



Dijital Veri Güvenliği Farkındalığı ve Bilgi Okuryazarlığı ile Alınan Hizmetiçi Eğitimin Etkisi¹

MAKALE TÜRÜ	Başvuru Tarihi	Kabul Tarihi	Yayın Tarihi
Araştırma Makalesi	06.12.2018	08.08.2019	25.10.2019

Ümmühan Avcı ² ve Esin Arslan ³
Başkent Üniversitesi

Öz

Bu araştırmanın amacı kamuya hizmet veren bir kurumda çalışmakta olan bireylerin dijital veri güvenliği farkındalıkları ve bilgi okuryazarlıkları ile aldıkları hizmetiçi eğitimin etkisinin incelenmesidir. Açıklayıcı sıralı karma yöntemle gerçekleştirilen bu araştırmanın çalışma grubunu 37'si kadın, 32'si erkek olan 69 personel oluşturmaktadır. Katılımcıların 47'si daha önce "Bilgi ve Dijital Veri Güvenliği" konulu bir hizmetiçi eğitim almış, 22'si ise almamıştır. Bu çalışmada veriler "Bilgi Okuryazarlığı Ölçeği" ve "Dijital Veri Güvenliği Farkındalığı Ölçeği" ile toplanmıştır. Ayrıca katılımcıların görüşleri yarı yapılandırılmış açık uçlu sorular aracılığı ile toplanmıştır. Verilerin analizinde Pearson Korelasyon ve MANOVA kullanılmıştır. Açık uçlu sorulardan elde edilen verilere içerik analizi yapılmıştır. Yapılan analizler sonucu; katılımcıların bilgi okuryazarlığı ile dijital veri güvenliği farkındalığı arasında orta düzeyde pozitif ve anlamlı bir ilişki olduğu görülmüştür. Ancak katılımcıların aldıkları hizmetiçi eğitimin, onların dijital veri güvenliği farkındalığı ve bilgi okuryazarlığına anlamlı bir etkisinin olmadığı saptanmıştır. Bu bulgunun olası nedenlerini araştırmak için katılımcıların hem aldıkları hizmetiçi eğitimin içeriğine hem de veriliş yöntemine ilişkin ayrıntılı görüşleri alınmıştır. Bu görüşler doğrultusunda katılımcılara yüz yüze eğitimler dışında çevrimiçi eğitimler de verilmesi, sanal dünyalar oluşturulması, sosyal ağlar üzerinde grup etkinlikleri ve çokluortam etkinlikleri oluşturulması gibi farklı eğitim içeriği ve yöntemlerine ilişkin önerilerde bulunulmuştur.

Anahtar sözcükler: Dijital veri güvenliği farkındalığı, bilgi okuryazarlığı, hizmetiçi eğitim.

¹Bu çalışmanın özeti 12th. International Computer & Instructional Technologies Symposium'da sunulmuştur.

²Sorumlu Yazar: Doç. Dr., Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, E-posta: uavci@baskent.edu.tr, <https://orcid.org/0000-0001-7007-1478>

³Öğrenci, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, E-posta: esin.kokturkar@baskent.edu.tr, <https://orcid.org/0000-0002-5201-2009>

Çağımızda teknolojinin hızlanarak ilerlemesi nedeniyle bireylerin içinde bulunduğumuz bilgi çağı olarak adlandırılan 21. yüzyıla ayak uydurmak zorunda oldukları bilinen bir gerçektir. Ancak yaşamakta olduğumuz 21. yüzyıl birçok değişikliğe tanıklık etmektedir. Teknoloji alanında birbirini izleyen hızlı gelişmeler, bu değişikliklerin en önemli nedenlerinden biridir. Bu yüzyılda toplumların gereksinimleri değişmiş, gelişmelere uyum sağlamak tüm bireyler için neredeyse zorunlu duruma gelmiş ve böylece ortaya bilgi toplumu kavramı çıkmıştır. Candy'e (2002) göre değişikliklere uyum sağlayabilenlerin işe alınmaları ve diğerleriyle yarışabilmeleri kolaylaşacak ve bu kişiler öne çıkacaklardır. Bilgi toplumundaki bu yenilenme sürecinde payı büyük olan bilgi ve iletişim teknolojileri; elektronik devlet, imza, öğrenme, ticaret, bankacılık ve iletişim gibi pek çok alanda yaşamımıza girmiştir. Günümüz bilgi çağında bilgisayar veya bilişim teknolojilerinin kullanıldığı, temel ekonomik etkinliklerin bilgi üzerine kurulduğu, insan kaynaklarını ve ticari uygulamaları bir araya getiren bilgi hizmetlerinin şekillendiği, bilginin ve bilgi kaynaklarının önem kazandığı bir toplum olabilmek önem kazanmıştır. Dolayısıyla, bilginin güvenliğini sağlayabilmek de çok önemli olmuştur. İnternetin yaygınlaşmasıyla bilişim sistemlerindeki bütünlük, gizlilik ve sürekliliğin sağlanması için birçok proje geliştirilmiş ve geliştirilmeye devam etmektedir. Böylece bilginin dijital ortamlarda üretilmesi ve saklanması ile bu verilerin güvenliğinin sağlanması önemlidir (Çek, 2017; Vural ve Sağıroğlu, 2008).

Toplumların ve ekonomilerin bilgiye dayalı olarak şekillendiği günümüzde, toplumsal yapıdaki değişimlerin getirisi olarak bireylerin sahip olması gereken özellikleri de yeniden gözden geçirerek güncelleştirmesi zorunlu olmuştur (Yüksel ve Adıgüzel, 2011). Bilgi ve bilgi ile ilgili beceriler (bilginin bulunması, üretilmesi, iletilmesi vb.) bilgi toplumunun bireylerinde bulunması gereken en önemli özelliklerin başında gelmektedir. Bu beceriler "bilgi okuryazarlığı" kavramı içinde değerlendirilmektedir. Bilginin üretimi, hızı, türü, yayılması ve güvenliği gibi öğelerin önem kazanması nedeniyle doğru ve güvenilir bilgiyi elde etmek için bilgi okuryazarı olmak önemli duruma gelmiştir (Aharony ve diğ., 2017; Polat ve Odabaş, 2008).

Bilgi ve Bilgi Okuryazarlığı

Bilgi bireylerin yaşamını, davranışını, iletişimini, gelişimini, üretmesini, tüketmesini vb. özelliklerini belirleyen etkenlerin başında yer almaktadır. Konuyla ilgili alanyazın tarandığında bilgi okuryazarlığına ilişkin birçok tanım bulmak olanaklıdır. Bilgi okuryazarlığı, gerekli bilginin kapsamını belirleme, etkili ve verimli bir şekilde bilgiye ulaşma, bilgiyi eleştirel bir bakış açısıyla değerlendirme, seçilen doğru bilgileri özümseme, etik ve yasal süreçleri göz önünde bulundurarak bilgiye erişme ve kullanma becerileridir (ACRL, 2000). Bilgi okuryazarlığı ayrıca bireylerin mesleki, sosyal, kişisel ve eğitimsel amaçlarına ulaşabilmeleri için, her alanda ve her zaman bilgiyi etkin bir biçimde arama, kullanma, yorumlama veya yeniden yapılandırma yeteneklerini kazanmaları şeklinde de yorumlanmıştır (Garner, 2006). Bilgi okuryazarlığı beceri ediniminin ötesinde, her biri farklı biçimlerdeki bilgilerle etkileşime giren ve dönüştürücü etki ile tamamlanan kapsamlı bir süreçtir. Bu tanıma

göre, bilgi okuryazarlığı yaşam boyu öğrenmenin temelidir. Çünkü eleştirel ve bağımsız öğrenmeyle desteklenen çok yönlü bir okuryazarlık gerektirir (Andretta, 2007). Bilgi okuryazarlığına ilişkin yapılan tanımlardan, bu kavramın yaşamın tüm alanlarındaki diğer okuryazarlık bilgi ve becerileriyle ilişkilendirildiği görülmektedir.

Tanımlar benzer yönler barındırmakla birlikte farklılıklar da göstermektedir. Ancak zaman içindeki gelişimleri izlendiğinde, kapsamın giderek genişlediği algısına ulaşılabilir. Bunun başlıca nedenleri, kavram kargaşasının önüne geçilmesi gereksinimi ve teknolojik gelişmelerle birlikte kavramın evrilmeye devam etmesi olarak açıklanabilir. Bu bağlamda bilgi okuryazarlığı kavramının, temel bilgi ve becerileri içermenin yanında teknolojik becerileri, bağımsız ve yaşam boyu öğrenme becerilerini, iletişim ve değişikliğe uyum sağlama becerilerini, eleştirel düşünme, sentezleme ve analiz etme becerilerini kapsayacak şekilde geliştiği gözlenmektedir.

Kurbanoglu (2010) bilgi okuryazarlığı becerilerini; temel bilgi becerileri, üst düzey düşünme becerileri ve bireysel bilgi becerileri olarak sınıflandırmıştır. Temel bilgi becerileri; bilgiye gereksinimi fark edip tanımlama, bilgiyi arama teknikleri geliştirme, bilgiyi bulma, sınıflama, kullanma, yorumlama, bütünleştirme ve iletme becerileri olarak tanımlanabilir. Üst düzey düşünme becerileri; sorgulayıp karar verme, analitik düşünerek sorun çözme, sentezleme, yaratıcı düşünerek yeni bilgi oluşturma ve bilgiyi içselleştirme becerilerini kapsar. Bireysel bilgi becerileri ise; iletişim ve işbirliği içerisinde takım çalışması, kişisel güdüleme gibi becerilerden oluşur.

