T.C.

KARAMANOĞLU MEHMETBEY ÜNİVERSİTESİ
SOSYAL BİLİMLERİ ENSTİTÜSÜ
YÖNETİM BİLİŞMİ SİSTEMLERİ ANA BİLİM DALI

KAMU ÇALIŞANLARININ BİLGİ GÜVENLİĞİ KONUSUNDAKİ FARKINDALIK DÜZEYLERİ ÜZERİNE BİR ARAŞTIRMA

Hazırlayan

Mehmet KÖSE

Yüksek Lisans Tezi

Danışman

Prof. Dr. Serkan ADA

KARAMAN-2025

T.C.

KARAMANOĞLU MEHMETBEY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU ÇALIŞANLARININ BİLGİ GÜVENLİĞİ KONUSUNDAKİ FARKINDALIK DÜZEYLERİ ÜZERİNE BİR ARAŞTIRMA

YÜKSEK LİSANS TEZİ

Mehmet KÖSE

Enstitü Anabilim Dalı: Sosyal Bilimler Enstitüsü
Enstitü Bilim Dalı : Yönetim Bilişim Sistemleri

"Bu tez 26/05/2025 tarihinde yüzyüze olarak savunulmuş olup aşağıdaki isimleri bulunan jüri üyeleri tarafından Oybirliği / Oyçokluğu ile kabul edilmiştir."

JÜRİ ÜYESİ	KANAATİ
Prof. Dr. Serkan ADA	Başarılı
Doç. Dr. Murat AK	Başarılı
Dr. Öğr. Üyesi Hasan Sadık TATLI	Başarılı

ETİK BEYAN METNİ

Enstitünüz tarafından Uygulama Esasları çerçevesinde alınan Benzerlik Raporuna göre yukarıda bilgileri verilen tez çalışmasının benzerlik oranının herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve Etik Kurul Onayı gerektiği takdirde onay belgesini aldığımı beyan ederim.

Etik kurul onay belgesine ihtiyaç var mıdır?

Evet ☒

Hayır ☐

(Etik Kurul izni gerektiren araştırmalar aşağıdaki gibidir:

- Anket, mülakat, odak grup çalışması, gözlem, deney, görüşme teknikleri kullanılarak katılımcılardan veri toplanmasını gerektiren nitel ya da nicel yaklaşımlarla yürütülen her türlü araştırmalar,
- İnsan ve hayvanların (materyal/veriler dahil) deneysel ya da diğer bilimsel amaçlarla kullanılması,
- İnsanlar üzerinde yapılan klinik araştırmalar,
- Hayvanlar üzerinde yapılan araştırmalar,
- Kişisel verilerin korunması kanunu gereğince retrospektif çalışmalar.)

Mehmet KÖSE

26.05.2025

ÖNSÖZ

Bu araştırmanın amacı, kamu sektöründe görev yapan kişilerin bilgi güvenliği konusundaki farkındalık düzeylerini belirlemektedir. Bu araştırma, kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeylerini değerlendirmenin ve anlamanın önemini vurgulamaktadır. Bilgi güvenliği, günümüzde dijitalleşme ve teknolojinin hızla ilerlemesiyle birlikte giderek daha fazla önem kazanmaktadır. Kamu kurumları ve kuruluşları, hassas ve önemli verilere erişim sağlayan birçok çalışanı bünyesinde barındırmaktadır. Bu nedenle, bu çalışanların bilgi güvenliği konusundaki farkındalık düzeylerinin yeterli olması, kurumların veri güvenliğini sağlama ve siber saldırılara karşı korunma açısından hayati önem taşımaktadır. Bu araştırmada nicel araştırma yöntemlerinden ilişkisel tarama yöntemi kullanılmıştır. Çalışma Karaman Sosyal Güvenlik İl Müdürlüğü örnekleminde gerçekleştirilmiştir. Çalışmanın tüm aşamalarında büyük bir özveri ile desteğini esirgemeyip yol gösteren değerli hocam ve tez danışmanım Prof. Dr. Serkan ADA hocama şükranlarımı sunarım. Büyük fedakarlıklar göstererek bana her zaman destek olan ve yardımlarını esirgemeyen aileme sevgilerimi sunarım. Ayrıca burada ismini anmadığım ve emeği geçen tüm hocalarıma ve dostlarıma sevgi ve saygılarımı sunarım.

Mehmet KÖSE

26.05.2025

İÇİNDEKİLER

KISALTMALAR

BGYS : Bilgi Güvenliği Yönetim Sistemi

BİGR : Bilgi ve İletişim Güvenliği Rehberi

BSI : British Standarts Institution

COBIT : Bilgi ve Bağlantılı Teknolojiler Kontrol Hedefleri Standardı

DDO : Dijital Dönüşüm Ofisi

IEC : The Electrotechnical Commission

ISACA : Bilgi Sistemleri Denetim ve Kontrol Derneği

ISF : Bilgi Güvenliği Forumu

ISO : The International Organization for Standardization

ITAF : Bilgi Güvenliği Denetimi ve Emniyeti Standartları

KVKY : Kişisel Verilerin Korunması Yasası

LAN : Yerel Alan Ağı

NIST : Ulusal Standartlar ve Teknoloji Enstitüsü

PAN : Kablosuz Kişisel Alan Ağları

PBC : Algılanan Davranışsal Kontrol

SIEM : Güvenlik Bilgi ve Olay Yönetimi

SoGP : Bilgi Güvenliği İçin İyi Uygulama Standard

SPSS : Sosyal Bilimler İçin İstatistik Programı

TAM : Teknoloji Kabul Modeli

TPB : Planlı Davranış Teorisi

TRA **:** Davranışsal Niyet Teorisi

TSE **:** Türk Standartları Enstitüsü

UDHB **:** Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

WAN **:** Geniş Alan Ağları

WLAN **:** Kablosuz Yerel Alan Ağları

TABLO LİSTESİ

ŞEKİL LİSTESİ

ÖZET

Başlık: Kamu Çalışanlarının Bilgi Güvenliği Konusundaki Farkındalık Düzeyleri Üzerine Bir Araştırma

Yazar: Mehmet Köse

Danışman: Prof. Dr. Serkan ADA

Kabul Tarihi: **Sayfa Sayısı:** 75

Bu araştırmanın amacı, kamu sektöründe görev yapan kişilerin bilgi güvenliği konusundaki farkındalık düzeylerini belirlemektedir. Bu araştırma, kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeylerini değerlendirmenin ve anlamanın önemini vurgulamaktadır. Bilgi güvenliği, günümüzde dijitalleşme ve teknolojinin hızla ilerlemesiyle birlikte giderek daha fazla önem kazanmaktadır. Kamu kurumları ve kuruluşları, hassas ve önemli verilere erişim sağlayan birçok çalışanı bünyesinde barındırmaktadır. Bu nedenle, bu çalışanların bilgi güvenliği konusundaki farkındalık düzeylerinin yeterli olması, kurumların veri güvenliğini sağlama ve siber saldırılara karşı korunma açısından hayati önem taşımaktadır. Bu araştırmada nicel araştırma yöntemlerinden ilişkisel tarama yöntemi kullanılmıştır. Çalışma Karaman Sosyal Güvenlik İl Müdürlüğü örnekleminde gerçekleştirilmiştir. Bu bağlamda kurumda çalışan 102 kişiye anket uygulanmıştır. Veri toplama yöntemi olarak araştırmacı tarafından hazırlanan demografik form ve "Bilgi Güvenliği Farkındalık Ölçeği" kullanılmıştır. Veriler Google Formlar aracılığıyla çevrimiçi ortamda toplanmıştır. Veriler SPSS 23 programı kullanılarak değerlendirilmiştir. Erkeklerin Bilgi Güvenliği Farkındalık Ölçeği ve alt boyut puanları kadınlara göre daha yüksek olduğu sonucuna erişilmiştir. Analiz sonuçlarına göre medeni durum, yaş, öğrenim durumu, meslekte toplam hizmet süresi, çalışma sınıfı ve iş yerindeki pozisyon grupları arasında Bilgi Güvenliği Farkındalık Ölçeği ve alt boyut puanları bakımından istatistiksel olarak anlamlı fark saptanmamıştır.

Anahtar Kelimeler: Bilgi Güvenliği, Farkındalık, Kamu Çalışanları

ABSTRACT

Title of Thesis: A Research on the Awareness Levels of Public Employees on Information Security

Author of Thesis:

Supervisor: Prof. Dr. Serkan ADA

Accepted Date: **Number of Pages:** 75

The purpose of this research is to determine the awareness levels of people working in the public sector about information security. This research emphasizes the importance of assessing and understanding public employees' awareness levels of information security. Information security is becoming increasingly important today with the rapid advancement of digitalization and technology. Public institutions and organizations employ many employees who have access to sensitive and important data. Therefore, it is vital that these employees have sufficient awareness of information security in terms of ensuring the data security of institutions and protecting against cyberattacks. In this study, the relational screening method, one of the quantitative research methods, was used. The study was carried out on the sample of Karaman Social Security Provincial Directorate. In this context, a survey was administered to 102 people working in the institution. The demographic form prepared by the researcher and the "Information Security Awareness Scale" were used as data collection methods. Data was collected online via Google Forms. The data were evaluated using the SPSS 23 program. It was concluded that men's Information Security Awareness Scale and subscale scores are higher than women. According to the analysis results, no statistically significant difference was detected between marital status, age, education level, total length of service in the profession, working class and position groups in the workplace in terms of Information Security Awareness Scale and sub-dimension scores.

