F. E. (1993). Corporate Culture, Customer Orientation, and Innovativeness in Japanese Firms: A Quadrad Analysis. *Journal of Marketing*, 57(1), 23-37.

Deshpande, R. and Webster, F. E. (1989). Organizational Culture and Marketing: Defining the Research Agenda. *The Journal of Marketing*, 53(1), 3-15.

Dhillon, G. and Backhouse, J. (2000). Information System Security Management in the New Millennium. *Communications of the ACM*, 43(7), 125-128.

Doğan, B. (2012). *Örgüt Kültürü.* (Birinci Baskıdan Tıpkı İkinci Basım). İstanbul: Beta Basım Yayın, 9, 13, 109, 114, 129.

Duncan, W. C. (1989). Organizational Culture: "Getting a Fix" on an Elusive Concept. *The Academy of Management Executive*, 3(3), 229-236.

Durmuş, B., Yurtkoru, E. S. ve Çinko, M. (2013). *Sosyal Bilimlerde SPSS'le Veri Analizi.* (Beşinci Baskı). İstanbul: Beta Basım Yayın, 143-144, 154, 157, 159, 164.

D'Arcy, J. and Greene, G. (2014). Security Culture and the Employment Relationship as Drivers of Employees' Security Compliance. *Information Management & Computer Security*, 22(5), 474-489.

Ebrahimi, A. P. and Naini, P. F. (2012). Exploring the Type of Relationship between Information Security Management and Organizational Culture (Case Study in TAM Iran Khodro Co.). *International Journal of Information, Security and Systems Management*, 1(1), 21-28.

Eloff, M. M. and Solms, S. H. (2000). Information Security Management: A Hierarchical Framework for Various Approaches. *Computers & Security*, 19(3), 243-256.

Erdem, R. (2007). Örgüt Kültürü Tipleri ile Örgütsel Bağlılık Arasındaki İlişki: Elazığ İl Merkezindeki Hastaneler Üzerinde Bir Çalışma. *Eskişehir Osmangazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 2(2), 63-79.

Erdem, R., Adıgüzel, O. ve Kaya, A. (2010). Akademik Personelin Kurumlarına İlişkin Algıladıkları ve Tercih Ettikleri Örgüt Kültürü Tipleri. *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 36, 73-88.

Erkmen, T. (2010). *Örgüt Kültürü İşletmelerin Başarısındaki En Temel Paradigma.* (Birinci Baskı). İstanbul: Beta Basım Yayın, 3, 9, 11, 15, 16, 21, 23, 27, 41, 133.

Ersoy, E. V. (2012). *ISO/IEC 27001 Bilgi Güvenliği Standardı Tanımlar ve Örnek Uygulamalar*. (Birinci Baskı). Ankara: ODTÜ Yayıncılık, 11-14.

Fatima, M. (2016). The Impact of Organizational Culture Types on the Job Satisfaction of Employees. *Sukkur IBA Journal of Management and Business*, 3(1), 13-32.

Field, A. (2009). *Discovering Statistics Using Spss*. (Third Edition). London: SAGE Publications, 233, 660, 675.

Fralinger, B. and Olson, V. (2007). Organizational Culture at the University Level: A Study Using the OCAI Instrument. *Journal of College Teaching & Learning*, 4(11), 85-97.

Fulford, H. and Doherty, N. F. (2003). The Application of Information Security Policies in Large UK-Based Organizations: An Exploratory Investigation. *Information Management & Computer Security*, 11(3), 106-114.

Furnell, S. and Thomson, K. L. (2009). From Culture to Disobedience: Recognising the Varying User Acceptance of IT Security. *Computer Fraud and Security*, 2, 5-10.

Furnell, S. M., Jusoh, A. and Katsabas, D. (2006). The Challenges of Understanding and Using Security: A Survey of End-Users. *Computers & Security*, 25(1), 27-35.

Fussell, R. S. (2005). Protecting Information Security Availability via Self-Adapting Intelligent Agents. *IEEE Conference Publications, 2005 IEEE Military Communications Conference*, 5, 2977-2982.

Gajanayake, R., Sahama, T. and Lane, B. (2013). The Role of Human Factors When Evaluating Information Accountability for eHealth Systems. *Studies in Health Technology and Informatics (Stud Health Technol Inform)*, 194, 97-102.

Garcia, L. E., Sanchez, M. G., Cuevas, H., Hernandez, R. and Vargas, B. E. (2012). Organizational Culture Diagnostic in Two Mexican Technological Universities Case Study. *Innovacion Y Desarrollo Tecnologico*, 4(4), 77-94.

Gaunt, N. (2000). Practical Approaches to Creating a Security Culture. *International Journal of Medical Informatics*, 60(2), 151-157.

Goffee, R. and Jones, G. (1996). What Holds the Modern Company Together?. *Harvard Business Review*, 74(6), 133-148.

Gökçen, H. (2011). *Yönetim Bilgi / Bilişim Sistemleri: Analiz ve Tasarım*. (İkinci Baskı). Ankara: Afşar Matbaacılık, 20.

Grzebiela, T. (2002). Insurability of Electronic Commerce Risks. *IEEE Conference Publications, Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, 1-9.

Gull, S. and Azam, F. (2012). Impact of Organizational Culture Type on Job Satisfaction Level of Employees' in Different Organizations of Lahore, Pakistan. *International Journal of Academic Research in Business and Social Sciences*, 2(12), 97-112.

Guttman, B. and Roback, E. (1995). *An Introduction to Computer Security: The NIST Handbook*. NIST Publication 800-12. Maryland: National Institute of Standards and Technology (NIST), 5, 144.

Gülnar, B. (2009). İletişim Doyumu Boyutları ile Örgütlenme Yapısı İlişkisi: Selçuk Üniversitesi Akademisyenleri Örneği. *Selçuk İletişim*, 5(4), 62-82.