Bilgi okuryazarı olan bireyler, öğrenmeyi öğrenmiş olan bireylerdir; dolayısıyla bilgiye ulaşabilen, bilgiyi düzenleyebilen ve diğer bireylerin öğrenebileceği şekilde bu bilgiyi nasıl düzenleyebileceğini bilen bireylerdir (Tuncer ve Balcı, 2013). Bilginin önemli olduğu, çeşitlendiği ve karmaşıklaştığı bir dönemde bilgiyi üretmek, bilgiyi yapılandırmak, bilgi alarak ve vererek bilgiyi paylaşmak ve bilgiye erişmek için teknolojinin kullanılması bilgi okuryazarlığı için önemlidir (Polat ve Odabaş, 2008). Alanyazında bilgi okuryazarlığı ile ilgili yapılan son raporlar, bilgi okuryazarlığının ve ilgili yetkinliklerin, eleştirel düşünmenin ve yaşam boyu öğrenmenin, işverenler için çok önemli olduğunu ortaya koymaktadır. Bilgi okuryazar işgücüne gereksinim duyulmasının ivediliği konusunda giderek artan bir fikir birliğine varılmıştır (American Management Association [AMA], 2012; Zhang, 2010; Perrault, 2007; Hart, 2005; Goad, 2002). Dolayısıyla kurum çalışanlarının çağımız bilgi toplumunun en önemli özelliklerinden olan bilgi okuryazarı olması önemlidir. Bu konuda hazırlanacak olan hizmetiçi eğitim programlarının, çalışanların bilgi okuryazarlık düzeylerine de katkı sağlayacağı düşünülmektedir.

Bilgi ve Dijital Veri Güvenliği

Bilişim teknolojilerinde yaşanan hızlı gelişmelerle birlikte açığa çıkan teknolojik dönüşüm sonucu daha büyük bilgiler daha küçük aygıtlar ile saklanabilir, çoğaltılabilir ve taşınabilir duruma gelmiştir. Bilgisayar, cep telefonu, internet, akıllı cihazlar gibi araçların etkin kullanılması ile birlikte bilgi güvenliği kavramı ortaya çıkmıştır. Bu süreçte bilgi alma ve verme gibi bilgi paylaşma davranışları (Ergün ve

Avcı Yücel, 2015) artmış ve bu durum bilgi güvenliği tanımının da değişmesine ve daha çok önem kazanmasına neden olmuştur.

Dijital veri güvenliği kavramı, çağımız bilgi güvenliği kavramına bilişim teknolojileri açısından bakıldığında öne çıkmaktadır (Yılmaz, Şahin ve Akbulut, 2015). Dijital verilerin işleme süreci, uygulama yazılımları ve internet ile ilgili gelişmeler ışığında daha da hızlanmıştır. İnsan yaşamını kolaylaştırmaya yarayan bu gelişmeler uygunsuz kullanım, bireylerin bilgi güvenliği tehditlerine karşı bilgisizliği, risk algısı zafiyeti ve telafisi güç sayılabilecek bilgi güvenliği risklerini de yanında getirmiştir. Telif hakları ve etik, gizlilik, şifreleme gibi elektronik ortamda verilerin korunması amacıyla dijital verilerin güvenliği önem kazanmıştır. Günümüzde bilgi güvenliği ISACA (2009) tarafından bilginin gizliliğini, bütünlüğünü ve istenilen zamanda erişilebilirliğini sağlamak olarak tanımlanmıştır. Bilginin gizliliği; bilginin yetkisiz kişilerin eline geçmemesini ve yetkisiz kişiler tarafından erişilmesini; bilginin bütünlüğü; yetkisiz kişilerce bilgiye karışılması, silinmesi, değiştirilmesi ya da herhangi bir şekilde zarar görmesinin önlenmesini, bilgiye erişilebilirlik; gereksinim duyulduğunda bilginin ilgili kişilerce ulaşılabilir ve kullanılabilir olmasını belirtir. Birbirinden bağımsız düşünülemeyecek bu bileşenler, bilgi güvenliğinin temel öğeleridir. Bilgi güvenliği sürecinde yer alan dijital veri güvenliği kavramı ise, dijital verilerin saklanması, çoğaltılması ve başka bir kaynağa taşınması sürecinde bütünlüğün bozulmasını önlemek ve izinsiz erişimlerden korumak için güvenli uygulama ortamı oluşturma çabası (Canbek ve Sağiroğlu, 2006) olarak açıklanmaktadır.

Yapılan bazı araştırmalar; insan etkeni dikkate alınmayarak gerçekleştirilecek sistemsel güvenlik uygulamalarının, dijital veri güvenliği risklerini gidermede etkisiz ve yetersiz olabileceğini göstermektedir (Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009; Yılmaz ve diğ., 2015). Ancak bireylerin üzerinde oluşturulacak olan farkındalıkla riskler giderilebilecek ya da olası en düşük düzeyde tutulabilecektir. Dolayısıyla özellikle kurumlarda yeni işe başlayanlar olmak üzere tüm çalışanlara, kurumun bilgi ve dijital veri güvenliği politikaları ile ilgili farklı kategorilerde hizmetiçi eğitim programları hazırlayarak bireylerin üzerinde farkındalık oluşturmak, bir gereksinim gibi görünmektedir. Hizmetiçi eğitim, bir kişiye gereken bilgi, beceri ve davranışların işinin gerektirdiği başarı düzeyine ulaşması için sistemli ve planlı bir şekilde öğretilmesidir (Can, Akgün ve Kavuncubaşı, 1995). Alanyazına göre belirtilen hizmetiçi eğitim ve farkındalık etkinlikleri kurumlarda en üst yönetimlerden başlanarak sıradizinin altlarında yer alan bütün kullanıcılara yönelik olarak hazırlanmalı ve sunulmalıdır (Şahinaslan ve diğ., 2009).

Araştırmanın Amacı ve Önemi

Teknolojik gelişmelere bağlı olarak ortaya çıkan bilgi okuryazarlığı ve dijital veri güvenliği farkındalığı günümüzde önemli konular arasına girmiştir. Birbiriyle ilişkili olduğu düşünülen bilgi okuryazarlığı ve dijital veri güvenliği farkındalığı konularında bilgi sahibi olabilmek için verilen hizmetiçi eğitimlerin ne kadar etkili olduğu, eksik yönlerinin neler olduğu ve nasıl geliştirilebileceği üzerine araştırmalar yapılması önem kazanmaktadır. Bilgi okuryazarlığı, bilgi toplumu ve bilgi

ekonomisinin temel bir disiplindir ve daha geniş anlamda eğitsel bağlamda çok az ilerleme kaydetmiştir. Bilgi okuryazarlığı yasadışı ve zararlı içeriğin çevrimiçi ve diğer yeni teknolojiler aracılığıyla yayılmasının etkileriyle mücadele etmektedir. Bu mücadelenin diğer adı, dijital veri güvenliği farkındalığının sağlanmasıdır. Temel anlamda oluşturulacak bir bilgi ve dijital veri güvenliği eğitimi ile bireylere bilgiye ilişkin temel kavramlardan başlanarak bilginin erişilebilirliğini, korunmasını, gizliliğini ve güvenliğini içeren hizmetçi eğitimler verilmesi önemlidir. Kurumlarda dijital veri güvenliği ile ilgili yasal düzenlemeler ve bunun yanı sıra bireysel sorumluluklar konusunda çalışanların bilgilendirilmesi için politikalar düzenlenmesine gereksinim vardır.

Maddi zarara ve yaşamsal tehlikeye yol açabilecek dijital veri güvenliği ile ilgili hem bireysel, teknik önlemler hem de yasalar yoluyla önlemler alınabilir. Ancak bu önlemlerin en başında insan etkeni yer almaktadır (Yılmaz, Şahin ve Akbulut, 2016). Bireyler ve kuruluşlar genellikle ciddi bir sorun yaşadıkları zaman bilgi güvenliği konusunda önlemler almaktadırlar. Oysa bilgi güvenliği işleyişin en başından en sonuna kadar önemli bir konudur. Bu nedenle bilgi güvenliği konusunda farkındalığın (Kruger ve Kearney, 2006) artırılması, böylece bilgi güvenliği kültürünün (Da Veiga ve Eloff, 2010; Nasir, Arshah, Ab Hamid ve Fahmy, 2019) bilgi okuryazarlığı desteği ile oluşturulması büyük önem taşımaktadır. Dolayısıyla dijital çağda vazgeçilmez olan bu iki kavram arasındaki ilişkinin incelenmesi önemlidir (Ramalho Correia ve Carlos Teixeira, 2003). Bu bağlamda nitelikli ve etkili hizmetçi eğitim vermeye önem göstermek gerekmektedir. Bilgi güvenliğine yönelik hizmetçi eğitim programlarının bireylerin istekleri dikkate alınarak etkileşimli bir şekilde düzenlenmesi gerekmektedir (Şahinaslan ve diğ., 2009). Böylece bireylerin bilgi okuryazarlıklarını ve dijital veri güvenliği farkındalık düzeylerini artırmak planlanmaktadır. Bir başka açıdan verilen hizmetçi eğitimlerin etkili olup olmadığını, bireylerin bilgi okuryazarlıkları ve dijital veri güvenliği farkındalıkları arasında bir ilişki olup olmadığını belirlemek bu sürece çok yönlü olarak bakabilmeyi destekleyecektir. Bu bağlamda bu çalışmada kamuya hizmet veren bir kurumda çalışanların dijital veri güvenliği farkındalıkları ve bilgi okuryazarlıkları ile aldıkları hizmetçi eğitimin etkisinin incelenmesi amaçlanmıştır.