Keywords: Information Security, Awareness, Public Employees

GİRİŞ

Bilgi güvenliği, günümüzün dijital çağında giderek daha fazla önem kazanan bir konudur. Özellikle kamu çalışanları, kamu kurumları ve kuruluşlarının bünyesinde yer aldıkları için, bu alandaki farkındalık düzeyleri son derece kritik bir öneme sahiptir. Kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeyleri, kurumların veri güvenliğini sağlama ve siber saldırılara karşı korunma açısından belirleyici bir faktördür (Özbilen ve Çağlar, 2020: 80).

Günümüzde bilgi güvenliği, sadece teknolojik altyapı ile değil, aynı zamanda insan faktörüyle de doğrudan ilişkilidir. Bu nedenle, kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeylerinin değerlendirilmesi ve geliştirilmesi büyük önem taşımaktadır. Araştırmalar, kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeylerinin çeşitli faktörlere bağlı olarak değişebileceğini göstermektedir. Örneğin, cinsiyet, yaş, eğitim düzeyi, görev süresi gibi kişisel özelliklerin yanı sıra teknik bilgiye sahip olma durumu da farkındalık düzeylerini etkileyebilir (Mart, 2012; Öztezcan, 2017; Özdemir, 2019).

Bu bağlamda, kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeylerini anlamak ve iyileştirmek için çeşitli araştırmalar yapılmaktadır. Bu araştırmalar genellikle anketler, ölçekler ve mülakatlar gibi yöntemlerle gerçekleştirilir ve çalışanların bilgi güvenliği konusundaki bilgi düzeyleri, farkındalık seviyeleri ve eğitim ihtiyaçları gibi konuları ele alır.

Özellikle, teknolojinin hızla geliştiği ve siber tehditlerin arttığı günümüzde, kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeylerinin sürekli olarak güncellenmesi ve geliştirilmesi gerekmektedir (Çavuş ve Erçağ, 2016). Bu bağlamda, kurumların bilgi güvenliği politikalarını belirlerken ve uygularken, çalışanların eğitim ihtiyaçlarını göz önünde bulundurmaları ve bu doğrultuda etkili eğitim programları düzenlemeleri önemlidir.

Bu bağlamda bu araştırmada kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeyleri incelenmektedir. Bu çalışmanın amacı, kamu sektöründe görev yapan kişilerin

bilgi güvenliği konusundaki farkındalık düzeylerini belirlemektedir. Bu araştırma, kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeylerini değerlendirmenin ve anlamanın önemini vurgulamaktadır. Bilgi güvenliği, günümüzde dijitalleşme ve teknolojinin hızla ilerlemesiyle birlikte giderek daha fazla önem kazanmaktadır. Kamu kurumları ve kuruluşları, hassas ve önemli verilere erişim sağlayan birçok çalışanı bünyesinde barındırmaktadır. Bu nedenle, bu çalışanların bilgi güvenliği konusundaki farkındalık düzeylerinin yeterli olması, kurumların veri güvenliğini sağlama ve siber saldırılara karşı korunma açısından hayati önem taşımaktadır.

Araştırmanın önemi, kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeylerini belirleyerek, varsa eksiklikleri ve ihtiyaçları tespit etmeye yöneliktir. Bu doğrultuda yapılan değerlendirmeler, kurumların bilgi güvenliği politikalarını geliştirmelerine ve çalışanların bilgi güvenliği konusunda daha bilinçli olmalarını sağlayacak eğitim programları oluşturmalarına olanak tanıyacaktır. Ayrıca, çalışanların bilgi güvenliği farkındalık düzeylerini artırmak için alınacak önlemlerin etkisinin değerlendirilmesi, kurumların güvenlik stratejilerini daha etkin bir şekilde uygulamalarına ve güvenlik açıklarını azaltmalarına yardımcı olacağı düşünülmektedir.

Sonuç olarak, bu araştırma kamu kurumlarının bilgi güvenliği alanındaki güçlü ve zayıf yönlerini belirlemelerine ve çalışanların bilgi güvenliği konusundaki farkındalık düzeylerini artırmaya yönelik stratejiler geliştirmelerine katkı sağlamaktadır. Bu bağlamda bu araştırmanın sonuçları önem taşımaktadır.

Bu çalışma dört ana bölümden oluşmaktadır. Birinci bölümde, araştırmanın kuramsal temellerini oluşturmak amacıyla bilgi güvenliği kavramı, bilgi güvenliğinin amaçları, önemi, eğitimi ve güvenliğin sağlanmasına yönelik kurumsal ve bireysel önlemler detaylı şekilde ele alınmıştır. Ayrıca bilgi güvenliği farkındalığı kavramı ile bu farkındalığı etkileyen unsurlar, insan faktörü, kamusal alanda bilgi güvenliği uygulamaları ve konuya ilişkin ulusal ve uluslararası araştırmalara yer verilerek kapsamlı bir literatür değerlendirmesi yapılmıştır. İkinci bölümde, araştırmanın yöntemi açıklanmış; araştırmanın evren ve örneklemi, veri toplama araçları, uygulanan ölçme araçları, veri toplama süreci ile verilerin analizinde kullanılan istatistiksel yöntemler ayrıntılı biçimde sunulmuştur. Üçüncü bölümde, kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeylerine ilişkin elde edilen bulgulara yer verilmiş, bu bulgular demografik

değişkenler bağlamında tablo ve grafiklerle desteklenerek analiz edilmiştir. Son bölümde ise araştırma sonuçları özetlenmiş, elde edilen bulgular literatürle karşılaştırılarak tartışılmış ve kamu kurumlarında bilgi güvenliği farkındalığının artırılmasına yönelik çeşitli politika ve uygulama önerileri sunulmuştur.

1.BÖLÜM: KAVRAMSAL ÇERÇEVE

1.1. Bilgi Güvenliği Kavramı

Bilgi, işlenmeye, iletilmeye ve saklanmaya başladığı andan itibaren korunmalıdır. Bilgi teknolojisinin yaygınlaşmasıyla birlikte, kuruluşlardaki bilgi varlıkları önemli hale gelmiş ve bununla birlikte yeni ve karmaşık güvenlik açıkları ortaya çıkmıştır (Xu vd., 2021: 1). "Bilgi" terimi "veri" ve "bilgi" terimleri kullanılarak açıklanır. "Veri", "bilgi" ve "bilgi birikimi" terimleri sıklıkla eşanlamlı olarak kullanılsada, birbirlerinden açıkça farklıdırlar ve farklı şeyleri temsil ederler. "Bilgi" terimini tanımlamak için, öncelikle "veri" ve "bilgi" terimlerini tanımlamak gerekir (Boisot ve Canals, 2004).

Veri, nesnelerin ve olayların özelliklerini temsil eden sembollerdir. Veri ham, yani işlenmemiş haldedir. Bilgi, işlenmesi onu kullanılabilir hale getirmeye yarayan işlenmiş verilerden oluşur. Nesnelerin ve olayların özelliklerini temsil eden bilgi, bunu düzenli ve kullanışlı bir şekilde yapar. Başka bir deyişle, bilgi "kim", "ne", "ne zaman", "nerede" ve "kaç tane" gibi soruların yanıtlarını içerir. Benzer şekilde, bilgi, olayları veya nesneleri yorumlamak için yeni bir bakış açısı açar, daha önce görülmemiş anlamları ortaya çıkarır veya beklenmedik bağlantıları aydınlatır. Bu nedenle bilgi, bilginin ifşası ve inşası için gerekli bir ortam veya materyaldir (Bellinger vd., 2004).

Bilgi genellikle zengin bir bilgi biçimi olarak kabul edilir. Ancak bu ayrım yetersizdir. Bilgi bir mesaj akışıdır, oysa bilgi, sahibinin inançlarına ve değerlerine bağlı olarak bu bilgi akışı yoluyla oluşur (Gurteen, 1999). Bu bağlamda bilgi, bilginin deneyler, deneyimler veya yorumlarla birleştirilmesinden ortaya çıkan bilgi olarak tanımlanabilir; kişisel olarak organize edilmiş bilgi, bilginin aksine bilgi eyleme yöneliktir ve bilgiyi uygulamaya koyma yeteneğini tanımlar (Aktan ve Vural, 2016).

Araştırma literatürüne bakıldığında, bilgi güvenliği tarihini bilgisayar güvenliği kavramıyla ilişkilendirildiği gözlemlenmektedir. İhtiyaç duyulan bilgisayar güvenliği, 2. Dünya Savaşı sırasında ortaya çıkmıştır. Bu dönemde, ilk ana bilgisayarlar geliştirilmiş ve iletişim kodlarının kırılmasına karşı koruma sağlamak için kullanılmıştır (Whitman ve Mattord, 2011: 4-5).

Bu zaman diliminde, en büyük güvenlik endişesi, bilgisayarların yetkisiz erişime karşı korunması ve fiziksel olarak güvende olmasıydı. Özellikle askeri ve devlet kurumlarında, bilgisayarların yabancılar tarafından ele geçirilmesi veya zarar görmesi büyük bir risk oluşturuyordu. Bu nedenle, cihazların ve sundukları hizmetlerin güvenliğini sağlamak için çeşitli güvenlik seviyeleri benimsenmiştir (Dlamini vd., 2008: 1905).

Günümüzde ise bilgi güvenliği, sadece bilgisayar sistemlerini ve ağları korumakla sınırlı kalmamıştır. Mobil cihazlar, bulut bilişim, büyük veri depolama ve internet ofis eşyaları gibi yeni teknolojilerin yaygınlaşmasıyla birlikte, bilgi güvenliği kapsamı genişlemiştir. Artık, kişisel verilerin korunması, kimlik hırsızlığına karşı önlemler, fidye yazılımları ve diğer siber saldırı türlerine karşı savunma da büyük önem taşımaktadır.