Hande, S. A. and Mane, S. B. (2015). An Analysis on Data Accountability and Security in Cloud. *IEEE Conference Publications, 2015 International Conference on Industrial Instrumentation and Control (ICIC)*, 713-717.

Harris, L. C. (1998). Cultural Domination: The Key to Market-Oriented Culture?. *European Journal of Marketing*, 32(3/4), 354-373.

Harris, S. (2013). *All-In-One CISSP Exam Guide*. (Sixth Edition). New York: McGraw-Hill, 22, 24, 159, 160, 298, 888.

Harris, S. G. (1989). A Schema-Based Perspective on Organizational Culture. *Academy of Management Best Papers Proceedings*, 178-182.

Harris, T. E. (1984). Organizational Cultures and the Role of Professional Communication. *Professional Communication in the Modern World: Proceedings of the American Business Communication Association Southeast Convention*, (31st, Hammond, LA), 125-138.

Hauke, J. and Kossowski, T. (2011). Comparison of Values of Pearson's and Spearman's Correlation Coefficients on the Same Sets of Data. *Quaestiones Geographicae*, 30(2), 87-93.

Higgins, H. N. (1999). Corporate System Security: Towards an Integrated Management Approach. *Information Management & Computer Security*, 7(5), 217-222.

Hofstede, G. (1981). Culture and Organizations. *International Studies of Management & Organization*, 10(4), 15-41.

Homburg, C. and Pflesser, C. (2000). A Multiple-Layer Model of Market-Oriented Organizational Culture: Measurement Issues and Performance Outcomes. *Journal of Marketing Research*, 37(4), 449-462.

Humphreys, E. (2011). Information Security Management System Standards. *Datenschutz und Datensicherheit - DuD*, 35(1), 7-11.

Information Systems Audit and Control Association. (2006). *Certified Information Systems Auditor (CISA)*. Illinois: Information Systems Audit and Control Association, 406.

International Standard. (2012). *ISO/IEC 27032:2012 Information Technology - Security Techniques - Guidelines for Cybersecurity*. Switzerland: International Organization for Standardization, vi.

Internet Crime Complaint Center. (2015). *2015 Internet Crime Report*. U. S. Department of Justice FBI: Internet Crime Complaint Center, 4, 12.

Istikoma, Fakhri, N. F., Ain, Q. and Ibrahim, J. (2015). Information Security Aligned to Enterprise Management. *Middle East Journal of Business*, 10(1), 62-66.

İnternet: Internet World Stats. Web: http://www.internetworldstats.com/stats.htm 4 Haziran 2017'de alınmıştır.

İnternet: Jeeshim and Kucc. (2002). Multicollinearity in Regression Models. *Multicollinearity.doc*, 625, (2003-05-09). Web: http://sites.stat.psu.edu/~ajw13/SpecialTopics/multicollinearity.pdf adresinden 8 Şubat 2017'de alınmıştır.

İnternet: Resmî Gazete. (2004). 5070 Sayılı Elektronik İmza Kanunu, Kabul Tarihi: 15.01.2004. Web: http://www.resmigazete.gov.tr/eskiler/2004/01/20040123.htm#1 14 Şubat 2017'de alınmıştır.

İnternet: Resmî Gazete. (2007a). 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki Kanun, Kabul Tarihi: 04.05.2007. Web: http://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm 14 Şubat 2017'de alınmıştır.

İnternet: Resmî Gazete. (2007b). İnternet Toplu Kullanım Sağlayıcıları Hakkındaki Yönetmelik, Kabul Tarihi: 01.11.2007. Web: http://www.resmigazete.gov.tr/eskiler/2007/11/20071101-4.htm 14 Şubat 2017'de alınmıştır.

İnternet: Türk Dil Kurumu. Web: http://www.tdk.gov.tr/index.php?option=com_gts&view=gts 19 Mart 2017'de alınmıştır.

İnternet: Türk Standardları Enstitüsü. Web: https://intweb.tse.org.tr/Standard/Standard/Standard.aspx?081118051115108051104119110104055047105102120088111043113104073087057070079072074116111055116074 19 Mart 2017'de alınmıştır.

İnternet: Yükseköğretim Kurulu. Web: http://yok.gov.tr/web/guest/_universitelerimiz 21 Nisan 2016'da alınmıştır.

İnternet: Yükseköğretim Kurulu. Web: https://istatistik.yok.gov.tr/ 13 Haziran 2017'de alınmıştır.

Jiang, X. and Fu, Q. (2011). Relationship between Universities Organizational Culture, Teachers' Psychological Empowerment and Organizational Citizenship Behavior. *IEEE Conference Publications, 2011 Fourth International Joint Conference on Computational Sciences and Optimization*, 699-703.

Johnson, G. R. (1983). Society and Culture: Systems Definitions for an Alternative Social Science Paradigm. *Annual Meeting of the American Anthropological Association*, (82nd, Chicago, IL, November 17-20), 1-64.

Jones, D. (2004). Confidentiality and Security of Information. *Intensive Care / Informatics, Anaesthesia and Intensive Care Medicine*, 5(12), 404-406.

Kanday, R. (2012). A Survey on Cloud Computing Security. *IEEE Conference Publications, 2012 International Conference on Computing Sciences*, 302-311.

Kannan, G. and Sivasubramanian, V. (2016). Transforming Risk Culture through Organizational Culture Leveraging COBIT 5 for Risk. *COBIT Focus*, 7/5/2016, 1-7.

Kent, K. and Souppaya, M. (2006). *Guide to Computer Security Log Management, Recommendations of the National Institute of Standards and Technology*. NIST Publication 800-92. Maryland: National Institute of Standards and Technology (NIST), 2.7-2.8.

Kim, E. B. (2013). Information Security Awareness Status of Business College: Undergraduate Students. *Information Security Journal: A Global Perspective*, 22(4), 171-179.

Knapp, K. J. and Ford, F. N. (2006). Information Security: Management's Effect on Culture and Policy. *Information Management & Computer Security*, 14(1), 24-36.

