DOI: 10.20491/isarder.2016.221

ISSN: 1309 - 0712
İşletme Araştırmaları Dergisi

Journal Of
Business Research
Turk
www.isarder.org

Cameron-Freeman Örgüt Kültürü Türleri Ekseninde Örgüt Kültürü ve Bilgi Güvenliği Algısı İlişkisi: Devlet Üniversitelerinde Bir Uygulama

The Relationship between Organizational Culture and the Perception of Information Security on the Axis of Cameron-Freeman Organizational Culture Types: An Application in Government Universities

Ertuğrul AKTAN
Bankacılık Düzenleme ve Denetleme Kurumu
İstanbul, Türkiye
ertugrulaktan80@gmail.com

Belgin AYDINTAN
Gazi Üniversitesi
İktisadi ve İdari Bilimler Fakültesi
İşletme Bölümü, Ankara, Türkiye
belginaydintan@gmail.com

Özet

Bu çalışmada, Cameron-Freeman örgüt kültürü türleri ekseninde Türkiye'deki devlet üniversitelerinin genel kültürel profilinin tanımlanması, bilgi güvenliği prensipleri temelinde akademik personelin bilgi güvenliği algısının ortaya konması ve korelasyon analizi ile örgüt kültürü türleri ve bilgi güvenliği algısı ilişkisinin incelenmesi amaçlanmıştır. Araştırmada, Türkiye'deki 106 devlet üniversitesinin 3.023 akademik personelinden anket yöntemi ile veri toplanmıştır. Anketin Cameron ve Freeman örgüt kültür türlerine ilişkin soruları, Cameron ve Quinn (2006) tarafından geliştirilen Örgütsel Kültür Değerlendirme Aracı dikkate alınarak hazırlanmıştır. Anketin bilgi güvenliği algısına ilişkin sorularının hazırlanmasında da, Chang ve Lin (2007) tarafından geliştirilen ölçekten yararlanılmıştır. Veri analizinde IBM SPSS 21 paket programı kullanılmıştır. Elde edilen bulgulara göre, hiyerarşinin Türkiye'deki devlet üniversitelerinin genel kültürel profilinde baskın olduğu ve erişilebilirlik algısı düzeyinin diğer bilgi güvenliği prensipleri algılarına göre yüksek çıktığı sonucuna ulaşılmıştır. Ayrıca örgüt kültürü türleri ile akademik personelin bilgi güvenliği algısı arasında istatistiksel olarak anlamlı ve orta düzeyde pozitif ilişki gözlemlenmiştir.

Anahtar Kelimeler: Örgüt Kültürü, Rekabetçi Değerler Modeli, Bilgi Güvenliği, Bilgi Güvenliği Prensipleri

Abstract

In this study, defining the overall cultural profile of the government universities in Turkey on the axis of Cameron-Freeman organizational culture types, presenting the academicians' perception of information security based on the principles of information security and investigating the relationship between the organizational culture types and the perception of information security by correlation analysis were aimed. In research, data were gathered from 3.023 academicians of 106 government universities in Turkey via survey method. Questions about the Cameron and Freeman organizational culture

types were prepared using the Organizational Culture Assessment Instrument developed by Cameron and Quinn (2006). In preparing the questions about the perception of information security, the scale developed by Chang and Lin (2007) was used. In data analysis, SPSS 21 package program was used. According to the findings, in overall cultural profile of the government universities in Turkey it was concluded that hierarchy was dominant culture and the perception level of availability was greater than other principles' perception of information security. Moreover, in between the organizational culture types and the academicians' perception of information security, statistically significant, positive and moderate level relationship was observed.

Keywords: *Organizational Culture, Competing Values Approach, Information Security, Principles of Information Security*

1. Giriş

Bilgi ve iletişim teknolojileri alanında, son yıllarda yaşanan büyük gelişmeler neticesinde tüm örgütsel iş süreçlerinde bilgiye olan bağımlılık artmaktadır. Bu durum, bilgiyi önemli bir stratejik kaynak durumuna getirmekte ve bilgi güvenliğinin sağlanması ihtiyacını doğurmaktadır. Bilgi güvenliğin amacı bilgi, donanım, yazılım ve çalışanlar gibi değerli varlıkların korunmasıdır. Bilgi güvenliğinin etkin bir şekilde tesis edilmesi için güvenlikle alakalı risklerin anlaşılması, bu kapsamda uygun kontrollerin geliştirilmesi ve uygulanması gerekmektedir. Çalışanlar kontrolleri ne derece uygulayabiliyorlarsa örgütteki bilgi güvenliği seviyesi de o derece artacaktır. Şayet çalışanlar kontrol ve prosedürlerin neden uygulandığını ve neyi hedeflediğini anlayamıyorlarsa en iyi şekilde tasarlanmış olsalar dahi teknik kontrol ve prosedürlerden istenilen fayda elde edilemeyecektir (Woodhouse, 2007, s. 767). Danışmanlık şirketi PricewaterhouseCoopers tarafından 2004'te yürütülmüş bilgi güvenliği ihlallerini konu alan anket çalışmasında da bir çok güvenlik ihlalinin teknolojik eksikliklerden ziyade insan hatalarından kaynaklandığı sonucuna ulaşılmıştır (Veiga ve Eloff, 2007, s. 362). 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.

Bilgi güvenliği, teknolojiyi, süreçleri ve insanları kapsamaktadır. Şifreleme sistemleri, anti virüs yazılımları, kimlik doğrulama mekanizmaları ve güvenlik duvarları gibi teknik 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, ss. 361-362). Güvenlik çözümleri ve yönetimin desteğiyle bütünleşen bir kültürel değişim olmadığı müddetçe teknolojik çözümlerden istenilen fayda elde edilememektedir. Üst yönetim desteğinin azalmasıyla birlikte güvenlik politikalarının uygulama seviyesinde de düşüş görülmektedir (Knapp ve Ford, 2006, s. 34).