1990'ların sonlarına doğru, siber saldırganlar daha karmaşık yöntemlere doğru evrilmeye başladılar. Artık solucanlar ve virüslerin ötesine geçerek, elektronik postaları veya web sitelerini hedef alarak kötü amaçlı kodlar yerleştirmeye başladılar. Bu tür saldırıların önüne geçmek için güvenlik duvarları uygulanmaya başlasada, internet kullanımının artmasıyla birlikte bu önlemler yetersiz kaldı. Bilgisayar korsanları, ücretsiz olarak erişilebilen araçlarla daha sofistike saldırılar gerçekleştirebilecek hale geldiler. 21. yüzyılın başlarında, bilişim teknolojilerinin endüstriler arasında yayılması ve mobil cihazların popüler hale gelmesiyle birlikte saldırı yöntemleri de değişime uğradı. Artık saldırganlar, finansal kazanç elde etmek için hackleme gibi farklı taktikleri tercih etmeye başladılar (Xu vd., 2021: 1-2).

Bilişim teknolojilerinin sürekli olarak gelişmesi, yeni tehditlerin ortaya çıkma olasılığını da beraberinde getiriyor. Bu nedenle, bilgi güvenliğini sağlamak için fiziksel güvenlik, bilgi güvenliği farkındalığı, kimlik yönetimi ve çevre güvenliği gibi alanlara odaklanılması önemlidir (Dlamini vd., 2008: 192). Bu açıdan bakıldığında, bilgi güvenliği alanındaki sürekli değişim ve gelişim, kuruluşların ve bireylerin bu alanda bilinçlenmesi ve sürekli olarak güvenlik önlemlerini güncellemesi gerektiğini vurgulamaktadır.

Bilgi güvenliğinin temel ilkeleri olan gizlilik, bütünlük ve erişilebilirlik, bilginin güvenliğinin sağlanmasında kritik öneme sahiptir (Güngör, 2015). Gizlilik ilkesi, bilgilerin yetkisiz kişilerin erişimine kapalı tutulması için gerekli kuralları içerir. Bu,

bilgilerin sadece yetkilendirilmiş kullanıcılar veya sistemler tarafından erişilebilir olmasını sağlar, böylece hassas bilgilerin gizliliği korunur. Bütünlük ilkesi ise, bilgilerin iletilirken veya depolanırken değiştirilmeden veya bozulmadan kalmasını sağlar. Bilginin göndericiden alıcıya güvenli bir şekilde iletilmesini ve bilginin manipülasyona uğramadan doğru olduğunun garanti edilmesini amaçlar. Bu sayede, bilgiye güvenilirlik kazandırılır ve bilgiyle ilgili güvenilir kararlar alınabilir. Erişilebilirlik veya tutarlılık ilkesi ise, bilginin ihtiyaç duyulduğunda uygun bir şekilde erişilebilir olmasını sağlar. Bu ilke, bilginin kullanıcıların gereksinimlerine ve yetkilerine uygun olarak zamanında erişilebilir olmasını hedefler. Bilgiye gerektiği anda ve gerektiği şekilde erişilebilmesi, iş sürekliliğini ve etkinliğini sağlar. Bu temel ilkelerin bir araya gelmesiyle, bilginin güvenliği sağlanır ve bilgi varlıkları etkin bir şekilde korunmuş olur. Bu nedenle, organizasyonlar bu ilkeleri dikkate alarak güvenlik politikalarını ve uygulamalarını oluşturmalı ve sürekli olarak gözden geçirmelidirler (ISO 27001 Bilgi Güvenliğinin Temel İlkeleri).

1.1.1. Bilgi Güvenliğinin Amacı

Bilgi güvenliği, kişisel bilgisayarlar ve mobil cihazlar gibi başlangıç noktalarından kurumsal ve ulusal düzeyde tüm iletişim cihazları ve kritik bilgi altyapılarını kapsayan geniş bir çerçevede bilgi sistemlerinin güvenlik yönetimini sağlamaktadır. Bu yönetim anlayışı, dijital ortamda saklanan verilerin, göndericiden alıcıya bütünlüğünü ve doğruluğunu korurken, saklanan veriye her zaman güvenli bir şekilde erişilebilmesini ve bilginin izinsiz ve yetkisiz erişimlerden korunmasını sağlamak için gereken tüm önlemleri içermektedir (Güngör, 2015).

Bilgi güvenliği, bilgi sistemlerinin sürekli, kesintisiz, kaliteli ve güvenilir bir şekilde çalışmasını sağlayarak kurum ve ülke imajının zedelenmesini önlemekte ve bilgi varlıklarının korunmasını ve yetkisiz kişilerin erişimini engellemektedir (Özdemir, 2019: 13; Güngör, 2015). Günümüzde bilgi güvenliği, sadece teknik önlemleri değil, aynı zamanda insan faktörünü de içeren kapsamlı bir yaklaşım gerektirmektedir. Bu nedenle, bilgi güvenliği politikalarının ve uygulamalarının oluşturulması ve sürdürülmesi, eğitim ve farkındalık programlarının yürütülmesi önemlidir. Ayrıca, sürekli olarak değişen tehditlerle başa çıkabilmek için güvenlik önlemlerinin düzenli olarak gözden geçirilmesi ve güncellenmesi gerekmektedir.

Bilgi güvenliği, sadece bir kurumun veya bir ülkenin değil, genel olarak küresel bilgi ekosisteminin sağlıklı işleyişi için kritik öneme sahiptir. Bu nedenle, bilgi güvenliğine yönelik yapılan her türlü yatırım, uzun vadede hem kurumların hem de toplumların çıkarına olacaktır.

1.1.2. Bilgi Güvenliği Eğitimi ve Önemi

Bilgi güvenliği eğitimi, önemini artıran bir dizi unsur içermektedir (Privia, 2023; Doğru, 2023):

- Farkındalığı Artırma: Bilgi güvenliği eğitimi, bireyleri ve kuruluşları potansiyel tehditler konusunda bilinçlendirerek farkındalığı artırır. Bilgisayar korsanlığı, kötü amaçlı yazılımlar, sosyal mühendislik saldırıları ve diğer saldırı türleri hakkında bilgi sahibi olmak, bireyleri olası risklere karşı uyanık olmaya teşvik eder.
- Saldırıları Tanıma: Bilgi güvenliği eğitimi, saldırıları tanıma ve tespit etme becerilerini geliştirir. Örneğin, e-posta dolandırıcılığı veya kimlik avı girişimi gibi saldırıları tanıma yeteneği, bireylerin bu tür saldırılara karşı korunmasına yardımcı olur.
- Doğru Uygulamaları Öğretme: Bilgi güvenliği eğitimi, güvenli parola oluşturma, güncel yazılım kullanma, düzenli veri yedeklemesi yapma gibi doğru güvenlik uygulamalarını öğretir. Bu uygulamalar, kişisel ve kurumsal bilgilerin korunmasında kritik bir rol oynar.
- İç Tehditleri Azaltma: Bilgi güvenliği eğitimi, çalışanların veya kullanıcıların bilinçli bir şekilde zararlı davranışlardan kaçınmalarını sağlar. Bilgiye yetkisiz erişim, veri hırsızlığı veya diğer iç tehditler, doğru eğitimle azaltılabilir.

Bu unsurlar, bilgi güvenliği eğitimlerinin etkinliğini artırmak ve bireyleri bilgi güvenliği konusunda daha bilinçli hale getirmek için temel prensipleri oluşturur.

1.1.3. Bilgi Güvenliğini Sağlamaya Yönelik Önlemler

Bilgi güvenliğini sağlamaya yönelik önlemler kurumsal ve bireysel olmak üzere iki alt başlık halinde incelenmektedir.

1.1.3.1. Kurumsal Bilgi Güvenliği Önlemleri

Bilgi güvenliğinin sağlanması için temel üç unsur vardır: yönetsel önlemler, teknolojik önlemler ve insan faktörü.

Yönetsel Önlemler: Teknolojik önlemlerin yanı sıra, yazılımsal ve donanımsal çözümlerle bilgi güvenliği sağlanamaz. Her kurum, bilgi güvenliğini kurum kültürünün bir parçası olarak kabul etmeli, güvenlik stratejileri oluşturmalı ve çalışanlarını bilgilendirerek gerekli hassasiyeti göstermelerini sağlamalıdır. Yönetsel önlemler kapsamında alınması gereken bazı önemli adımlar şunlardır (Yıldız, 2014):

- Risk yönetimi sürecinin belirlenmesi ve uygulanması.
- Kurumun bilgi güvenliği politikalarının oluşturulması ve uygulanması.
- Standartlar, yönergeler ve prosedürlerin belirlenerek çalışanlara iletilmesi ve uygulanması.
- Düzenli olarak güvenlik denetimlerinin yapılması ve sonuçların değerlendirilmesi.

Bu adımlar, kurumun bilgi güvenliğini sağlamak için temel bir çerçeve oluşturur ve güvenliği sadece teknik önlemlerle değil, aynı zamanda kurumsal yönetim ve kültürle de ilişkilendirir.

Teknolojik Önlemler: Bilgi güvenliğinin sağlanması için gerekli olan yazılım ve donanım önlemlerini içerir. Bilgi güvenliğinin sağlanması hem kurumlar hem de bireyler için teknolojik önlemlerin alınmasıyla mümkündür.