Knapp, K. J., Marshall, T. E., Rainer, R. K. and Morrow, D. W. (2006). The Top Information Security Issues: What Can Government Do to Help?. *Information Systems Security*, 15(4), 51-58.

Knapp, K. J., Morris, R. F., Marshall, T. E. and Byrd, T. A. (2009). Information Security Policy: An Organizational-Level Process Model. *Computers & Security*, 28(7), 493-508.

Koçel, T. (2014). *İşletme Yöneticiliği*. (Genişletilmiş On Beşinci Baskı). İstanbul: Beta Basım Yayın, 162.

Koskosas, I., Kakoulidis, K. and Siomos, C. (2011). Information Security: Corporate Culture and Organizational Commitment. *International Journal of Humanities and Social Science*, 1(3), 192-198.

Kruger, H. A. and Kearney, W. D. (2006). Prototype for Assessing Information Security Awareness. *Computers & Security*, 25(4), 289-296.

Lacey, D. (2010). Understanding and Transforming Organizational Security Culture. *Information Management & Computer Security*, 18(1), 4-13.

Lapina, I., Kairisa, I. and Aramina, D. (2015). Role of Organizational Culture in the Quality Management of University. *Procedia - Social and Behavioral Sciences*, 213(1), 770-774.

Lee, C. C. and Yang, J. (2000). Knowledge Value Chain. *The Journal of Management Development*, 19(9), 783-793.

Lemieux, V. (1998). Applying Mintzberg's Theories on Organizational Configuration to Archival Appraisal. *The Journal of the Association of Canadian Archivists*, 46, 32-85.

Li, L., He, W., Ivan, A., Xu, L., Anwar, M. and Yuan, X. (2014). Does Explicit Information Security Policy Affect Employees' Cyber Security Behavior? A Pilot Study. *IEEE Conference Publications, 2014 Enterprise Systems Conference*, 169-173.

Lim, J. S., Chang, S., Maynard, S. and Ahmad, A. (2009). Exploring the Relationship between Organizational Culture and Information Security Culture. *Proceedings of the 7th Australian Information Security Management Conference*, 88-97.

Lunenburg, F. C. (2011). Understanding Organizational Culture: A Key Leadership Asset. *National Forum of Educational Administration and Supervision Journal*, 29(4), 1-12.

Lunenburg, F. C. (2012). Organizational Structure: Mintzberg's Framework. *International Journal of Scholarly, Academic, Intellectual Diversity*, 14(1), 1-8.

Malyuk, A. and Miloslavskaya, N. (2016). Cybersecurity Culture as an Element of IT Professional Training. *IEEE Conference Publications, 2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC)*, 205-210.

Mataracıoğlu, T. ve Özkan, S. (2011). Governing Information Security in Conjunction with Cobit and ISO 27001. *International Journal of Network Security & Its Applications (IJNSA)*, 3(4), 111-116.

Meijer, A. (2001). Accountability in an Information Age: Opportunities and Risks for Records Management. *Archival Science*, 1(4), 361-372.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C. and Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia - Social and Behavioral Sciences,* 147, 424-428.

Mintzberg, H. (1979). *The Structuring of Organizations.* (Facsimile Edition). New Jersey: Pearson Education, 97, 292.

Mintzberg, H. (1980). Structure in 5's: A Synthesis of the Research on Organization Design. *Management Science*, 26(23), 322-341.

Mintzberg, H., Ahlstrand, B. and Lampel, J. (1998). *Strategy Safari a Guided Tour through the Wilds of Strategic Management*. (First Edition). New York: The Free Press, 264-266.

Murat, G. ve Açıkgöz, B. (2007). Yöneticilerin Örgüt Kültürü Algılamalarına İlişkin Bir Analiz: Zonguldak Karaelmas Üniversitesi Örneği. *Zonguldak Karaelmas Üniversitesi Sosyal Bilimler Dergisi*, 3(5), 1-20.

Nicholson, N., Schuler, R. S. and Ven, A. H. V. (1998). *The Blackwell Encyclopedic Dictionary of Organizational Behavior*. (Revised Edition). Massachusetts: Blackwell Publishers, 376.

Niekerk, J. F. V. and Solms, R. V. (2010). Information Security Culture: A Management Perspective. *Computers & Security*, 29(4), 476-486.

Nonaka, I. (1994). A Dynamic Theory of Organizational Knowledge Creation. *Organization Science*, 5(1), 14-37.

Nunn, N. (2012). Culture and the Historical Process. *Economic History of Developing Regions*, 27(S1), 108-126.

Ocbian, M. M. and Dichoso, M. A. (2015). Empowering Secondary School Teachers through Administrative Tasks. *Asia Pacific Journal of Multidisciplinary Research*, 3(4), 19-27.

Okenyi, P. O. and Owens, T. J. (2007). On the Anatomy of Human Hacking. *Information Systems Security*, 16(6), 302-314.

Onwubiko, C. and Lenaghan, A. P. (2007). Managing Security Threats and Vulnerabilities for Small to Medium Enterprises. *IEEE Conference Publications, 2007 IEEE Intelligence and Security Informatics*, 244-249.

Ouchi, W. G. and Price, R. L. (1993). Hierarchies, Clans, and Theory Z: A New Perspective on Organization Development. *Organizational Dynamics*, 21(4), 62-70.

O'Hagan, K. (1999). Culture, Cultural Identity, and Cultural Sensitivity in Child and Family Social Work. *Family Social Work*, 4(4), 269-281.

O'Reilly, C. A., Chatman, J. and Caldwell, D. F. (1991). People and Organizational Culture: A Profile Comparison Approach to Assessing Person-Organization Fit. *Academy of Management Journal*, 34(3), 487-516.

Önel, D. ve Dinçkan, A. (2007). Bilgi Güvenliği Yönetim Sistemi Kurulumu. *TÜBİTAK UEKAE (Ulusal Elektronik ve Kriptoloji Enstitüsü)*, Doküman Kodu: BGYS-001, Sürüm 1.00, 1-16.

