Kalite Yönetim Direktörlerinin Bilgi Güvenliği Farkındalığı: İstanbul İli Örneği

Çiğdem ÇELİKÇÖP [1]
Onur YARAR [2]

ÖZ

Araştırma kamu hastanelerinde görev yapan kalite yönetim direktörleri ve kalite birim sorumlularının bilgi güvenliği farkındalıklarını belirlemek amacıyla yapılmıştır. Araştırmanın evrenini İstanbul ilinde faaliyet gösteren Kamu Hastaneler Birliğine bağlı 72 hastanenin kalite yönetim direktörleri ve kalite birim sorumluları oluşturmaktadır. Kamu Hastaneler Birliğine bağlı 6 genel sekreterliğe araştırma izni başvurusu yapılmış ancak 67 hastane için çalışma onayı alınmıştır. Örneklem seçilmemiş, evrende izin verilen hastanelerin tamamına ulaşılmış olup; toplam 87 kişiden veri toplanmıştır.

Araştırma için 02.12.2016 tarihinde etik kurul izni alınmış sonrasında Aralık 2016-Nisan 2017 tarihleri arasında 5 aylık bir sürede veri toplama süreci tamamlanmıştır. Katılımcılara yüz yüze ve elektronik anket uygulaması uygulanmıştır.

Araştırmada veriler kalite direktörlerinin tanımlayıcı özelliklerini belirlemeye yönelik form ve "Bilgi Güvenliği Farkındalık Ölçeği" ile toplanmıştır.

Araştırmada elde edilen veriler SPSS (Statistical Package for the Social Sciences) Windows 22.0 programı kullanılarak analiz edilmiştir. Verilerin değerlendirilmesinde tanımlayıcı istatistiksel yöntemleri olarak frekans, yüzde, ortalama, standart sapma, t-testi, anova testi kullanılmıştır.

1 Hemşire, Yakacık Doğum ve Çocuk Hastalıkları Hastanesi
2 Yrd. Doç. Dr., Okan Üniversitesi Sağlık Bilimleri Fakültesi

Araştırma sonucunda kalite yönetim direktörlerinin, “Kişisel Verilerin Korunması” düzeyinin yüksek; “Saldırı ve Tehditlere Yönelik Farkındalık” düzeyinin orta; “Bilgi Güvenliği Farkındalığı Genel” düzeyinin orta seviyede olduğu belirlenmiştir. Araştırmada ayrıca bilgi güvenliği farkındalığına yönelik cinsiyet ve meslek grubuna göre farklılıklar bulunduğu sonucuna ulaşılmıştır.

Anahtar Kelimeler: Bilgi Güvenliği, Kalite Yönetim Direktörleri , Kalite

Information Security Awareness of Quality Management Directors: The Case of Istanbul Province

ABSTRACT

The aim of this research is to determine the information security awereness of quality Management Directors and quality unit managers who serve in public hospitals. The population of the research is constituted by the quality Management Directors and quality unit responsibles who work at 72 hospitals affliated to 6 subsidiary general secretaries of public hospital, union in Istanbul. 6 General Secretaries have been applied forre search permits of 72 hospitals, but 67 hospitals have been approved for the research. The sample was not selected, all the hospitals permitted in the population have been reached and data collected from a total of 87 people.

After the approval of the local ethics committee on 02.12.2016, the data collection process was completed between December 2016 and April 2017in a period of 5 months.The participants were interviewed face to face and the electronic questionnaire was applied.

The data was collected with a form and "Information security awareness Scale" is used to determine the descriptive characteristics of the quality directors and responsibles.

The results were analyzed using the SPSS (Statistical Package for the Social Sciences) Windows

22.0 program. As descriptive statistical methods for evaluating data, frequency, percentage, average, standard deviation, T-Test, ANOVA test were used.

In conclusion, it has been determined;the level of " information security awareness''is moderate, the level of ‘’protection of personal data" of quality directors is high, the level of "awareness of attacks and threats" off quality directors is moderate.The reserch also found that there were differences according to gender and occupation group in terms of information security awarness.

Keywords: Security, Quality management directors, Quality.

1. GİRİŞ

Bilgi güvenliği, bilgiye sahip olan taraflar dışındaki bireyler ya da kurumlar tarafından söz konusu bilginin kullanılmasını, değiştirilmesini, yayılmasını, zarara uğratılmasını, manipüle edilmesini vb. engellemek amacıyla oluşturulan bir sistemi ifade etmektedir (Keser, Güldüren, 2015:1167-1184) .