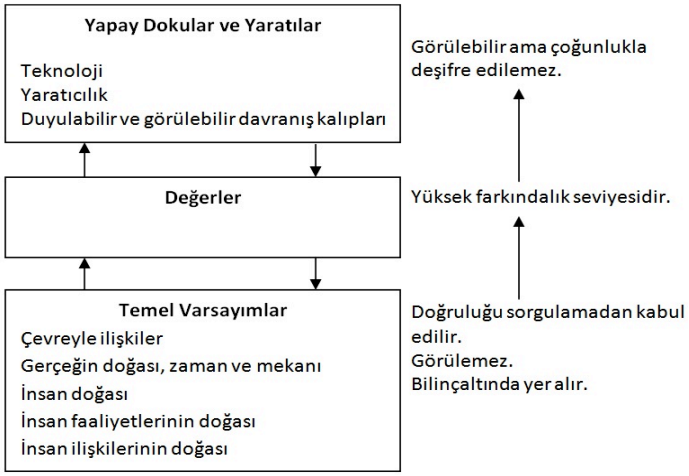
Örgütlerin sahip olduğu kültür türleriyle çalışanların bilgi güvenliği algısı arasındaki ilişkinin düzeyi, bilgi güvenliği uygulamalarında başarıyı elde etmede üst yönetime rehber niteliği taşıyacaktır. Bu açıdan değerlendirildiğinde örgüt kültürü, bilgi güvenliği başarımının sağlanmasında stratejik bir öneme sahip olmaktadır. Bu çerçevede mevcut araştırma, Türkiye'deki devlet üniversitelerinin genel kültürel profilini tanımlamayı, akademik personelin bilgi güvenliği prensipleri temelinde algı düzeyinin ortaya konmasını ve örgüt kültürü türleri ile akademik personelin bilgi güvenliği algısı arasındaki ilişkinin varlığını tespit etmeyi amaçlamaktadır.

2. Örgüt Kültürü

Bireylerin ve örgütlerin davranışlarını etkileyen birçok kültür seviyesi mevcuttur. En geniş kültür seviyesi dinî, kıtasal, ülkesel vb. farklılıklar temelinde oluşmaktadır. Davranışları etkileyen 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, s. 17).

Örgüt kültürü, 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, s. 33). 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, s. 4).

Örgüt kültürü, grupların dış çevreyle uyum ve iç çevreyle bütünleşme süreçlerinde karşılaştıkları problemleri çözmeye çalışırken elde ettikleri, keşfettikleri, geliştirdikleri temel varsayımların bütünüdür. Bu varsayımlar geçerlilikleri kabul edildiği ölçüde karşılaşılan problemlerin çözümünde kullanılmaya devam edilmekte ve gruba dâhil olan yeni bireylere bu problemlerle karşılaşmaları hâlinde nasıl algılanılması, düşünülmesi ve hissedilmesi gerektiğini gösteren doğru birer yol haritası olarak aktarılmakta ve öğretilmektedir (Schein, 1984, s. 3).

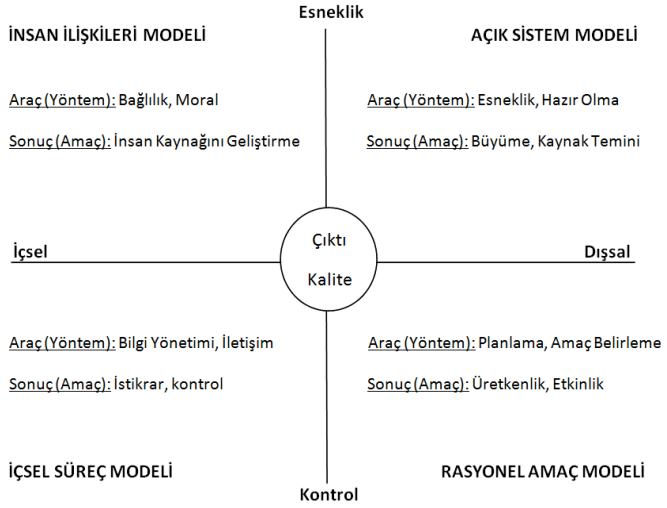


Şekil 1. Örgüt Kültürü Katmanları
Kaynak: Schein, 1984, s. 4

Şekil 1'de görüleceği üzere örgüt kültürü üç farklı katmanda analiz edilmektedir. Başlangıç katmanı görülebilir dokular (yaratılar) olup, 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. Bireylerin neden süregelen şekilde davranış sergilediklerini analiz edebilmek için ise ikinci katmana yani davranışları şekillendiren değerlere bakılması gerekmektedir. Fakat değerlerin doğrudan gözlemlenebilmesi zor olup, değerlerin ne anlama geldiği, kilit örgüt üyeleriyle yapılacak görüşmeler ve yaratıların analizi ile elde edilebilmektedir. Bireylerin davranışları altında yatan esas sebepler ise gizli ve bilinçaltı ögeler olup, bu ögeler 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 (Schein, 1984, ss. 3-4).

2.1. Cameron ve Freeman Örgüt Kültürü Türleri Modeli

Örgütsel kültür disiplininin geliştiği ilk aşamalarda kültür, örgütsel yaşamın sübjektif tarafını yansıtan bir kavram olarak algılanmakta ve nitel gözlem metotlarıyla ele alınmaktayken, son zamanlarda örgütsel kültür alanında yapılan çalışmalarda araştırmacılar nicel anket metotlarını uygulamakta ve karşılaştırılabilir kültür boyutlarını tanımlamaktadırlar (Denison, 1996, ss. 619-620). Nitel araştırmalar aşırı tanımlamayı amaç edinmekte olup, sunmuş olduğu avantajlar araştırmanın maliyet unsurunu da beraberinde getirmektedir. Bununla birlikte nitel araştırma metotları örgütler arasında analitik karşılaştırma yapma olanağı da sunmamaktadır. Sonuç olarak, örgüt kültürü, örgüt kültürünün sistematik gözlemine olanak sağlayan güvenilir ve kolay yönetilebilir araçlarla ölçülemedikçe birçok önemli teorik soru cevapsız kalacaktır (Quinn ve Spreitzer, 1991, s. 116). Nicel metot savunucularının başında gelen araştırmacılardan Robert E. Quinn ve John Rohrbaugh (1981) tarafından geliştirilen, örgüt kültürünü ölçümleyen Rekabetçi Değerler Modeli (Competing Values Approach) Şekil 2'de gösterilmiştir.



Şekil 2. Örgütsel Etkinlik İçin Rekabetçi Değerler Modeli
Kaynak: Quinn ve Rohrbaugh, 1983, s. 369

Örgütsel Etkinlik İçin Rekabetçi Değerler Modeli'nde örgütsel etkinliğin kriterleri içsel-dışsal, esnek-kontrollü ve araç (yöntem)-sonuç (amaç) olmak üzere üç ayrı rekabetçi değerler boyutunda sınıflandırılmıştır. İçsel-dışsal ve esnek-kontrollü 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. Bir diğer ifadeyle, bu 4 modelin bütünleştirilmesi ile Örgütsel Etkinlik İçin Rekabetçi Değerler Modeli oluşmaktadır. 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 bir yönetim tarzına ve düzenli bir örgüt yapısına sahip olduğu yansıtılmaktadır. Üçüncü boyut ise planlama, hedef belirleme gibi önemli süreçlerde kullanılacak araçlara (yöntemlere) ve bu araçların kullanımı ile elde edilecek üretkenlik, kaynak temini gibi sonuçlara (amaçlara) odaklanmaktadır (Quinn ve Rohrbaugh, 1981, ss. 130-131; 1983, ss. 369-370).