Özdemir, A. A. (2015). Rekabet Eden Değerler Modeliyle Örgüt Kültürü İncelemesi: Kamu Kurumunda Görgül Bir Araştırma. *İş, Güç Endüstri İlişkileri ve İnsan Kaynakları Dergisi*, 17(1), 29-53.

Öztürk, U. C. (2015). Örgüt Kültürü Algısında Cinsiyet Faktörünün Etkisi ve Bir Uygulama. *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, 6(12), 62-86.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies. *Computers & Security*, 66, 40-51.

Parsons, K. M., Young, E., Butavicius, M. A., Mccormac, A., Pattinson, M. R. and Jerram, C. (2015). The Influence of Organizational Information Security Culture on Information Security Decision Making. *Journal of Cognitive Engineering and Decision Making*, 9(2), 117-129.

Pfleeger, C. P., Pfleeger, S. L. and Margulies, J. (2015). *Security in Computing*. (Fifth Edition). Massachusetts: Prentice Hall, 8-12.

Polding, B. E. (2016). Creating an Innovative Culture. *Journal of Leadership Studies*, 10(1), 68-69.

Quinn, R. E. and Rohrbaugh, J. (1981). A Competing Values Approach to Organizational Effectiveness. *Public Productivity Review*, 5(2), 122-140.

Quinn, R. E. and Rohrbaugh, J. (1983). A Spatial Model of Effectiveness Criteria: Towards a Competing Values Approach to Organizational Analysis. *Management Science*, 29(3), 363-377.

Quinn, R. E. and Spreitzer, G. M. (1991). The Psychometrics of the Competing Values Culture Instrument and an Analysis of the Impact of Organizational Culture on Quality of Life. *Research in Organizational Change and Development*, 5, 115-142.

Rathje, S. (2009). The Definition of Culture: An Application-Oriented Overhaul. *Interculture Journal*, 8, 35-58.

Reid, R. and Niekerk, J. V. (2014). From Information Security to Cyber Security Cultures. *IEEE Conference Publications, 2014 Information Security for South Africa*, 1-7.

Ryan, S. D. and Bordoloi, B. (1997). Evaluating Security Threats in Mainframe and Client/Server Environments. *Information & Management*, 32, 137-146.

Safa, N. S., Solms, R. V. and Futcher, L. (2016). Human Aspects of Information Security in Organisations. *Computer Fraud & Security*, 2, 15-18.

Safa, N. S., Sookhak, M., Solms, R. V., Furnell, S., Ghani, N. A. and Herawan, T. (2015). Information Security Conscious Care Behaviour Formation in Organizations. *Computers & Security*, 53, 65-78.

Saikia, B. and Singh, R. (2014). A Comparative Study on Countermeasures for Handling Multicollinearity in Regression Analysis. *Asian-African Journal of Economics and Econometrics*, 14(2), 163-174.

Sayles, L. R. and Wright, R. V. L. (1985). The Use of Culture in Strategic Management. *Issues and Observations*, 5(4), 63-78.

Schein, E. H. (1984). Coming to a New Awareness of Organizational Culture. *Sloan Management Review*, 25(2), 3-16.

Schein, E. H. (1990). Organizational Culture. *American Psychologist*, 45(2), 109-119.

Schein, E. H. (1996). Culture: The Missing Concept in Organization Studies. *Administrative Science Quarterly*, 41(2), 229-240.

Schein, E. H. (2009). *The Corporate Culture Survival Guide*. (New and Revised Edition). San Francisco: Jossey-Bass, 27-28.

Schwartz, H. and Davis, S. M. (1981). Matching Corporate Culture and Business Strategy. *Organizational Dynamics*, 10, 30-48.

Scott, T., Mannion, R., Davies, H. and Marshall, M. (2003). The Quantitative Measurement of Organizational Culture in Health Care: A Review of the Available Instruments. *Health Services Research*, 38(3), 923-945.

Shaw, R. M. (2012). *The Influence of Organizational Culture on Employee Attitudes towards Information Security Policy* (Doctoral dissertation, Capella University, 2012). Dissertation Abstracts International, A 73/07 (E), 47-48, 50, 58, 70, 74, 94-95, 102.

Shurbagi, A. M. A. and Zahari, I. B. (2012). The Relationship between Organizational Culture and Job Satisfaction in National Oil Corporation of Libya. *International Journal of Humanities and Applied Sciences (IJHAS)*, 1(3), 88-93.

Skemp, L. E., Dreher, M. C. and Lehmann, S. P. (2016). Discovering the Culture of Your Community. *Reflections on Nursing Leadership*, 42(3), 1-24.

Smircich, L. (1983). Concepts of Culture and Organizational Analysis. *Administrative Science Quarterly*, 28(3), 339-358.

Solms, B. V. and Solms, R. V. (2004). The 10 Deadly Sins of Information Security Management. *Computer & Security*, 23(5), 371-376.

Solms, R. V. and Niekerk, J. V. (2013). From Information Security to Cyber Security. *Computers & Security*, 38, 97-102.

Soomro, Z. A., Shah, M. H. and Ahmed, J. (2016). Information Security Management Needs More Holistic Approach: A Literature Review. *International Journal of Information Management*, 36(2), 215-225.

Stanciu, V. and Tinca, A. (2016). Students' Awareness on Information Security between Own Perception and Reality - An Empirical Study. *Accounting and Management Information Systems*, 15(1), 112-130.

Stanton, J. M., Stam, K. R., Mastrangelo, P. and Jolton, J. (2005). Analysis of End User Security Behaviors. *Computers & Security*, 24(2), 124-133.

Tajuddin, S., Olphert, W. and Doherty, N. (2015). Relationship between Stakeholders' Information Value Perception and Information Security Behaviour. *AIP Conference Proceedings*, 1644(1), 69-77.

Tang, M., Li, M. and Zhang, T. (2016). The Impacts of Organizational Culture on Information Security Culture: A Case Study. *Information Technology and Management*, 17(2), 179-186.