Araştırmanın alt problemleri şu şekildedir:

1. Bireylerin bilgi okuryazarlığı ve dijital veri güvenliği farkındalıkları arasında anlamlı bir ilişki var mıdır?
2. Bireylerin bilgi okuryazarlığı ve dijital veri güvenliği farkındalıkları hizmetçi eğitim alma durumlarına göre anlamlı farklılık göstermekte midir?
3. Bireylerin uygulanan hizmetçi eğitim programına ilişkin görüşleri nelerdir?

Yöntem

Bu çalışmada nicel ve nitel yöntemlerin bir arada ele alındığı karma araştırma yöntemi kullanılmıştır. Karma araştırma yöntemlerinden ise açıklayıcı sıralı karma yöntem (Explanatory Sequential Mixed Design) kullanılmıştır. Bu araştırma

kapsamında nicel verilerin derlenmesinin ardından bu verileri açıklamak amacıyla nitel veriler toplanmıştır (Creswell, 2009).

Katılımcılar

Araştırmaya Ankara’da kamuya hizmet veren ve dijital veri güvenliği işleyişinin önemli olduğu büyük ölçekli bir kurumda çalışmakta olan 69 personel katılmıştır. Araştırmanın gerçekleştirildiği kurumda toplam 15 birim bulunmaktadır. Uygulamalar bu birimlerden 13’ünde bulunan personel üzerinde yürütülmüştür. Kalan iki birime izin alınamadığı için ulaşılamamıştır.

Dağıtılan 98 anketten 71’inden dönüt alınabilmiştir. Ancak 2 anket eksik işaretlendiği için araştırma dışı bırakılmış ve sonuç olarak toplam 69 gönüllü katılımcı üzerinden analizler gerçekleştirilmiştir. Katılımcıların yaşları 25 ile 57 aralığında olup demografik özellikleri Tablo 1’de yer almaktadır.

Tablo 1

Katılımcıların Demografik Özellikleri

Cinsiyet	f	%
Erkek	32	46.4
Kadın	37	53.6
Toplam	69	100
Öğrenim Düzeyi	f	%
Lise	2	2.9
Önlisans	12	17.4
Lisans	31	44.9
Yüksek Lisans	22	31.9
Doktora	2	2.9
Toplam	69	100

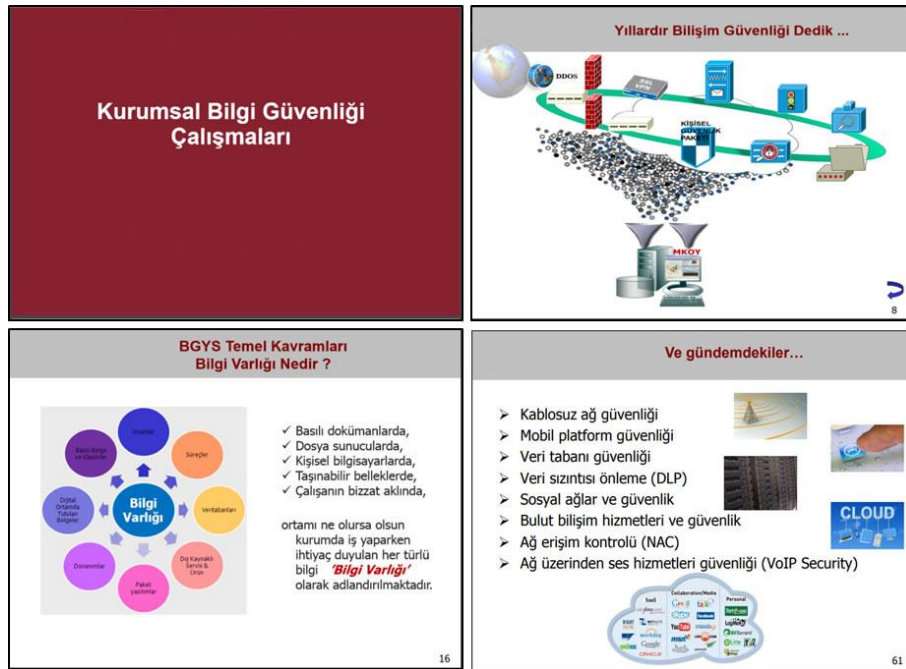
Araştırmaya katılan 69 kişinin 30’unun (% 43.5) öğrenim gördüğü bölümün Bilgi İletişim Teknolojileri (BİT) ile ilişkili, 39’unun (% 56.5) ise ilişkisiz olduğu belirlenmiştir. Bunun yanında araştırmaya katılanların 47’si (% 68.1) daha önce “Bilgi ve Dijital Veri Güvenliği” konulu bir eğitim almış, 22’si (% 31.9) ise daha önce böyle bir eğitim almamıştır. Buradaki dağılım müdahalesiz olup tamamen gönüllü katılımcıların daha önce eğitim alıp almama durumuna göre gerçekleşmiştir.

Hizmetçi Eğitimin İçeriği

Çalışanlara; bilgi ve bilişim güvenliği temel kavramlarını tanıtmak, dijital veri güvenliği risklerine karşı alınması gereken önlemler ile ilgili bilgi vermek ve kurumda yapılan çalışmalar konusunda bilgilendirmek amacıyla bir günlük hizmetçi eğitim yapılmıştır. Ancak ilgili kurumda dijital veri güvenliği farkındalığı sağlamak amacıyla bu ve benzeri eğitimler belirli aralıklarla yapılmıştır ve yapılmaya devam etmektedir. Verilen eğitimler iki bölümden oluşmaktadır. Birinci bölümde; bilginin önemi ve bilgi güvenliği, bilişim güvenliği tehditleri ve alınabilecek önlemler, bilgi güvenliği yönetim sistemi ve uygulanmasının önemi konularına yer verilmiş olup

belirtilen konuları aktarmak üzere bir danışmanlık firması eğitmeni görevlendirilmiştir. İkinci bölümde ise; risk analizi ve risk yönetimi, kurumsal bilgi güvenliği ve bilgi güvenliği politikası, kurumsal bilgi güvenliği yönetim sistemi konularına yer verilmiş olup kurum çalışanlarından bu konuda uzman bir personel konuyu aktarmak üzere görevlendirilmiştir. Kurumun bilgi güvenliği biriminde çalışan bu uzman personel, kurumda ortaya çıkacak olası dijital güvenlik risklerine karşı deneyimli ve uygulanması gereken politikaları ve bilgi güvenliği yönetim sisteminden sorumlu kişidir. Buradaki amaç bu bilgilerin kurumun tüm personeline aktarılmasını sağlamak ve böylece kurumun dijital güvenliğini güvence altına almaktır. Eğitimin içeriği danışman firma ve uzman personelce belirlenmiştir.

Eğitim resim ve metinlerden oluşan PowerPoint sunumları aracılığıyla yapılmıştır. PowerPoint dışında herhangi bir dijital öğretim teknolojisi ya da materyalinden yararlanılmamıştır (Şekil 1). Yüz yüze gerçekleştirilen eğitimde sunuş yoluyla öğretim ve soru-cevap yöntemi kullanılmıştır. Araştırmacılar söz konusu eğitime katılmamıştır.



Şekil 1. Verilen hizmetçi eğitimde kullanılan sununun ekran görüntülerinden örnekler

Veri Toplama Araçları

“Bilgi Okuryazarlığı” düzeyinin belirlenmesine yönelik Adıgüzel (2011) tarafından geliştirilmiş olan ölçek, çalışmanın içeriği yönüyle uyumlu bulunmuş ve

araştırmacının izni alınarak bu çalışmada kullanılmıştır. Beşli likert tipinde olan bu ölçekte 5 “Her zaman”, 4 “Çoğu zaman”, 3 “Bazen”, 2 “Ara sıra” ve 1 “Hiçbir zaman” için kullanılmıştır. Adıgüzel (2011) tarafından yürütülen çalışmaya 230 gönüllü öğrenci katılmıştır. Ölçek bilgiye erişme, bilgiyi kullanma, bilgi gereksinimini tanımlama, bilgiyi kullanmada etik ve yasal düzenlemeler olmak üzere toplam 4 faktörden oluşmaktadır. Ölçeğin Cronbach Alpha iç güvenilirlik katsayısı 0.928 bulunmuştur. Ölçek maddelerinde olumlu ya da olumsuz madde ayrımı yoktur. Ölçekten en yüksek 145 puan, en düşük 29 puan alınabilmektedir.