Sağlık sektörü, bilgi güvenliği konusunda en üst düzey güvenliğe ihtiyaç duyan alanlardan biridir. 2000'li yılların başında, dünya genelinde sağlık kuruluşları elektronik veri tabanı kullanarak hastalarının bilgilerini gizleme konusunda ciddi ölçekli çalışmalara rağmen söz konusu veri tabanlarına gerçekleştirilen saldırılar da ciddi oranda artış göstermiş ve yıllar içerisinde milyonlarca hastanın özel bilgileri yasadışı yollarla üçüncü kişilerin eline geçmiştir (Samy, Ahmad, 2009: 540-543).

Dijital ortamda gerçekleştirilen bu saldırıların temel sebebi, hastalara dair bazı gizli ve önemli bilgilerin, üçüncü kişiler tarafından kullanımının maddi ve manevi anlamda çeşitli getirilerinin bulunmasıdır. Hastaların kimlik bilgileri, sağlık sorunlarına dair geçmişleri, medikal anlamda görüntüler, mevcut rahatsızlıklar, rahatsızlık tehditleri, tedavi içerikleri ve geçmişleri, diyet programları, cinsel sağlık sorunları, genetik bilgileri, psikolojik profilleri, fiziksel anlamdaki eksiklikleri vb. birçok veri ve bilgi kötü amaçlı olarak çeşitli kişiler tarafından kullanılabilecek durumdadır (Appari, Johnson, 2010: 279-314).

HIV/AIDS gibi bazı rahatsızlıklar hastalar açısından son derece hassas içerikli olabilmekte, buna istinaden de bu hastalar için üst düzeyli bir korumaya ihtiyaç duyulmaktadır. Özellikle cinsel sorunlar, genetik bozukluklar ve mental rahatsızlıklar gibi bireyi toplumdan ayıracak sağlık sorunlarına dair bir bilgi gizliliğine etkili bir şekilde ihtiyaç duyulmaktadır (Omotosho, Emuoyibofarhe, 2014: 11-18).

Elektronik sağlık kayıtları, hastalara dair geniş ölçekli bilgileri içerisinde bulunduran bir sistem olmakla birlikte taşıdığı öneme paralel olarak bu sistemin kullanımında nitelikli çalışanların varlığına ihtiyaç duyulmaktadır. İster sağlık personeli olsun isterse sistemin başındaki çalışanlar olsun, sağlık kuruluşları açısından önemli olan sürecin yetkin bireylere bırakılması ve bu bireylerin konuya dair hukuki ve etik odaklı yaklaşımlarının sorgulanması gerekmektedir (Öğütçü, Gürel, Cula, 2011: 88-96).

Sağlık kurumları son teknolojiden yararlanarak güvenlik önlemlerini alsalar da, insan kaynaklı bilgi güvenliği açıklarının hiçbir zaman önüne geçemezler, çünkü sağlık kurumlarının bilgi güvenliği konusunun en zayıf halkası insan faktörüdür. En ufak ciddiyetsizlik ve sorumsuzluk kurumlar için maddi ve manevi, telafisi mümkün olmayan sorunlara yol açar. Bilgi güvenliği farkındalığı oluşturmaktaki amaç; kişilerin bilgi eksikliğinden kaynaklı hata ve risklerini en aza indirmek ve çalışanların bu tehditlerden haberdar olmasını sağlamaktır. (Şahinarslan, Kandemir, Şahinarslan, 2009: 189-194).

Güvenlik teknolojilerinden önce sağlık kurumlarının en üst çalışanından en alt çalışanına kadar bilgi güvenliği farkındalık faaliyetlerinin benimsenmesi, geliştirilmesi önem arz etmektedir (Sağlık Bakanlığı Bilgi Güvenliği Politikalar Kılavuzu, 2014).

2. YÖNTEM

Amaç

Araştırma İstanbul ili kamu hastanelerinde bilgisayar ve bilgi teknolojilerini en etkin kullanan kalite yönetim direktörleri ve kalite birim sorumlularının bilgi güvenliği farkındalık düzeylerini belirlemek, kalite yönetim süreçlerinde bilgi güvenliği ve bilgi yönetimi kavramlarının önemini vurgulamak amacıyla yapılmıştır.

Araştırmanın Modeli: Araştırma ilişkisel tarama modelinde tasarlanmıştır. İlişkisel tarama modelleri mevcut durumu değiştirme çabası olmayıp olduğu gibi ortaya koyan modellerdir. Araştırmada, kalite direktörlerinin bilgi güvenliği farkındalığı ve tanımlayıcı özelliklere göre farklılıklarını belirlemeye yönelik bir model belirlenmiştir.

Araştırmanın Evren ve Örneklemi: Araştırmanın evrenini İstanbul ilinde faaliyet gösteren kamu hastaneler birliğine bağlı 72 hastanenin kalite yönetim direktörleri ve kalite birim sorumluları oluşturmaktadır. Kamu Hastaneler Birliğine bağlı 6 genel sekreterliğe araştırma izni başvurusu yapılmış ancak 67

hastane için çalışma onayı alınmıştır. Örneklem seçilmemiş, evrende izin verilen hastanelerin tamamına ulaşılmış olup; toplam 87 kişiden veri toplanmıştır.