Quinn ve Rohrbauh'un örgütsel etkinlik için geliştirmiş oldukları Rekabetçi Değerler Modeli, Cameron ve Freeman Örgüt Kültürü Türleri Modeli'nin temelini oluşturmaktadır. Şekil 3'te görülen Cameron ve Freeman Örgüt Kültürü Türleri Modeli'ndeki dört örgüt kültür türü, hiyerarşi, pazar, klan ve adhokrasi olarak tanımlanmaktadır. Her bir kültür türü 4 ana özellik çerçevesinde başlıca karakteristikler içermektedir. Örgüt kültür türlerini yansıtan bu 4 ana özellik, baskın özellikler, örgütsel liderlik, örgüte bağlılık ve stratejik vurgular olarak tanımlanmıştır (Cameron ve Freeman, 1991, s. 28).

Şekil 3. Cameron ve Freeman Örgüt Kültürü Türleri Modeli
Kaynak: Cameron ve Freeman, 1991, s. 29

Hiyerarşi: Şekil 3'ün sol alt çeyreğinde yer alan hiyerarşi kültürü, içsel devamlılık ve mekanik süreçler üzerine kurulu olup, 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. Hiyerarşik örgütler durağanlık ve verimlilik temalı kültüre hâkim olup, işlerin düzenli ve verimli bir şekilde yürütülmesi esastır. Resmî kural ve politikalar, örgüt bireylerini bir arada tutmaktadır (Cameron ve Quinn, 2006, s. 38). Hiyerarşilerde 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, s. 30).

Pazar: Şekil 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 kurallarla içsel kontrolün sağlandığı hiyerarşik kültürün 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. Örgütü bir arada tutan bağ, kazanmaya verilen önemdir. 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, ss. 39-40). Pazarlarda örgütü bir arada tutan temel bağ, sonuç odaklılık, üretim ve rekabet temelli olup, stratejik vurgular arasında rekabetçi avantaj ve pazar üstünlüğü elde etme yer almaktadır (Cameron ve Freeman, 1991, s. 30).

Klan: Şekil 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 örgütleri betimlemektedir. İktisadi bir teşekkülden ziyade geniş bir aile algısı hâkimdir. Takım çalışması, çalışanların katılımcılığı ve örgüte duydukları sadakat, klan türü örgütlerin 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 olan bağlılık ve moralle elde edilecek kişisel gelişimden uzun dönemli kazanç elde etme vurgusu vardır. Başarı, içsel örgüt iklimi ve insan odaklı olarak tanımlanmaktadır. Klan örgütler, takım çalışması, çalışan katılımcılığı ve fikir birliği temelinde kuruludur (Cameron ve Quinn, 2006, ss. 41-43). Klanlarda örgütü bir arada tutan temel bağ, gelenekler ve kişiler arası uyum temelli olup, stratejik vurgular arasında insan kaynakları gelişimi, yüksek seviyede moral ve örgüte duyulan bağlılık yer almaktadır (Cameron ve Freeman, 1991, s. 30).

Adhokrasi: Şekil 3'ün sağ üst çeyreğinde dışsal konumlama ve organik süreçler altında yer alan dördüncü kültür türü de adhokrasi olarak adlandırılmaktadır. Adhokrasi kelimesinin kökü İngilizce "ad hoc"a dayanmakta olup, geçici, özel amaçlı ve dinamik anlamlarına sahiptir. Adhokrasi örgütleri, genellikle uzay, yazılım geliştirme,

danışmanlık ve film yapımcılığı gibi endüstrilerde görülmektedir. Bu tür örgütler, yaratıcı ve yenilikçi olmaya ve doğan yeni fırsatlara çabuk uyum sağlamaya çalışır. Pazar ve hiyerarşilerin aksine, adhokrasilerde merkezî güç veya otorite ilişkileri bulunmamaktadır. Güç, sorunlarla karşılaşıldığı ana dayalı olarak bireyler veya görev takımları arasında iletilmektedir. Adhokrasi kültür türü, dinamizm, girişimcilik ve yaratıcı çalışma alanlarıyla tanımlanmaktadır. Çalışanlar, ellerini taşın altına koymaya ve risk almaya isteklidirler. Adhokrasi örgüt türünde liderler vizyon sahibi, yaratıcı ve risk odaklı olarak görülmektedir. Örgütü bir arada tutan bağ, tecrübeye ve yenilikçiliğe olan bağlılıktır. Adhokrasilerin 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, ss. 43-45). Hiyerarşilerin aksine adhokrasilerde 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, s. 30).

3. Bilgi Güvenliği

Bilgi, kağıt 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 yaygın olmakta, saldırılar hırslı ve karmaşık bir hâl almaktadır. Bilgi sistemlerine ve servislerine bağımlılık, örgütleri güvenlik tehditlerine maruz bırakmaktadır (British Standard, 1999, s. 1).

Bilgi güvenliği modeli, gizlilik, bütünlük ve erişilebilirlikten oluşmaktadır (Fussell, 2005, s. 2977). Başka 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" şeklinde tanımlanmaktadır (Canbek ve Sağıroğlu, 2006, s. 168). 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, s. 138).

Bilgi güvenliği çok boyutlu olmasına karşın, temel olarak üç bilgi güvenliği prensibinden söz edilmektedir: Gizlilik, bütünlük, erişilebilirlik. Temel bilgi güvenliği prensiplerine ek olarak, sorumluluk (izlenebilirlik) kavramı da bilgi güvenliği kapsamında ele alınmaktadır (Canbek ve Sağıroğlu, 2006, s. 170; Chang ve Lin, 2007, s. 444; Harris, 2013, s. 298; Kanday, 2012, s. 302; Türkiye Bilişim Derneği, 2006, s. 3).

Gizlilik: Gizlilik, bilginin sadece yetkilendirilmiş kişilerin, varlıkların ya da süreçlerin erişimine açılmasıdır (British Standard, 1999, s. 1; Türk Standardı, 2006, s. 4). Benzer bir ifadeyle, bilginin yetkisiz kişiler, programlar veya süreçler tarafından erişilemiyor olması gerekmektedir (Harris, 2013, s. 160). Bilgi sistemlerinin ve

iletişiminin kasıtlı veya yanlışlıkla yetkisiz kişilerin erişimine açılmasının engellenmesi için gizlilik korunuyor olmalıdır (Onwubiko ve Lenaghan, 2007, s. 246). Yani gizlilik ile "sadece siz görebilirsiniz" prensibine vurgu yapılmakta olup, erişim hakkının sadece yetkisi olanlarla sınırlandırılması ifade edilmektedir (Jones, 2004, s. 404).