Bilgi güvenliğine yönelik alınabilecek teknolojik önlemler şunlardır (Özdemir, 2019: 44):

- Şifreleme teknolojileri: Hassas bilgilerin korunması için kullanılan şifreleme yöntemleri.
- Sayısal İmza: Elektronik belgelerin güvenliği için kullanılan kimlik doğrulama yöntemleri.

- Güvenlik duvarı: Ağ trafiğini kontrol ederek kötü amaçlı yazılımların ve saldırıların engellenmesini sağlayan sistemler.
- Yedekleme: Veri kaybını önlemek için düzenli olarak yapılan veri yedekleme işlemleri.
- Antivirüs: Bilgisayar sistemlerini kötü amaçlı yazılımlardan koruyan yazılım çözümleri.
- Yazılım Güvenliği: Yazılımların güvenlik açıklarının tespit edilerek giderilmesi ve güvenli yazılım geliştirme yöntemlerinin uygulanması.
- Ağ güvenliği: Ağ trafiğini izleyerek ve denetleyerek ağ üzerindeki tehditlerin tespit edilmesi ve engellenmesi.
- İnternet güvenliği: İnternet üzerinde gezinirken kullanıcıların güvenliğini sağlamak için alınan önlemler.
- Kullanıcı hesabı güvenliği: Kullanıcıların hesaplarının güvenliğini sağlamak için şifreleme, kimlik doğrulama ve yetkilendirme yöntemlerinin kullanılması.

Eğitim ve Farkındalık: Bilgi ve iletişim teknolojilerindeki gelişmeler, bilgi güvenliği tehditlerinin artmasına neden olmuştur. Bu nedenle, bilgi güvenliği konusunda farkındalık oluşturulması giderek daha önemli hale gelmektedir. Kurumlar, bilgi güvenliği eğitimlerine önem vermeli ve periyodik olarak personel ihtiyaçlarına göre tekrarlanmalıdır. Ayrıca, farkındalık oluşturmak için "bilinçlendirme toplantıları", "posterler", "seminerler" ve "e-posta bültenleri" gibi yöntemler kullanılmalıdır. Bu etkinliklerde gizliliğin önemi vurgulanmalı ve bilgi güvenliği konusundaki en iyi uygulamalar paylaşılmalıdır (Öztezcan, 2017).

1.1.3.2. Bireysel Bilgi Güvenliği Önlemleri

Kurumsal düzeyde büyük önem taşıyan bilgi güvenliği, bilgi teknolojilerinin gelişimiyle birlikte bireysel düzeyde de gereklilik haline gelmiştir. Bireylerin bilgi güvenliğini sağlaması için alınması gereken önlemler aşağıda sıralanmıştır (Gülmüş, 2010; Akıncan, 2022):

- Bilgisayarlara antivirüs ve antimalware yazılımları yüklenmelidir ve bu yazılımlar düzenli olarak güncellenmelidir.
- Lisanssız yazılımlar yüklenmemeli ve güvenilir olmayan kaynaklardan yazılım indirilmemelidir.
- E-posta eklentileri dikkatle incelenmeli ve güvenilmeyen e-postalar açılmadan silinmelidir.
- İnternette her site ziyaret edilmemeli ve açılır pencerelere (popuplar) dikkat edilmelidir.
- İnternete bağlanan tüm cihazlar için virüs bulaşabileceği unutulmamalı ve gerekli önlemler alınmalıdır.
- Güvenlik yazılımları düzenli olarak güncel tutulmalı ve sistemler düzenli olarak taranmalıdır.
- USB gibi harici cihazlar taranmadan kullanılmamalıdır ve güvenilir kaynaklardan alınmalıdır.
- Her hesap için ayrı ve güçlü parolalar kullanılmalıdır.
- Kablosuz hotspot'lar hakkında bilgi sahibi olunmalı ve cihazların erişilebilir güvenlik ayarları yapılmalıdır.
- Güvenli bağlantı sağlamayan "http://" protokolü yerine "https://" protokolünü kullanan web siteleri tercih edilmelidir.
- ADSL modem güvenliği sağlanmalı, modem arayüzü şifrelenmeli ve modem şifreleri belirli aralıklarla değiştirilmelidir.
- Bankacılık ve çevrimiçi alışveriş işlemleri ortak alan bilgisayarlarından yapılmamalı ve çevrimiçi alışverişler için sanal kartlar kullanılmalıdır.
- Sosyal paylaşım sitelerinde gizlilik kurallarına dikkat edilmelidir.
- Dosya veya veriler farklı güvenli ortamlarda yedeklenmelidir ve düzenli olarak yedeklenen verilerin güncel olduğundan emin olunmalıdır.

Bu önlemler bireylerin bilgi güvenliğini sağlayarak kişisel ve hassas verilerinin korunmasına yardımcı olacaktır.

1.1.4. Bilgi Güvenliği Politikaları

Politika bir kurallar bütünüdür ve sistemin davranış şeklini belirten bir durumdur. Bilgi güvenliği politikası ise bilgi varlıklarının nasıl kullanılması gerektiğine ilişkin kurallar bütünüdür. Bilgi güvenliğinin temel unsurlarından hareketle ihtiyaç duyulan çok çeşitli alanlarda politika geliştirilmesi ihtiyacı kaçınılmazdır (Can ve Ünalır, 2010). Birbirine bağlı bilgi sistemleri ve ağlar, kurum ve kuruluşları sahip oldukları bilgilerin korunması için belirgin önlemler alınması gerektiği ihtiyacı gibi önemli bir duruma itmektedir. "Güvenlik kültürü" iş rekabetinin çok önemli bir parçası haline gelmiştir ve güvenlik politikası iş yönetiminin önemli bir bileşenidir (Luma ve Abazi, 2019).

Kurumlar ve kuruluşlar, işleyişleri ve refahları için gerekli olan büyük miktarda bilgi üretir, kullanır, depolar ve iletir. Bilgiler gerektiğinde gizli tutulmalı, gerektiğinde erişilebilir hale getirilmeli ve değiştirilmeye ve bütünlüğünün kaybolmasına karşı korunmalıdır. Bilgi ve teknoloji kullanıcılarının standartlarını, sınırlarını ve sorumluluklarını tanımlayan bir bilgi güvenliği politikası oluşturmak, bilgi ihlalleri tehdidini ele almanın temel bir yaklaşımıdır (Bhaharin vd. 2019; Can ve Ünalır, 2010).

Bilgi güvenliği politikası, bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak için önlemlerin uygulanmasına ilişkin ilkeleri belirleyen bir belgedir. Güvenlik politikaları, kurumlar veya kuruluşlar içinde kabul edilebilir güvenlik düzeyini tanımlayan ve tüm çalışanlar ve onlarla iş birliği yapan diğer tüm kurum ve kuruluşlar tarafından uyulması gereken bir dizi kuraldır (Kalman, 2003).

Bilgi güvenliği politikası ve içinde oluşturulan ilgili belgeler, kurum tarafından oluşturulan önlemlerin hangilerinin onaylandığını veya onaylanmadığını belirtir. Her kurum ve kuruluş farklı şekilde yapılandırıldığı için güvenlik politikaları da farklıdır. Ancak kurumsal bilgi güvenliği politikaları genellikle çalışan sorumlulukları, güvenlik denetim araçları, amaç ve hedefler ile kurumsal bilgilerin temel işlevlerini yönetme, koruma, dağıtma ve güvence altına alma kuralları ve uygulamaları hakkında genel açıklamalar içerir (Can ve Ünalır, 2010).

Bilgi güvenliği politikalarının temel amacı, çalışanlar ve ilgili taraflarca uyulması gereken bilgi güvenliği koşullarını ana hatlarıyla belirtmek ve yazılı kurallar oluşturmaktır. Bilgi güvenliği politikalarının diğer alt amaçları arasında her kurumdaki çalışanlar arasında bilgi güvenliği farkındalığını artırmak, teknik ve idari bilgi güvenliği önlemlerini uygulamak, ilgili taraflarla yapılan anlaşmalar için gizlilik hükümleri oluşturmak, kurumun itibarını korumak, kurumun birincil ve ikincil iş faaliyetlerinin mümkün olan en az kesintiyle devam etmesini sağlamak ve çalışanları bilgi güvenliği gerekliliklerine uygun hareket etmeye yönlendirmek yer alır. Ayrıca bilgi güvenliği politikaları kurumlara bir dizi fayda sağlar (Meral, 2022).

Can ve Akbaş (2014) çalışmalarında bilgi güvenliği politikalarının kurum çalışanlarını ve üçüncü kişileri yasal sorumluluktan koruduğunu, kurumu gizli bilgilere yetkisiz erişimden, bunların ifşa edilmesinden ve değiştirilmesinden koruduğunu ve kurumun BT kaynaklarının gereksiz yere kullanılmasını ve israf edilmesini önlediğini bulmuşlardır. Kurumlar, yapıları, iş süreçleri ve ihtiyaçları ile uyumlu güvenlik politikaları oluşturmalı ve üst düzey yönetimin desteğini almalıdır. Üst düzey yönetim desteği, kurum içinde bilgi güvenliğinin sağlanması için gerekli bağlılığı gösterir ve kurum çalışanlarının bilgi güvenliğine daha fazla önem vermesini sağlar (Öztürk, 2008).