“Dijital Veri Güvenliği Farkındalığı” düzeyinin belirlenmesine yönelik olarak ise Yılmaz ve diğ. (2015) tarafından geliştirilmiş olan “Dijital Veri Güvenliği Farkındalığı Ölçeği” araştırmanın içeriği yönüyle uyumlu bulunmuş ve yine araştırmacının izni alınarak bu çalışmada kullanılmıştır. Araştırmacılar tarafından ölçek hazırlanma sürecinde alanyazın taraması yapılmış ve 93 maddeden havuz oluşturulmuştur. Ölçeğin yapı geçerliğini belirlemek için açımlayıcı faktör analizi yapılmıştır. Cronbach Alpha iç güvenilirlik katsayısı 0.945 bulunmuştur. Beşli likert tipinde olan bu ölçekte 5 “Kesinlikle Katılıyorum” ve 1 “Kesinlikle Katılmıyorum” aralığında dereceleme yapılmıştır. Araştırmacıların elde ettiği ölçekte daha sonra doğrulayıcı faktör analizi gerçekleştirilmiştir. Sonuçta 32 madde ve tek faktörden oluşan bu ölçek toplam 935 katılımcıya uygulanmıştır.

Bu araştırma kapsamında katılımcıların bilgi okuryazarlık düzeylerini belirlemek üzere Adıgüzel (2011) tarafından geliştirilmiş olan, 29 sorudan oluşan “Bilgi Okuryazarlığı Ölçeği” ve katılımcıların bilgi güvenliği farkındalık düzeylerini belirlemek üzere Yılmaz ve diğ. (2015) tarafından geliştirilmiş olan, 32 sorudan oluşan “Dijital Veri Güvenliği Farkındalığı Ölçeği” kullanılmıştır. Veri toplama araçları e-posta aracılığıyla ya da basılı olarak katılımcılara dağıtılmış ve doldurmaları için iki hafta süre verilmiştir.

Ayrıca nicel verilerden elde edilecek bulguların olası nedenlerini açıklayabilmek ya da destekleyebilmek, verilen eğitimin içeriğine ilişkin bilgi elde edebilmek ve katılımcıların görüşlerini alabilmek amacıyla açık uçlu sorulardan oluşan yarı yapılandırılmış bir form oluşturulmuştur. Alanda uzman bir öğretim üyesinin de görüşleri alınmış ve bu görüşler çerçevesinde gerekli düzeltmeler yapıp forma son şekli verilerek odak görüşme grubuna uygulanmıştır. Aşağıda açık uçlu sorular yer almaktadır.

1. Aldığımız “Bilgi ve Dijital Veri Güvenliği” eğitiminin içeriğine ilişkin görüşlerinizi aşağıdaki soruları yanıtlayarak açıklayınız.
 - a. Sizce eğitimin içeriği ve eğitimde kullanılan materyaller (sunum vb.) yeterli miydi? Yanıtınız evet ise hangi yönleriyle yeterliydi? Açıklayınız.
 - b. Sizce eğitimin içeriği ve eğitimde kullanılan materyaller (sunum vb.) yetersiz miydi? Yanıtınız evet ise hangi yönleriyle yetersizdi? Eğitim içeriğine neler eklenmesini önerirsiniz? Açıklayınız.

2. Aldığınız “Bilgi ve Dijital Veri Güvenliği” eğitiminin verilme şekline ilişkin görüşlerinizi aşağıdaki soruları yanıtlayarak açıklayınız.
 - a. Sizce bu eğitim sadece yüz yüze eğitim yerine uzaktan eğitimle mi verilmeliydi? Açıklayınız.
 - b. Sizce bu eğitim hem yüz yüze hem de uzaktan eğitim birlikte kullanılarak mı verilmeliydi? Açıklayınız.
3. Diğer önerileriniz.

Verilerin Analizi

Nicel verilerin analizinde normallik varsayımı için gruplar arası basıklık ve çarpıklık katsayıları test edilmiştir. Bağımsız değişkenler için çarpıklık katsayıları -0.107 ile -0.664 arasında, basıklık katsayıları 0.154 ile 0.657 arasında bulunmuştur. Bağımlı değişken için çarpıklık katsayısı 0.795, basıklık katsayısı -1.410 bulunmuştur. Bu dağılımların normal aralıkta (-1.5 +1.5) olduğu görülmüştür (Tabachnick ve Fidell, 2013). Verilerin analizinde SPSS 19.0 paket programı kullanılmıştır. Anlamlılık düzeyi için $p < .01$ alınmıştır.

Verilerin analizi sürecinde “bilgi okuryazarlığı” ile “dijital veri güvenliği farkındalığı” arasındaki ilişkiyi belirlemek için basit korelasyon (Pearson korelasyon katsayısı) analizi kullanılmıştır. Bunun yanında katılımcıların “bilgi ve dijital veri güvenliği eğitimi” alma durumlarına göre “bilgi okuryazarlığı” ve “dijital veri güvenliği farkındalığı” düzeylerinde anlamlı bir fark olup olmadığını araştırmak için tek yönlü çok değişkenli varyans analizi (MANOVA) kullanılmıştır. Varyans-kovaryans matrisliği homojenliği varsayımı için Box’s M testi sonuçları ($M=2.736$, $F=0.87$, $p=.452$) ve Levene testi sonuçları incelenmiş, bilgi okuryazarlığı için ($F=0.304$, $p=.583$) değerleri ve dijital veri güvenliği için ($F=2.030$, $p=.159$) değerleri bulunmuştur.

Araştırmada bilgi ve dijital veri güvenliği” hizmetiçi eğitimini alan 47 katılımcının 29’undan açık uçlu sorulara yanıt alınabilmiştir. Bu eğitime ilişkin katılımcı görüşleri sonucu elde edilen veriler içerik analizi yöntemiyle değerlendirilmiştir. İçerik analizinde öncelikle birbiri ile benzerlik gösteren veriler belirli temalar kapsamında bir araya getirilir. Sonrasında bu kavramlar okuyucunun anlayabileceği biçime yönelik olarak yeniden sentezlenir ve yorumlanır (Yıldırım ve Şimşek, 2005). Bu kapsamda, bu çalışmada kodlama yöntemi kullanılarak veriler arası ilişkiler açığa çıkarılmış ve tümevarımcı yaklaşıma göre kodlanmıştır. Kodlanan veriler okuyucunun anlayacağı biçimde tema haline getirilmiş ve ortaya çıkan temalar yorumlanmıştır.

Geçerlik ve Güvenirlik

Bu çalışmada nicel veriler üzerinde hesaplanan Cronbach alfa iç tutarlık katsayısı sırasıyla “Bilgi Okuryazarlığı Ölçeği” için .91, ”Dijital Veri Güvenliği Farkındalığı Ölçeği” için .93 olarak bulunmuştur. Kayış (2009)’a göre alfa

katsayısının $0.80 \leq \alpha < 1.00$ aralığında olması ölçeğin yüksek derecede güvenilir olduğunu belirtmektedir.

Nitel verilerin analizinde bulguların inandırıcılığını artırmak için katılımcı kontrolü sağlanmıştır. Katılımcı kontrolü ile veriler analiz edildikten sonra katılımcılara bulgular gösterilerek yapılan yorum ve analizlerin yaşantılarını yansıtmayı yansıtmadığı değerlendirilmektedir (Cho ve Trent, 2006). Creswell'e (2009) göre, nitel araştırmalarda tema ve kodların farklı araştırmacılar tarafından desteklenmesi gerçekleştirilen araştırmanın güçlenmesini sağlamaktadır. Bu çalışmada görüşmelerden elde edilen yanıtlarla oluşturulan veriler, araştırmacının kendisi ve bir uzman tarafından kodlanmış ve kodlayıcılar arası iç geçerlik katsayısı (Cohen's Kappa) 0.86 olarak bulunmuştur. Katılımcı görüşleri bulgular kısmında doğrudan alıntı yoluyla verilmiştir.

Bulgular

Bilgi Okuryazarlığı ve Dijital Veri Güvenliği Farkındalığı Arasındaki İlişki

Araştırma katılımcılarının “Bilgi okuryazarlıkları” ve “Dijital veri güvenliği farkındalıkları” arasındaki ilişki, Pearson korelasyon katsayısı ile incelenmiştir. Verilerin analizinde elde edilen korelasyon Tablo 2’de verilmiştir.

Tablo 2

<i>Bilgi Okuryazarlığı ve Dijital Veri Güvenliği Farkındalığı Arasındaki İlişki Sonuçları</i>		
Bilgi güvenliği farkındalığı ortalaması		
	r	.417*
Bilgi okuryazarlığı ortalaması	p	.000
	N	69

* $p < .01$, Pearson korelasyon katsayısı kullanılmıştır.

Tablo 2’deki verilerde bilgi okuryazarlığı ile dijital veri güvenliği farkındalığı arasında orta düzeyde pozitif ve anlamlı bir ilişki olduğu görülmektedir ($r=0.417$, $p < .01$). Büyüköztürk’e (2014) göre korelasyon katsayısı, mutlak değer olarak 0.70-1.00 arasında ise yüksek; 0.70-0.30 arasında ise orta; 0.30-0.00 arasında ise düşük düzeyde bir ilişkiyi göstermektedir. Buna göre bilgi okuryazarlığı düzeyi arttığında, dijital veri güvenliği farkındalığının da arttığı söylenebilir.