Bütünlük: Bütünlük, bilginin ve bilgi işleme metotlarının doğruluğunun ve tamlığının korunmasıdır (British Standard, 1999, s. 1). Bilgisayar ağlarının sunmuş olduğu servislerin tam, eksiksiz, tutarlı, güvenilir ve güncel olduğundan emin olabilmek, bütünlüğün korunmasıyla sağlanır (Onwubiko ve Lenaghan, 2007, s. 246). Bilgi, yetkisiz modifikasyonlardan korunmalı, tam ve eksiksiz olmalıdır. Bütünlüğü sağlayan güvenlik mekanizmalarında bilginin tamlığı ve yetkisiz olarak 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, s. 159). Veri ve ağ güvenliği anlamında bütünlük prensibi ile, bilgide sadece yetkili kişilerce değişiklik yapılabilmesi garantisi sunulmaktadır (Kanday, 2012, s. 303).

Erişilebilirlik: Erişilebilirlik, yetkili kişilerin bilgi ve varlıklarına erişiminin korunmasıdır (British Standard, 1999, s. 1). Diğer bir ifadeyle, bilgisayar ağ ve servislerinin içeriğine, tanımlanan yetki seviyelerinde erişim sağlanabilmesinin korunmasıdır (Onwubiko ve Lenaghan, 2007, s. 246). 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, s. 159). Şayet servis veya bileşenler erişilemez durumda ise gizlilik ve bütünlüğün sağlanıyor olması bir anlam ifade etmeyecektir (Fussell, 2005, s. 2977).

Sorumluluk: Sorumluluk 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, s. 363). 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 olayı, sonradan analiz edilmesi için kayıt altına almaktır. İzlenebilirliğin tam manasıyla yerine getirilebilmesi için olayların kayıtlarını tutmak için bir kayıt tutma (logging) sistemine ve bu kayıtları araştıracak bir hesap inceleme (auditing) sistemine ihtiyaç duyulur (Canbek ve Sağıroğlu, 2006, s. 170). Sorumluluğun izlenmesi, kullanıcı, sistem ve uygulama etkinliklerinin kaydedilmesi ile gerçekleşmektedir (Harris, 2013, s. 248). Sorumluluk prensibi, bilgi güvenliğini etkileyen her çalışanı eylemlerinden dolayı sorumlu tutmaktadır (Chang ve Lin, 2007, s. 444). Şayet bilgi sahiplikleri açıkça tanımlanmamış 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, s. 375).

4. Örgüt Kültürü ve Bilgi Güvenliği İlişkisi

Bilgisayar Güvenliği Enstitüsü (Computer Security Institute) ve Federal Soruşturma Bürosu (Federal Bureau of Investigation) 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, s. 439). Çalışanların örgüt başarısında kritik öneme sahip olduğu yadsınamaz bir gerçektir, fakat hâlâ bilgi güvenliği konusundaki en zayıf halkayı çalışanlar teşkil etmektedirler. Örgüt içi kaynaklı güvenlik olayları sayıca örgüt dışı kaynaklı olanları geçmekte ve bu durum örgütlerin çalışmasına olan en büyük tehdit olarak algılanmaktadır (Vroom ve Solms, 2004, s. 193).

Sekiz yüz yetmiş dört bilgi güvenliği sertifikalı uzmana (CISSPs) 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 olmuştur (Rainer ve Diğ., 2007, ss. 100-101).

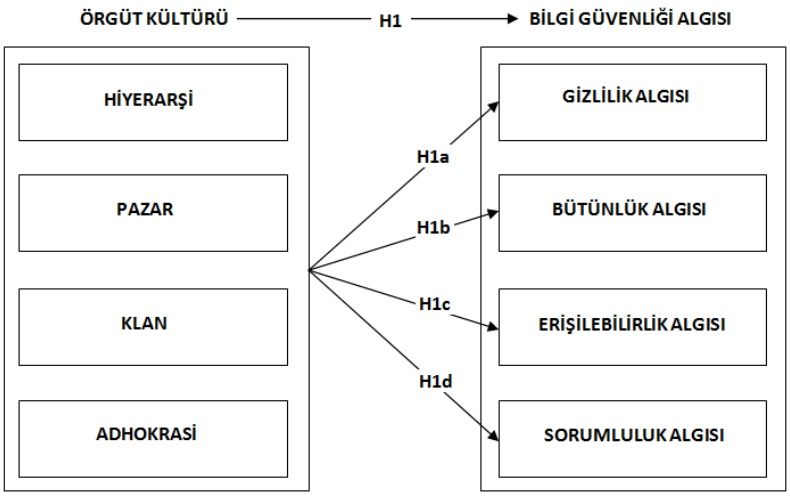
Örgüt kültürü, en temel ifadeyle öğrenilen davranışlar sistemidir. Öğrenilen davranışlar, bilgi güvenliği süreçlerinin başarısını önemli ölçüde etkileyen son kullanıcı farkındalık seviyesini yansıtmaktadır. Son zamanlarda bilgi güvenliği bilgi teknolojileri konusu olmaktan çıkıp, ağırlıklı olarak yönetimi ilgilendiren bir konu olmaya başlamıştır (Woodhouse, 2007, s. 769). Örgüt kültürü genel olarak bireylerin tutum ve davranışlarını yöneten ve şekillendiren paylaşılan değer, inanç, varsayım ve uygulamalar olarak tanımlandığına göre çalışanların davranışlarının güvenlik faaliyetleri üzerinde nasıl bir etkiye sahip olabileceğinin araştırılmasında örgüt kültürünü anlamak faydalı olacaktır (Lim ve Diğ., 2009, s. 88).

Şekil 1'deki Schein'in örgüt kültürü katmanlarına bilgi güvenliği perspektifinden bakıldığında başlangıç katmanı olan görülebilir dokulara (yaratılara) örnek olarak bilgi sistemlerine ve kaynaklarına yetkisiz erişimi engelleyen kilitli kapılar gibi fiziksel güvenlik önlemleri ve bilgi güvenliği politikaları verilebilir. Bilgi güvenliği politikasını oluşturan ve yöneticiler tarafından vurgulanan bilgi güvenliği stratejisi de ikinci katmandaki benimsenen ve paylaşılan değerleri ifade edebilir. Son katman bilinçaltı varsayımlarda da bilgi güvenliğinin önemine duyulan inançlar yer almaktadır. Özetle örgüt kültürünün bilgi güvenliği üzerinde pozitif veya negatif anlamda çok büyük etkisi olmaktadır (Vroom ve Solms, 2004, ss. 195-196).

5. Metodoloji

5.1. Araştırmanın Hipotezleri

Şekil 4'te gösterilen araştırmanın 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 ve sorumluluk üzerine algılarıdır.



Şekil 4. Araştırmanın Hipotez Çatısı

Örgüt kültürü ile, bilgi güvenliği ve bilgi güvenliği prensipleri algıları arasındaki ilişkilerin sorgulanmasında aşağıdaki hipotezler kullanılmıştır:

H1: Örgüt kültürü ile bilgi güvenliği algısı arasında anlamlı bir ilişki vardır.

