Geliş Tarihi:26.03.2018 Doi: 10.18026/cbayarsos.439489 Kabul Tarihi:22.06.2018

SİBER UZAYDA YETERİNCE GÜVENLİ DAVRANIYOR MUYUZ? İSTANBUL İLİNDE YÜRÜTÜLEN NİCEL BİR ARAŞTIRMA

A. Naci ÜNAL[1]
Ahu ERGEN[2]

ÖZ

Siber uzay ortamı; bankacılık, sulama, enerji üretimi, ulaşım finans, sağlık, haberleşme, ulusal savunma sistemleri gibi farklı alanlarda oluşturulan ve yayılan bilgi yığınlarından oluşmaktadır. Böylesine etkili bir ortamda yer alan bilgiyi her tür etkiden koruyabilmek ve sürdürülebilirliğini sağlamak önemli bir problem olarak karşımıza çıkmaktadır. Bu problemin çözümü ise "Siber Güvenlik"ten geçmektedir. Bu çalışma ile bireylerin, siber uzay ortamında gerçekleştirdikleri faaliyetler esnasında siber güvenlikle ilgili davranışları ölçülmüştür. Araştırmada kolayda örnekleme yöntemi kullanılmış, İstanbul'da yaşayan 18 yaş ve üzeri 335 bireyden internet ortamında anket yoluyla veriler toplanmıştır. Siber güvenlik davranışının demografik faktörlere göre farklılaşıp farklılaşmadığı T-Test ve ANOVA ile analiz edilmiştir. Kadınların yazılım güncelleme sıklığının erkeklerden yüksek olduğu, özel sektör çalışanlarında cihaz güvenliği davranışı sıklığının kamu çalışanlarından yüksek olduğu, internette geçirilen süre arttıkça pro-aktif farkındalık sıklığının arttığı görülmüştür. Sonraki çalışmalarda bireylerin siber güvenlik davranışına neden olan ve bu davranışa engel olan faktörlerin araştırılması önerilmektedir.

Anahtar Kelimeler: *Siber Uzay, Siber Güvenlik, Siber Güvenlik Davranışı, Siber Güvenlik Farkındalığı*

CYBER SECURITY BEHAVIOUR: A RESEARCH CONDUCTED IN ISTANBUL

ABSTRACT

Cyber space consists of huge data stemming and spreading from different areas such as banking systems, energy production, watering systems, transportation systems, finance systems, health care systems, communications systems and national security systems. It poses a critical issue to sustain and protect such big data from various effects. The solution to this problem lies in the so-called "cyber security". This study is about the cyber security behavior of individuals

[1] Bahçeşehir Üniversitesi, Mühendislik Fakültesi, Dr. Öğr. Üyesi,
mail: ahmetnaci.unal@vs.bau.edu.tr
[2] Bahçeşehir Üniversitesi, Meslek Yüksekokulu, Doç. Dr. Ahu Ergen,
mail: ahu.ergen@vs.bau.edu.tr

involved in cyber space activities. Data is collected via online survey from 335 individuals in Istanbul through convenience sampling. T-test and ANOVA technics are used to investigate potential differences based on demographic variables. The findings show that women update their software more often than men. Private sector employees display more device security behavior than public sector employees. The study also demonstrates that proactive awareness increases along with the time spent on internet. Future researchers are recommended to investigate potential factors promoting and preventing cyber security behavior.

Keywords: *Cyber space, Cyber security, Cyber security behavior, Cyber security awareness*

Giriş

DARPA (Defense Advanced Research Projects Agency - İleri Savunma Araştırma Projeleri Ajansı) tarafından geliştirilen internet 1990'lı yılların başında ticari amaçlı olarak kullanılmaya başlanmıştır. 2017 yılı verilerine göre internet; 3.885.567.619 kişi tarafından aktif olarak kullanılmaktadır. Bu sayı tüm dünya nüfusunun % 51,7'sine eşittir (Internetworldstats, 2018). İnternet ortamının; sanal oluşuna rağmen, bu ortamda yapılan faaliyetlerin sonuçları fizikseldir. Fiziksel ortamla sanal ortamın etkileşiminde bağlantı noktaları insanlar tarafından sağlanmamakta, erişimlerin çoğu bilgi sistemlerine bağlı çeşitli sensörler tarafından gerçekleştirilmekte ve yönetilmektedir. Giderek büyüyen etki alanından dolayı önceleri "sanal ortam" ya da "siber dünya" olarak isimlendirilen internet ortamı artık "siber uzay" olarak adlandırılmaktadır. Siber Uzay; Amerika Birleşik Devletleri Savunma Bakanlığı Askeri Terimler Sözlüğü (Department of Defense Dictionary of Military and Associated Terms) dokümanında "internet, iletişim ağları, bilgisayar sistemleri, gömülü işlemciler ve denetleyiciler de dâhil olmak üzere bilgi teknolojisi altyapılarının birbirlerine bağlı olduğu ağdan oluşan küresel bir ortam" ya da "Uluslararası Telekomünikasyon Birliği (International Telecommunication Union-ITU) tarafından "bilgisayar ağları üzerinden iletişimi sağlayan ortam" olarak tanımlanmaktadır. ABD Silahlı Kuvvetleri; Siber Uzay Operasyonları Konsept Kabiliyet Planı 2016-2028 isimli resmi yayınında siber uzay; hava, kara, deniz ve uzaydan oluşan dört boyuta ilave beşinci boyut olarak adlandırılmaktadır. Bu beş boyutun her birinin birbirlerinden bağımsız olduğu, ancak siber uzay düğümlerinin (bağlantı

noktalarının) her bir boyutla irtibatlı olduğu da ayrıca belirtilmektedir.

Siber uzay ortamının mevcudiyetini her tür etkiden koruyabilmek ve sürdürülebilirliğini sağlamak da büyük bir problem olarak karşımıza çıkmaktadır. Bu problemin çözüm yolu ise ITU tarafından; siber çevre, organizasyonlar ve kullanıcının varlıklarını korumak için kullanılabilir araçlar, politikalar, güvenlik konseptleri, güvenlik önlemleri, kurallar, risk yönetimi, eylemler, eğitimler, uygulamalar ile teknolojiler bütünü" olarak tanımlanan "Siber Güvenlik" kavramıdır. Siber güvenlikle hedeflenen; Türk Dil Kurumu Büyük Türkçe Sözlüğü'nde "Kurallardan yararlanarak kişinin veriye yönelttiği anlam" şeklinde tanımlanan "bilgi"nin korunmasıdır. 21.yy'da "bilginin" sahip olduğu önem göz önüne alındığında; birey, toplum ve hatta ülkeler bazında kullanılmakta olan bilişim sistemlerinde karşılaşılabilecek sorunların büyük bir kaosa sebep olması olasıdır. Bu kaosa sebep olabilecek ve ülkeler bazında (birbirlerine göre bazı farklılıklar gösterse de) olmazsa olmaz bazı oluşumlar "Kritik Altyapılar" olarak adlandırılmıştır.

Türkiye'de de Kritik Altyapılar; "işlediği bilginin gizliliği, bütünlüğü veya erişebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapıları" ifade eder şeklinde Resmi Gazete'de yayımlanarak yürürlüğe giren "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" dokümanında yer almaktadır (Resmi Gazete, 2018). Kritik Altyapı kavramı ülkeden ülkeye farklılıklar gösterse de değişmeyen tek faktör, bu yapıda bulunan sistemlerin neredeyse tamamının siber güvenlik ihtiyacının olmasıdır. Bu kapsamda siber güvenlik; siber uzay ortamında, güvenlik risklerine karşı, kuruluşun ve kullanıcı varlıklarının ele geçirilmesinin önlenmesine ve korunmasına gayret eder. Genel siber güvenlik hedefleri erişilebilirlik, bütünlük ve gizlilik olmak üzere üç temel yapıda incelenebilir (ITU-T Rec., 2008). Erişilebilirlik; bilgi ve bilgi sistemlerinin yetkisiz bozulmalara karşı korunması anlamına gelir. Kısaca, bilgi ve bilgi sistemlerine zamanında ve güvenilir bir şekilde erişilmesini sağlamaktır. Bütünlük; bilgilerin yetkisiz modifikasyon veya imhadan korunması anlamına gelir. Bilgi ve bilgi sistemlerinin doğru, tam ve bozulmamış olmasını sağlamaktır. Gizlilik ise; bilginin yetkisiz erişime veya açıklanmaya karşı korunması anlamına gelir. Bilgiye erişme hakkına sahip olanların bunu yapabilmelerini sağlarken, yetkilendirilmemiş kişilerin bunu yapmalarını engeller (Security 101, 2018).