Thomas, D. R. and Dyall, L. (1999). Culture, Ethnicity, and Sport Management: A New Zealand Perspective. *Sport Management Review*, 2(2), 115-132.

Thomson, K. and Niekerk, J. F. V. (2012). Combating Information Security Apathy by Encouraging Prosocial Organisational Behaviour. *Information Management & Computer Security*, 20(1), 39-46.

Thomson, K., Solms R. V. and Louw, L. (2006). Cultivating an Organizational Information Security Culture. *Computer Fraud & Security*, 10, 7-11.

Tonta, Y. (2004, 21-24 Ekim). *Bilgi Yönetiminin Kavramsal Tanımı ve Uygulama Alanları*. Kütüphaneciliğin Destanı Sempozyumunda sunuldu, Ankara.

Topal, M., Eyduran, E. ve Yağanoğlu, A. M. (2010). Çoklu Doğrusal Bağlantı Durumunda Ridge ve Temel Bileşenler Regresyon Analiz Yöntemlerinin Kullanımı. *Atatürk Üniversitesi Ziraat Fakültesi Dergisi*, 41(1), 53-57.

Trcek, D., Trobec, R., Pavesic, N. and Tasic, J. F. (2007). Information Systems Security and Human Behaviour. *Behaviour & Information Technology*, 26(2), 113-118.

Türk Standardı. (2006). *TS ISO/IEC 27001 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler*. Ankara: Türk Standardları Enstitüsü, 4.

Türkiye Bilişim Derneği. (2006). *Bilişim Sistemleri Güvenliği El Kitabı Sürüm 1.0*. Ankara: Türkiye Bilişim Derneği, 3.

Uzun, Ö. ve Tamimi, Y. (2007). Örgüt Kültüründe Güç Mesafesi Boyutunun Metaforlarla Analizi (Tekstil Sektöründe Faaliyet Gösteren Bir İşletme Örneği). *Eskişehir Osmangazi Üniversitesi Sosyal Bilimler Dergisi*, 8(1), 221-246.

Veiga, A. D. (2015). The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study. *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)*, 22-33.

Veiga, A. D. and Eloff, J. H. P. (2007). An Information Security Governance Framework. *Information Systems Management*, 24(4), 361-372.

Veiga, A. D. and Martins, N. (2015). Information Security Culture and Information Protection Culture: A Validated Assessment Instrument. *Computer Law & Security Review*, 31(2), 243-256.

Vroom, C. and Solms, R. V. (2004). Towards Information Security Behavioural Compliance. *Computer & Security*, 23(3), 191-198.

Vupa, Ö. ve Alma, Ö. G. (2008). Doğrusal Regresyon Çözümlemesinde Çoklu Bağlantı Probleminin Sapan Değer İçeren Küçük Örneklemlerde Bir Simülasyon Çalışması ile Saptanması ve Sonuçları. *Selçuk Üniversitesi Fen Fakültesi Fen Dergisi*, 2(32), 41-51.

Vural, Y. ve Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 23(2), 507-522.

Wadia, M. S. (1965). The Concept of Culture. *Journal of Retailing*, 41(1), 21-31.

Wallendorf, M. and Reilly, M. D. (1983). Distinguishing Culture of Origin from Culture of Residence. *Advances in Consumer Research*, 10(1), 699-701.

Woodhouse, S. (2007). Information Security: End User Behavior and Corporate Culture. *IEEE Conference Publications, 7th IEEE International Conference on Computer and Information Technology (CIT 2007)*, 767-774.

Xiao, Y., Meng, K. and Takahashi, D. (2012). Accountability Using Flow-Net: Design, Implementation, and Performance Evaluation. *Security and Communication Networks*, 5(1), 29-49.

Yaşar, H. ve Çakır, H. (2015). Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 3(2), 488-507.

Yazıcı, E. O., Giritli, H., Oraz, G. T. and Acar, E. (2007). Organizational Culture: A Comparative Analysis from the Turkish Construction Industry. *Engineering, Construction and Architectural Management*, 14(6), 519-531.

Yılmaz, M. (2009). Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi. *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, 49(1), 95-118.

EKLER

EK-1. Anket formu

DOKTORA TEZ ÇALIŞMASI ANKET FORMU
Gazi Üniversitesi Bilişim Enstitüsü Yönetim Bilişim Sistemleri (YBS) Anabilim Dalı

Değerli Hocam,

Bu anket, üniversitelerde örgüt kültürünün bilgi güvenliği algısı üzerine etkisini ortaya koymayı amaçlamaktadır. Anket formu üç bölümden oluşmaktadır. İlk bölümde örgüt kültürüne, ikinci bölümde bilgi güvenliğine, üçüncü bölümde ise ankete katılan akademik personelin kişisel ve mesleki niteliklerine ilişkin sorular bulunmaktadır.

Anket formunu doldurmaya zaman ayırdığınız için teşekkür eder, saygılarımı sunarım.

Ertuğrul AKTAN

I. ÜNİVERSİTENİN ÖRGÜT KÜLTÜRÜ

Lütfen 1 - 24. soruları, çalışmakta olduğunuz üniversiteyi dikkate alarak cevaplayınız. (1=Kesinlikle katılmıyorum, 5= Kesinlikle katılıyorum düzeylerini temsil etmekte ve 1'den 5'e doğru puanlamada katılım düzeyi artmaktadır.)