Üst düzey yönetimin destekleyici tutum ve davranışları, bilgi güvenliği çalışmalarının amacına ulaşmak için önemlidir. Bilgi güvenliği politikası, temel politika olarak oluşturulmalıdır. Diğer güvenlik politikaları, temel politika ile uyumlu ve uyumlu olmalıdır (TÜBİTAK BİLGEM YTE, 2021).

Alshaikh ve diğerleri (2015) çalışmalarında bilgi güvenliği politika geliştirme modeli ortaya koymuştur. Önerilen model geliştirme, uygulama ve bakım ve değerlendirme aşamalarından oluşmaktadır. Her aşama yapılması gereken adımları anlatmaktadır. Politika geliştirme aşaması temel olarak politika geliştirme ekibinin kurulması, kurum dış paydaşlarının belirlenmesi, rol ve sorumluluk atamaları adımlarından oluşmaktadır. Temel adımları takiben kurumun güvenlik gereksinimlerinin belirlenmesi, mevcut güvenlik politika ve prosedürlerinin değerlendirilmesi, politika bileşenlerinin belirlenerek taslak politika dokümanının oluşturulması ve gözden geçirilmesi adımları yer almaktadır. Önerilen modelde geliştirilen bilgi güvenliği politikasının uygulama ve bakım aşamasında, politikanın çalışanlara ve dış paydaşlara duyurulması, hangi

kanallardan erişilebileceğinin belirlenmesi, politika hakkında yeterli farkındalığın sağlanması ve politikanın uygulanması için gerekli faaliyetlerin yürütülmesi adımları ifade edilmektedir. Politikanın son aşaması olan değerlendirme aşamasında ise politikanın güncelliğinin sağlanması adına düzenli aralıklarla gözden geçirilmesi, politika hakkında çalışanlar ve dış paydaşlardan geri bildirim alınması, politikanın bu doğrultuda olgunlaştırılması ve bilgi güvenliği olaylarının değerlendirilmesi ve risk değerlendirme yaklaşımının gözden geçirilmesi adımlarından bahsedilmektedir.

Bilgi güvenliği politikalarının oluşturulması ve uygulanması sırasında bilgi güvenliği politikalarının tüm yönleri değerlendirilmeden başarılı bir bilgi güvenliği güvencesi mümkün değildir (Henkoğlu ve Yılmaz, 2013). Bilgi güvenliği politikası açık ve anlaşılır bir şekilde yazılmalıdır. Kurum çalışanları ve dış paydaşlar tarafından açıkça anlaşılabilir olmalı ve gizli bilgiler içermemelidir. İyi bir güvenlik politikası kullanıcıların işini zorlaştırmamalı, kullanıcı tepkilerine yol açmamalı ve kullanıcılar için uygulanabilir olmalıdır (Vural, 2007).

Bilgi güvenliği politikası genel olarak aşağıdaki başlıkları içermelidir (Anlık Güvenlik Politikası, 2010):

- Genel Açıklama: Ele alınan konu hakkında temel bilgileri sağlar.
- Amaç: Politikanın neden gerekli olduğunu belirtir.
- Kapsam: Politikanın neyi ve kimi kapsadığını belirtir.
- Hedef Kitle: Politikada belirlenen ilkelere uyulması konusunda ilgili önerileri ve rehberliği içerir.
- Yönergeler: Bu kurallar politika belgesinin ana gövdesini oluşturur ve maddelerde uyulması gereken ilkeleri ana hatlarıyla belirtir.
- Tanımlar: Bu bölüm teknik terimleri açıklar.
- Sürüm: Bu, politika belgesi güncellendiğinde ilgili değişikliklerin dahil edilebilmesi için belgenin sürüm numarasıdır.

1.1.5. Bilgi Güvenliği Standartları

Bu başlık altında, bilgi güvenliği alanında ulusal ve uluslararası düzeyde kabul görmüş standartlar tanıtılmıştır. ISO/IEC 27001 ve 27002, bilgi güvenliği yönetim sistemi kurulumu ve kontrol kılavuzları olarak öne çıkarken; NIST SP 800 serisi, COBIT, ITAF

ve SoGP gibi standartlar, güvenlik denetimi, risk yönetimi ve iyi uygulamalar çerçevesinde detaylandırılmıştır. IEEE 802 standartları ağ güvenliğine odaklanırken, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Rehberi ve KVKK gibi ulusal düzenlemelere de yer verilerek kamu kurumlarında bilgi güvenliği uygulamaları incelenmiştir.

1.1.5.1. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi

Günümüzde bilgi güvenliği yönetimi için en yaygın kullanılan standartlar ISO/IEC 27000 serisi kapsamındaki standartlardır. Bu sandartlardan en önemlisi olan ISO/IEC 27001, ilk olarak İngilterede geliştirilen BS 7799 standartına dayanmaktadır. Bu standat, 1993 yılında BSI (British Standards Institution) tarafından yayınlanmış ve 1995 yılında resmi bir İngiliz Standardı olarak kabul edilmiştir. 1998 yılında ise ikinci bölümü olan BS 7799-2 bilgi güvenliği yönetim sisteminin nasıl uygulanacağına dair detaylarını içerecek şekilde yayınlanmıştır. Bu gelişmeler, bilgi güvenliği alanında uluslararası kabul görecek bir standartlaşmanın temelini atmıştır (Çek, 2017).

2000 yılında ISO ve IEC'nin oluşturduğu ortak çalışma grubu, BS 7799-1 standardını esas alarak ISO/IEC 17799 standardını oluşturmuştur. Bu standart, bilgi güvenliğine ilişkin politika, organizasyon, varlık yönetimi gibi 10 ana başlık altında 127 kotrol maddesi içermektedir. ISO-IEC 17799, 2005 yılında revize edilerek ISO/IEC 27001:2005 ismi ile yayınlanmış ve Türkiye'de TSE tarafından TS ISO/IEC 27001:2005 adıyla Türkçeye çevrilmiştir. Standart, 2013 yılında tekrar güncellenerek TS ISO/IEC 27001:2013 olarak kabul edilmiştir. ISO/IEC 27001 standardı, bilgi güvenliği yönetim sistemlerinin kurulması, işletilmesi ve sürekli iyileştirilmesi için bir çerçeve sunmakta; kontrol ögeleri ile ne yapılması gerektiği tanımlarken, nasıl yapılacağına dair uyulama detaylarını kurumların kendi risk analizlerini ve ihtiyaçlarını bırakmaktadır (Özkan & Tuncer, 2021).

1.1.5.2. ISO/IEC 27002 Bilgi Güvenliği Kontrol Kılavuzu

ISO / IEC 27001'in gerekliliklerine dayanan bir Bilgi Güvenliği Yönetim Sistemi (BGYS) çerçevesinde, güvenlik kontrollerinin seçimi ve uygulanmasına yönelik yol gösterici bir standart olan ISO/IEC 27002: 2022, bilgi güvenliği kontrollerini detaylandıran ve ISO 27001'deki gereksinimler genişleten bir kontrol kılavuzu niteliğindedir Bu standart, bilgi güvenliğinin şirketler açısından taşıdığı önemi

vurgulamakta ve bilgi güvenliği risklerine karşı alınması gereken önlemleri sistematik bir şekilde ortaya koymaktadır. Ayrıca kurumların bilgi varlıklarını koruma yükümlülüğünü, risk temelli yaklaşımla kontrol altına alma gereği açıklamayı amaçlamaktadır (Disterer, 2013: 93).

ISO 27001 ve ISO 27002 farklı hedeflere sahiptirler. Temel fark ISO 27001, bir uluslararası bilgi güvenliği yönetim standardıdır. ISO 27002 ise bilgi güvenliği kontrollerinin nasıl uygulanabileceğine kılavuz olarak yönlendiren bir destekleyici standarttır (ISO 27001 vs. ISO 27002, t.y.).

1.1.5.3. NIST SP 800 Serisi Standartları

Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technogy), tarafından kuruluşların siber güvenlik risklerini yönetmelerine yardımcı olmak için siber tehditleri ele alan ve kuruluşların hizmetlerini destekleyen bir dizi güvenlik standardı ve rehberlik dokümanlarıdır. NIST SP 800 serisi standartları, siber güvenlik uygulamaları, bilgi güvenliği yönetimi, risk değerlendirme, risk işleme ve kontrol önlemlerinin belirlenmesi gibi faaliyetler için uluslararası kabul görmüş yayınları arasında yer almaktadır. Bu serinin amacı, bilgi güvenliği ve siber güvenlik alanında en iyi uygulamaları, yöntemleri ve kontrolleri tanımlamak ve yaymak ve kuruluşlara rehberlik etmektir. NIST Özel Yayınlar 800 serisi olarak tanınan bu dokümanlar, bilgi sistemlerinin güvenlik faaliyetleri için rehberlik sağlayan pek çok standardı kapsamaktadır (Calder, 2018).

1.1.5.4. COBIT Standartları

Bilgi Sistemleri Denetim ve Kontrol Derneği (ISACA) tarafından bilgi teknolojisi yönetimi için oluşturulan COBIT (Bilgi ve Bağlantılı Teknolojiler Kontrol Hedefleri Standardı), bilgi ve bağlantılı teknolojilerin yönetimi için bir çerçeve olarak kullanılan bir dizi standart ve rehberlikler bütünüdür. COBIT, bilgi teknolojileri yönetimi, bilgi güvenliği, risk yönetimi ve iş sürekliliği gibi alanlarda en iyi uygulamaları ve kontrol hedeflerini tanımlamaktadır (ISACA, 2019).