Türkiye'de internete erişim ve bilgisayar kullanım oranları geçmiş yıllarla karşılaştırıldığında artış eğilimindedir. Türkiye'deki girişimlerde internet erişimi % 95,9, bilgisayar kullanımı %97,2'dir. Hanelerde internet erişimi %80,7, bilgisayar kullanımı ise %56,6'dır (TÜİK, 2018). Bu yüksek oranlar Türkiye'de siber güvenlik konusunun gerek literatürde, gerekse uygulamada farklı boyutlarıyla araştırılmasını gerektirmektedir.

Bu çalışmada; bireylerin, siber uzay ortamında gerçekleştirdikleri faaliyetler esnasında siber güvenlikle ilgili davranışlarının ölçülmesi amaçlanmıştır.

1. Literatür Tarama

1.1 Siber güvenlik

İş yerlerindeki teknolojik gelişmeler çalışanların her zaman her yerden bilgiye ulaşmasına, çok sayıda mekânda çok sayıda cihazdan çalışmalarına olanak sağlamakta, böylelikle bireysel verimlilik ve iş süreçlerinin etkililiği artmaktadır. İşletmeler bu nedenle çalışanlarına uzaktan erişim ve bulut temelli depolama, taşınabilir bilgisayar, tablet ve mobil telefonlar sağlamaktadır. Ne var ki, yeni teknolojilerin benimsenmesi aynı zamanda siber tehditlerden kaynaklı riskleri de artırmaktadır (Blythe, 2013). Örneğin, 1986 yılında sadece bir bilgisayar virüsü varken, 2008 itibariyle yaklaşık 60,000 virüs tespit edilmiştir (Shih vd, 2008:478). Günümüzde ise virüs sayısından çok, zararlı yazılımların sebep olduğu sorunlar ön plâna çıkmaktadır. ESET tarafından yayınlanan 2015 Siber Güvenlik Raporuna göre Asyalı online kullanıcıların %93'ünün online güvenlik sorunlarının farkında olmalarına rağmen sadece %40'ının temel siber güvenlik sorunlarına doğru cevaplar bulabildiği görülmektedir. Ayrıca bu bölgedeki kullanıcıların %38'i tehlikesini bildikleri halde riskli online davranışlar sergilemektedirler (Muniandy vd; 2017:10).

Siber tehditlerin varlığı, siber güvenlik kavramını gündeme getirmektedir. Siber güvenlik, "küresel olarak birbirine bağlı elektronik verilerin veya ekipmanların, kriminal amaçlarla, yetkisiz veya kazayla kullanımına karşı korunması ve bu korumayı sağlamak için gereken teknoloji ve süreçler" şeklinde tanımlanmaktadır. İnsanları siber uzayda güvende tutacak tek bir davranış olmadığı gibi, siber güvenlik; çoklu, birbiriyle ilişkili ve pek çok faktörden etkilenebilecek davranışlar gerektirmektedir. Örneğin, bir kullanıcıyı güçlü bir parola kullanması konusunda harekete geçiren güdü, bir e-dolandırıcılık (oltalama) linkini takip etmesini etkileyen güdüden çok farklı olabilmektedir (Coventry vd, 2014). Siber güvenlik kavramı sıklıkla bilgi güvenliği yerine de kullanılmaktadır. Her ne kadar

kavramlar arasında bir benzerlik olsa da, siber güvenlik geleneksel bilgi güvenliğinin ötesinde olup, sadece bilgi kaynaklarının korunmasını değil bireylerin kendilerini ve diğer varlıkları korumasını da içeren daha kapsamlı bir kavramdır. Bilgi güvenliğinde insan faktörüne, süreçteki güvenliği sağlama rolü nedeniyle atıfta bulunulurken, siber güvenlikte insan siber saldırıların hedefi veya bilmeden bir parçası boyutuyla yer almaktadır (Von Solms ve Niekerk, 2013:97). İnsan davranışlarını istismar eden siber güvenlik tehditleri sürekli evrim geçirirken, bir çok bilgi güvenliği ihlalinde "insan" en önemli faktör olarak ortaya çıkmaktadır. Azımsanmayacak oranda güvenlik açığı (parola paylaşımı, bilinmeyen e-postaların ve eklerin açılması, vb.) işletme içi çalışanlardan kaynaklanmaktadır. Bu tür davranışlar işletmeyi, bilgisayar korsanlarına karşı savunmasız bırakabilir ve işletme varlıklarını tehditlere karşı açık hale getirebilir (Abawajy, 2014). İnternet bir çok faydasının yanında, kullanıcılar açısından bir çok riski de barındırmaktadır. Bu riskler; bazen maddi, bazen de doğrudan fiziksel ve ruhsal sorunlara yol açabilmektedir. Araştırmalar incelendiğinde internet kullanıcılarının genel olarak zararlı yazılımlar ile ilgili güvenlik önlemlerinin farkında olduğunu, ancak internet üzerinden oluşabilecek tehlikeler hakkında farkındalıklarının yetersiz olduğunu göstermektedir (Erol vd; 2015).

1.2 Siber güvenlik farkındalığı

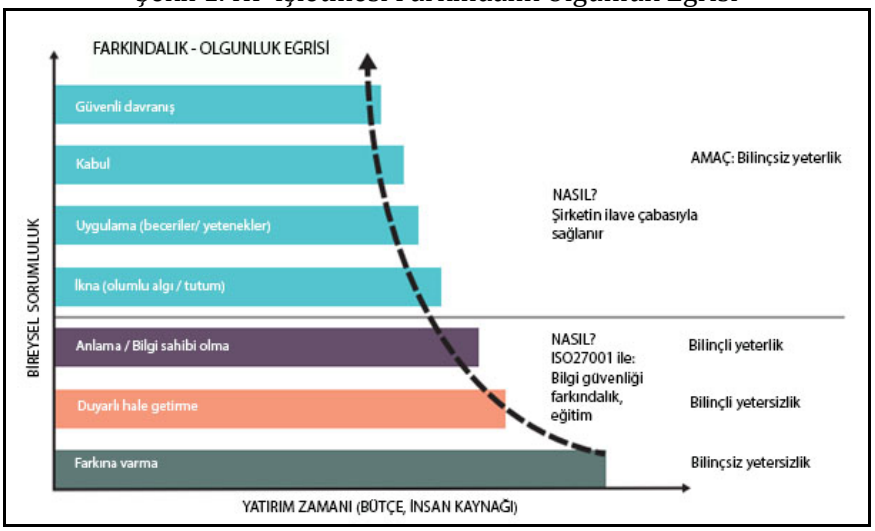
Siber saldırılara karşı gelebilmek için siber güvenlik farkındalığı her geçen gün önem kazanmaktadır. İşletim sistemleri ve programları günümüzde çok daha korumalı hale getirildiğinden, siber saldırganlar dikkatlerini insan faktörüne yöneltmeye başlamıştır. Abawajy'in (2014) son kullanıcıların bilgi güvenliği farkındalığını ve davranışını iyileştirmek için kullanılan çeşitli yöntemleri değerlendirdiği araştırmasında öne çıkan yöntemler, web tabanlı eğitim materyalleri, içeriksel eğitimler ve gömülü eğitimlerdir. Eminağaoğlu vd. (2009)'a göre de bilgi güvenliği risklerine karşı koymada etkili ve güçlü mekanizmalar eğitim ve farkındalıktır. Eğitimlere ilaveten uzun soluklu, süreklilik arz eden farkındalık kampanyaları düzenlenmelidir. Çünkü insanlar eğitimde öğrendikleri konseptleri zamanla unutmaktadırlar. Kullanıcılara eğitimin yanı sıra posterler, broşürler, animasyon filmler, animasyonlu elektronik mesajlar, ödüllü çevrimiçi yarışmalar gibi etkili ve verimli farkındalık materyalleri sağlanmalıdır. Bu materyaller uzmanlar tarafından çalışanlar için kullanıcı dostu ve cezbedici şekilde tasarlanmalıdır. Görsel malzemeler kısa, ilgi çekici,

eğlenceli, animasyon ve karikatürlerle zenginleştirilmiş olmalıdır. Uzun, kapsamlı ve resmi dille yazılmış rapor ve makaleler yerine, kısa cümleler içerecek sloganlar şeklinde hazırlanmalıdır. Bu tür materyaller içinde etkileşimli, bilgisayar temelli eğitimlere en güzel örnek olarak video oyunları verilebilir. Bu alanda iki tür oyun mevcuttur: insan etkileşimli oyunlar ve kaynak yönetimi simülasyonları. Kişiye siber saldırıyı konu alan oyunlarda kişi, düşmanla veya bir sorunla karşı karşıya kalmakta ve doğru eylemi yerine getiremezse ceza almaktadır. Kaynak yönetimi simülasyonlarında ise oyuncu sanal bir ortamı, sınırlı kaynakları kullanarak yönetmektedir. Oyunlar ve simülasyonlar her geçen gün etkili öğrenme araçları olarak kabul edilmeye başlanmıştır (Cone vd, 2009). Unutulmaması gereken nokta şudur ki bilgi güvenliğinin farkındalığı sağlanırken bunun çalışanlar için sıkıcı bir iş ya da yeni bir işyükü olarak algılanmasına engel olunmalı, iletişimi kolay, hızlı ve anlaşılır olmalıdır (Eminağaoğlu vd; 2009).