Araştırmanın Etik Yönü ve İzinleri: Araştırma için Sağlık Bilimleri Üniversitesi Kartal Koşuyolu Yüksek İhtisas EAH Girişimsel Olmayan Klinik Araştırmalar Etik Kurulu'ndan 02.12.2016 tarihinde Sayı:2016.5/2-13 numaralı izin alınmıştır.6 Aralık 2016- 28 Nisan 2017 tarihleri arasında veri toplama süreci tamamlanmıştır.

Veri Toplama Aracı: Katılımcılara yüz yüze ve elektronik anket uygulaması uygulanmıştır. Araştırmada veriler kalite direktörlerinin tanımlayıcı özelliklerini belirlemeye yönelik form ve "Bilgi Güvenliği Farkındalık Ölçeği" ile toplanmıştır. Araştırmada Keser ve Güldüren (2015) tarafından geliştirilen bilgi güvenliği farkındalık ölçeği kullanılmıştır. Sorular 5'li Likert Tipi derecelendirme ölçeğine göre hazırlanmıştır. Ölçek 34 madde olup; "saldırı ve tehditler" ile "kişisel verilerin korunması" olmak üzere 2 alt boyuttan oluşmaktadır. Ölçekte yer alan ilk 16 madde saldırı ve tehditlere yönelik farkındalıkları, 17 ile 34. maddeler arasında yer alanlar ise kişisel verilerin korunmasına yönelik farkındalıklarını belirlemeye yönelik sorulardır.

Verilerin Analizi: Araştırmada elde edilen veriler SPSS (Statistical Package for the Social Sciences) Windows 22.0 programı kullanılarak analiz edilmiştir. Verilerin değerlendirilmesinde tanımlayıcı istatistiksel yöntemleri olarak frekans, yüzde, ortalama, standart sapma, t-testi, anova testi kullanılmıştır. Elde edilen bulgular %95 güven aralığında, %5 anlamlılık düzeyinde değerlendirilmiştir.

Araştırmanın Sınırlılıkları: Araştırma İstanbul ili Kamu Hastaneler Birliğine bağlı kurumlardaki kalite yönetim direktörleri ve kalite birim sorumlularına yapılmıştır. Çalışmanın sadece İstanbul ilinde yapılması ve ankete sadece kalite yönetim direktörleri, kalite birim sorumlularının dahil edilmesi araştırmayı sınırlamıştır.

3. BULGULAR

Tablo 1. Tanımlayıcı Özelliklerin Dağılımı

Tablolar	Gruplar	Frekans (n)	Yüzde (%)
Cinsiyet	Erkek	11	12,6
	Kadın	76	87,4
	Toplam	87	100,0
Görev	Hekim	5	5,7
	Hemşire	61	70,1
	Ebe	10	11,5
	Teknisyen	11	12,6
	Toplam	87	100,0
Eğitim Düzeyi	Ön Lisans	16	18,4
	Lisans	30	34,5
	Lisansüstü	41	47,1
	Toplam	87	100,0
Yaş	20-30 yaş arası	13	14,9
	31-40 yaş arası	49	56,3
	41-50 yaş arası	25	28,7
	Toplam	87	100,0

Tablo 1'de direktörler cinsiyet değişkenine göre 11'i (%12,6) erkek, 76'sı (%87,4) kadın olarak dağılmaktadır.

Direktörler görev değişkenine göre 5'i (%5,7) Hekim, 61'i (%70,1) Hemşire, 10'u (%11,5) Ebe, 11'i (%12,6) Teknisyen olarak dağılmaktadır.

Direktörler eğitim düzeyi değişkenine göre 16'sı (%18,4) ön lisans, 30'u (%34,5) lisans, 41'i (%47,1) lisansüstü olarak dağılmaktadır.

Direktörler yaş değişkenine göre 13'ü (%14,9) 20-30 yaş arası, 49'u (%56,3) 31-40 yaş arası, 25'i (%28,7) 41-50 yaş arası olarak dağılmaktadır.

Tablo 2. Bilgi Güvenliği Farkındalığının Cinsiyete Göre Ortalamaları

	Grup	Sayı (n)	Ortalama (ort)	Standart Sapma (s.s)	t	p
Kişisel Verilerin Korunması	Erkek	11	4,242	0,658	1,774	0,080
	Kadın	76	3,822	0,745		
Saldırı ve Tehditlere Yönelik Farkındalık	Erkek	11	3,659	0,890	3,574	0,001
	Kadın	76	2,723	0,801		
Bilgi Güvenliği Farkındalığı Genel	Erkek	11	3,968	0,740	2,902	0,005
	Kadın	76	3,305	0,704		

Tablo 2'de erkek katılımcıların saldırı ve tehditlere yönelik farkındalık puanları ($\bar{x}$ =3,659), kadın katılımcıların saldırı ve tehditlere yönelik farkındalık puanlarından ($\bar{x}$ =2,723) yüksek bulunmuştur.