COBIT, ilk olarak 1996'da piyasaya sürüldü ve en son sürümü 2019'da yayımlanmıştır. Bu dokümanlar, kuruluşların bilgi ve bağlantılı teknolojileri etkili bir şekilde

yönetmelerine yardımcı olmak için çeşitli kontrol hedefleri ve en iyi uygulamalar sunmaktadır. İşletme hedeflerini desteklemek, riskleri yönetmek, kaynakları etkin bir şekilde kullanmak, bilgi ve teknoloji ile ilgili faaliyetleri izlemek ve performansı değerlendirmek için çeşitli kontrol hedefleri sağlamaktadır. Bu kontrol hedefleri, bilgi güvenliği, süreç performansı, risk yönetimi, kaynak yönetimi ve iş birliği gibi alanlarda odaklanmaktadır. Kuruluşların bilgi ve bağlantılı teknolojilerle ilgili süreçleri ve kontrolleri kurmalarını, uygulamalarını ve iyileştirmelerini sağlamayı amaçlayan COBİT, ayrıca kuruluşlar arasında bir dil ve anlayış sağlayarak paydaşlar arasında etkili iletişimi ve iş birliğini teşvik etmektedir (ISACA, 2018).

COBIT'in kontrol hedeflerini açıklayan bir standardı kesin olarak COBIT 5 olarak bilinmektedir. Bu standart, organizasyonların bilgi teknolojileri süreçlerini etkin bir şekilde yönetmelerini, riskleri azaltmalarını ve hedeflere ulaşmalarını sağlamak için bir dizi kontrol hedefi sunmaktadır. COBIT 5, planlama ve organizasyon, edinme ve uygulama, teslim ve destek, izleme ve değerlendirme, iş sürekliliği ve risk optimizasyonu olmak üzere beş ana hedef kategorisine dayanan 37 kontrol hedefini tanımlamaktadır. Bu kontrol hedefleri, organizasyonların bilgi teknolojilerini etkili bir şekilde yönetmelerine ve kontrol etmelerine yardımcı olmaktadır. COBIT, bilgi teknolojileri hizmetlerinin iş gereksinimlerine uygun olarak sağlanmasını, risklerin yönetilmesini ve stratejik hedeflere ulaşılmasını desteklemektedir (ISACA, 2019).

1.1.5.5. ITAF Standartları

ITAF (Bilgi Güvenliği Denetimi ve Emniyeti Standartları), bilgi güvenliği denetimi ve emniyeti için bir standartlar setidir. ITAF, ISACA tarafından geliştirilmiş ve bilgi teknolojileri denetimini desteklemek amacıyla kullanılan bir çerçevedir. Denetim ve güvenlik görevlilerinin planlanması, yerine getirilmesi ve raporlanması teknikleri ve kılavuzlarını sunmaktadır. Standart üç kategoriye ayrılmaktadır. 100 serisi genel standartları, 1200 serisi performans standartlarını, 1400 serisi ise raporlama standartlarını oluşturmaktadır. ITAF standartları, bilgi güvenliği denetimi sürecinde izlenmesi gereken adımları, en iyi uygulamaları ve kontrol hedeflerini tanımlamaktadır. Bu standartlar, denetim profesyonellerine, bilgi güvenliği kontrolünün etkin bir şekilde yapılmasına yardımcı olur ve riskleri azaltmaya yönelik öneriler sunmaktadır (ISACA, 2022).

ITAF, şu bileşenlerden oluşmaktadır (ISACA, 2022):

- Genel Kontroller: Bilgi sistemlerinin güvenliğini ve işletimini etkileyen genel kontrolleri içerir. Örnek olarak, fiziksel güvenlik önlemleri, erişim kontrolü ve değişiklik yönetimi gibi konular bulunur.
- Uygulama Kontrolleri: Uygulama sistemlerinin güvenliğini ve işletimini etkileyen kontrolleri içerir. Örnek olarak, veri girişi kontrolleri, yetkilendirme mekanizmaları ve veritabanı yönetimi gibi konular bulunur.
- Operasyon Kontrolleri: Bilgi teknolojileri operasyonlarının güvenliğini ve işletimini etkileyen kontrolleri içerir. Örnek olarak, sistem izleme, yedekleme ve geri yükleme, olay yönetimi gibi konular bulunur.
- Bilgi Güvenliği Kontrolleri: Bilgi güvenliği yönetimine yönelik kontrolleri içerir. Örnek olarak, politika ve prosedürlerin oluşturulması, risk değerlendirmesi, olay yanıtı ve felaket kurtarma gibi konular bulunur.

1.1.5.6. SoGP Standardı

SoGP (Bilgi Güvenliği İçin İyi Uygulama Standard) standardı ilk olarak 1996 yılında Bilgi Güvenliği Forumu (ISF) tarafından yayımlanmıştır. Bilgi güvenliği için en iyi uygulamaların ayrıntılı bir dokümantasyonunu temsil etmektedir. Standart iki yılda bir yayınlanmakta ve revize edilmektedir. Ücretsiz olarak kullanılabilen İyi Uygulama Standardı, ISO/IEC 27002 ve COBIT v4.1'den türetilmiştir. Bu standartlar ve hem araştırmaya hem de gerçek dünya deneyimine dayanan işlevsel bir bilgi güvenliği metodolojisini ana hatlarıyla belirtmektedir (Whitman ve Mattord, 2019).

SoGP İyi Uygulama Standardı Standartı, altı temel güvenlik hususunu ele almaktadır (Kavak, 2023):

- Bilgisayar kurulumları; esas olarak bilgi teknolojisi uzmanlarını hedeflemekte ve kritik iş uygulamalarını destekleyen donanım ve yazılımları ele almaktadır.
- Kritik iş uygulamaları; kuruluşun faaliyetlerinin bağlı olduğu uygulamalardır. Bu yön öncelikle iş süreçlerinden sorumlu kişileri ve sistem jeneratörlerini hedef almaktadır.

- Güvenlik yönetimi; güvenlikle ilgili karar vericileri ve denetçileri hedef almaktadır. Kuruluş genelinde güvenlik uygulamalarıyla ilgili olarak yönetim düzeyinde karar vermeyi yönetmektedir.
- Ağlar; benzersiz güvenlik açıkları nedeniyle özel bir kategori oluşturmaktadır. Bu güvenlik hususu, genellikle ağ yöneticileri, ağ hizmeti uzmanları ve ağ hizmeti sağlayıcılarının güvenliği hedeflenmekte ve bir kuruluşun ağ oluşturma gereksinimlerinin doğasını ve uygulamasını ele almaktadır.
- Sistem geliştirme; sistem geliştiricilerine hitap etmekte olup sistem gereksinimlerinin tanımlanması, tasarımı ve uygulanması ile ilgilenmektedir.
- Son kullanıcı ortamı; son kullanıcı ortamlarında çalışan işletme yöneticilerini ve bireylerin güvenliği hedeflenmektedir.

1.1.5.7. IEEE 802 Standartları

IEEE 802 standartları, kablosuz ağlar, Ethernet ve yerel alan ağı (LAN) teknolojileri gibi bilgisayar ağlarıyla ilgili teknik spesifikasyonları belirlemek için kullanılan bir dizi standarttır. Elektrik ve Elektronik Mühendisleri Derneği (Institute of Electrical and Electronics Engineers- IEEE) tarafından geliştirilen bu standartlar, bilgisayar ağlarının uyumlu ve etkin çalışmasını sağlamak amacıyla oluşturulmuştur (Kavak, 2023).

IEEE 802 standartları, farklı katmanlarda çalışan ağ protokollerini kapsar. Aşağıda, bazı önemli IEEE 802 standartlarının örneklerini bulabilirsiniz (Guo ve Congdon, 2021):

- IEEE 802.3 (Ethernet): Kablolu yerel alan ağlarında (LAN) kullanılan Ethernet standartlarını belirlemektedir. Bu standartlar, veri iletimi için çerçeve yapısını, veri hızlarını ve ağ topolojilerini tanımlamaktadır.
- IEEE 802.11 (Wi-Fi): Kablosuz yerel alan ağlarında (WLAN) kullanılan WiFi standartlarını belirlemektedir. Bu standartlar, kablosuz ağ bağlantısını, frekans bantlarını, güvenlik protokollerini ve hızları tanımlamaktadır.
- IEEE 802.15 (Bluetooth): Kablosuz kişisel alan ağlarında (PAN) kullanılan Bluetooth standartlarını belirlemektedir. Bu standartlar, kısa mesafeli kablosuz iletişimi, bağlantı protokollerini ve güvenlik özelliklerini tanımlamaktadır.

- IEEE 802.16 (WiMAX): Geniş alan ağlarında (WAN) kullanılan WiMAX standartlarını belirletendir. Bu standartlar, yüksek hızlı kablosuz internet erişimini, veri hızlarını ve mesafeleri tanımlamaktadır.
- IEEE 802.1 (LAN/MAN Yönetimi): Yerel alan ağları (LAN) ve geniş alan ağları (MAN) yönetimi için standartlar oluşturulmaktadır. Bu standartlar, ağ yapılandırması, ağ yönetimi protokolleri ve ağ güvenliği gibi konuları kapsamaktadır.

IEEE 802 standartları, bilgisayar ağlarının uyumlu bir şekilde çalışmasını sağlamakta ve farklı cihazların birbirleriyle iletişim kurabilmesini sağlayan ortak bir dil oluşturulmaktadır. Bu standartlar, ağ teknolojilerinin gelişmesine ve ilerlemesine katkıda bulunmakta ve endüstri genelinde kabul görmektedir (Kavak, 2023).