Ünver (2015) ise siber güvenlik bilincinin oluşması için şu önerileri sunmaktadır: *"Bilgi güvenliğine ilişkin eğitimlere ilkokuldan itibaren başlanmalı ve öğrencinin tüm eğitim hayatı boyunca ilgili dersler içinde konunun yer alması sağlanmalıdır. Yapılacak bir "Ulusal Siber Güvenlik Eğitimi" programıyla yerel yönetimler ve il özel idareleri marifetiyle tüm vatandaşlara eğitimler verilmeli ve "Siber Vatandaş" bilinci oluşturulmalıdır. Belirli bir süre için uygun görülecek bir ay "Ulusal Siber Güvenlik Ayı" olarak belirlenmeli ve bir ay boyunca yurdun her köşesinde konuyla ilgili farklı yaş gruplarına ve farklı kesimlerine yönelik etkinlikler düzenlenmeli ve medyanın konuyu halka duyurması sağlanmalıdır. Ulusal seviyede tatbikatlar sürdürülmeli, kurumların kendi bünyelerinde yapacakları tatbikatlara destek verilmelidir. Bilgi güvenliği farkındalığının ölçümü yapılmalı ve bu ölçüm sonuçları değerlendirilerek yeni programlar geliştirilmelidir. Tüm bu öneriler hazırlanacak olan bir "Ulusal Farkındalık Programı" çerçevesinde bütüncül bir yaklaşımla yapılmalıdır"*. Bada ve Sasse'ye göre (2014) siber güvenlik farkındalık kampanyaları profesyonelce hazırlanmalı ve etki yaratacak şekilde organize edilmelidir. İnsanlara korku aşılamak etkili bir iletişim taktiği değildir. Korku; insanların savsaklamasına, konuyu zihinlerinde geriye atmalarına, ertelemelerine neden olur. Güvenlik riskleri abartılmamalıdır. Tek başına farkındalık yeterli değildir. Bu sadece dikkat çekmeye yarar. Güvenlik eğitimi insanlara bilgi sağlamaktan çok daha fazlası olmalıdır. Hedefi olmalıdır, yapılabilir olmalıdır. Gerçekten doğru olan davranış zor ve karmaşıktır. Basit ve tutarlı, insanların kolay

takip edebileceği kurallara ihtiyaç vardır. İnsanlar davranış değişikliğine yöneldiğinde, eğitim ve geri bildirimlerle değişim sürecinde sürdürülebilirliği sağlamak gerekmektedir. Diğer yandan etkili bir güvenlik farkındalığı programı oluşturmanın kestirme bir yolu bulunmamaktadır. Her şirket öncelikle çalışanlarının benimsemesini istediği, kendine özgü güvenlik kültürünü tanımlamalıdır. Eğer bu yönde görünür bir çaba sağlanmıyorsa, çalışanlar şirketin güvenlik konusunda ciddi olmadığını düşünmeye başlarlar. Bu nedenle, yeni bir düşünme biçimine ihtiyaç vardır. Kısacası, durağan ve klasik bilgisayar temelli bilgi güvenliği eğitim paketleri çalışanlar üzerinde çok az etki yaratmaktadır. Etki yaratabilmek için güvenlik eğitimi her işin kendi doğasına uygun olarak, kendi bağlamında hazırlanmalı ve belirli güvenlik ihtiyaçlarını karşılamalı, çalışanlara verilmesi hedeflenen temel mesajlar düzenli aralıklarla hatırlatılmalıdır. Çoğu şirket siber güvenlik konusuna sadece ISO standartlarının önerdiği ölçüde yatırım yapmaktadır. Oysa kurum içinde siber güvenlik farkındalığının oluşabilmesi için daha fazla adıma ihtiyaç vardır.

Şekil 1. HP İşletmesi Farkındalık Olgunluk Eğrisi



Kaynak: Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, M. A., & Passingham, N. (2015). Awareness is only the first step. A framework for progressive engagement of staff in cyber security, Hewlett Packard, Business white paper.

Şekil 1'de HP firmasının farkındalık olgunluk eğrisi yer almaktadır. Bu eğri üzerinde siber güvenlik davranışına giden yolda adım adım hangi aşamaların gerçekleşmesi gerektiği özetlenmiştir.

Güvenlik davranışını değiştirmek için bir şirketin çalışanlarının güvenlikle ilgili bilgi ve becerilerine yatırım yapması gerektiği vurgulanmaktadır. En üst seviye olan "güvenli davranışa" ulaşmak bir anda olamayacaktır. Amaca yönelik her adım için farklı faaliyetler gerekmektedir. Etkili farkındalık (eğrideki "farkına varma" ve "duyarlı hale getirme" basamakları), farklı kanallardan tutarlı ve sürekli iletişim yapmayı gerektirmektedir. Bilgisayar temelli bir eğitim ile verilecek mesajlar, tutarlı ve anlaşılır ifadelerden oluşan posterler ve basılı malzemelerle desteklenmelidir. Bu iletişim faaliyetlerinin amacı çalışanda "bilinçsiz bir yeterlik" (farkında olmadan yeterliği kazanıp uygulamak) yaratmaktır. Yani, çalışanları siber güvenlik tehditlerine ve önlemlerine yeterince hazırlanmış hale getirmektir. Eğrinin en altındaki "bilinçsiz yetersizlik" ifadesi ise bunun tam tersi olup, bilgi ve beceri transferi eksikliğinden kaynaklı yetersizlik anlamına gelmektedir. Eğrinin "anlama" ve "ikna" adımları için şirketin tepe yönetimi konuya canı gönülden müdahil olmalıdır. Çalışanın motivasyonu yönetimle etkileşiminin bir sonucudur. "Uygulama" aşamasında, duygusal boyut öne çıkmaktadır. Güvenlik rolleri tayin edilerek çalışanların şirketin güvenliği için kişisel bir sorumluluk duygusu geliştirmesi sağlanabilir. Eğrideki son iki adım olan "kabul" ve "güvenli davranış" ise çalışanların özverileri ve şirkete olan bağlılıklarına, kazandıkları siber güvenlik becerilerini zaman içinde kullanmaya yönelik istekliliklerine dayanmaktadır (Beyer vd, 2015).

1.3 Siber Güvenlik Davranışı

Bir çok şirkette, güvenlik konuları ile ilgili farkındalık üst düzey yöneticiler arasında artmaktadır, ne var ki halen fazlaca reaktif düzeydedir. Daha pro-aktif bir bakış açısı, baş gösteren sorunlara çözüm için daha yararlı olacaktır. Farkındalık ilk adımı oluşturmaktadır. Çalışanların güvenlik davranışını yönetmek halen büyük bir zorluktur. Dow Kimyasalları güvenlik yöneticisi Theresa Jones "En büyük zorluk davranışları değiştirmektir. Dow çalışanlarının davranışlarını değiştirebilseydim güvenlik sorununu sanırım çözmüştüm" şeklinde bir demeç vermiş (Johnson ve Goetz, 2007), siber güvenliği sağlamada insan davranışlarını değiştirmenin zorluğuna vurgu yapmıştır. Bu noktada şirket yöneticileri; olası bilgi güvenliği açıkları ve tehditlerin şirkete nasıl zarar verebileceğini, mahrem bilginin ifşasına nasıl yol açabileceğini çalışanlara açıkça iletmelidir. Çalışanları bilgi güvenliği konusunda güncel tutmak ve onların bilgilerini artırmak siber güvenlik davranışları üzerinde etkili olacaktır. Bilgi güvenliği açıklarına yönelik, bilgi güvenliği politikaları

ve prosedürlerini geliştirmek diğer bir etkili yaklaşımdır. Bilgi güvenliği politika ve prosedürleri tüm çalışanlar için açık, kısa, kestirme ve kolay olmalıdır (Safa vd, 2015). Diğer yandan, sorumluluk, güven, iletişim ve işbirliği, güvenlik kültürünün önemli dört ayağıdır. Bu nedenle, çalışanların kurumsal güvenlik konusunda aktif rol oynamaları için onları motive edecek bir yaklaşım geliştirmek gerekmektedir. Çalışanlar neyi koruyacaklarını, neden koruyacaklarını, şirketin bu konuda kendilerine nasıl yardımcı olacağını bilmelidir (Beyer vd, 2015).