Erkek katılımcıların bilgi güvenliği farkındalığı genel puanları ($\bar{x}$ =3,968), kadın katılımcıların bilgi güvenliği farkındalığı genel puanlarından ($\bar{x}$=3,305) yüksek bulunmuştur.

Araştırmaya katılan direktörlerin kişisel verilerin korunması puanları ortalamalarının cinsiyet değişkenine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan t-testi sonucunda grup ortalamaları arasındaki fark istatistiksel açıdan anlamlı bulunmamıştır ($p>0,05$).

Tablo 3. Bilgi Güvenliği Farkındalığının Göreve Göre Ortalamaları

	Grup	Sayı (n)	Ortalama (ort)	Standart Sapma (s.s)	F	p	Fark
Kişisel Verilerin Korunması	Hekim	5	4,044	0,099	1,885	0,138	
	Hemşire	61	3,812	0,791			
	Ebe	10	3,678	0,594			
	Teknisyen	11	4,328	0,621			
Saldırı ve Tehditlere Yönelik Farkındalık	Hekim	5	3,763	0,128	6,826	0,000	1>2 4>2 1>3 4>3
	Hemşire	61	2,730	0,835			
	Ebe	10	2,319	0,636			
	Teknisyen	11	3,517	0,785			
Bilgi Güvenliği Farkındalığı Genel	Hekim	5	3,912	0,098	4,430	0,006	4>2 1>3 4>3
	Hemşire	61	3,302	0,748			
	Ebe	10	3,038	0,518			
	Teknisyen	11	3,947	0,663			

Tablo 3'de araştırmaya katılan direktörlerin kişisel verilerin korunması puanları ortalamalarının görev değişkenine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan tek yönlü varyans analizi (Anova) sonucunda grup ortalamaları arasındaki fark istatistiksel açıdan anlamlı bulunmamıştır($p>0.05$).

Araştırmaya katılan görevi hekim olan kalite yönetim direktörlerinin saldırı ve tehditlere yönelik farkındalıkları diğer meslek gruplarına göre en yüksek iken, görevi ebe olan kalite yönetim direktörlerinin saldırı ve tehditlere yönelik farkındalıkları diğer meslek gruplarına göre en düşük olduğu görülmüştür.

Araştırmaya katılan görevi teknisyen olan kalite yönetim direktörlerinin bilgi-güvenliği farkındalıkları diğer meslek gruplarına göre en yüksek iken, görevi ebe olan kalite yönetim direktörlerinin bilgi güvenliği farkındalıklarının diğer meslek gruplarına göre en düşük olduğu görülmüştür.

Tablo 4. Kalite Yönetim Direktörleri ve Kalite Birim Sorumlularının Bilgi Güvenliği Farkındalığı ile İlgili En Fazla Katıldıkları İfadeler

En fazla katıldıkları ifadeler	Ortalama	Standart Sapma	Ölçek Alt Boyutu
Kişisel Mahremiyet nedir biliyorum	4,218	0,769	Kişisel Verilerin Korunması
Şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan E-postaları açmanın taşıdığı riski biliyorum	4,184	0,896	Kişisel Verilerin Korunması
İstenmeyen Elektronik Posta (Spam) Nedir Biliyorum	4,126	0,913	Kişisel Verilerin Korunması
Bilgi Güvenliği İle İlgili Sorumluluklarımın Ne Olduğunu Biliyorum	4,046	0,834	Kişisel Verilerin Korunması

Tablo 4'de "Kişisel Mahremiyet Nedir Biliyorum" ifadesine direktörlerin, çok yüksek (4,218±0,769) düzeyde katıldıkları saptanmıştır.

"Şüpheli veya Bilinmeyen Kaynaklardan Gelen Özellikle Eklentisi Olan E-postaları Açmanın Taşıdığı Riski Biliyorum" ifadesine direktörlerin, yüksek (4,184±0,896) düzeyde katıldıkları saptanmıştır.

"İstenmeyen Elektronik Posta (spam) Nedir Biliyorum" ifadesine direktörlerin yüksek (4,126±0,913) düzeyde katıldıkları saptanmıştır.

"*Bilgi Güvenliği İle İlgili Sorumluluklarımın Ne Olduğunu Biliyorum*" ifadesine direktörlerin, yüksek (4,046±0,834) düzeyde katıldıkları saptanmıştır.