H1a: Örgüt kültürü ile bilgi güvenliğinin gizlilik prensibi algısı arasında anlamlı bir ilişki vardır.

H1b: Örgüt kültürü ile bilgi güvenliğinin bütünlük prensibi algısı arasında anlamlı bir ilişki vardır.

H1c: Örgüt kültürü ile bilgi güvenliğinin erişilebilirlik prensibi algısı arasında anlamlı bir ilişki vardır.

H1d: Örgüt kültürü ile bilgi güvenliğinin sorumluluk prensibi algısı arasında anlamlı bir ilişki vardır.

5.2. Araştırmada Kullanılan Yöntem ve Teknikler

Araştırmada veri toplama aracı olarak anket kullanılmıştır. Anketin Cameron ve Freeman örgüt kültür türlerine ilişkin soruları, Cameron ve Quinn (2006, ss. 26-28) tarafından geliştirilmiş 24 sorulu Örgütsel Kültür Değerlendirme Aracı (Organizational Culture Assessment Instrument) dikkate alınarak hazırlanmıştır. Örgütsel Kültür Değerlendirme Aracı 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, s. 151). Anketin bilgi güvenliği algısına ilişkin sorularının hazırlanmasında da, bilgi güvenliği yönetim standardı BS 7799-1'den uyarlanarak hazırlanmış olan, bilgi güvenliğinin, gizlilik, bütünlük, erişilebilirlik ve sorumluluk prensipleri ile tanımlandığı 19 sorulu anketten yararlanılmıştır (Chang ve Lin, 2007, ss. 457-458). Yararlanılan anketler Türkçeye tercüme edilmiş, ifade ve imlâ yapısı açısından değerlendirildikten sonra deneklere uygulanmıştır.

Ölçek bağlamında ise 5'li Likert ölçeği kullanılmış olup, 1 "Kesinlikle katılmıyorum", 2 "Katılmıyorum", 3 "Ne katılıyorum ne katılmıyorum", 4 "Katılıyorum", 5 "Kesinlikle katılıyorum" düzeylerini temsil etmektedir.

Üç bölümden oluşan veri toplama aracının 1. kısmında çalışılmakta olunan üniversitenin örgüt kültür türünü betimleyen, 2. kısmında akademik personelin bilgi güvenliği algısını ortaya çıkaran ve 3. kısmında da katılımcıların demografik bilgilerini içeren sorular yer almaktadır.

5.3. Araştırmanın Evreni ve Örneklemi

Araştırmanın evreni Türkiye'deki devlet üniversitelerinde çalışmakta olan profesör, doçent, yardımcı doçent, öğretim görevlisi, okutman, araştırma görevlisi ve uzman unvanlarındaki akademik personelden oluşmakta olup, evrendeki akademik personelin tamamına ulaşılmaya çalışılmıştır. Veri toplama yöntemi olarak tesadüfi olmayan örnekleme yöntemlerinden kolayda örnekleme yöntemi kullanılmıştır.

Anket formunun Google Formlar internet 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 analizine, elde edilen geri dönüşlerden kullanılabilir durumda olan 3.023 anket formu dâhil edilmiştir. Anket verilerinin analizinde IBM SPSS 21 paket programından yararlanılmıştır.

5.4. Araştırmanın Sınırları

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

Türkiye'deki 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, kullanılan anket formundaki bilgi güvenliği prensiplerinden gizlilik, bütünlük, erişilebilirlik ve sorumluluk boyutlarının sorularıyla sınırlıdır. Bilgi güvenliğinin başlıca temel 3 ana prensibi gizlilik, bütünlük ve erişilebilirliğin yanı sıra sorumluluk haricinde de kimlik sınaması, 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.

6. Analiz ve Bulgular

Güvenirlik katsayısı hesaplama tekniklerinden Cronbach alfa iç güvenirlik katsayısı yöntemi kullanılmıştır. Cronbach alfa iç güvenirlik katsayısının 0,7'den büyük olması ölçeği güvenilir kılmaktadır (Field, 2009, s. 675).

Tablo 1. Güvenirlik İstatistikleri

Değişkenler	Madde Sayısı	Cronbach Alfa
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

N=3.023

Tablo 1 incelendiğinde ölçek için hesaplanan Cronbach alfa iç güvenirlik katsayılarının tamamının 0,7 değerinden büyük olduğu görülmekte olup, ölçeğin bütünü itibariyle güvenilir olduğu sonucuna ulaşılmıştır.

Tablo 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.

Tablo 2. Araştırma Evreninde Yer Alan Kişilerin Demografik Özellikleri

Demografik Özellikler		Frekans	Yüzde
Cinsiyet	Kadın	1.272	42,1
	Erkek	1.751	57,9
	Toplam	3.023	100,0
Yaş	25'ten küçük	55	1,8
	25-34 arası	1.291	42,7
	35-44 arası	934	30,9
	45-54 arası	541	17,9
	55 veya 55'ten büyük	202	6,7
	Toplam	3.023	100,0
Mesleki Deneyim	1-5 yıl	1.149	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	3.023	100,0
İdari Görev	Var	832	27,5
	Yok	2.191	72,5
	Toplam	3.023	100,0

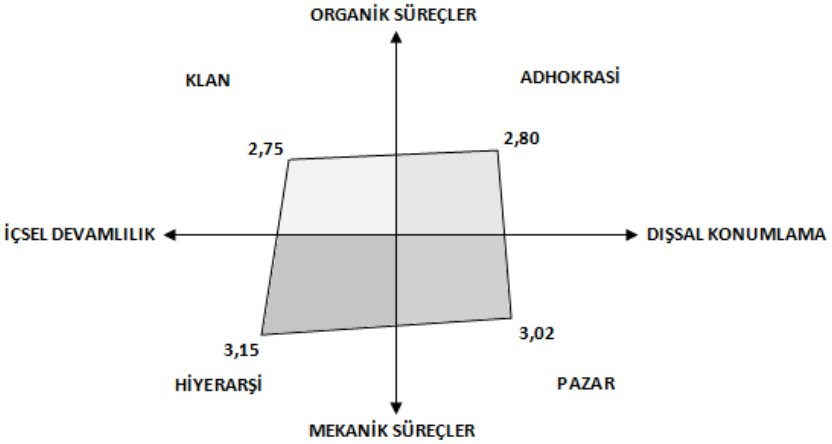
Değişkenlerin frekans analizi sonuçları Tablo 3'te verilmiştir. Hiyerarşi, 3,1465 ortalama değeri ile Türkiye'deki devlet üniversitelerinin genel kültürel profilinde baskın çıkmıştır. Akademik personelin bilgi güvenliği algısı ölçümünde de erişilebilirlik

algısının, 3,5824 ortalama değeri ile diğer bilgi güvenliği prensipleri algılarına nazaran yüksek değere sahip olduğu görülmüştür.