Siber güvenlikte en zayıf halka: İnsan

Zayıf güvenlik davranışlarının olası sebepleri oldukça geniş bir konudur. Yeterli bilgi ve beceriye sahip olmamak pek çok sebepten sadece bir tanesidir. İnsan davranışını etkileyen çok sayıda faktör mevcut olup bunlar sosyal bilimler literatüründe farklı davranış teorileri ile açıklanmaktadır (Coventry vd, 2014). Literatürde bilgi güvenliği ve bilgi güvenliği yönetim sistemleri konularının sıklıkla araştırıldığı, bilgi güvenliğinin "en zayıf halkası" olarak insan faktörünün görüldüğü ve insanı bilinçlendirme üzerinde durulduğu görülmektedir (Güldüren vd; 2016:693). Her ne kadar pek çok çalışmada "insan" en zayıf halka olarak görülüyor olsa da bu alandaki araştırmalar henüz dağınıktır. Teorik temel oluşturma ve davranışsal eğilimleri ampirik olarak ölçmeye yönelik araştırmalar az sayıdadır (Blythe, 2013). Siber güvenliğin insan boyutunu anlamak için genel olarak insan davranışını etkileyen faktörlerin ve siber güvenlik davranışının anlaşılması gereklidir. Bu durum çalışanların davranışlarını etkileyen faktörlere yönelik daha fazla araştırma gerektirmektedir (Ng vd, 2009:824).

İnsanların neden güvenli siber davranışlar göstermediği üzerine yapılan kapsamlı bir araştırmanın bulgularına göre sebepler aşağıda özetlenmiştir (Coventry vd, 2014):

(i) Her an internete bağlı olmak; hem bir alışkanlık, hem de bir beklenti haline gelmiştir. Bu her yerden ve her zaman bağlı olma ihtiyacı güvenilir olmayan bağlantı riskine neden olmaktadır.

(ii) İnsanlar "katılıyorum" tuşuna basmaya ve uyarı mesajları almaya alışkın hale gelmişlerdir. Neyi kabul ettiklerini okumamakta veya davranışlarının sonuçlarını düşünmeden, doğrudan ilgili alana basmaktadırlar. Her zaman rasyonel, düşünerek hareket etmemektedirler.

(iii) Kolay yolu seçme eğilimi güvenliğe karşı her zaman galip gelmektedir.

(iv) Çekicilik (bağlı olma isteği, müzik, video, uygulama indirme, paylaşımda bulunmanın çekiciliği gibi) güvenliğe karşı galip gelmektedir.

(v) Finansal maliyetler (güvenlik yazılımları ile yazılım güncellemelerinin pahalı olması) her zaman güvenlik kazançlarını karşılamamaktadır.

(vi) Güvenli olmayan davranışlarda bulunma isteği (anlık kazancın, eğlencenin ve zevkin; soyut ve gelecekte oluşabilecek bir riske karşı galip gelmesi gibi), güvenlik risklerini göz ardı etmeye neden olabilmektedir.

(vii) Farklı araçların nasıl kullanıldığını anlamak, güncel kalmak, doğru giriş yapmak, parolaları hatırlamak fazlaca çaba sarfetmeyi gerektirmektedir.

(viii) Algılanan faydanın noksanlığı (davranış değişikliğiyle güvenliğin sağlanamayacağına yönelik inanç).

(ix) Risk algısının noksanlığı (saldırı olmayacağını düşünerek ya da kişisel bilgilerinin çok da değerli ve önemli olmadığını düşünerek kısa bir süreliğine güvensiz bir şekilde bağlanmak).

(x) Değişim ihtiyacını algılamamak ve kurallara uyulmadığında olumsuz sonuçlarla karşılaşılacağına dair inancın olmaması. Örneğin, bir insan interneti çok uzun süre sorun yaşamadan kullanırsa, riske maruz kalacağına daha az inanmaktadır.

(xi) Hile ve dolandırıcılığı tespit edebilecek beceri ve neyi, nasıl yapmak gerektiğine dair bilgi eksikliği.

(xii) Hangi bilgiye güvenileceğini bilmemek (kimler güvenilir kaynaklardır, çelişkili tavsiyelerde bulunulduğunda kime inanılacağını bilmemek).

(xiii) Siber uzayda meşgulken, dikkat başka noktaya yönelmişken, güvenli davranmayı unutmak.

(xiv) Görgü kuralı engeli (parolaları, bilgiyi, cihazları paylaşmak bir nevi güven ve samimiyet göstergesidir).

(xv) Yanlış ve eksik zihinsel modeller (kullanıcıların kendi davranışları, güvenlik riskleri ve hangi açılardan tehditlere açık oldukları konularında net fikirlerinin olmaması).

(xvi) Düşük duyarlılık düzeyi (duyarlı olmak güvenli davranışa yol açar ve tehditlere açık olduğuna inanan bireyler güvenli davranışlar sergilemeye daha meyillidirler).

(xvii) Siber saldırganların korku ve tehditi kullanarak güvensiz davranışlara sebep olması (örneğin bir e-dolandırıcı, kişinin para veya siteye giriş hakkının kaybolacağına onu inandırarak, kullanıcının hemen cevap vermesini isteyebilir).

(xviii) Güvenlik tehditlerini anlama ve bu tehditlere tepki verme konusunda kendini olduğundan daha yetenekli görmek.

(xix) Güvenlikle ilgili sorumluluklarını kendisinden daha bilgili olduğunu düşündüğü kişilere delege etmek.

Ponemon Institute tarafından yayınlanan bir raporda ise kurumların %78'inden fazlasının son iki yıl içinde en az bir veri ihlali sorunu yaşadıkları ve bu kurumların sadece %8'inin veri ihlallerinin ana nedenini dış kaynaklı olarak gösterdiği belirtilmiştir. Aynı raporda, çalışanların mobil cihaz kullanımının iyi yönetilmemesinin çok önemli bir sorun olduğu ve çalışanların veri taşıyan mobil cihazlarını kaybettiklerinde kurumlarını bilgilendirmedikleri tespitinde de bulunulmaktadır (Ünver, 2015).

Siber uzayda güvenli davranışlar

Arachilage ve Love (2014) bilgisayar kullanıcılarının; e-dolandırıcılık saldırılarına karşı gelebilmeleri için gereken bilgi seviyelerini araştırdığı çalışmalarında, kavramsal ve prosedürel bilginin, kullanıcının e-dolandırıcılık tehditinden kaçınma davranışını güçlendiren, öz-yeterliliğini olumlu yönde etkileyen bir faktör olduğu sonucuna ulaşmıştır. Coventry vd. (2014)'e göre herkesin bilmesi ve takip etmesi gereken on siber güvenlik davranışı şunlardır:

(i) Güçlü parolalar kullanmak ve onları güvenli şekilde yönetmek

(ii) Anti virüs yazılımları ve güvenlik duvarı kullanmak

(iii) Her zaman anti virüs yazılımlarının en son sürümünü kullanmak

(iv) Web sayfasındaki işlemi bitirdikten sonra siteden çıkmak ve bilgisayarı kapatmak

(v) Sadece güvenilir bağlantıları, bilgisayarları ve cihazları kullanmak (Wi-Fi de dahil)

(vi) Riskler hakkında bilgi sahibi olmak ve oltalama tuzakları ile siber sahtekarlıklardan kaçınmaya çalışmak

(vii) Sadece güvenilir, güvenli siteler ve hizmetler kullanmak

(viii) Her türlü çevrimiçi etkileşimde minimum düzeyde kişisel bilgi vermek ve kimliği gizli tutmak

(ix) İnternete bağlıyken fiziksel çevreye dikkat etmek

(x) Siber suçları ve suçluları ilgili yerlere raporlamak

Anward vd. (2017:442) beyan edilen siber güvenlik davranışının ölçümünde dört farklı araştırmacının çalışmalarından ((Vance et al. (2012), Shih et al. (2008), Davinson and Sillence

(2010), ve Ng et al. (2009)) uyarladıkları şu soruları kullanmışlardır: "Farklı sosyal medya hesaplarım için farklı parolalar kullanırım", "Sosyal medya sitelerimde genellikle gizlilik/güvenlik ayarlarını gözden geçiririm", "Bilgisayarımdaki anti-virüs yazılımını güncel tutarım", "Sıradışı bilgisayar hareketlerini takip ederim (örneğin bilgisayarın yavaşlaması veya donması, pop-up pencerelerin açılması), "Tanımadığım insanlardan gelen e-posta dosyalarını açmam", "Hassas bilgileri asla e-posta veya sosyal medya yoluyla göndermem (hesap numarası, parola vb.)", "Bilgisayarımdaki önemli dosyaların yedeğini alırım", "Aldığım kötü amaçlı yazılım uyarılarına karşı her zaman harekete geçerim", "Sosyal medya sitelerinden gelen tanımadığım kısa URL'lere, nereden geldiğini bilmiyorsam tıklamam". Muniandy vd. (2017:1-9) ise Malezya'da yüksek öğrenim gören gençlerin siber güvenlik davranışlarını, parola kullanımı, yemleme, sosyal mühendislik, online dolandırıcılık ve kötü amaçlı yazılım boyutlarından oluşan ölçek yardımıyla ölçmüşlerdir. Bulgulara göre cevaplayıcıların tüm boyutlarda savunmasız oldukları ve davranışlarının siber güvenlik tehditlerine maruz kalmayı olası hale getirdiği görülmüştür.