Tablo 5. Kalite Yönetim Direktörleri ve Kalite Birim Sorumlularının Bilgi Güvenliği Farkındalığı ile İlgili En Az Katıldıkları İfadeler

En Az Katıldıkları İfadeler	Ortalama	Standart Sapma	Ölçek Alt Boyutu
Sosyal Mühendislik Saldırısına Uğramamak İçin Nasıl Hareket Etmem Gerektiğini Biliyorum	2,517	1,140	Saldırı ve Tehditlere Yönelik Farkındalık
Hizmet Aksatma (denial Of Service - Dos) Saldırısı Nedir Biliyorum	2,575	1,030	Saldırı ve Tehditlere Yönelik Farkındalık
Bilgisayarımda Casus Yazılım (spyware) Olup Olmadığını Anlayabilirim	2,621	1,164	Saldırı ve Tehditlere Yönelik Farkındalık
Siber Zorbalığa Karşı Kendimi Nasıl Koruyacağımı Biliyorum	2,621	1,070	Saldırı ve Tehditlere Yönelik Farkındalık

Tablo 5'de *"Sosyal Mühendislik Saldırısına Uğramamak İçin Nasıl Hareket Etmem Gerektiğini Biliyorum"* ifadesine direktörlerin, zayıf (2,517±1,140) düzeyde katıldıkları saptanmıştır.

"Hizmet Aksatma (Denial of Service - Dos) Saldırısı Nedir Biliyorum" ifadesine direktörlerin, zayıf (2,575±1,030) düzeyde katıldıkları saptanmıştır.

"*Bilgisayarımda Casus Yazılım (spyware) Olup Olmadığını Anlayabilirim*" ifadesine direktörlerin orta (2,621±1,164) düzeyde katıldıkları saptanmıştır.

"*Siber Zorbalığa Karşı Kendimi Nasıl Koruyacağımı Biliyorum*" ifadesine direktörlerin, orta (2,621±1,070) düzeyde katıldıkları saptanmıştır.

Tablo 6. Bilgi Güvenliği Farkındalığı Puan Ortalamaları

	Sayı (n)	Ortalama	Standart Sapma	Min.	Max.
Kişisel Verilerin Korunması	87	3,875	0,744	1,830	5,000
Saldırı ve Tehditlere Yönelik Farkındalık	87	2,841	0,866	1,190	4,560
Bilgi Güvenliği Farkındalığı Genel	87	3,388	0,739	1,590	4,790

Tablo 6'da araştırmaya katılan direktörlerin "Kişisel Verilerin Korunması" düzeyi yüksek (3,875±0,744); "Saldırı ve Tehditlere Yönelik Farkındalık" düzeyi orta (2,841±0,866); "Bilgi Güvenliği Farkındalığı Genel" düzeyi orta (3,388±0,739); olarak saptanmıştır.

4. TARTIŞMA

Kalite yönetim direktörlerinin bilgi güvenliği farkındalığının belirlendiği bu çalışmada elde edilen bulgular ilgili literatür ile benzerlikler ve farklılıklar gösterebilmektedir.

Yılmaz, Şahin, Akbulut, (2016) Balıkesir ilindeki özel ve kamu okullarında görev yapan 1446 öğretmen üzerinde yapmış olduğu "Öğretmenlerin Digital Veri Güvenliği Farkındalığı" çalışmasında; erkek öğretmenlerin digital veri güvenliği farkındalığının, kadın öğretmenlere göre daha yüksek olduğunu ortaya koymuştur. Yaptığımız çalışmada kalite yönetim direktörlerinin bilgi güvenliği farkındalığının cinsiyete göre değiştiği; erkek kalite yönetim direk-

törlerinin, kadın kalite yönetim direktörlerine göre bilgi güvenliği farkındalığının daha yüksek olduğu görülmüştür. Elde edilen sonuç, Yılmaz, Şahin, Akbulut'un (2016) çalışmasını destekler niteliktedir.

Çalışma bulgusuna göre erkeklerin kadınlara oranla daha fazla internet ve bilgisayar kullandığı ve bilgi güvenliği farkındalıklarının bu sebepten daha yüksek olduğu düşünülmektedir.

Ramachandran vd. (2012) bir kurumun 4 farklı (personel, muhasebe, bilgi işlem, pazarlama) departmanında yaptığı, farklı meslek gruplarının bilgi güvenliği farkındalığı ve güvenlik kültürlerini inceleyen çalışmasında, mesleklerin bilgi güvenliği farkındalığı faktöründe etkisi olduğunu savunmuştur. Muhasebe departmanının bilgi güvenliği farkındalığı kültürü yüksek çıkarken, pazarlama departmanının bilgi güvenliği farkındalığı kültürü düşük çıkmıştır. Bilgi işlem ve personel departmanlarının bilgi güvenliği farkındalığı kültürü de iki birim arasında yer almıştır.