1.1.5.8. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (DDO), 2018 yılında Resmî Gazete'de yayımlanan 30474 sayılı Kararname ile kurulmuştur. Amacı, kamu kurumlarının dijital dönüşümünü koordine etmek ve yapay zekâ ve büyük veri, özellikle siber güvenlik alanlarında merkezi çalışmalar yürütmektir. Bu kapsamda, kamu kurumları ve kritik altyapı kuruluşları için bilgi güvenliği önlemlerini içeren Bilgi ve İletişim Güvenliği Rehberi (BİGR) 27 Temmuz 2020 tarihinde yayımlanmıştır. 2019/2 sayılı Cumhurbaşkanlığı Genelgesi uyarınca rehberin uygulanması zorunlu hale getirilmiştir. Ancak uyumsuzluk durumunda yaptırımlara ilişkin net bir düzenleme bulunmamaktadır (Maden, 2024).

ISO/IEC 27002:2002 rehberi, varlık grupları ve uygulama teknolojisi alanlarına yönelik güvenlik önlemlerini sistematik biçimde ele almaktadır. Varlık grupları; ağlar ve sistemler, uygulamalar, giyilebilir teknolojiler, Nesnelerin İnterneti (loT) cihazları, personel ve fiziksel konumlar gibi başlıklar altında sınıflandırılmaktadır. Ayrıca kişisel verilerin işlenmesi, anlık mesaşlaşma uygulamaları, bulut bilişim sistemleri ve kriptografik uygulamalar gibi güncel dijital alanlar da standart kapsamında değerledirilmektedir (ISO/IEC,2022).

Kuruluşlar, bilgi varlıklarını envantere kaydettikten sonra bu varlıklarını ana ve alt kategorilere ayırarak sınıflandırmakta; ardından her varlık için risk temelli bir yaklaşımla

kritiklik seviyesi belirlemektedir. "Ek C.3: Mevcut Durum ve Boşluk Analizi Formu"nu kullanarak mevcut durum ve boşluk analizleri yapar. Kontrollerin uygulanma seviyesi "Tamamen", "Çoğunlukla", "Kısmen", "Hiçbir şekilde" veya "Uygulanamaz" olarak işaretlenir. "Ek C.4: Politika Uygulama Yol Haritası Oluşturma Formu" kullanılarak uygunsuzlukları ele alma planı oluşturulur ve gerekirse telafi edici kontroller "Ek C.5: Telafi Edici Kontroller Kayıt Formu" kullanılarak kaydedilir (Maden, 2024).

Enerji sektörü gibi bazı sektörlere özel ek tedbirler de Rehber kapsamında yer almaktadır. Rehber, ISO/IEC 27001 standardı ile uyumlu yapıdadır. Enerji ve Tabii Kaynaklar Bakanlığı ile bağlı kuruluşlarda Rehber'e dayalı denetimler yürütülmekte, gerektiğinde bu denetimleri Bakanlık personeli üstlenmektedir. Ayrıca, DDO tarafından 10 Ekim 2021 tarihinde yayımlanan "Bilgi ve İletişim Güvenliği Denetim Rehberi" uyarınca, denetim süreci üç ana başlık altında yürütülmektedir: denetimin planlanması, uygulanması ve raporlanması. Denetim sürecinde; denetim ekibi oluşturulmakta, denetim kapsamı belirlenmekte ve program kurumlara bildirilmektedir. Denetim sırasında, Rehber'de tanımlanan tedbirler doğrultusunda kurumlar değerlendirilmekte ve "Süreç Etkinliği" ile "Tedbir Etkinliği" tabloları doldurulmaktadır. Bulgular, kritiklik seviyeleri ve denetim dönem bilgileri ile birlikte raporlanmakta, sürecin sonunda denetim çıktıları DDO'ya iletilmektedir (Maden, 2024).

1.1.5.9. Kişisel Verilerin Korunması Yasası

Ulusal Siber Güvenlik Stratejisi kapsamında 24 Mart 2016 tarihinde kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu, 7 Nisan 2016 tarihinde yürürlüğe girmiştir. Bu kanunun amacı, gerçek kişilerin kişisel verilerinin işlenmesinde temel hak ve özgürlüklerini korumak ve tüzel kişilerin kişisel verilerinin işlenmesine ilişkin yükümlülüklerini, usul ve esaslarını düzenlemektir. Kanunda öngörülen istisnalar haricinde, kişisel veriler ilgili kişinin rızası olmaksızın işlenemez, üçüncü kişilere açıklanamaz ve yurt dışına aktarılamaz. Ancak siber saldırıların ve bilgi güvenliği ihlallerinin azaltılmasında caydırıcı olabilecek başka yasal düzenlemeler de bulunmaktadır. Örnek olarak TCK 243, 244 ve 245 gösterilebilir (Özbilen ve Çağlar, 2020).

1.1.6. Bilgi Güvenliği ile İlişkili Teoriler

Bilgi güvenliği alanında bireylerin davranışlarını açıklamak ve güvenlik odaklı tutumların nasıl şekillendiğini anlamak, etkili stratejiler geliştirmek açısından büyük önem taşımaktadır. Bu kapsamda, bireylerin bilişsel, sosyal, motivasyonel ve davranışsal süreçlerini esas alan çeşitli teorik yaklaşımlar geliştirilmiştir. Söz konusu teoriler, bireylerin bilgi güvenliğiyle ilgili tehdit algıları, bu tehditlere karşı geliştirdikleri başa çıkma stratejileri, teknoloji kullanımına dair tutumları, öz-kontrol düzeyleri ve çevresel faktörlerin davranış üzerindeki etkileri gibi çok boyutlu etkenleri ele almaktadır. Bu bölümde, bilgi güvenliği ile yakından ilişkili olan Koruma Motivasyonu Teorisi, Planlı Davranış Teorisi, Sosyal Bilişsel Kuram, Genel Suç Teorisi, Teknoloji Kabul Modeli ve Durumsal Suç Önleme Teorisi ayrıntılı olarak incelenmiştir.

1.1.6.1. Koruma Motivasyonu Teorisi

Koruma Motivasyonu Teorisi, ilk olarak Rogers (1975) tarafından geliştirilmiş ve daha sonra 1983 yılında revize edilmiştir. Teori, bireylerin koruyucu davranışlara yönelmelerinde ikna edici iletişimin etkisini açıklamak amacıyla ortaya konmuş olup, özellikle korku temelli uyarıların birey üzerindeki etkisini ve bu etkiyi yönlendiren bilişsel süreçleri temel alır (Rogers, 1975; Marikyan ve Papagiannidis, 2023).

Koruma Motivasyonu Teorisi, bireylerin tehdit karşısındaki davranışlarını iki temel bilişsel değerlendirme süreci üzerinden açıklar: tehdit değerlendirmesi ve başa çıkma (coping) değerlendirmesi. Tehdit değerlendirmesi, bireyin tehditten ne derece etkileneceğine (algılanan duyarlılık) ve bu tehdidin ne kadar ciddi olduğuna (algılanan şiddet) yönelik algılarını içerirken; başa çıkma değerlendirmesi, bireyin önerilen davranışı uygulayabilme yeterliliği (öz-yeterlik), bu davranışın etkinliği (tepki etkinliği) ve davranışın maliyetine (tepki maliyeti) dair algılarını kapsar (Floyd vd., 2000).

Koruma Motivasyonu Teorisinin ortaya çıkışı, daha önce sağlık davranışlarını açıklamak için kullanılan teorilerin (örn. Health Belief Model, Theory of Reasoned Action, Subjective Expected Utility Theory) sınırlılıklarını aşma hedefiyle şekillenmiştir. Bu teorilerin bazı temel değişkenleri içermediği veya bu değişkenler arasındaki ilişkileri yeterince açıklayamadığı görülmüştür. Örneğin, bireyin önerilen davranışın işe

yarayacağına (tepki etkinliği) ya da davranışı uygulayabileceğine (öz-yeterlik) dair inancı gibi önemli unsurlar, önceki teorilerde sınırlı şekilde ele alınmıştır (Floyd vd., 2000).

Koruma Motivasyonu Teorisi, bireylerin koruyucu davranış geliştirmesinin, bu iki değerlendirme sürecinin sonucunda ortaya çıktığını varsayar. Buna göre, tehdit değerlendirmesi yüksek (yani tehdit ciddi ve birey tehdit altında hissediyor) ve başa çıkma değerlendirmesi güçlü (yani birey önerilen davranışı uygulayabileceğini ve bunun etkili olacağını düşünüyor) olduğunda, bireyin koruyucu davranış gösterme olasılığı artmaktadır. Bu değerlendirmelerin herhangi birinin zayıf olması durumunda ise motivasyon düşmektedir (Rogers, 1975; Marikyan ve Papagiannidis, 2023).

1.1.6.2. Planlı Davranış Teorisi

Planlı Davranış Teorisi (TPB- Theory of Planned Behavior), Fishbein ve Ajzen'in Davranışsal Niyet Teorisi'ni (TRA) genişleterek, bireyin davranışlarının yalnızca niyetle açıklanamayacağını ve bireyin kontrolü dışındaki bazı faktörlerin de davranış üzerinde etkili olabileceğini savunur (Ajzen, 1991; Darsono, 2005). TPB modeline göre bireylerin davranışlarının temel belirleyicisi, bireyin davranışa yönelik niyetidir (Behavioral Intention- BI) ve bu niyet; bireyin davranışa yönelik tutumu (Attitude- A), sosyal çevresinin etkisi (Subjective Norm- SN) ve algılanan davranışsal kontrol (Perceived Behavioral Control- PBC) gibi üç temel bilişsel faktör tarafından şekillendirilir (Turan, 2011).