Siber güvenlik davranışıyla ilişkili faktörler

Hoy ve Milne'nin (2010:41-42) 18-24 yaş arası A.B.D'de yaşayan bireylerin Facebook gizliliğine yönelik farkındalık, inanç ve davranışlarının incelendiği araştırmada, kadınların sosyal ağlarda kişisel verilerinin reklam amaçlı kullanımına erkeklere göre daha fazla tepki gösterdiği, her iki cinsiyetten katılımcıların yarısının verilerin nasıl kullanıldığı hakkında bilgileri olmadığı ve kadınların gizlilik konusunda koruyucu davranışları erkeklere göre daha proaktif şekilde uyguladıkları bulgularına ulaşılmıştır. Karacı vd. (2017:2079)'nin Bilgisayar Mühendisliği ile Bilgisayar ve Öğretim Teknolojileri Öğretmenliği (BÖTE) bölümlerinden 170 öğrenci ile siber güvenlik davranışlarını ölçtükleri araştırmanın bulgularına göre ise; öğrencilerin siber güvenliğe yönelik davranışlarının siber güvenliği sağlayacak düzeyde olduğu görülmektedir. Bulgulara göre öğrenciler kişisel gizliliklerini koruyabilmekte, güvenilmeyen uygulamalardan kaçınmakta ve güvenlik için önlem alabilmektedirler. Ayrıca kredi kartı veya banka kartı gibi ödeme bilgilerini koruyabilmekte ve internet üzerinde gezinirken arkalarında iz bırakmamaktadırlar. Erkek ve kızların siber güvenlik davranışları arasında anlamlı bir farklılık tespit edilmemiştir. Kişisel güvenliği koruma açısından ise BÖTE bölümünde kızların, Bilgisayar Mühendisliği bölümünde ise erkeklerin daha olumlu siber güvenlik

davranışına sahip oldukları, internet-bilgisayar güvenlik eğitimi alan veya bu konuda iş deneyimi olan öğrencilerin ise siber güvenlik davranışlarının daha olumlu olduğu görülmüştür. Güvenlik davranışıyla ilgili bir diğer araştırmanın bulgusu ise göstermektedir ki bireyler; tehditlerin gerçekleşme olasılığının (algılanan duyarlılık) ve güvenlik kontrollerinin etkililiğinin (algılanan faydalar) farkına vardıklarında, uygun önleyici davranışı gösterme konusunda bilinçli kararlar verebilmektedirler. Güvenlik farkındalığı programları kullanıcıların güvenlik tehditlerinin vereceği hasar ve olasılık hakkında eğitmeye odaklanmalıdır. Böylelikle çalışanlar, işletmenin verilerini ve diğer bilgiye dayalı varlıklarını korumada kendi rollerini ve sorumluluklarını anlayabilirler. Özellikle, güvenlik farkındalığı mesajları tasarlanırken zararın ciddiyetine ve gerçekleşme olasığına vurgu yapılması önerilmektedir (Ng vd, 2009:823).

Bilgi güvenliğine uyma davranışını iyileştirmede, çalışanların geçmiş ve otomatik davranışlarının önemine işaret eden Koruyucu Motivasyon Kuramı (KMK) ise geçmiş davranışların bireyin tehdit değerlemesini ve onlarla başa çıkma becerisini etkilediğini savunmaktadır. Bu kuram; tehditlerin nasıl algılandığını açıklayan üç faktörü içermektedir. Bunlar; ödüller ya da faydalar, tehditin ciddiyeti ve tehdite yönelik algılanan duyarlılıktır. Bu kuram aynı zamanda bireyin tehditle başa çıkma becerisini de içermektedir. Bunlar, tepkinin etkililiği (tehditi ortadan kaldırmanın algılanan faydasına yönelik inanç), tepki maliyeti (koruyucu davranışın bireye maliyeti) ve öz-yeterliliktir (bireyin koruyucu davranışı yerine getirebileceğine yönelik inanç derecesi). Neredeyse tüm KMK boyutları çalışanların bilgi güvenliği politikalarına riayet etme eğilimlerini etkilemektedir (Vance vd, 2012:190). Öte yandan, koruyucu güvenlik davranışı (güçlü bir şifre kullanma vb.) ve hastalıkları önleyici sağlık davranışları (sağlıklı bir diyet ile kalp hastalıklarından kaçınma vb.) arasında paralellik kurulabilmektedir. Her iki davranış da istenmeyen durumlara yol açabilecek önleyici ve koruyucu davranışları sergilemeyle ilgilidir. Buradan hareketle Ng vd. (2009:815-817) sağlık literatüründen uyarlanan "Sağlık İnanç Modelini" (SİM) kullanarak bilgisayar güvenlik davranışını araştırmışlardır. 134 çalışandan toplanan verilerle yürütülen araştırmada algılanan duyarlılık, algılanan fayda ve öz yeterliliğin, e-postalarla ilgili güvenlik davranışının belirleyicileri olduğu bulgusuna ulaşılmıştır. Li vd. (2016:103) ise siber güvenlik farkındalığını ve çalışanlar üzerindeki etkisini test etmek için bu kez, "Sağlık İnanç Modelini" "Koruyucu Motivasyon Kuramı" ile entegre ettikleri bir

model önererek, arkadaş davranışları arasındaki ilişkiler, harekete geçme, çalışanın siber güvenlik deneyimi, tehdit algılaması (algılanan ciddiyet, algılanan duyarlılık ve algılanan engeller), tepki algılaması (tepkinin yaratacağı fayda ve güvenlikle ilgili özyeterlilik) ve siber güvenlik davranışı arasındaki ilişkileri ortaya koymaya çalışmışlardır. Bu çalışmalarının sonucunda çalışanın iş arkadaşlarının davranışlarının ve kendisinin siber güvenlik deneyiminin, örgütteki siber güvenlik davranışını geliştirdiği görülmüştür. Arkadaş davranışı harekete geçmeyi olumlu yönde etkilemektedir. Çalışanın deneyimlerinin ise tehdit algılaması ve tepki verme üzerinde olumlu etkisi görülmüştür. Sonuç olarak, çalışanların tehdit algılamaları ve tepki algılamalarının siber güvenlik davranışı ile olumlu ilişki içinde olduğu görülmektedir (Li vd, 2016:103-104).

2. Metodoloji

Araştırmanın temel amacı; siber güvenlik davranışının demografik faktörlere göre farklılaşıp farklılaşmadığını ortaya koymaktır. Bu nedenle siber güvenlik davranışı faktörlere ayrılmış, her bir faktörün demografik değişkenlere göre farklılık gösterip göstermediği T-Test ve ANOVA ile analiz edilmiştir. Bu araştırmanın bulguları, örneklem büyüklüğü ve örnekleme yöntemi nedeniyle il ve ülke bazında genellenebilir değildir. Ne var ki, siber güvenlik davranışını ölçmeye yönelik Türkiye'de yapılmış az sayıda nicel araştırmadan biri olması sebebiyle önemlidir.

Araştırmanın ana kütlesi İstanbul'da yaşayan 18 yaş ve üzerindeki bireyler olarak belirlenmiştir. Bu araştırmada örneklem, zaman ve bütçe kısıtı nedeniyle İstanbul ilinden seçilmiştir. Araştırmada örnekleme yöntemi olarak tesadüfi olmayan örnekleme yöntemlerinden, kolayda örnekleme kullanılmıştır. %95 güven aralığında çalışılmıştır. Veri toplama için anket formu hazırlanmış, cevaplayıcılardan on-line anket ile toplanan 350 formdan, 15'i tutarsız cevaplardan dolayı elenmiş, araştırma kapsamına 335 anket dâhil edilmiştir.

Araştırma öncesi 40 örneklem ile yapılan pilot testin ardından gerekli görülen ifadeler daha anlaşılır bir dille yeniden yazılmıştır. Siber güvenlik davranışı "hiçbir zaman", "nadiren", "bazen", "sıklıkla", "her zaman" ifadelerinden oluşan 5'li sıklık ölçeği ile demografik değişkenler ise nominal ölçek kullanılarak ölçülmüştür.