Yaptığımız çalışmada mesleği teknisyen ve doktor olan kalite yönetim direktörlerinin bilgi güvenliği farkındalığı, görevi hemşire ve ebe olan kalite yönetim direktörlerinin bilgi güvenliği farkındalığından yüksek bulunmuştur. Elde edilen sonuç ile bu çalışma, Ramachandran vd. (2012) çalışmasını destekler niteliktedir.

Hekim ve teknisyenlerin görevlerinden dolayı bilgi teknolojilerini daha etkin kullanmaları ve karşılaşılan risk, tehditlerden haberdar olmalarını gerektirdiği için bilgi güvenliği farkındalığının yüksek çıkmasının sebebi olarak düşünülmektedir.

Gerçeker B. "Sağlık Kuruluşlarında Örgüt İklimi ve Bilgi Güvenliğinin İlişkisi" (2012) çalışması İzmir'de bulunan 13 hastanenin 107 yönetici görevinde bulunan kişilere yapılmıştır. Çalışmanın amacı sağlık kuruluşlarında örgüt iklimi ve bilgi güvenliği ilişkisini belirlemektir (Gerçeker, 2012).

Eğitimi lisans ve lisansüstü olan katılımcıların bilgi güvenliği farkındalığı, eğitimi ön lisans ve altı olan katılımcılardan yüksek çıkmıştır. Eğitim düzeyi arttıkça bilgi güvenliği farkındalığı artmaktadır. Yaptığımız çalışmada kalite yönetim direktörlerinin bilgi güvenliği farkındalığı eğitim düzeyine göre an-

lamlı bulunmamıştır ve Gerçeker B.'nin "Sağlık Kuruluşlarında Örgüt İklimi ve Bilgi Güvenliğinin İlişkisi" (2012) çalışmasını desteklememektedir.

Karadağ M., Abuhanoğlu H., "Sosyokültürel Özelliklerin Bilgi Güvenliği Farkındalığı Üzerine Etkisi: Gülhane Askeri Tıp Fakültesi Eğitim Hastanesi'nde Bir Çalışma." (2015) araştırmaya Gülhane Askeri Tıp Fakültesi Eğitim Hastanesi'nde görevli 314 çalışan katılmıştır. Yaşı büyük olan katılımcıların bilgi güvenliği farkındalığı, yaşı küçük katılımcılardan yüksek çıkmıştır (Karadağ,Abuhanoğlu,2015:379-386).Yaptığımız çalışmada kalite yönetim direktörlerinin bilgi güvenliği farkındalığı katılımcıların yaşına göre anlamlı bulunmamıştır ve Karadağ M., Abuhanoğlu"Sosyokültürel Özelliklerin Bilgi Güvenliği Farkındalığı Üzerine Etkisi: Gülhane Askeri Tıp Fakültesi Eğitim Hastanesinde Bir Çalışma"yı desteklememektedir.

Kişisel mahremiyet nedir biliyorum, şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum, istenmeyen elektronik posta (Spam) nedir biliyorum gibi ölçeğin kişisel verilerin korunması alt boyutuna ait ifadelere katılımcıların en yüksek düzeyde katıldıkları görülmektedir.

Katılımcıların günlük hayatta sıklıkla kullanılan ifadelerde ve kişisel verilerinin korunmasına yönelik farkındalıklarının yüksek olduğu görülmüştür.

Fakat yine aynı dağılım üzerindeki değerlendirmelere bakıldığında, ölçeğin Saldırı ve Tehditlere Yönelik Farkındalık alt boyutuna ait sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum, Hizmet aksatma (Denial of Service-Dos) saldırısı nedir biliyorum gibi ifadelere en düşük düzeyde katıldıkları görülmektedir.

Buna göre katılımcılar çoğunlukla bilişim dünyasına dair teknik terimleri içeren ve bilgi güvenliği tehdidi oluşturan unsurlar üzerinde yeterli bilgi birikimi ve farkındalık sahibi değillerdir.Bu durum katılımcıların anlık olarak karşılaştıkları çalışmalarını engelleyen, illegal uygulama ve saldırılar karşısında yeterli bilgi ve sorun çözme kapasitesine sahip olmadıkları sorununu beraberinde getirmektedir. Bu sorun aynı zamanda katılımcılar açısından sürecin tam olarak anlaşılmasını ve gün içerisinde sık olarak tekrarlanan risklerde, yeterli refleksi göstermelerini, sorumlu teknik ekipleri harekete geçirmelerini

ve gerektiğinde kendi başlarına, anlık güvenlik tehditlerine karşı tepki verebilmelerini de engellemektedir.