1.	Üniversitede, kişisel ilişkiler iyi seviyededir. Çalışma ortamı geniş bir aile gibidir. Çalışanlar kendilerinden çok şey paylaşmaktadırlar.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
2.	Üniversite, çok dinamik ve girişimci bir yerdir. Çalışanlar, ellerini taşın altına koymaya ve risk almaya isteklidirler.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
3.	Üniversite, sonuç odaklı bir yapıya sahiptir. İşin yapılması vurgusu vardır. Çalışanlar, kurumsal hedeflere ulaşmada rekabetçi ve başarı odaklıdırlar.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
4.	Üniversite, çok kontrollü ve planlı bir yerdir. Genellikle resmî prosedürler, çalışanların ne yapacağına yön vermektedir.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
5.	Üniversiteyi yönetenler, genellikle akıl hocası, yardım edici veya eğitici olarak görülmektedir.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
6.	Üniversiteyi yönetenler, genellikle girişimci, yenilikçi veya risk alan kişiler olarak görülmektedir.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐

EK-1. (devam) Anket formu

7.	Üniversiteyi yönetenler, genellikle rekabetçi, üretken veya sonuç odaklı kişiler olarak görülmektedir.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
8.	Üniversiteyi yönetenler, genellikle işlerin düzenli ve verimli bir şekilde yürütülmesinden sorumlu yöneticiler olarak görülmektedir.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
9.	Üniversitedeki yönetim tarzı; takım çalışması, fikir birliği ve çalışan katılımcılığı ile nitelendirilmektedir.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
10.	Üniversitedeki yönetim tarzı; bireysel risk alma, yeniliği araştırma, çalışanların bağımsızlığı ve bireyselliği ile nitelendirilmektedir.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
11.	Üniversitedeki yönetim tarzı; üniversiteler arası rekabet, akademik talepleri karşılama ve başarıyı elde etme ile nitelendirilmektedir.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
12.	Üniversitedeki yönetim tarzı; iş güvenliği, kural ve düzenlemelere uygunluk, istikrarlı ilişkiler ile nitelendirilmektedir.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
13.	Üniversiteyi bir arada tutan bağ, sadakat ve karşılıklı güvendir. Üniversiteye bağlılık yüksek düzeydedir.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
14.	Üniversiteyi bir arada tutan bağ, yenilik ve araştırma geliştirmeye olan bağlılıktır. Üniversitede, önde gelen yenilikçi bir eğitim kuruluşu olma vurgusu vardır.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
15.	Üniversiteyi bir arada tutan bağ, kurumsal hedefleri gerçekleştirmeye ve başarıyı elde etmeye verilen önemdir.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
16.	Üniversiteyi bir arada tutan bağ, resmî kurallar ve politikalar doğrultusunda kusursuz çalışan bir örgütün devamlılığına verilen önemdir.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
17.	Üniversitede, kişinin gelişimine vurgu vardır. Örgüt içinde yüksek güven, şeffaflık ve katılımcılık süregelmektedir.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐

EK-1. (devam) Anket formu

18.	Üniversitede, yeni kaynaklar elde etme ve zorlu mücadelelere girme vurgusu vardır. Yeni şeyler denemek ve yeni fırsatlar aramak değer ifade etmektedir.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
19.	Üniversitede, kurumsal rekabet ve başarı vurgusu vardır. Kurumsal hedeflere ulaşmak ve eğitim-öğretimde başarılı olmak baskındır.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
20.	Üniversitede, süreklilik ve istikrarlı olma vurgusu vardır. Verimliliğin, kontrolün sağlanması ve faaliyetlerin kusursuz yürütülmesi önemlidir.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
21.	Üniversite başarıyı; insan kaynakları gelişimi, takım çalışması ve çalışanların kurumsal bağlılığı temelinde tanımlamaktadır.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
22.	Üniversite başarıyı; benzersiz, lider ve en yenilikçi üniversiteye sahip olma temelinde tanımlamaktadır.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
23.	Üniversite başarıyı; eğitim-öğretimde kazanma ve diğer üniversitelerden daha başarılı olma temelinde tanımlamaktadır. Rekabetçi liderlik, anahtar kelimedir.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
24.	Üniversite başarıyı; verimlilik temelinde tanımlamaktadır. Güvenilirlik, kusursuz iş planlaması ve kaynakların etkin kullanımı kritik öneme sahiptir.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐

EK-1. (devam) Anket formu

II. ÜNİVERSİTEDEKİ BİLGİ GÜVENLİĞİ

Lütfen 25 - 43. soruları, çalışmakta olduğunuz üniversitedeki bilgi güvenliği uygulamalarını dikkate alarak cevaplayınız. (1=Kesinlikle katılmıyorum, 5= Kesinlikle katılıyorum düzeylerini temsil etmekte ve 1'den 5'e doğru puanlamada katılım düzeyi artmaktadır.)

25.	Üniversitede, kişisel ve işle alakalı önemli bilgilerin korunmasını sağlamak amacıyla güvenlik kontrollerinin (şifreleme sistemleri gibi) uygulandığını düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
26.	Erişim yetkisi olmayan kullanıcıların, üniversite bilgi kaynaklarına erişiminin engellendiğini düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
27.	Çalışanların, bilginin yayınlanmasında ve transferinde üniversite politika ve düzenlemelerine uymak zorunda olduğunu düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
28.	Üniversitede, önemli bilgilerin, kötü niyetli müdahaleler (bilgi sistemlerine zorla girme ve casus yazılımlar gibi) tarafından çalınmasına karşı korunduğunu düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
29.	Üniversitede, önemli bilgilerin, yetkisiz ifşadan korunması için bilgi güvenliği ölçümlerinin uygulandığını düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
30.	Üniversitede, bilgi kaynaklarının sürekli olarak güncellendiğini ve düzenli olarak bilgi yedeklerinin oluşturulduğunu düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
31.	Üniversitede, düzenli olarak risk değerlendirmesinin yapıldığını ve bilgi kaybı olasılığının azaltılması için güvenlik planlarının güncellendiğini düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
32.	Çalışanların, üniversite bilgi sistemleri veritabanlarına (web sitesi, elektronik belge yönetim sistemi, öğrenci ve personel bilgi sistemi veritabanları gibi) önemli bilgileri koyduklarını düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐

EK-1. (devam) Anket formu

33.	Üniversitede, yetkisiz kullanıcılar tarafından bilgi değişikliği (bilginin oluşturulması, değiştirilmesi ve silinmesi gibi) yapılmasının engellenmesi için güvenlik kontrollerinin (değişim yönetimi prosedürleri gibi) tesis edildiğini düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
34.	Üniversitede, bilginin doğruluğunun ve güvenilirliğinin artırılması amacıyla veritabanlarının düzenli olarak bakımının yapıldığını düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
35.	Üniversitede, bilgi sistemlerinin bozulması ve bilgi servislerinin kesintiye uğrama olasılığının azaltılmasına önem verildiğini düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
36.	Üniversitede, özel bilgi kaynaklarına sadece yetkili kullanıcılara sağlanmış olan haklar çerçevesinde erişilebilmesini sağlayan erişim kontrol prosedürlerinin var olduğunu düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
37.	Kullanıcıların, erişim yetkileri dâhilinde üniversite bilgi sistemlerine (e-posta, öğrenci ve personel bilgi sistemi gibi) herhangi bir zamanda ve herhangi bir yerden erişebildiğini düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
38.	Üniversitede, örgütsel bilgi güvenliği politika ve düzenlemelerine aykırı davrananlara yaptırım uygulayan prosedürlerin var olduğunu düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
39.	Üniversitede, bilgi güvenliği hakkında yararlı eğitim ve öğretimlerin verildiğini düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
40.	Üniversitede, bilgi güvenliği ile alakalı etiketlerin ve uyarıcı işaretlerin bilgisayarlara ve iletişim cihazlarına görünecek bir şekilde yapıştırıldığını düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐

EK-1. (devam) Anket formu

41.	Üniversitede, bilgi güvenliği faaliyetlerini sağlamlaştırmak ve bilgi güvenliği sorunlarına müdahale edebilmek için yönetim yapısının, rol ve sorumluluklarla uyumlu bir şekilde kurulduğunu düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
42.	Üniversitede, bilgi güvenliği kontrollerinin uygun bir şekilde oluşturulduğunu ve çalışanların bu kontrollerle alakalı bilgi güvenliği protokollerini, normlarını ve düzenlemelerini takip ettiklerini düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐
43.	Üniversitede, rutin olarak bilgi güvenliği denetimlerinin yönetildiğini ve bilgi suistimaline veya bilgi sistemlerine girme teşebbüslerine ait geçmiş kayıt ve verilerin muhafaza edildiğini düşünüyorum.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐

III. KİŞİSEL BİLGİLER

Lütfen aşağıdaki sorulara cevap veriniz.

1. Çalışmakta Olduğunuz Üniversiteyi Yazınız: .....
2. Akademik Personel Olarak Mesleki Deneyiminiz: ☐ 1-5 yıl ☐ 6-10 yıl ☐ 11-15 yıl ☐ 16-20 yıl ☐ 21 veya üzeri yıl
3. Cinsiyetiniz: ☐ Kadın ☐ Erkek

EK-1. (devam) Anket formu

4. Yaşınız: ☐ 25'ten küçük ☐ 25-34 arası ☐ 35-44 arası ☐ 45-54 arası ☐ 55 veya 55'ten büyük
5. İdari Göreviniz: ☐ Var ☐ Yok

EK-2. Örneklemin çalışılan üniversite itibarıyla dağılımı

Üniversiteler	Frekans	Yüzde
Abant İzzet Baysal Üniversitesi	4	0,1
Abdullah Gül Üniversitesi	2	0,1
Adana Bilim ve Teknoloji Üniversitesi	3	0,1
Adıyaman Üniversitesi	17	0,6
Adnan Menderes Üniversitesi	4	0,1
Afyon Kocatepe Üniversitesi	50	1,7
Ağrı İbrahim Çeçen Üniversitesi	12	0,4
Ahi Evran Üniversitesi	21	0,7
Akdeniz Üniversitesi	18	0,6
Aksaray Üniversitesi	22	0,7
Alanya Alaaddin Keykubat Üniversitesi	3	0,1
Amasya Üniversitesi	26	0,9
Anadolu Üniversitesi	89	2,9
Ankara Sosyal Bilimler Üniversitesi	6	0,2
Ankara Üniversitesi	47	1,6
Ankara Yıldırım Beyazıt Üniversitesi	17	0,6
Ardahan Üniversitesi	17	0,6
Artvin Çoruh Üniversitesi	18	0,6
Atatürk Üniversitesi	81	2,7
Balıkesir Üniversitesi	39	1,3
Bandırma Onyedi Eylül Üniversitesi	3	0,1
Bartın Üniversitesi	16	0,5
Batman Üniversitesi	6	0,2
Bayburt Üniversitesi	17	0,6
Bilecik Şeyh Edebali Üniversitesi	10	0,3
Bingöl Üniversitesi	17	0,6
Bitlis Eren Üniversitesi	16	0,5
Boğaziçi Üniversitesi	7	0,2
Bozok Üniversitesi	15	0,5
Bursa Teknik Üniversitesi	4	0,1
Bülent Ecevit Üniversitesi	27	0,9
Celâl Bayar Üniversitesi	44	1,5
Cumhuriyet Üniversitesi	30	1,0
Çanakkale Onsekiz Mart Üniversitesi	8	0,3
Çankırı Karatekin Üniversitesi	7	0,2
Çukurova Üniversitesi	17	0,6
Dicle Üniversitesi	45	1,5
Dokuz Eylül Üniversitesi	14	0,5
Dumlupınar Üniversitesi	25	0,8