Araştırmada siber güvenlik davranışını ölçmek için Egelman ve Peer'in (2015) geliştirdiği 16 soruluk SeBIS ölçeğinden faydalanılmıştır. Ölçeği geliştirdikten sonra Egelman vd. (2016) tarafından gözlenen güvenlik davranışı ve SeBIS anket sorularına verilen cevaplar arasındaki olası boşlukları tespit etmeye yönelik bir de deney gerçekleştirilmiştir. Yazarlar ankete verilen cevaplarla, gerçekleşen davranışları bu deneyle karşılaştırmışlardır. Deney sonucunda, farkındalık boyutunun "e-dolandırıcılık" davranışı ile yüksek düzeyde ilişkili olduğu, şifre oluşturma boyutu ile "kolay kırılamayan şifreler oluşturma" davranışının yüksek ilişkili olduğu bulgusuna ulaşılmıştır. Bu bulgular da SeBIS ölçeğinin güvenilir ve geçerli bir araç olarak gelecek araştırmalarda kullanılacağının bir göstergesi olarak kabul edilmektedir (Egelman vd. 2016).

3. Bulgular

Bu bölümde cevaplayıcıların sosyo-demografik özellikleri, değişkenlerin faktör ve güvenilirlik analizleri, T-test ve ANOVA bulguları yer almaktadır. Cevaplayıcıların %46,2'si kadındır. %8,4'ü 18-25, %33,1'i 26-35, %41,9'u 36-49, %16,6'sı ise 50 ve üzeri yaş aralığındadır. Yüksek lisans, doktora, tıpta uzmanlık vb. mezunu oranı %41,6, lisans mezunu oranı %47,6, önlisans mezunu oranı ise %7,8'dir. Örneklemin eğitim seviyesi Türkiye ortalamasının oldukça üzerindedir. Çalışanların %67,4'ü özel sektör çalışanı, %8'i kamu çalışanıdır. Örneklemin %33,4'ünün geliri 10000 TL ve üzeridir. %54,6'sının ise 2000-4000 TL aralığındadır (Tablo 1).

Tablo 1. Cevaplayıcıların sosyo-demografik özellikleri

	Sıklık	Yüzde		Sıklık	Yüzde
Yaş			**Meslek**		
18-25	28	8,4	Kamu Çalışanı	29	8,8
26-35	110	33,1	Özel sektör	223	67,4
36-49	139	41,9	Emekli	34	10,3
50 ve üzeri	55	16,6	Öğrenci	13	3,9
Toplam	332		Ev hanımı	8	2,4
Cinsiyet			İşsiz	17	5,1
Kadın	153	46,2	Serbest meslek	7	2,1
Erkek	178	53,8	*Toplam*	331	
Toplam	331		**Gelir**		
Eğitim			1.001TL-2.000TL	4	1,2
Master, doktora, tıpta uzmanlık vb.	138	41,6	2.001TL-4.000TL	35	10,7
Lisans	158	47,6	4.001TL-6.000TL	77	23,6
Önlisans	26	7,8	6.001TL-7.000TL	32	9,8
Lise	8	2,4	7.001TL-9000TL	69	21,2
Ortaokul	1	0,3	10000TL ve üzeri	109	33,4
Eğitimsiz	1	0,3	*Toplam*	326	
Toplam	332				

Cevaplayıcıların siber güvenlik davranışı sıklıkları Tablo 2'de yer almaktadır. Cep telefonunun kilidini açmak için bir PIN veya parola kullanımı, dizüstü bilgisayar ya da tabletin kilidini açmak için şifre (parola) kullanımı davranışları en sık yapılan iki davranıştır.

Tablo 2. Siber güvenlik davranışı sıklık ve ortalama değerlerleri.

Siber Güvenlik Davranışı	Ort.	Std. Sap.
Cep telefonumun kilidini açmak için bir PIN veya parola kullanırım.	4,28	1,382
Dizüstü bilgisayar ya da tabletimin kilidini açmak için şifre (parola) kullanırım.	4,22	1,398
Bilgisayarımı uzun süre kullanmayacaksam ekranını otomatik olarak kilitlenecek şekilde ayarlarım.	3,92	1,446
Zorunlu olmadıkça şifrelerimi (parolalarımı) değiştirmem.	3,59	1,312
Kullandığım programların güncel olduğundan emin olmaya çalışırım.	3,53	1,137
Bilgisayarımdan (her) uzaklaştığımda, bilgisayar ekranımı kendim kilitlerim.	3,43	1,453
Yeni bir internet hesabı oluşturduğumda, bu hesabın bulunduğu sitenin istediğinden daha güvenli bir şifre (parola) oluştururum.	3,24	1,208
Anti virüs yazılımımın düzenli olarak kendisini	3,22	1,297

güncellediğini takip ederim.		
Sahip olduğum farklı hesaplar için farklı şifreler kullanırım.	3,22	1,212
Zorunlu değilse, şifremde özel karakterler (., ',? vb.) kullanmam.	3,22	1,471
Bir yazılım güncellemesi uyarısı aldığımda, yüklemeyi hemen yaparım.	3,13	1,142
Web sitelerine göz atarken, ilgili bağlantıya tıklamadan önce bağlantının adresini görmek için fareyi bağlantının üzerinde gezdiririm.	2,90	1,342
Web siteleriyle bilgi paylaşırken sitenin güvenli olup olmadığını sorgulamam (örneğin SSL, https://, bir kilit simgesi).	2,39	1,289
URL'ye (arama çubuğu) bakmadan, görünüşüne ve verdiği hisse göre web sayfalarına girdiğimi bilirim.	2,39	1,185
Birisi bana bir internet bağlantısı gönderdiğinde, hiç düşünmeden açarım.	1,93	0,967
Eğer bir güvenlik sorunuyla karşılaşırsam, bir başkasının bu güvenlik sorununu düzelteceğini düşünerek yaptığım işleme devam ederim.	1,92	1,166

3.1 Faktör ve güvenilirlik analizleri

Verilen yanıtların faktör analizine uygunluğunu değerlendirmek için KMO örneklem uygunluğu testi gerçekleştirilmiştir. KMO ölçütünün 0.709 düzeyinde kabul edilebilir olduğu saptanmıştır. Bartlett's testinin ise 0.05'ten küçük olduğu saptanmış, faktör analizi sonucunda elde edilen modelin anlamlı olduğu anlaşılmıştır. Siber güvenlik davranışı sıklık ölçeğinin on altı sorusu faktör analizine tabi tutulmuş ve sonuçlar Tablo 3'te gösterilmiştir. Faktör analizinde varimax yöntemi kullanılmış, faktörlerin güvenilirliği Cronbach's Alpha katsayısı ile hesaplanmış, Alpha katsayısı 0.6'nın üzerinde olan faktörler güvenilir kabul edilmiştir. Alpha değerleri Tablo 3'te yer almaktadır. Analiz sonucunda özdeğeri 1'den büyük ve toplam varyansın %64.3'ünü açıklayan üç faktör elde edilmiştir.

Tablo 3. Siber güvenlik davranışı ifadelerinin faktör analizi sonuçları.

Faktörler	**Faktör Ağırlığı**	**Özdeğer**	**Faktör Açıklayıcılığı**	**Güvenilirlik (Cronbach's Alpha değeri)**
F1. Cihaz güvenliği		2,606	% 32,5	0,705
Dizüstü bilgisayar ya da tabletimin kilidini	0,784			

açmak için şifre (parola) kullanırım.				
Bilgisayarımdan (her) uzaklaştığımda, bilgisayar ekranımı kendim kilitlerim.	0,784			
Bilgisayarımı uzun süre kullanmayacaksam ekranını otomatik olarak kilitlenecek şekilde ayarlarım.	0,759			
F2.Pro-aktif farkındalık		1,480	% 18,5	0,604
Web siteleriyle bilgi paylaşırken sitenin güvenli olup olmadığını sorgulamam (örneğin SSL, https://, bir kilit simgesi).	0,766			
Birisi bana bir internet bağlantısı gönderdiğinde, hiç düşünmeden açarım.	0,748			
URL'ye (arama çubuğu) bakmadan, görünüşüne ve verdiği hisse göre web sayfalarına girdiğimi bilirim.	0,719			
F3. Yazılım güncelleme		1,07	% 13,3	0,698
Anti virüs yazılımımın düzenli olarak kendisini güncellediğini takip ederim.	0,858			
Kullandığım programların güncel olduğundan emin olmaya çalışırım.	0,85			

Faktör analizi sonucunda; ilk faktör cihaz güvenliği, ikinci faktör pro-aktif farkındalık; üçüncü faktör ise yazılım güncelleme olarak isimlendirilmiş, sırasıyla Cronbach's Alpha değerleri 0.705,

0.604 ve 0.698 olarak hesaplanmıştır. Ölçeği geliştiren Egelman ve Peer'in (2015) çalışmasında ise 16 ifade cihaz güvenliği, pro-aktif farkındalık, yazılım güncelleme ve şifre oluşturma şeklinde dört faktör altında toplanmıştır.