5. SONUÇ VE ÖNERİLER

Kalite Yönetim Direktörlerinin bilgi güvenliği farkındalıklarını belirlemek için yapılan çalışmanın sonuçlarına bakıldığında katılımcılar açısından farkındalık düzeyine dair net bilgiler elde edilmektedir. Gündelik kullanım ve kişisel verilerini korumaya yönelik farkındalıklarının yüksek olduğu görülmektedir. Bilgi güvenliği farkındalığı ile ilgili ifadelere verdiği cevapların dağılımlarına bakıldığında, genel olarak katılımcıların bilgi güvenliği konusunda yerleşik bir farkındalıklarının bulunduğu görülmektedir. Fakat dijital dünyaya ait olan teknik terimleri içeren bilgi güvenliği riskleri hakkında yeterli bilgi ve farkındalık sahibi değillerdir.

Sonuç olarak katımcıların "Kişisel verilerin korunması düzeyi yüksek, saldırı ve tehditlere yönelik farkındalık düzeyi orta, bilgi güvenliği farkındalığı genel düzeyi orta'' olarak saptanmıştır.

Araştırmadan elde edilen sonuçlardan şu öneriler çıkarılabilir;

Sadece teknoloji yöntemlerini kullanarak bilgi güvenliğinin sağlanması düşüncesinden uzaklaşıp insan faktörü sisteme dahil edilmeli, en üst yöneticiden başlayarak tüm personelin katılması sağlanmalıdır. Bilgi güvenliği süreci değişimlere ve iyileştirmelere ihtiyaç duymaktadır, güncelliğini koruma adına gerekirse bağımsız kurumlarca belli aralıklarla denetlenmeli, risk ve tehditler tanımlanmalı ve önlem alınmalıdır. Bilgi güvenliği farkındalığı çalışmaları belirli zamanda başlayan ve biten bir süreç olmamalı ve kurum kültürü haline getirilmelidir.

KAYNAKÇA

- Keser, H., Güldüren, C.(2015). "Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması". K. Ü. Kastamonu Eğitim Dergisi, 23(3):1167-1184.
- Samy,GN.,Ahmad,R.(2009)."ThreatstoHealthInformationSecurity",FifthInternationalConferenceonInformation Assuranceand Security Xi'an, China,540-543.

- Appari, A., Johnson, ME. (2010). "Int. J. Internet and Enterprise Management", 6(4):279-314.
- Omotosho, A.,Emuoyibofarhe, J. (2014). "A Criticism of the Current Security, Privacy and Accountability Issues in Electronic Health Records". International Journal of Applied Information Systems, 8:11-18.
- Öğütçü, G., Gürel, N., Cula, S. (2011). "Elektronik Sağlık Kayıtlarının İçeriği, Hassasiyeti ve Erişim Kontrollerine Yönelik Farkındalık ve Beklentilerin Değerlendirilmesi". VIII. Ulusal Tıp Bilişimi Kongresi,Antalya, 88-96.
- Şahinaslan, E., Kandemir, R., Şahinaslan, Ö.(2009). "Bilgi Güvenliği Farkındalık Eğitimi Örneği", Akademik Bilişim 09-11. Akademik Bilişim Konferansı Bildirileri, Urfa, 67:189-194.
- SağlıkBakanlığıSağlıkBilgiSistemleriGenelMüdürlüğü(2014).BilgiGüvenliği-PolitikalarKılavuzu
- Yılmaz,E.,Şahin,Y.L.,Akbulut,Y.(2016)."ÖğretmenlerinDijitalVeriGüvenliği-Farkındalığı".SakaryaUniversity Journal of Education,6(2):26-45.
- Ramachandran, S., Rao, V.S., Goles, T., Dhillon, G.(2016). "Variations in Information Security Culture Across Professions: A Qualitative Study". The University of Texas, College of Business, Working Paper, Texas, 22(7): 34- 38.
- Gerçeker, B.(2012)."Sağlık Kuruluşlarında Örgüt iklimi ve Bilgi Güvenliğinin İlişkisi" İzmir Dokuz Eylül Üniversitesi,SağlıktaKaliteGeliştirmeveAkreditasyonAnabilimDalıYüksekLisansTezi.
- Karadağ, M., Abuhanoğlu, H.(2015)."Sosyo-Kültürel Özelliklerin Bilgi Güvenliği Farkındalığı Üzerine Etkisi: Gülhane Askeri Tıp Fakültesi Eğitim Hastanesinde Bir Çalışma", The Journal of Academic Social Science Studies, (36):379-386

EKLER

I.BÖLÜM
(KİŞİSELBİLGİLER)

1.Cinsiyetiniz?
( ) Erkek ( ) Kadın

2.Yasınız.

( ) 20 den az ( ) 20-30 ( ) 31-40 ( ) 41-50 ( )51 ve üzeri

3. Eğitim Durumunuz.

( ) Lise ( ) Ön lisans ( ) Lisans ( ) Lisans Üstü

4.Göreviniz.