Tablo 3. Değişkenlerin 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

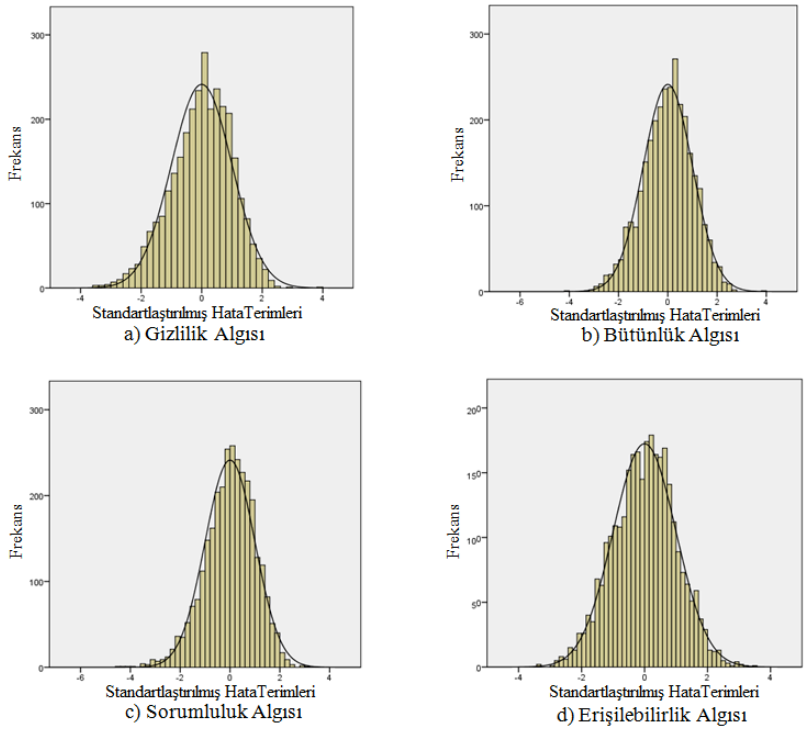
Türkiye'deki devlet üniversitelerinin Cameron ve Freeman Örgüt Kültürü Türleri Modeli'ne göre genel örgüt kültürü profili Şekil 5'te verilmiştir.



Şekil 5. Türkiye'deki Devlet Üniversitelerinin Genel Örgüt Kültürü Profili

Tüm gözlem verileri, bir bütün olarak ele alındığında, devlet üniversitelerinde hiyerarşi kültürünün hâkim olduğu ve hiyerarşi kültürünü pazar kültürünün izlediği anlaşılmaktadır. Bir diğer ifadeyle Türkiye'deki devlet üniversitelerinin kültür yapısında mekanik süreçlerin organik süreçlere göre genel olarak baskın olduğu söylenebilir.

Değişkenler arası Pearson Korelasyon Analizi yapabilmek için değişkenlerin normal dağıldığı varsayımının sağlanması gerekmektedir (Hauke ve Kossowski, 2011, s. 88). Şekil 6'daki histogramlarda gizlilik, bütünlük, erişilebilirlik ve sorumluluk algısı bağımlı değişkenlerinin gözlemlenen ve beklenen değerler farkının (hata terimlerinin) normal dağıldığı görülmektedir.



Şekil 6. 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, s. 32). Tablo 4'te yer alan Pearson korelasyon matrisindeki r katsayıları değerlendirildiğinde ise Cameron ve Freeman örgüt kültürü türleri hiyerarşi, pazar, klan ve adhokrasi ile akademik personelin gizlilik, bütünlük, erişilebilirlik ve sorumluluk algıları arasında istatistiksel olarak $p<0.01$ anlamlılık düzeyinde, pozitif ve orta düzeyde ilişkinin var olduğu ve korelasyon katsayılarının 0,450 ile 0,561 arasında değerler aldığı görülmektedir.

Tablo 4. Korelasyon Matrisi

Pearson Korelasyon	Hiyerarşi	Pazar	Klan	Adhokrasi	Gizlilik Algısı	Bütünlük Algısı	Erişilebilirlik Algısı	Sorumluluk 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

* Korelasyon $p<0.01$ düzeyinde anlamlıdır (2 yönlü)

Hiyerarşi, pazar, klan ve adhokrasi örgüt kültürü türlerinin, bilgi güvenliği prensiplerinden gizlilik, bütünlük, erişilebilirlik ve sorumluluk algıları ile anlamlı ve pozitif ilişki içinde olmasından dolayı H1a, H1b, H1c ve H1d hipotezleri ile birlikte H1 hipotezi kabul edilmiştir.

7. Sonuç ve Tartışma

Mevcut araştırmada elde edilen bulgular, Türkiye'deki devlet üniversitelerinin genel kültürel profilinin tanımlanması, akademik personelin bilgi güvenliği prensipleri temelinde algı düzeyinin ortaya konması ve örgüt kültürü türleriyle akademik personelin bilgi güvenliği algısı arasındaki ilişkinin tespit edilmesi açısından anlamlıdır.

Hiyerarşi, Türkiye'deki devlet üniversitelerinin genel kültürel profilinde baskın çıkmıştır. Araştırmanın evrenindeki üniversitelerin, resmî kurallar, politikalar, prosedürler, anlaşılır tanımlamalar ve görevler temelli formel işleyiş süreçlerine hâkim birer devlet kuruluşu olduğu düşünüldüğünde, hiyerarşi kültürünün baskın çıkması anlamlı karşılanmalıdır. Bunun yanı sıra üniversitelerde pazar kültürünün de hiyerarşi kültüründen sonra önemli ölçüde yer aldığı gözlemlenmiştir. Bu durumun yüksek öğretim alanında üniversitelerarası yaşanan rekabet ortamında üniversitelerin ortaya koyduğu rekabetçi avantaj elde etme stratejisiyle, başarı ve sonuç odaklılık anlayışıyla açıklanması mümkündür. Hiyerarşi ve pazar kültürlerinin ortak yönü değerlendirildiğinde ise devlet üniversitelerinin genel kültür yapısının kontrollü bir yapıya sahip mekanik süreçleri yansıttığı sonucuna ulaşılmıştır.

Akademik personelin bilgi güvenliği algısı değerlendirildiğinde erişilebilirlik prensibi algısı, diğer bilgi güvenliği prensipleri algılarına nazaran yüksek çıkmıştır. Bu durum, üniversitelerde bilgi sistemlerinin internet ve intranet üzerinden öğrencilerin, personelin, diğer araştırmacı ve eğitmenlerin erişimine açık olduğu algısının genel bir göstergesidir.