Hizmetçi Eğitim Alma Durumlarına Göre Bilgi Okuryazarlığı ve Dijital Veri Güvenliği Farkındalığı Analizi

Bilgi ve dijital veri güvenliği eğitimi alan ve almayan katılımcıların “bilgi okuryazarlığı” ve “dijital veri güvenliği farkındalık” düzeyleri bakımından anlamlı bir farklılık gösterip göstermediğine ilişkin tek faktörlü MANOVA uygulamasına ilişkin çıktılar incelenmiştir. Katılımcıların “bilgi ve dijital veri güvenliği eğitimi” alma durumlarına göre bilgi okuryazarlığı ve dijital veri güvenliği farkındalığı puanları üzerine yapılan MANOVA sonuçları, eğitimi alma veya almama bakımından anlamlı bir farklılık göstermediğini ortaya koymaktadır. [Wilks’ Lambda (Λ)=0.966, $F_{(2)}$

$t(66)=1.14, p>0.01$ ($p=.325$)). Bu bulgu, bilgi okuryazarlığı ve dijital veri güvenliği farkındalığı puanlarından oluşan doğrusal bileşenlerden elde edilecek puanların eğitimi alma durumuna bağlı olarak değişmediğini gösterir.

Tablo 3

Bilgi Okuryazarlığı ve Dijital Veri Güvenliği Farkındalığı Puanlarının Hizmetçi Eğitim Alma Durumuna Göre Ortalama ve Standart Sapma Değerleri ve ANOVA Sonuçları

Değişken	Hizmetçi Eğitim	n	\bar{x}	S	sd	F	p
Bilgi Okuryazarlığı	Alan	47	3.85	0.46	1-67	2.205	.142
	Almayan	22	4.03	0.43			
Dijital Veri Güvenliği Farkındalığı	Alan	47	4.27	0.48	1-67	0.841	.362
	Almayan	22	4.38	0.36			

Tek yönlü ANOVA sonuçlarına (Tablo 3) bakıldığında bilgi okuryazarlığı ($F_{(1, 67)}= 2.205, p>.01$) ve dijital veri güvenliği farkındalık ($F_{(1, 67)}=0.841, p>.01$) puanları hizmetçi eğitim alma durumuna göre anlamlı farklılık göstermemektedir.

Uygulanan Hizmetçi Eğitim Programına İlişkin Katılımcı Görüşleri

Hizmetçi eğitim alma durumuna ilişkin MANOVA bulgularının anlamlı çıkmamasının olası nedenlerini araştırmak için hizmetçi eğitim almış katılımcılara uygulanan açık uçlu soruların kodlayarak analizi yapılmış ve elde edilen sonuçlar iki başlık altında toplanmıştır.

Alınan hizmetçi eğitimin içeriğine ilişkin bulgular. Çalışma grubundaki katılımcılarla yapılan görüşmeler sonucunda alınan eğitimin içeriğine ilişkin olarak elde edilen bulgular Tablo 4'te verilmiştir.

Tablo 4

Hizmetçi Eğitimin İçeriğine İlişkin Temalar, Kodlar ve Kod Sıklıkları

İçerik	Kod Sıklıkları (f)	Toplam
Etkileşimli olmaması	5	25
Fazla kuramsal olması	4	
Gündelik yaşama uygun olmaması	3	
Sadece sunumdan oluşması	3	
Yetersiz	3	
Yüzeysel olması	3	
Akıcı bir anlatım olmaması	3	
Zengin/Dolu olmaması	2	
Yalın olmaması	1	
Güncel olmaması	1	
Anlaşılır olması	2	5
Yeterli	1	
Konu sıralaması olması	1	
Grafik ve görseller olması	1	
Sunum olması	1	

Katılımcılardan alınan “bilgi ve dijital veri güvenliği eğitimi”ne ilişkin verilerin değerlendirilmesi sonucunda verilen eğitimin içerik yönüyle yetersiz olduğu yönünde belirlemelerde bulunulmuştur. İçerik sırasıyla en çok etkileşimli olmama, fazla kuramsal olma, gündelik yaşama uygun olmama, sadece sunumdan oluşma, yüzeysel olma, akıcı olmama, zengin olmama, yalın ve güncel olmama yönleriyle yetersiz olarak değerlendirilmiştir. Bu konuda belirtilen bazı görüşler şöyledir:

“İçerik daha yalın ve gündelik yaşama uygun anlatılmalıydı. Fazla kuramsal buldum.” (K8).

“Eğitim içeriği yetersizdi, yüzeysel bir eğitimdi, daha interaktif olabilirdi.” (K17).

“İçeriği tam olarak yeterli bulmadım. Konunun ufak bir PP sunumundan öteye gitmesini bekledim. İnteraktif uygulamalar daha etkili olabilirdi.” (K22).

“Eğitimi içerik yönüyle yeterli bulmadım. Bence bir güne sığdırılabilecek kadar kısa bir konu değildi. Konunun her gün yeniden güncellenen bir konu olması nedeniyle anlatımı akıcı bulmadım.” (K3).

Bunun yanı sıra katılımcılar içeriği sırasıyla anlaşılır olma, sunum, konu sıralaması, grafik ve görseller yönleriyle yeterli değerlendirmiştir. Bu görüşlere bir örnek:

“Sunum içeriği yeterli ve etkiliydi. Konu sıralaması yönüyle başarılıydı. Kullanılan grafik ve görseller, konunun daha anlaşılır bir duruma gelmesine yardımcı oluyordu.” (K11).

Alınan hizmetiçi eğitimin veriliş biçimine ilişkin bulgular. Çalışma grubundaki katılımcılarla yapılan görüşmeler sonucunda alınan eğitimin verilme şekline ilişkin olarak elde edilen bulgular Tablo 5’te verilmiştir.

Tablo 5

Hizmetiçi Eğitimin Veriliş Biçimine İlişkin Temalar, Kodlar ve Kod Sıklıkları

	Verilme Şekli	Kod Sıklıkları (f)	Toplam
Yeterli	Yüz yüze olması	2	6
	Katılımcılar arası etkileşimli olması	2	
	Eğitmen-katılımcı etkileşimli olması	2	
Yetersiz	Yüz yüze olması	4	12
	Etkileşimli olmaması	3	
	Yüzeysel anlatım olması	2	
	Uzaktan eğitim olmaması	3	

Hizmetiçi eğitimin veriliş şekli yönüyle değerlendirilmesi sonucunda, her ne kadar kod sıklıkları birbirine yakın olsa da bu eğitimin verilme şeklinin yetersiz olduğu belirtilebilir. Eğitimin verilme şekli en çok sırasıyla yüz yüze olma, uzaktan eğitim olmama, etkileşimli olmama, yüzeysel anlatım olması gibi yönleriyle yetersiz olarak değerlendirilmiştir. Bu konuda iki katılımcının görüşü şöyledir:

“Eğitimin uzaktan eğitim olanakları ile daha yararlı olabileceğini düşünüyorum.” (K10).

“Eğitim bir günlük yüz yüze eğitim ve devamında uzaktan eğitim şeklinde olmalı, böylece hem eğitmenler hem de katılımcılar için süre kısıtı daha etkili değerlendirilebilir.” (K20).

Bunun yanı sıra katılımcılar eğitimin veriliş şeklini yüz yüze olma, katılımcılar arası ve eğitmen–katılımcı arası etkileşime olanak tanıma yönleriyle yeterli olarak değerlendirmişlerdir. Bu konuda bir katılımcının görüşü şöyledir:

“Anlatım sırasında anlaşılamayan hususların irdelenebilmesi açısından yüz yüze eğitim etkili olmuştur. Ayrıca diğer katılımcılar ve eğitmenle fikir alışverişinde bulunularak verimli bir tartışma ortamı yaratılabilmiştir.” (K15).

Tartışma, Sonuç ve Öneriler

Bu araştırmada kamuya hizmet veren bir kurumda çalışmakta olan bireylerin dijital bilgi güvenliği farkındalıkları ve bilgi okuryazarlıkları ile aldıkları hizmetiçi eğitimin incelenmesi amaçlanmıştır. Araştırmanın sonuçlarına göre, katılımcıların “bilgi okuryazarlık” düzeyleri ile “dijital veri güvenliği farkındalıkları” arasında pozitif ve anlamlı bir ilişkinin varlığı belirlenmiştir. Bu ilişki orta düzeydedir ve buna göre, dijital veri güvenliği farkındalığının bilgi okuryazarlığı düzeyine bağlı olarak arttığı söylenebilir.

MANOVA bulgularına göre katılımcıların bilgi okuryazarlığı ve dijital veri güvenliği farkındalıklarının bilgi ve dijital veri güvenliği hizmetiçi eğitimini alma durumları bakımından anlamlı bir farklılık göstermediği saptanmıştır. Araştırmada belirtilen bilgi ve dijital veri güvenliği hizmetiçi eğitiminin temel amacı, katılımcılara bilgi ve bilişim güvenliğinin temel kavramlarını tanıtmak, dijital veri güvenliği risklerine karşı alınması gereken önlemler ile ilgili bilgi vermek ve katılımcıları kurumda yapılan çalışmalar konusunda bilgilendirmektir. Kurumda verilen hizmetiçi eğitimin katılımcılara katkı sağlamamış olması göze çarpan en önemli sonuçlardandır. Bu bulgunun olası sonuçlarını incelemek üzere katılımcıların aldıkları hizmetiçi eğitimin içeriği ve veriliş yöntemi konusunda görüşleri toplanmıştır ve katılımcıların görüşlerinin olumlu olmadığı gözlenmiştir. Katılımcılar hizmetiçi eğitimin sadece PowerPoint sunum aracı kullanılarak yüz yüze verildiğini belirtmişlerdir. Katılımcıların görüşleri arasında en fazla dikkat çeken bulgu, aldıkları hizmetiçi eğitimin içeriğinin çok fazla kuramsal olması ve etkileşimli olmamasıdır. Ayrıca katılımcılar en fazla hizmetiçi eğitimin yüz yüze olması yönünde olumsuz düşüncelerini belirtmişlerdir. Dolayısıyla bu çalışmanın sonuçlarında daha iyi bir hizmetiçi eğitim verilebilmesi için izlenebilecek yollar ve yöntemler ile ilgili önerilerde bulunulmaya çalışılmıştır.