( ) Hekim ( ) Hemşire ( )Ebe ( ) Teknisyen ( ) Diğer

5.Çalıştığınız hastane türü.

( )Eğitim Araştırma ( )Hizmet Hastanesi ( )Dal Hastanesi

6.Toplam Is Tecrübeniz.

( ) 1 yıldan az ( ) 1-5 yıl arasında ( ) 6-10 yıl arasında ( ) 10 yıldan fazla

7.Mevcut Is Yerinde Çalışma Süreniz.

( ) 1 yıldan az ( ) 1-5 yıl arasında ( ) 6-10 yıl arasında ( )10 yıldan fazla

8.Kaç yıldır bilgisayar kullanıyorsunuz?

( ) 1-5 Yıl ( ) 11-15 Yıl ( ) 21-25 Yıl ( ) 31-35 Yıl ( ) 41 Yıl ve üzeri

( ) 6-10 Yıl ( ) 16-20 Yıl ( ) 26-30 Yıl ( ) 36-40 Yıl

9.Kaç yıldır internet kullanıyorsunuz?

( ) 1-5 Yıl ( ) 11-15 Yıl (+) 21-25 Yıl ( ) 31-35 Yıl ( ) 41 Yıl ve üzeri

( ) 6-10 Yıl ( ) 16-20 Yıl ( ) 26-30 Yıl ( ) 36-40 Yıl

II. BÖLÜM

(BİLGİ GÜVENLİĞİ FARKINDALIK DÜZEYİ BELİRLEME ÖLÇEĞİ)

Aşağıda bilgi güvenliği farkındalığına yönelik görüşlerinizi tanımlayan 34 madde bulunmaktadır. Aşağıdaki ifadelere ne derece katılıp-katılmadığınızı seçeneğin yanındaki kutuya (X) işareti koyarak belirtiniz. Lütfen her soruyu dikkatli okuyunuz ve boş madde bırakmayınız.

	Maddeler	Hiç Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Tamamen Katılıyorum
1	Bilgisayarıma kötü niyetli kod (malicious code) bulaşıp bulaşmadığını anlayabilirim.					
2	Kötü niyetli yazılımlara (malware) karşı alınması gereken güvenlik tedbirlerini biliyorum.					
3	Aldatmaca (hoax) nedir biliyorum.					
4	Zincir e-postalara (chain e-mail) karşı nasıl hareket etmem gerektiğini biliyorum.					
5	Bilgisayarımda casus yazılım (spyware) olup olmadığını anlayabilirim.					
6	Bilgisayarıma casus yazılım yüklenmesini engelleme yöntemlerini biliyorum.					
7	Kimlik hırsızlığı (identity theft) nedir biliyorum.					
8	Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.					
9	Sahte virüs koruma yazılımının ne olduğunu biliyorum.					
10	Hizmet aksatrma (Denial of Service - DoS) saldırısı nedir biliyorum.					
11	Kimlik avı (phishing) saldırısı nedir biliyorum.					
12	Sosyal mühendislik (social engineering) saldırısı nedir biliyorum.					
13	Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum.					
14	Siber zorbalık (cyberbullying) nedir biliyorum.					
15	Siber zorbalığa karşı kendimi nasıl koruyacağımı biliyorum.					
16	Siber zorbalığa karşı çocuklarımı nasıl koruyacağımı biliyorum.					
17	Bilgi güvenliğinin ne anlama geldiğini biliyorum.					
18	Bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum.					
19	Kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum.					
20	Bilgi sistemlerinde kullanılan virüs koruma yazılımını nasıl kullanacağımı biliyorum.					
21	Bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (realtime protection) özelliğini kullanmaktayım.					
22	Bilgisayarımdaki virüs koruma yazılımının otomatik güncelleştirme yapmasını sağlayabilirim.					

23	Dijital imza (digital signature) nedir biliyorum.					
24	Şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum.					
25	E-posta gönderirken "Gizli" (BCC) alanının sağladığı avantajları biliyorum.					
26	İstenmeyen elektronik posta (spam) nedir biliyorum.					
27	İstenmeyen elektronik posta miktarını azaltmak için gerekli bilgiye sahibim.					
28	Sosyal ağ sitelerini (social networking sites) güvenli olarak nasıl kullanacağımı biliyorum.					
29	USB sürücülerini (USB drives) kullanırken dikkat edilmesi gereken hususları biliyorum.					
30	Taşınabilir cihazlara (portable devices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum.					
31	Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.					
32	Kişisel mahremiyet nedir biliyorum.					
33	Çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum.					
34	Mavidiş (Bluetooth) teknolojisi ile veri aktarımı konusunda bilgi sahibiyim.					

Teşekkürler...