Bireylerin bilinçaltı varsayımları temelinde şekillenen örgüt kültürü öğrenilen davranışlar bütünüdür. Bilgi güvenliği uygulamalarında başarının elde edilmesi, başta yöneticiler olmak üzere tüm çalışanların bilgi güvenliğinin gerekliliği hususunda farkındalıklarının oluşturulmasına bağlıdır. Bilgi güvenliği farkındalık seviyesini de öğrenilen davranışlar yansıtmaktadır. Bununla birlikte, örgüt kültürünün temelini teşkil eden bilinçaltı varsayımlar da örgüt üyelerinin bilgi güvenliği algısını şekillendirmektedir. Nitekim, bu araştırmada da Türkiye'deki devlet üniversitelerinin sahip olduğu kültür türleriyle akademik personelin bilgi güvenliği algısı arasında pozitif anlamlı bir ilişki tespit edilmiştir. Elde edilen bu bulgunun, araştırmanın evreni olan devlet üniversiteleri hariç diğer örgüt türleri için de anlam ifade edeceği öngörülmektedir. Buradan hareketle, çalışanların bilgi güvenliği algısının ve örgüt kültürü ile bilgi güvenliği algısı arasındaki ilişki düzeyinin, örgütlerin uzun dönemli bilgi güvenliği stratejileri doğrultusunda kültür türleri özelliklerinden hareketle bilgi güvenliği farkındalığının oluşturulmasına katkı sağlayacağı umulmaktadır.

Kaynakça

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

Büyüköztürk, Ş., (2015). Sosyal Bilimler İçin Veri Analizi El Kitabı, Pegem Akademi, Ankara.

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

Cameron, K. S., Quinn, R. E., (2006). Diagnosing and Changing Organizational Culture, Jossey-Bass, San Francisco.

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

Chang, S. E., Lin, C. S., (2007). "Exploring Organizational Culture for Information Security Management", Industrial Management & Data Systems, Vol. 107, No. 3, 438-458.

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, Vol. 21, No. 3, 619-654.

Deshpande, R., Webster, F. E., (1989). "Organizational Culture and Marketing: Definig the Research Agenda", The Journal of Marketing, Vol. 53, No. 1, 3-15.

Field, A., (2009). Discovering Statistics Using Spss, SAGE Publications, London.

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

Harris, S., (2013). All-In-One CISSP Exam Guide, Mc Graw Hill, United States.

Hauke, J., Kossowski, T., (2011). "Comparison of Values of Pearson's and Spearman's Correlation Coefficients on the Same Sets of Data", Quaestiones Geographicae, Vol. 30, No. 2, 87-93.

Jones, D., (2004). "Confidentiality and Security of Information", Anaesthesia and Intensive Care Medicine, Vol. 5, No. 12, 404-406.

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

Knapp, K. J., Ford, F. N., (2006). "Information Security: Management's Effect on Culture and Policy", Information Management & Computer Security, Vol. 14, No. 1, 24-36.

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

Meijer, A., (2001). "Accountability in an Information Age: Opportunities and Risks for Records Management", Archival Science, Vol. 1, No. 4, 361-372.

Onwubiko, C., 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.

Quinn, R. E., Rohrbaugh, J., (1981). "A Competing Values Approach to Organizational Effectiveness", Public Productivity Review, Vol. 5, No. 2, 122-140.

Quinn, R. E., Rohrbaugh, J., (1983). "A Spatial Model of Effectiveness Criteria: Towards a Competing Values Approach to Organizational Analysis", Management Science, Vol. 29, No. 3, 363-377.

Quinn, R. E., 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, Vol. 5, 115-142.

Rainer, R. K., Marshall, T. E., Knapp, K. J. Montgomery, G. H., (2007). "Do Information Security Professionals and Business Managers View Information Security Issues Differently?", Information Systems Security, Vol. 16, 100-108.

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

Schein, E. H., (1984). "Coming to a New Awareness of Organizational Culture", Sloan Management Review, Vol. 25, No. 2, 3-16.

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

Solms, B. V., Solms, R. V., (2004). "The 10 Deadly Sins of Information Security Management", Computer & Security, Vol. 23, No. 5, 371-376.

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

Türkiye Bilişim Derneği, (2006). Bilişim Sistemleri Güvenliği El Kitabı Sürüm 1.0, Türkiye Bilişim Derneği Yayınları, Ankara.

Veiga, A. D., Eloff, J. H. P., (2007). "An Information Security Governance Framework", Information Systems Management, Vol. 24, No. 4, 361-372.

Vroom, C., Solms, R. V., (2004). "Towards Information Security Behavioural Compliance", Computer & Security, Vol. 23, No. 3, 191-198.

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

YÖK (Yükseköğretim Kurulu) Web, URL Adresi: http://yok.gov.tr/web/guest/universitelerimiz, Son Erişim: 21 Nisan 2016.

The Relationship between Organizational Culture and the Perception of Information Security on the Axis of Cameron-Freeman Organizational Culture Types: An Application in Government Universities

Ertuğrul AKTAN
Banking Regulation and Supervision Agency,
İstanbul, Turkey
ertugrulaktan80@gmail.com

Belgin AYDINTAN
Gazi University
Faculty of Economics and Administrative, Sciences, Department of Business,
Ankara, Turkey
belginaydintan@gmail.com

Extensive Summary

1. Introduction

As a result of attacks to computer systems and networks, encountering the loss of money, time, prestige and information is inevitable for the organizations. Therefore, dependency on computer systems in over all business processes raises the need to ensure the security of information held in electronic form. Implementing effective information security involves understanding security-related risk, then developing and implementing appropriate controls. In general the better employees are at applying the controls the more secure the organization will be, because even the best designed technical controls and procedures will be of limited value if the staff involved do not understand why they have been implemented and what they are accomplishing (Woodhouse, 2007, p. 767). Therefore, senior management must recognize that information security can no longer solely rely on technical and physical controls (Lim et al., 2009, p. 88). The role of the employees is vital to the success of any company, yet unfortunately they are also the weakest link when it comes to information security. In order to understand the enormous influence that the employee has on the business with regard to information security, the role that people play in securing information must first be examined (Vroom and Solms, 2004, p. 193).

If there's no management support and the culture change that embraces security and management's backing, all information security programs will fail even if technology is great. Without management's visible support, running an effective security program will be an uphill battle (Knapp and Ford, 2006, p. 34). In this respect, organizational culture has a strategic importance in achieving information security success. Because of the organizational culture has values and preconscious assumptions that affect the behavior of employees and organizational artifacts, the existence of relationship between organizational culture and the employees' perception of information security is discussed. In order to achieve the desired level of information security, as investment in technological solutions, information security awareness of employees, organizational cohesions and understanding the purposes of information security are increasingly becoming an important case (Chang and Lin, 2007, p. 439).