3.2 Hipotezlerin test edilmesi

Bu çalışma ile Türkiye'de henüz çok az araştırılmış olan siber güvenlik davranışı demografik faktörler bağlamında araştırılacaktır. Faktör analizi sonucunda bağımlı değişken (siber güvenlik davranışı) üç faktöre ayrılmış, araştırma amacından ve literatürden yola çıkarak aşağıdaki hipotezler oluşturulmuştur.

H1: Siber güvenlik davranışının cihaz güvenliği boyutu yaşa göre farklılık göstermektedir.

H2: Siber güvenlik davranışının pro-aktif farkındalık boyutu yaşa göre farklılık göstermektedir.

H3: Siber güvenlik davranışının yazılım güncelleme boyutu yaşa göre farklılık göstermektedir.

H4: Siber güvenlik davranışının cihaz güvenliği boyutu cinsiyete göre farklılık göstermektedir.

H5: Siber güvenlik davranışının pro-aktif farkındalık boyutu cinsiyete göre farklılık göstermektedir.

H6: Siber güvenlik davranışının yazılım güncelleme boyutu cinsiyete göre farklılık göstermektedir.

H7: Siber güvenlik davranışının cihaz güvenliği boyutu eğitim durumuna göre farklılık göstermektedir.

H8: Siber güvenlik davranışının pro-aktif farkındalık boyutu eğitim durumuna göre farklılık göstermektedir.

H9: Siber güvenlik davranışının yazılım güncelleme boyutu eğitim durumuna göre farklılık göstermektedir.

H10: Siber güvenlik davranışının cihaz güvenliği boyutu mesleğe göre farklılık göstermektedir.

H11: Siber güvenlik davranışının pro-aktif farkındalık boyutu mesleğe göre farklılık göstermektedir.

H12: Siber güvenlik davranışının yazılım güncelleme boyutu mesleğe göre farklılık göstermektedir.

H13: Siber güvenlik davranışının cihaz güvenliği boyutu gelire göre farklılık göstermektedir.

H14: Siber güvenlik davranışının pro-aktif farkındalık boyutu gelire göre farklılık göstermektedir.

H15: Siber güvenlik davranışının yazılım güncelleme boyutu gelire göre farklılık göstermektedir.

H16: Siber güvenlik davranışının cihaz güvenliği boyutu internette geçirilen zamana göre farklılık göstermektedir.

H17: Siber güvenlik davranışının pro-aktif farkındalık boyutu internette geçirilen zamana göre farklılık göstermektedir.

H18: Siber güvenlik davranışının yazılım güncelleme boyutu internette geçirilen zamana göre farklılık göstermektedir.

Siber güvenlik davranışının sosyo-demografik özelliklere göre farklılık gösterip göstermediğini anlamak için T-test ve ANOVA analizi yapılmıştır.

Siber güvenlik davranışının yazılım güncelleme boyutunun cinsiyete göre farklılık gösterip göstermediğini anlamak için yapılan T-testi sonucunda, Tablo 4'te gruplar arasında anlamlı farklılık bulunduğu görülmektedir. Kadınların yazılım güncelleme sıklığının erkeklerinkinden daha yüksek olduğu görülmektedir. H6'nın %5 anlamlılık düzeyinde istatistiksel olarak doğru olduğuna karar verilmiştir. H4 ve H5 ise reddedilmiştir (p>0.05).

Tablo 4. Yazılım güncelleme sıklığının cinsiyet değişkenine göre T-testi sonuçları.

	Cinsiyet	**N**	**Ort.**	**Std. Sapma**	**t**	**p**
Yazılım Güncelleme	Kadın	153	3,52	1,01	-3,004	0,003
	Erkek	171	3,17	1,09		

ANOVA testi sonucunda, cihaz güvenliği düzeyinin yaşa göre farklılık gösterdiği tespit edilmiştir F(3,322)=2,882. Post-hoc testlere göre 26-35 yaş aralığı ortalaması (4,03) 18-25 yaş ortalamasından (3,37) yüksektir. H1'in %5 anlamlılık düzeyinde istatistiksel olarak doğru olduğuna karar verilmiştir. Yazılım güncelleme F=1,823, p=0,143 ve pro-aktif farkındalık F=1,868, p=0,135 ise yaşa göre farklılık göstermemiştir. H2 ve H3 reddedilmiştir.

Eğitim seviyesine göre farklılığa bakıldığında, ANOVA testi sonucunda yazılım güncelleme F=2,397, p=0,093, pro-aktif farkındalık F=1,408, p=0,246 ve cihaz güvenliği F=0,531, p=0,588 boyutlarının hiçbirinin farklılık göstermediği görülmektedir. H7, H8 ve H9 reddedilmiştir.

ANOVA testi sonucunda, cihaz güvenliği düzeyinin mesleğe göre farklılık gösterdiği tespit edilmiştir F(6,319)=3,243. Post-hoc testlere göre özel sektör çalışanı ortalaması (4,00) kamu çalışanı ortalamasından (3,30) yüksektir. H10'un %5 anlamlılık düzeyinde istatistiksel olarak doğru olduğuna karar verilmiştir. Yazılım güncelleme F=1,823, p=0,143 ve pro-aktif farkındalık F=0,481,

p=0,823 ise mesleğe göre farklılık göstermemiştir. H11 ve H12 reddedilmiştir.

Gelir seviyesine göre farklılığa bakıldığında, ANOVA testi sonucunda yazılım güncelleme F=1,120, p=0,350, pro-aktif farkındalık F=1,169, p=0,324 ve cihaz güvenliği F=1,365, p=0,237 boyutlarının hiçbirinin gelire göre farklılık göstermediği görülmektedir. H13, H14 ve H15 reddedilmiştir.

İnternette geçirilen zamana göre farklılığa bakıldığında ANOVA testi sonucunda pro-aktif farkındalık düzeyinin farklılık gösterdiği tespit edilmiştir F(3, 322)=3,290, p<0,021. Post-hoc testlere göre haftada 1-5 saat arası zamanını internette geçirenlerin ortalaması (1,57) günde 1-2 saat (2,28), günde 3-5 saat (2,29) ve günde 5 saatten fazla geçirenlerden (2,21) düşüktür. H17'nin %5 anlamlılık düzeyinde istatistiksel olarak doğru olduğuna karar verilmiştir. Yazılım güncelleme F=1,231, p=0,298, ve cihaz güvenliği F=0,079, p=0,971 boyutlarının anlamlı farklılık göstermediği görülmektedir. H16 ve H18 reddedilmiştir.

4. Sonuç

Bulgular göstermektedir ki, kadınların yazılım güncelleme sıklığı erkeklerden yüksektir. Türkiye'de erkeklerin çalışma hayatında sayılarının kadınlardan çok daha fazla olduğu düşünüldüğünde erkeklere yönelik siber güvenlik farkındalık kampanyalarının, bulundukları statü, yaş, meslek, yaşam tarzı gibi faktörler göz önünde tutularak tasarlanması önerilmektedir. Ayrıca erkeklerin düşük yazılım güncelleme sıklığının altında yatan nedenleri ortaya koyan araştırmalar yapılması gelecek araştırmacılara önerilmektedir. Pek çok araştırma kadınların gizlilik ve güvenlik açıkları konusunda erkeklere göre genellikle daha fazla kaygı duyduklarını göstermekteyken, Anwar vd. (2017:440)'nin çalışmasında erkeklerin siber güvenlik davranışı ortalamaları kadınlardan daha yüksek bulunmuştur. A.B.D'de 579 çalışanla, cinsiyetin siber güvenlik davranışı ve inançları üzerindeki rolünün araştırıldığı çalışmanın bulgularına göre; bilgisayar becerileri, geçmiş deneyim, davranışı tetikleyen ipuçları , güvenlik ile ilgili öz yeterliliği, beyan edilen siber güvenlik davranışı boyutlarında istatistiksel olarak anlamlı cinsiyet bazlı farklılıklar olduğu görülmektedir. Aynı araştırmada kadınların öz-yeterlilik boyutu erkeklerden istatistiksel olarak anlamlı derecede düşük çıkmıştır. Bu bulgu cinsiyete özel siber güvenlik eğitimleri ve uygulamaları geliştirmenin önemine dikkat çekmektedir. Bireylerin evlerinde nasıl güvenli şekilde bilgisayar kullanacaklarını daha iyi anlamayı amaçlayan araştırmada

Harrington vd. (2006) cinsiyetin siber güvenlik tutum ve davranışı üzerinde anlamlı etkisi olmadığı bulgusuna ulaşmışlardır.