“Bilgi ve dijital veri güvenliği farkındalığı” gibi güncelliğini koruyan hizmetiçi eğitimler gerçekleştirilirken katılımcıların yaş, eğitim düzeyi, bulunduğu pozisyon gibi demografik özellikleri de dikkate alınarak planlama yapmak önemlidir (McCormac ve diğ., 2017; Vroom ve Von Solms, 2004). Hizmetçi eğitim,

yetişkinlere yönelik çalışma ve verilen hizmeti artırmayı amaçlamalı ve hizmet öncesindeki eğitimin çok ötesinde planlanmalıdır (Ersoy, 1996a). Hizmetiçi eğitime katılan çalışanlar yetişkin bireylerdir. Yetişkinlerin özellikleri (yaşları, deneyimleri, öğrenim durumları) eğitim sürecinde önemli rol oynamaktadır. Bu nedenle hizmetiçi eğitimde bireylerin bilgi okuryazarlıklarının da içinde olduğu çeşitli bireysel özellikleri dikkate alınmalıdır (Pattinson, Butavicius, Parsons, McCormac ve Calic, 2015; Seferoğlu, 2004). Hizmetiçi eğitim etkinlikleri yaş, cinsiyet, kişilik ve okul gibi farklı ortamlardan gelen bireyleri bir araya toplar. Bu nedenle hizmetiçi eğitim için düzenlenen etkinliklerin geliştirilebilir olması, etkileşime ve değişime açık olması, başarılı olması, hedef kitlenin gereksinim, istek ve beklentilerini karşılayabilir olması, belirlenen amaçlar doğrultusunda kısa ve uzun sürede kullanılabilir olması gerekmektedir (Ersoy, 1996b). Bu çalışmada belirtilen hizmetiçi eğitimin de bu kapsamda değerlendirilerek yeniden planlanmasının yararlı olacağı düşünülmektedir.

Çağımız bilgi toplumunda, bilgi okuryazarlığının öğrenen kurumların karakterinin önemli bir parçası olduğu ve kurum çalışanlarının önemli bir özelliği olduğu düşünülmektedir (Bruce, 1999). Bilgi okuryazarlığı, işyerinde küçük ve büyük işletmeler için olumlu sonuç üreten temel bir beceridir (Thompson, 2003). İşverenler, bilgi okuryazarlığını işgücünde önemli görmektedir. Çünkü sürekli olarak yeni beceriler öğrenme isteği ve becerisi olan bireylerin işgücüne gereksinim duymaktadırlar. Çalışanlar, en üst düzey işletme değeri sunmak için bilgi ile etkileşim konusunda kendine güvenli ve yetkin olmalıdır (Cheuk, 2008). Dolayısıyla kurum çalışanlarının da bilgi okuryazarlığı becerilerinin geliştirilmesi hem örgütsel yapıya hem de bireylere katkı sağlayacaktır.

Bireylerin bilgi ve becerileri dikkate alınarak hazırlanmış sistemli, geniş kapsamlı ve sıklıkla gerçekleştirilecek bilgi okuryazarlığı eğitim programları ile bilgi okuryazarlığı becerileri başta olmak üzere, çağın gerektirdiği dijital niteliklerin bireylere kazandırılması olanaklı olacaktır (Özel, 2016). Karakaş'ın (1999) belirttiği bireylerin doğacak olan bilgi gereksinimlerini nasıl sağlayabileceklerinin, doğru bilgilere nasıl ulaşabileceklerinin onlara öğretilmesi gerektiği önerisi de bu anlamda eğitim planlamalarına önemli katkı sağlayacaktır. Bilgi okuryazarlığı eğitim programlarının nitelikli bir şekilde hazırlanması sürecinde kişilerin öncelikle bildiklerinin ve gereksinim duyduklarının belirlenmesi önem taşımaktadır. Dolayısıyla bireylerin bilgiye niçin ve ne şekilde eriştiklerinin belirlenmesi önemlidir (Stern, 2003). Bu çerçevede kurumlarda çalışan her bir bireyin çeşitli test yöntemleriyle bilgi okuryazarlık düzeyleri analiz edildikten sonra hizmetiçi eğitim programlarını planlamak yararlı olabilir. Çünkü yeni gelişen teknolojilerle birlikte bilgi okuryazarlığı ve beraberinde gelecek olan bilgi teknolojileri okuryazarlığı günümüz toplumunda önem kazanmaktadır. Nitekim bireylerin bilgi okuryazarlıkları arttığında dijital veri güvenliği farkındalıklarının da arttığı, bu çalışmada ulaşılan bilgi okuryazarlığı ile dijital veri güvenliği farkındalığı arasındaki pozitif ilişki ile görülmektedir.

Teknolojik yeniliklerle birlikte eğitim alanında da her alanda olduğu gibi önemli ilerlemeler gözlemlenmiş ve bazı reformlar gerçekleşmiştir. Eğitim, zaman ve

mekandan bağımsızlaştırılarak daha ekonomik duruma gelmiş ve bu çerçevede daha büyük kitlelere ulaşmak artık olanaklı olmuştur. Gerçekleşen yenilikler ve reformlar sayesinde dünyada birçok kurumun gündeminde yer alan uzaktan eğitim modelleri, büyük kitlelerin eğitiminde ülkemizdeki kurumların da gündemine girmiş olup tercih edilir duruma gelmiştir (Özmen ve Ediz, 2002). Hizmetiçi eğitim alan kişilerin iş yaşamlarını ve güdülenmelerini olumsuz etkilemeden eğitim almalarını sağlamak hizmetiçi e-öğrenmenin temel hedefidir. Bu nedenle günümüzde birçok kurum ve kuruluş internet altyapılı eğitime büyük yatırımlar yapmaktadır. Verilen hizmetiçi e-öğretimlerin zaman ve mekandan esneklik sağlayarak hem işgücü kaybını engelleyeceği hem de kurumun mali yüküne katkı sağlayacağı düşünülmektedir.

Dijital veri güvenliği konusunda yaşanan sorunların en aza indirilmesi için, bireylerin bilgi okuryazarlık düzeyleri artırılmalı, toplum genelinde bilişim teknolojilerini kullanan bireylerin farkında olması ve önlem alması gereken bir konu olan dijital veri güvenliği farkındalığına yönelik bilinçlendirme çalışmaları yapılmalı, eğitimler verilmeli, bu konudaki yeni yaklaşımlar takip edilmeli ve farkındalığı arttıracak projeler yapılandırılmalıdır (Yılmaz ve diğ., 2016). Çalışanlarda “dijital veri güvenliği farkındalığı” oluşturmak için de öncelikle kurum içi gereksinim analizlerinin yapılması önemlidir. Bu analizlere göre çeşitli planlamaların yapılması ve uygulamaya geçilmesi önerilebilir. Şahinaslan ve diğ. (2009) yaptıkları çalışmalarında grup içi yüz yüze eğitimlerin yanında internet tabanlı etkileşimli sanal eğitimler, oyun tabanlı eğitimler, e-öğrenme eğitimleri, animasyonlar ve film gösterileri, e-posta bültenleri, karikatür destekli sunumlar gibi çok daha farklı yöntemler olduğunu belirtmişlerdir. Belirtilen çeşitli eğitim yöntemlerini kullanarak eğitimin çeşitliliği ve etkililiği artırılabilir, bireylerin “bilgi ve dijital veri güvenliği” farkındalıklarında daha büyük sıçramalar yakalanabilir. Belirlenen hedeflere ulaşmak için klasik eğitim-öğretim yöntemlerini geride bırakmak ve en güncel teknoloji desteklerini kullanmak etkili olabilir, böylece yeni öğrenmeler kolaylaştırılabilir. Benzer şekilde katılımcılar da etkileşim kurabilecekleri, tekdüze olmayan, kendilerine zaman kazandıracak, güdülenmelerini arttıracak eğitimlere gereksinim duyduklarını belirtmişlerdir. Yeni teknolojilerin eğitim-öğretim yaşamına bütünleştirilmesi ile öğrenmeler kalıcı ve eğlenceli duruma getirilebilir. Tüm bu örneklerle ek olarak aşağıdaki öneriler verilebilir:

- Sadece yüz yüze eğitimler değil çevrimiçi eğitimler de verilerek zaman ve mekân bağımsızlığı sağlanabilir. Böylece çalışmaya yönelik güdülenme ve çalışmanın bütünlüğü bozulmayabilir.
- Sanal dünyalar oluşturulup çalışanların bu dünyalarda rol almaları sağlanarak gerçek yaşam becerileri kazanmaları sağlanabilir.
- Sosyal ağlar üzerinde grup etkinlikleri hazırlanıp bilgi güvenliği farkındalığı artırılabilir.
- Eğitimler sonrasında katılımcılara test edici e-posta ya da sosyal ağlar aracılığı ile bildirimler gönderip kazanılmış farkındalık düzeyleri ölçülebilir.