Hence, in this research, defining the overall cultural profile of the government universities in Turkey on the axis of Cameron-Freeman organizational culture types,

presenting the academicians' perception of information security based on the principles of information security and investigating the relationship between the organizational culture types and the academicians' perception of information security by correlation analysis were aimed.

Cameron-Freeman Organizational Culture Types: Cameron and Freeman (1991) developed an approach to representation of organizational culture, consisting of four dimensions that describe opposing or competing values of culture types. This framework is referred as the Competing Values Framework (CVF) and is illustrated in Figure 1. This framework includes four types of cultures, namely hierarchy, market, clan and adhocracy. The hierarchy concerns the internal maintenance with control and stability. The organizational culture compatible with hierarchy is characterized by a formalized and structured place to work. The market focuses on the outside positioning, control and stability and so defines a results-oriented workplace. The clan focuses on internal maintenance with a sense of flexibility. It is called a clan because of its similarity to a family-type organization. The fourth culture type, adhocracy is characterized by a dynamic, entrepreneurial, and creative workplace. The focus of adhocracy is on the external positioning with a high degree of flexibility and individuality (Cameron and Freeman, 1991, p. 30; Cameron and Quinn, 2006, pp. 38-45).

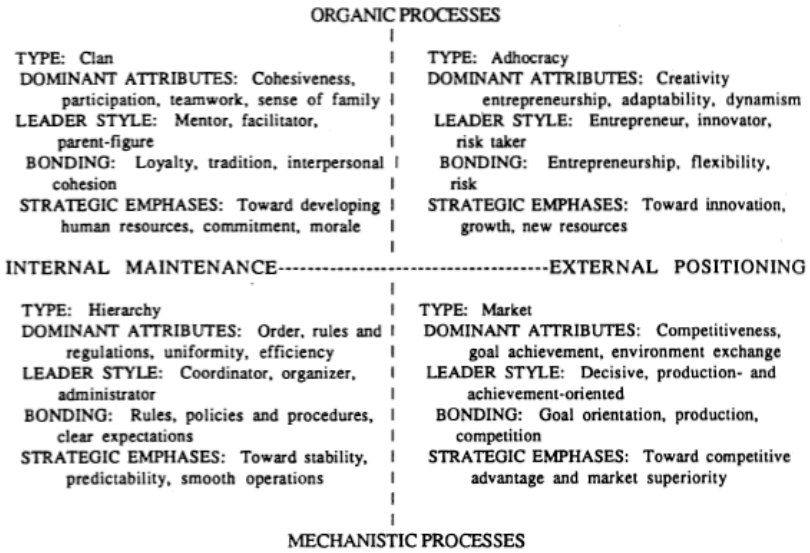


Figure 1. Cameron-Freeman Organizational Culture Types
Reference: Cameron and Freeman, 1991, p. 29

Information Security: Information security consists of three main attributes: 1) Availability that is the prevention of loss of, or loss of access to, data and resources. 2) Integrity that is the prevention of unauthorized modification of data and resources. 3) Confidentiality that is the prevention of unauthorized disclosure of data and resources (Harris, 2013, p. 298). Accountability was also mentioned as another important principle of information security by previous researchs (Chang and Lin, 2007, p. 444; Harris, 2013, p. 298; Kanday, 2012, p. 302). Accountability is holding employees fully accountable for their conduct related to information security (Chang and Lin, 2007, p. 444). Accountability is tracked by recording user, system, and application activities, is done through auditing functions and mechanisms within an operating system or

application (Harris, 2013, p. 248).

Research hypotheses are defined as follows;

H1: There is a meaningful relationship between organizational culture and the perception of information security.

H1a: There is a meaningful relationship between organizational culture and the perception of confidentiality principle of information security.

H1b: There is a meaningful relationship between organizational culture and the perception of integrity principle of information security.

H1c: There is a meaningful relationship between organizational culture and the perception of availability principle of information security.

H1d: There is a meaningful relationship between organizational culture and the perception of accountability principle of information security.

2. Method

The study was conducted on academicians working in the government universities in Turkey. The data was collected from 3,023 academicians of 106 government universities in Turkey via survey method between 19.01.2016 and 21.04.2016. For measuring organizational culture, the Organizational Culture Assessment Instrument (OCAI) developed by Cameron and Quinn (2006, pp. 26-28) was utilized. For the scale of the perception of information security, reliable questionnaire developed by Chang and Lin (2007, pp. 457-458) was used. The respondents were supposed to answer 24 questions for OCAI and 19 questions for the perception of information security questionnaire, both based on a five point Likert scale between strongly disagree and strongly agree. In data analysis phase, SPSS 21 package program was used.

3. Findings

Reliability statistics (Cronbach's Alpha) for the CVF culture types and the perception of the principles of information security were greater than 0.7 that suggested that measurement model exhibited adequate reliability. According to the findings of the research, in overall cultural profile of the government universities in Turkey it was concluded that hierarchy was dominant culture and the perception level of availability was greater than other principles' perception of information security. Moreover, in between the Cameron-Freeman organizational culture types (hierarchy, market, clan and adhocracy) and the academicians' perception of information security based on the principles of information security (confidentiality, integrity, availability and accountability), positive and statistically significant relationship was observed by the Pearson correlation coefficients (r) between 0.450 to 0.561 at significance level $p<0.01$. According to the result of Pearson Correlation Analysis, H1a, H1b, H1c, H1d and therefore H1 hypotheses were accepted.

4. Discussion

The hierarchy has been dominated in general cultural profile of the government universities in Turkey. The dominance of hierarchy cultures should be meaningfully addressed when universities in the research are thought to be government institutions dominating the formal processes of formal rules, policies, procedures, understandable

definitions and tasks. In addition, it has been observed that market culture in universities take a significant place after the hierarchy culture. This can be explained in terms of result orientation with the strategy of achieving the advantages in the competitive environment in higher education. When common aspects of hierarchy and market cultures are evaluated together, the general cultural profile of the government universities can be defined with a sense of mechanical processes.

When the academicians' perception of information security is evaluated, the perception level of availability principle has been greater than other principles' perception of information security. This is a general indication of the academicians' perception that information systems in universities are open to access by students, staff, other researchers and trainers over the Internet and Intranets.

Preconscious assumptions that form the basis of organizational culture also shape the employees' perception of information security. In support of this, meaningful relationship has been found between the culture types possessed by government universities in Turkey and the academicians' perception of information security.

Findings in the current research are meaningful in terms of defining the general cultural profile of the government universities in Turkey, revealing the academicians' perception level of information security based on the principles of information security and determining the relationship between the organizational culture types and the academicians' perception of information security. It is envisaged that these findings will also be meaningful for other organizations except for the government universities. From this point of view, it is hoped that the employees' perception level of information security and the relationship between organizational culture and the perception of information security will contribute to the establishment of awareness of information security in the direction of long-term information security strategies.