EK-2. (devam) Örneklemin çalışılan üniversite itibarıyla dağılımı

Düzce Üniversitesi	26	0,9
Ege Üniversitesi	67	2,2
Erciyes Üniversitesi	224	7,4
Erzincan Üniversitesi	20	0,7
Erzurum Teknik Üniversitesi	3	0,1
Eskişehir Osmangazi Üniversitesi	15	0,5
Fırat Üniversitesi	43	1,4
Galatasaray Üniversitesi	7	0,2
Gazi Üniversitesi	204	6,7
Gaziantep Üniversitesi	26	0,9
Gaziosmanpaşa Üniversitesi	52	1,7
Gebze Teknik Üniversitesi	18	0,6
Giresun Üniversitesi	25	0,8
Gümüşhane Üniversitesi	20	0,7
Hacettepe Üniversitesi	37	1,2
Hakkari Üniversitesi	3	0,1
Harran Üniversitesi	4	0,1
Hitit Üniversitesi	19	0,6
Iğdır Üniversitesi	9	0,3
İnönü Üniversitesi	47	1,6
İstanbul Medeniyet Üniversitesi	13	0,4
İstanbul Teknik Üniversitesi	36	1,2
İstanbul Üniversitesi	78	2,6
İzmir Katip Çelebi Üniversitesi	10	0,3
İzmir Yüksek Teknoloji Enstitüsü	11	0,4
Kafkas Üniversitesi	21	0,7
Kahramanmaraş Sütçü İmam Üniversitesi	27	0,9
Karabük Üniversitesi	12	0,4
Karadeniz Teknik Üniversitesi	32	1,1
Karamanoğlu Mehmet Bey Üniversitesi	30	1,0
Kastamonu Üniversitesi	21	0,7
Kırıkkale Üniversitesi	10	0,3
Kırklareli Üniversitesi	19	0,6
Kilis 7 Aralık Üniversitesi	28	0,9
Kocaeli Üniversitesi	45	1,5
Mardin Artuklu Üniversitesi	11	0,4
Marmara Üniversitesi	14	0,5
Mehmet Akif Ersoy Üniversitesi	22	0,7
Mersin Üniversitesi	41	1,4
Mimar Sinan Güzel Sanatlar Üniversitesi	11	0,4

EK-2. (devam) Örneklemin çalışılan üniversite itibarıyla dağılımı

Muğla Sıtkı Koçman Üniversitesi	79	2,6
Mustafa Kemal Üniversitesi	27	0,9
Muş Alparslan Üniversitesi	18	0,6
Namık Kemal Üniversitesi	50	1,7
Necmettin Erbakan Üniversitesi	17	0,6
Nevşehir Hacı Bektaş Veli Üniversitesi	71	2,3
Niğde Üniversitesi*	38	1,3
Ondokuz Mayıs Üniversitesi	15	0,5
Ordu Üniversitesi	12	0,4
Orta Doğu Teknik Üniversitesi	25	0,8
Osmaniye Korkut Ata Üniversitesi	6	0,2
Pamukkale Üniversitesi	87	2,9
Recep Tayyip Erdoğan Üniversitesi	12	0,4
Sakarya Üniversitesi	92	3,0
Selçuk Üniversitesi	77	2,5
Siirt Üniversitesi	22	0,7
Sinop Üniversitesi	15	0,5
Süleyman Demirel Üniversitesi	46	1,5
Şırnak Üniversitesi	3	0,1
Trakya Üniversitesi	27	0,9
Tunceli Üniversitesi**	7	0,2
Türk-Alman Üniversitesi	3	0,1
Uludağ Üniversitesi	23	0,8
Uşak Üniversitesi	15	0,5
Yalova Üniversitesi	9	0,3
Yıldız Teknik Üniversitesi	13	0,4
Yüzüncü Yıl Üniversitesi	29	1,0
Toplam	3023	100,0

* 7 Eylül 2016 tarihli ve 29824 sayılı Resmî Gazete'de yayımlanan 6745 Sayılı Kanun gereğince Niğde Üniversitesi'nin adı Ömer Halisdemir Üniversitesi olarak değiştirilmiştir.

** 7 Eylül 2016 tarihli ve 29824 sayılı Resmî Gazete'de yayımlanan 6745 Sayılı Kanun gereğince Tunceli Üniversitesi'nin adı Munzur Üniversitesi olarak değiştirilmiştir.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: AKTAN, Ertuğrul
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 16/04/1980 Ankara
Medeni hali	: Evli
Telefon	: 0 (212) 214 55 47
e-posta	: ertugrulaktan80@gmail.com

Eğitim Derecesi	Okul/Program	Mezuniyet yılı
Doktora	Gazi Üniversitesi Yönetim Bilişim Sistemleri	Devam Ediyor
Yüksek Lisans	Işık Üniversitesi İşletme Anabilim Dalı	2012
Yüksek Lisans	Hacettepe Üniversitesi Elektrik ve Elektronik Mühendisliği	2007
Lisans	Hacettepe Üniversitesi Elektrik ve Elektronik Mühendisliği	2003

İş Deneyimi, Yıl	Çalıştığı Yer	Görev
Kasım 2006 - devam ediyor	BDDK	Bankacılık Başuzmanı (Bilişim)
Mart 2006 - Kasım 2006	Mikes A.Ş.	Sistem ve Güvenilirlik Mühendisi
Temmuz 2004 - Eylül 2005	Hacettepe Meslek Yüksekokulu	Öğretim Görevlisi

Yabancı Dili

İngilizce

Yayınlar

1. Aktan, E., Aydıntan, B. (2016). Cameron-Freeman Örgüt Kültürü Türleri Ekseninde Örgüt Kültürü ve Bilgi Güvenliği Algısı İlişkisi: Devlet Üniversitelerinde Bir Uygulama. **İşletme Araştırmaları Dergisi.** 8(4).

2. Aktan, E. (2015). Yeni Ekonomik Sistemde Elektronik Pazarlama. **Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi.** 1(38).

3. Aktan, E. (2012). Bilgi, Bilgi Yönetimi ve Bilgi Güvenliği. **Bilgi Eksenli Kuram ve Uygulamalar Sorgulayıcı ve Çözümleyici Yaklaşımlar Sempozyumu.** Ankara Üniversitesi Yayınları No: 348.

Hobiler

Su altı dalış, Yüzme, Tiyatro

GAZİLİ OLMAK AYRICALIKTIR.