- Çokluortam etkinlikleri artırılarak katılımcıların birden çok duyusuna seslenilerek eğitimlerin kalıcı olması sağlanabilir.

Bu çalışmanın sonuçları araştırmaya katılan 69 katılımcı ile sınırlıdır, başka kurumu içermemektedir. Başka kurumların ve belki de diğer şehirlerdeki kurumların da dahil edilmesiyle daha fazla bir anlayış kazanmak için farklı bir çalışma yapılabilir. Ayrıca hizmetiçi eğitimi alan katılımcılardan 29'undan açık uçlu sorulara yanıt alınabilmiş olması, hizmetiçi eğitim almayan 22 katılımcı olması da yorumlamaya bir sınırlılık olarak görülebilir.

Kaynakça

- ACRL (The Association of College and Research Libraries) (2000). Information literacy competency standards for higher education. Retrieved from <https://alair.ala.org/handle/11213/7668>
- Adıgüzel, A. (2011). Bilgi okuryazarlığı ölçeğinin geliştirilmesi. *Dicle Üniversitesi Ziya Gökalp Eğitim Fakültesi Dergisi*, 17, 15-28.
- Aharony, N., Limberg, L., Julien, H., Albright, K., Fourie, I., and Bronstein, J. (2017). Information literacy in an era of information uncertainty. *Proceedings of the Association for Information Science and Technology*, 54(1), 528-531.
- American Management Association (2012). *AMA 2012 critical skills survey*. New York, NY: American Management Association. Retrieved from <http://playbook.amanet.org/wp-content/uploads/2013/03/2012-Critical-Skills-Survey-pdf.pdf>
- Andretta, S. (Ed). (2007). *Change and challenge: Information literacy for the 21st century*. Adelaide: Auslib Press.
- Bruce, C. S. (1999). Workplace experiences of information literacy. *International Journal of Information Management*, 19(1), 33-47.
- Büyüköztürk, Ş. (2014). *Sosyal bilimler için veri analizi el kitabı*. Ankara: Pegem A Yayıncılık.
- Can, H., Akgün, A. ve Kavuncubaşı, Ş. (1995). *Kamu ve özel kesimde personel yönetimi*. Ankara: Siyasal Kitapevi.
- Canbek, G. ve Sağıroğlu, Ş. (2007). Bilgisayar sistemlerine yapılan saldırılar ve türleri: Bir inceleme. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 23(1-2), 1-12.
- Candy, P. C. (2002). *Lifelong learning and information literacy*. White paper prepared for UNESCO. Retrieved from <https://pdfs.semanticscholar.org/f94d/1b7db0ed803048bf2781fec5bb1daa64c3f7.pdf>

- Cheuk, B. (2008). Delivering business value through information literacy in the workplace. *Libri*, 58(3), 137-43.
- Cho, J., and Trent, A. (2006). Validity in qualitative research revisited. *Qualitative Research*, 6(3), 319-340.
- Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed method approaches*. 3rd. Ed., Thousand Oaks, CA: Sage.
- Çek, E. (2017). *Kurumsal bilgi güvenliği yönetimi ve bilgi güvenliği için insan faktörünün önemi* (Yayınlanmamış doktora tezi). İstanbul Bilgi Üniversitesi, İstanbul.
- Da Veiga, A., and Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196-207.
- Ergün, E. ve Avcı-Yücel, Ü. (2015, Aralık). *Üniversite öğrencilerinin çevrimiçi öğrenme ortamlarında bilgi paylaşma öz yeterlik algılarının incelenmesi*. Uluslararası Yükseköğretimde Kalite Konferansında sunulan sözlü bildiri, Sakarya, Türkiye.
- Ersoy, Y. (1996a). Hizmet içi eğitim ve yetiştirme kursunu geliştirme-I. *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi*, 12, 151-160.
- Ersoy, Y. (1996b). Hizmet içi eğitim ve yetiştirme kursunu geliştirme-II. *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi*, 12, 161-169.
- Garner, S. D. (2006). *High-level colloquium on information literacy and lifelong learning*. Bibliotheca Alexandrina, Alexandria, Egypt. UNESCO. Retrieved from <http://www.ifla.org/files/assets/information-literacy/publications/high-level-colloquium-2005.pdf>
- Goad, T. W. (2002). *Information literacy and workplace performance*. Westport, CT: Quorum Books.
- Hart, P. (2005). Rising to the challenge: Are high school graduates prepared for college and work. A work conducted for achieve, a nonprofit organization for education reform, Washington, DC. Retrieved from <https://www.achieve.org/rising-challenge>
- ISACA (Information System Audit and Control Association) (2009). Review Manual 2009. Rolling Meadows, IL: Information Systems Audit and Control Association Press.
- Karakaş, S. (1999). Üniversite kütüphanesi kullanıcılarının beklentileri ve kullanıcı tatmini. *Ankara Üniversitesi Dil ve Tarih-Cografya Fakültesi Dergisi*, 39, 1-2.
- Kayış, A. (2009). Güvenilirlik analizi. Ş. Kalaycı (Ed.), *SPSS uygulamalı çok değişkenli istatistik teknikleri* (ss. 404-419). Ankara: Asil Yayın Dağıtım.

- Kruger, H. A., and Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289-296.
- Kurbanoğlu, S. S. (2010). Bilgi okuryazarlığı: Kavramsal bir analiz. *Türk Kütüphaneciliği*, 24(4), 723-747.
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., and Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, 69, 151-156.
- Nasir, A., Arshah, R. A., Ab Hamid, M. R., and Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications*, 44, 12-22.
- Özel, N. (2016). Üniversite öğrencilerinin bilgi okuryazarlığı becerilerinin değerlendirilmesi: Ankara üniversitesi örneği. *Bilgi Dünyası*, 17(2), 247-264.
- Özmen, A. ve Ediz, İ. G. (2002, Mayıs). *Uzaktan eğitim ve dumlupınar üniversitesi modeli*. Açık ve Uzaktan Eğitim Sempozyumunda sunulan bildiri, Anadolu Üniversitesi, Eskişehir.
- Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., and Calic, D. (2015). *Factors that influence information security Behavior: An Australian web-based study*. In Proceedings of human aspects of information security, privacy, and trust (pp. 231-241), Springer International Publishing.
- Perrault, A. (2007). American competitiveness in the internet age: Information literacy summit. Washington, DC. Retrieved from <https://drive.google.com/file/d/0B3SNep9j56rIODA2MTI3MDktOTE4My00MjkwLWJhMTgtOWZkYjI4MGQzZTVj/view?ddrp=1&hl=en>
- Polat, C. ve Odabaş, H. (2008, Mart). *Bilgi toplumunda yaşam boyu öğrenmenin anahtarı: Bilgi okuryazarlığı*. Küreselleşme, Demokratikleşme ve Türkiye Uluslararası Sempozyumunda sunulan sözlü bildiri, Antalya.
- Ramalho Correia, A. M., and Carlos Teixeira, J. (2003). Information literacy: an integrated concept for a safer Internet. *Online Information Review*, 27(5), 311-320.
- Seferoğlu, S. S. (2004). Öğretmenlerin hizmet içi eğitiminde yeni yaklaşımlar. *Akdeniz Üniversitesi Eğitim Fakültesi Dergisi*, 1, 83-95.
- Stern, C. (2003). Measuring students' information literacy competency. A. Martin and H. Rader (Eds.), *Information and IT literacy: Enabling learning in the 21st century* (pp. 112-119). London: Facet.
- Şahinaslan, E., Kantürk, A., Şahinaslan, Ö. ve Borandağ, E. (2009, Şubat). *Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri*. XI. Akademik Bilişim Konferansında sunulan sözlü bildiri, Şanlıurfa.

- Tabachnick, L.S., and Fidell, B.G. (2013). *Using Multivariate Statistics* (6th. Ed.). Boston, MA: Pearson.
- Thompson, S. (2003). *Information literacy meeting of experts*. Conference report sponsored by the US National Commission on Libraries and Information Science and the National Forum on Information Literacy. Retrieved from http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/themes/info_lit_meeting_prague_2003.pdf
- Tuncer, M. ve Balcı, K. (2013). Öğretmen adaylarının bilgi okuryazarlık özyeterliklerinin bazı deđişkenler açısından karşılaştırılması. *International Journal of Social Science*, 6(5), 719-737.
- Vroom, C., and Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, 23(3), 191-198.
- Vural, Y. ve Sađırođlu, Ő. (2008). Kurumsal bilgi güvenliđi ve standartları üzerine bir inceleme. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, 23(2), 507-522.
- Yıldırım, A. ve ŐimŐek, H. (2005). *Sosyal bilimlerde nitel araştırma yöntemleri*. 6. baskı, Ankara: Seçkin Yayınevi.
- Yılmaz, E., Őahin, Y. L. ve Akbulut, Y. (2015). Dijital veri güvenliđi farkındalıđı ölçeđinin geliŐtirilmesi. *AJIT-e: Online Academic Journal of Information Technology*, 6(21), 23-40.
- Yılmaz, E., Őahin, Y. L. ve Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliđi farkındalıđı. *Sakarya University Journal of Education*, 6(2), 26-45.
- Yüksel, I. ve Adıgüzel, A. (2011). A glance at standard development studies and accreditation process as sustaining tools for quality in teacher education in Turkey. *International Journal of Instruction*, 4(2), 39-50.
- Zhang, X., Majid, S., and Foo, S. (2010). Environmental scanning: An application of information literacy skills at the workplace. *Journal of Information Science*, 36, 719-32.