Araştırmanın bir diğer bulgusu ise cihaz güvenliği davranış sıklığının özel sektör çalışanlarında, kamu çalışanlarına göre daha yüksek oluşudur. Kamu kurumlarında 29 Kasım 2017 tarihinde beşincisi düzenlenen Ulusal Siber Savunma Tatbikatına ilave olarak kamu çalışanlarının siber güvenlik davranış sıklığını geliştirici çalışmalara ağırlık verilmesi önerilmektedir.

Benzer şekilde gelir düzeyine göre de siber güvenlik davranış sıklığının farklılık göstermediği görülmüştür. Yüksek gelir ve eğitime sahip sosyal sınıflara mensup bireylerin siber güvenlik sıklıkları ile düşük eğitim ve gelir grubundakilerin davranışları arasında anlamlı fark görülmemiştir. Bu bulgu toplumun her sosyal sınıfında siber güvenlik farkındalığının sağlanmasına ihtiyaç olduğunu işaret etmektedir. Coventry vd, (2014)'e göre kitlelerin davranışlarını değiştirmek için pek çok alanda kitle iletişim araçları kullanılmaktadır. TV reklamları, popüler programlara ürün yerleştirme, kimi zaman internet reklamları ve sosyal medya üzerinden yapılan iletişim kampanyaları ile güvenli sürüş, sigara, obezite, gibi sosyal konuların iletişimi yapılarak davranış değişikliği yaratılmaya çalışılmaktadır. Mesajı kişiselleştirmeyi başaran kampanyaların daha iyi sonuçlar verdiği görülmektedir. Örneğin sigara tüketimini bıraktırmakla ilgili olarak genç kızlara "kirli bir küllüğü öpmek gibi" mesajı verilirken, anne babalara "sigara dumanı çocuklarınızın ciğerlerine zarar vermektedir" mesajı verilerek daha etkili hale getirilmektedir. Siber güvenlik ile ilgili olarak ise henüz mesajların büyük çoğunluğunun kitlesel olduğu, belirli hedef kitlelere farklı formatlarda mesajların tasarlanmadığı görülmektedir.

Diğer bir bulgu ise internette geçirilen süre arttıkça pro-aktif farkındalık sıklığının da arttığı yönündedir. Başka bir ifadeyle internette az zaman geçiren bireylerin siber güvenlik davranışları sık göstermedikleri tespit edilmiştir. Bu durum bireysel olarak büyük siber güvenlik açıklarına sebep olmaktadır. İnternette az zaman geçiriyor olmak, siber riske daha az maruz kalınacağı anlamına gelmemektedir. Toplumun bu kesiminin de siber güvenlik farkındalığını artırmak gerekmektedir.

Çalışmada ayrıca, siber güvenlik davranışı sıklığının bireylerin eğitim düzeyine göre farklılık göstermediği görülmüştür. Bu bulgu eğitim sisteminde siber güvenlikle ilişkili içerik bulunmasının önemine işaret etmektedir. Özellikle ilkokul ve ortaokul müfredatlarına farklı yaş gruplarındaki öğrencilerin ilgisini

çekecek yaratıcı içerik ve teoriyi barındıran siber güvenlik ile ilgili uygulamalı, eğlenceli, farkındalığı artırıcı derslerin, ünitelerin ya da faaliyetlerin eklenmesi mevcutların ise sürekli güncel tutulması önerilmektedir.

Araştırma kolayda örnekleme yöntemiyle yapıldığından genellenemez. Ne var ki, Türkiye'de konuyla ilgili yapılmış ender çalışmalardan olması itibariyle, siber güvenlik davranışına dair önemli bulgular içermektedir. Gelecekte bu konuda yapılacak araştırmaların siber güvenlik davranışlarına neden olan ve engel olan faktörleri ortaya koymak için nitel yöntemler kullanılarak daha derin içgörü elde etmeyi amaçlayan çalışmalar olması önerilmektedir.

KAYNAKÇA

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237-248.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 69, 437-443.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38, 304-312.

Bada, M., & Sasse, A. (2014). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? Global Cyber Security Capacity Centre: Draft Working Paper.

Beautement, A., Sasse, M. A., & Wonham, M. (2009, August). The compliance budget: managing security behaviour in organisations. In Proceedings of the 2008 workshop on New security paradigms (pp. 47-58). ACM.

Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, M. A., & Passingham, N. (2015). Awareness is only the first step. A framework for progressive engagement of staff in cyber security, Hewlett Packard, Business white paper.

Blythe, J. (2013). Cyber security in the workplace: Understanding and promoting behaviour change. Proceedings of CHItaly 2013 Doctoral Consortium, 1065, 92-101.

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. computers & security, 26(1), 63-72.

Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices. gov. uk report.

CTR Uluslararası Belgelendirme ve Denetim Ltd. Şti. Web Sitesi, http://belgelendirme.ctr.com.tr/iso-27001.html (02.03.2018)

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among Internet users. Computers in Human Behavior, 26(6), 1739-1747.

Department of Defense Dictionary of Military and Associated Terms, https://fas.org/irp/doddir/dod/jp1_02.pdf pg.44 (18.01.2018)

Egelman, S., Harbach, M., & Peer, E. (2016, May). Behavior ever follows intention?: A validation of the security behavior intentions scale (SeBIS). In Proceedings of the 2016 CHI conference on human factors in computing systems (pp. 5257-5261). ACM.

Egelman, S., & Peer, E. (2015, April). Scaling the security wall: Developing a security behavior intentions scale (sebis). In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (pp. 2873-2882). ACM.

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies–A case study. information security technical report, 14(4), 223-229.

Erol, O., Şahin, Y. L., Yılmaz, E., & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. Journal of Human Sciences, 12(2), 75-91.

Güldüren, C., Çetinkaya, L., & Keser, H. (2016). Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. İlköğretim Online, 15(2).

Harrington, S., Anderson, C., & Agarwal, R. (2006). Practicing safe computing: Message framing, self-view, and home computer user security behavior intentions. ICIS 2006 Proceedings, 93.

Internetworldstats, http://www.internetworldstats.com/stats.htm (17.01.2018)

ITU (International Telecommunication Union https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Introduction%20to%20the%20Concept%20of%20IT%20Security.pdf pg.18, pg.43 (17.01.2018)

ITU-T Rec., ITU-T Rec. X.1205 (04/2008) Overview of cybersecurity, https://www.itu.int/rec/T-REC-X.1205-200804-I (22.01.2018)

Johnson, M. E., & Goetz, E. (2007). Embedding information security into the organization. IEEE Security & Privacy, 5(3).

Karacı, A., Akyüz, H. İ., & Bilgici, G. (2017). Üniversite Öğrencilerinin Siber Güvenlik Davranışlarının İncelenmesi. Kastamonu Eğitim Dergisi, 25(6), 2079-2094.

Li, L., Xu, L., He, W., Chen, Y., & Chen, H. (2016, December). Cyber Security Awareness and Its Impact on Employee's Behavior. In International Conference on Research and Practical Issues of Enterprise Information Systems (pp. 103-111). Springer, Cham.

Li, Y., & Siponen, M. T. (2011, July). A Call For Research On Home Users' Information Security Behaviour. In PACIS (p. 112).

Mariea Grubbs Hoy & George Milne (2010) Gender Differences in PrivacyRelated Measures for Young Adult Facebook Users, Journal of Interactive Advertising, 10:2, 28-45, DOI: 10.1080/15252019.2010.10722168.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815-825.

Resmi Gazete, http://www.udhb.gov.tr/doc/siberg/SOME_2013-2014_EylemPlani.pdf (17.01.2018)

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo, & R. Petty (Eds.), Social psychophysiology. New York: Guilford Press.

Rosenstock, I. M. (1974). The health belief model and preventive health behavior. Health Education Monographs 2.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. Computers & Security, 53, 65-78.

Security 101, https://www.cmu.edu/iso/aware/presentation/security101-v2.pdf [22.01.2018]

Shih, D. H., Lin, B., Chiang, H. S., & Shih, M. H. (2008). Security aspects of mobile phone virus: a critical survey. Industrial Management & Data Systems, 108(4), 478-494.

The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028 http://www.fas.org/irp/doddir/army/pam525-7-8.pdf (17.01.2018)

TÜİK, http://www.tuik.gov.tr/PreTablo.do?alt_id=1028 (14.02.2018)

Türk Dil Kurumu Büyük Türkçe Sözlüğü, http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5a5f59db572c44.38695410 (17.01.2018)

Ulusal Siber Savunma 2017, http://hgm.ubak.gov.tr/tr/haber/86 (14.02.2018).

Ünver, M. Ulusal Siber Güvenliğin Sağlanmasında Farkındalık Çalışmaları, http://www.bilgiguvenligi.org.tr/s/2246/i/Mustafa_Unver-Ulusal_Siber_G%C3%BCvenligin_Saglanmasinda_Farkindalik_Calismalari.pdf (13.10.2015).

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. Information & Management, 49(3-4), 190-198.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.