The Effect of In-Service Training with Digital Data Security Awareness and Information Literacy¹

ARTICLE TYPE	Received Date	Accepted Date	Published Date
Research Article	12.06.2018	08.08.2019	10.25.2019

Ümmühan Avcı ² and Esin Arslan ³
Başkent University

Abstract

The aim of this research is to examine the effect of in-service training with digital data security awareness and information literacy of individuals working in a public service organization. The participants of this explanatory sequential mixed design study consisted of a total of 69 staff (37 female and 32 male). Forty seven of the participants had previously received an in-service training on “Information and Digital Data Security”, while 22 did not. In this study, data were collected by using “Information Literacy Scale” and “Digital Data Security Awareness Scale”. In addition, participants' opinions were collected through semi-structured open ended questions. Pearson Correlation and MANOVA were used for the data analysis. The data obtained from the open ended questions were analysed by using content analysis technique. The results of the study demonstrated a moderately positive and significant relationship between participants' information literacy and digital data security awareness. However, it was found that the in-service training did not have a significant effect on participants' digital data security awareness and information literacy. In order to examine the possible reasons for this result, detailed views of the participants on both the content and the method of in-service training process were obtained. In line with these views, some suggestions were given about different educational contents and methods such as providing online in-service trainings rather than face-to-face trainings, creating virtual worlds, group activities on social networks and creating multimedia activities.

Keywords: dijital data security awareness, information literacy, in-service training.

¹The abstract of this study was presented at the 12th. International Computer & Instructional Technologies Symposium.

²*Corresponding Author:* Assoc. Prof., Faculty of Education, Computer Education and Instructional Technologies, E-mail: uavci@baskent.edu.tr, <https://orcid.org/0000-0001-7007-1478>

³Student, Faculty of Education, Computer Education and Instructional Technologies, E-mail: esin.kokturkarслан@gmail.com, <https://orcid.org/0000-0002-5201-2009>

Purpose and Significance

The information literacy and digital data security awareness that arise due to current technological developments have become important issues today. It is important to conduct researches on how effective in-service training programs are, how they are lacking and how they can be improved in order to be informed about information literacy and digital data security awareness which are thought to be related to each other. With a basic knowledge and digital data security education; starting from the basic concepts related to information, it is important to provide in-service trainings including the accessibility, protection, confidentiality, and security of information. It is necessary to inform the staffs about the legal regulations and individual responsibilities about digital data security by organizing policies and procedures in institutions.

The most important precautions for digital data security are the human factor. Individuals and organizations generally take precautions about information security when they have a serious problem. However, information security is an important issue from the beginning to the end. Therefore, it is important to raise awareness about information security and thus to create information security culture with the support of information literacy. Therefore, it is important to examine the relationship between these two concepts which are indispensable in the digital age. In this context, it is necessary to pay attention to providing qualified and effective in-service training. In-service training programs for information security should be organized in an interactive manner taking into account the wishes of individuals. Thus, it is planned to increase the awareness levels of individuals' information literacy and digital data security. In another aspect, determining whether the in-service trainings given are effective, whether there is a relationship between the individuals' awareness of information literacy and digital data security, will support this process in a multi-faceted manner. In this context, It is aimed to examine the effect of in-service training with digital data security awareness and information literacy of individuals working in a public service organization.

The sub-problems of the research are as follows:

1. Is there a meaningful relationship between information literacy and digital data security awareness of individuals?
2. Do individuals' awareness of information literacy and digital data security differ significantly according to in-service training?
3. What are the views of individuals regarding the in-service training program?

Method

The sample of this explanatory sequential mixed design study consisted of a total of 69 staff (37 female and 32 male). It was determined that 30 (43.5%) of the 69 people who participated in the research were related to Information and Communication Technologies (ICT) and 39 (56.5%) were unrelated. In addition, forty-seven of the

participants had previously received an in-service training on “Information and Digital Data Security”, while 22 did not. Within the scope of this research, data were collected by using "Information Literacy Scale" consisting of 29 likert type questions and "Digital Data Security Awareness Scale" consisting of 33 likert type questions. Data collection tools were distributed to participants either via e-mail or in print, and they were given two weeks to complete.

In addition, a semi-structured form consisting of open-ended questions was created in order to explain or support the possible reasons for the findings to be obtained from quantitative data, to obtain information about the content of the training and to get the opinions of the participants. The opinions of a faculty member who were experts in the field were also taken and the necessary corrections were made and the form was finalized and applied to the focus group. The following are open-ended questions.

1. Explain your opinions on the content of the “Information and Digital Data Security” training you have received by answering the following questions.
 - a. Do you think the content of the training and the materials used in the training (presentation, etc.) were sufficient? If yes, in which ways was it sufficient? Please explain.
 - b. Do you think the content of the training and the materials used in the training (presentation, etc.) were insufficient? If yes, in which ways was it insufficient? What do you recommend adding to the training content? Please explain.
2. Explain your opinions on the way of giving of the “Information and Digital Data Security” training you have received by answering the following questions.
 - a. Do you think this training should be given by distance education instead of face-to-face education? Please explain.
 - b. Do you think this training should be given by using both face-to-face and distance education together? Please explain.
3. Other suggestions.

Pearson Correlation and MANOVA were used for the data analysis. The data obtained from open ended questions were analysed by using content analysis technique.

Results and Conclusions

The results of the study demonstrated a moderately positive and significant relationship between participants’ information literacy and digital data security awareness. However, it was found that the in-service training did not have a significant effect on participants’ digital data security awareness and information

literacy. In order to examine the possible reasons for this result, detailed views of the participants on both the content and the method of in-service training process were obtained. As a result, it was seen that there were mostly not positive opinions about the in-service training process. It was stated that in-service training was given face to face by using PowerPoint presentation tool. The most remarkable finding among the participants' views was that the content of the in-service training they received was too theoretical and not interactive. In addition, the participants stated that they were dissatisfied with the fact that the most in-service training was face to face.

When conducting in-service trainings, it is important to plan by taking into consideration the demographic characteristics of the participants such as age, education level and position. In-service training should aim at increasing adult work and provision and should be planned well beyond pre-service training. Employees participating in in-service training are adult individuals. Characteristics of adults (age, experience, educational status) play an important role in the education process. Therefore, in-service training should take into account the various individual characteristics of individuals, including information literacy. In-service training activities bring together individuals from different backgrounds such as age, gender, personality and school. For this reason, the activities organized for in-service training should be developed, open to interaction and change, to be successful, to meet the needs, demands and expectations of the target audience, and to be used in a short and long time in line with the determined objectives. It is considered that it would be beneficial to re-plan the in-service training mentioned in this study by evaluating in this context.

It may be useful to plan in-service training programs after analyzing the information literacy levels of each individual working in the institutions with various test methods. Because information literacy along with emerging technologies and information literacy that will come with it are gaining importance in today's society. As a matter of fact, it is seen that digital data security awareness increases when individuals' information literacy increases, with the positive relationship between information literacy and digital data security awareness reached in this study.

The main goal of in-service e-learning is to ensure that people receiving in-service training without affecting their work life and motivation. For this reason, many institutions and organizations are investing heavily in internet-based education. It is thought that in-service e-trainings will provide flexibility from time and space to prevent labor loss and contribute to the financial burden of the institution.

In order to minimize the problems of digital data security, information literacy levels of individuals should be increased, awareness raising activities should be conducted regarding the digital data security awareness, which should be aware of the individuals using information technologies in the society and trainings should be given and new approaches should be followed. In order to create digital data security awareness among employees, it is important to conduct internal needs analyzes first.

According to these analyzes, it may be suggested to make various plans and implement them.

Suggestions

Some suggestions were given about different educational contents and methods such as providing online in-service trainings rather than face-to-face trainings, creating virtual worlds, group activities on social networks and creating multimedia activities.

- Time and place independence can be ensured by providing not only face-to-face trainings but also online trainings. Thus, the motivation and integrity of the work may not be impaired.

- Virtual worlds can be created and staffs can gain real-life skills by taking part in these worlds.

- Group activities can be prepared on social networks and information security awareness can be increased.

- After the trainings, the participants can send notifications via tester e-mail or social networks and the levels of acquired awareness can be measured.

- By increasing the multimedia activities, it can be ensured that the trainings are permanent by addressing the multiple senses of the participants.

Diversity and effectiveness of education can be increased by using the various education methods mentioned and greater leaps can be achieved in individuals' awareness of "information and digital data security". In order to achieve the set goals, leaving behind the classical methods of education and using the most up-to-date technology supports can be effective so that new learning can be facilitated. Similarly, the participants stated that they needed trainings that could interact, non-uniform, save time and increase their motivation. By integrating new technologies into education, learning can be made permanent and enjoyable.