Model, bireyin bilgiye rasyonel biçimde ulaşarak davranışlarını planladığını varsayar. Ajzen (1991) ve Ajzen ve Madden (1986), PBC ile niyet arasında istatistiksel bir ilişki tespit etmişlerdir (Turan, 2011). Lin (2007) ise, davranışın yalnızca niyetle değil, aynı zamanda PBC ile de doğrudan ilişkili olduğunu ortaya koymuştur. TPB'nin uygulamalarında A değişkeni, bireyin belirli bir davranış (örneğin internetten alışveriş) hakkındaki olumlu veya olumsuz genel tutumunu ifade ederken, SN bireyin yakın çevresinin görüşlerinin birey üzerindeki etkisini yansıtmaktadır. Buna göre, birey olumlu bir tutum sergilemese dahi, sosyal çevresinin beklentileri doğrultusunda davranışı gerçekleştirebilir (Brown, 1999).

Algılanan Davranışsal Kontrol (PBC), bireyin davranışı gerçekleştirmek için gerekli kaynaklara, bilgiye ve imkânlara sahip olup olmadığına dair algısını ifade eder (Turan,

2011). PBC, öz yeterlik ve kolaylaştırıcı koşullar bileşenleriyle birlikte ele alınır. SE bireyin kendi yeterliliğine olan inancını tanımlarken, kolaylaştırıcı koşullar bireyin gerekli altyapı ve koşullara sahip olup olmadığını belirtir. Ajzen (1991) tarafından geliştirilen PBC kavramı, bireyin davranışa yönelik niyetlerini ve davranışı gerçekleştirme olasılığını açıklamak üzere modellenmiştir. Özellikle teknik bilgi gerektiren davranışlar söz konusu olduğunda, PBC'nin davranışın oluşumundaki belirleyici rolü vurgulanmaktadır (Turan, 2011).

1.1.6.3. Sosyal Bilişsel Kuram

Sosyal Bilişsel Kuram, ilk olarak 1941 yılında Miller ve Dollard tarafından tanımlanmış; daha sonra 1965 yılında Albert Bandura tarafından gözden geçirilmiş ve 1986 yılında "Sosyal Bilişsel Kuram" adıyla literatüre kazandırılmıştır. Bu kuram, insan davranışını bireysel, davranışsal ve çevresel etmenler arasındaki sürekli bir etkileşim süreci olarak açıklamaktadır. Ayrıca davranışların, bilişsel süreçler aracılığıyla düzenlendiğini öne sürmektedir. Davranışların sergilenmesinde, bireyin davranış sonucuna ilişkin beklentileri belirleyici bir rol oynamaktadır. Kurama göre zihinsel süreçler bireyin gerçeklik algısını şekillendirir; birey sahip olduğu bilgileri değerlendirir ve bu değerlendirme süreci, bireyin değerleri ile beklentileri doğrultusunda davranışlarına yön verir (Seyhan, 2013).

Sosyal Bilişsel Kuram beş temel bileşenden oluşmaktadır (Butler, 2001):

- Karşılıklı belirleyicilik,
- Gözlem yoluyla öğrenme,
- Öngörü yetisi,
- Kendini düzenleme becerisi,
- Kendini yansıtma kapasitesi.

Bu bileşenlerden biri olan "kendini yansıtma kapasitesi"nin en önemli biçimi öz-yeterliktir. Öz-yeterlik; bireyin belirli bir alandaki başarısı, azmi, çevresel destek ya da baskılar ve davranışın gerçekleştirileceği sıradaki psikolojik durumu gibi çeşitli faktörlerin etkileşimi sonucu gelişmektedir. Sosyal Bilişsel Kuram, tedaviye uyum, alkol kullanımı, bağışıklama hizmetlerine katılım gibi çeşitli sağlık davranışlarının yanı sıra, çocukların ahlaki gelişimleri ve değer yargılarının anlaşılmasında da etkili bir kuramsal

çerçeve sunmaktadır. Sosyal Bilişsel Kuram, bireylerin bilgi güvenliği davranışlarını da açıklamada etkili bir çerçeve sunar; özellikle öz-yeterlik düzeyi yüksek bireylerin, tehditleri tanıma ve uygun güvenlik önlemlerini uygulama olasılıkları daha yüksektir (Butler, 2001; Seyhan, 2013).

1.1.6.4. Genel Suç Teorisi

1990 yılında Michael Gottfredson ve Travis Hirschi, Hirschi'nin teorisini daha da geliştirerek "Genel Caydırma Teorisi" adını verdikleri yeni bir teori geliştirdiler. Önceki teorinin aksine, "öz kontrol" faktörünü, bir kişiyi suç işlemekten alıkoyan faktörlerle destekliediler ve bu öz kontrolün gücünün, suç işleyip işlememeye karar vermede en önemli faktör olduğunu iddia ettiler (Dolu, 2009). Teorinin merkezindeki öz kontrol mekanizması, ailelerin kontrol ve disiplin çabalarıyla bireyde suç işlemekten caydırmak için gelişen kontrol mekanizması olarak tanımlanmaktadır (Coştan, 2014).

Genel olarak, sosyal kontrol teorilerine göre, bir kişiyi suç işlemekten alıkoyan en önemli faktör, kendisine değer veren sosyal çevresindekilerin beklentilerini boşa çıkarmama isteğidir. Sosyal kontrol teorilerine göre, bir kişiyi suç işlemekten alıkoymanın en etkili yolu, çocukluk döneminde öz kontrolü geliştirmek ve güçlendirmektir. Ayrıca, anlamlı faaliyetleri teşvik etmek, sosyal değerleri aşılamak ve gençler arasında baskıcı eğitim yerine teşvik etmek suçun önlenmesine katkıda bulunur (Dolu, 2009). Bu bakış açısı ayrıca bilgi güvenliğinde bireysel sorumluluğun önemini vurgular. Bilinçli kullanıcı davranışı ve öz kontrole dayalı dijital etik anlayışı geliştirmenin siber suçu önlemek için temel bir savunma hattını temsil ettiğine inanılmaktadır.

1.1.6.5. Teknoloji Kabul Modeli

Teknoloji Kabul Modeli (Technology Acceptance Model-TAM), Davis (1986) tarafından geliştirilmiş ve 1989 yılında yayımlanmış olup, bireylerin yeni bilgi teknolojilerini kabul etme davranışlarını açıklamak amacıyla sosyal psikoloji temelli bir kuramdır. Bu model, özellikle Fishbein ve Ajzen'in (1975) "Nedensel Davranış Teorisi"ne dayanmaktadır (Akt. Ma ve Liu, 2005).

Modelin temelini oluşturan iki ana değişken şunlardır (Davis, 1989, akt. Ma ve Liu, 2005):

- Algılanan Kullanışlılık: Bireyin, belirli bir sistemin iş performansını artıracağına olan inancıdır.
- Algılanan Kullanım Kolaylığı: Bireyin, sistemin kullanımının çaba gerektirmediğine yönelik algısıdır.

Bu iki değişken, kullanıcıların sistem hakkındaki tutumlarını ve dolayısıyla davranışsal niyetlerini ve gerçek kullanım davranışlarını etkilemektedir. Davis'in (1989) çalışmasında hem algılanan kullanışlılık hem de algılanan kullanım kolaylığının sistem kullanımına olan etkisinin anlamlı olduğu, ancak PU'nun daha güçlü bir yordayıcı olduğu bulunmuştur (Ma ve Liu, 2005).

Teknoloji kabul modeli çerçevesinde bir teknolojinin kullanımının artırılması için öncelikle teknolojinin "yararlı" olduğuna dair kullanıcı algısının güçlendirilmesi gerekmektedir. Algılanan kullanım kolaylığı ise bu algının oluşmasında dolaylı bir rol oynamakta, yani kullanım kolaylığı, teknolojinin yararlılığına dair algıyı etkilemektedir (Ma ve Liu, 2005).

TAM'ın amacı bilgisayar kullanıcılarının davranışlarını açıklamaktır. Bu model, geniş bir yelpazede bilgi teknolojisi ürünleri kullanan son kullanıcıların davranışlarını açıklamaya çalışan bir yöntemdir. Aynı zamanda TAM, aşırı muhafazakâr kullanıcıların davranışlarını kendi gerekçeleriyle açıklamayı amaçlayan bir modeldir. Araştırmacıların ve uygulayıcıların ideal bir modelde kabul edilebilir adımlar atması için, bu modelin yalnızca öngörücü değil aynı zamanda açıklayıcı olması gerekir. Bu nedenle, TAM'ın odak noktası, niyetleri, tutumları ve içsel inançları etkileyen dış faktörlerin etkilerini açıklamaktır (Davis ve diğerleri, 1989).

1.1.6.6. Durumsal Suç Önleme Teorisi

Bu yaklaşımın temel amacı, suç fırsatlarını azaltmak için suçun yoğun olarak işlendiği fiziksel ve sosyal çevreyi yeniden tasarlamak ve organize etmektir. Bu, suç işleme fırsatlarını azaltır ve potansiyel suçlular suç işlemek için daha büyük riskler alırlar, bu da caydırıcı görevi görür. Bu teorinin önde gelen savunucularından Ronald Clarke, 1983 yılında temel işlevlerini tanımladı ve bunu literatürde suç önlemeye yönelik yeni bir yaklaşım olarak yerleştirdi. Clarke, fiziksel ve sosyal çevreyi organize etme kavramını literatüre sokarak, suçun önlenmesinin potansiyel suçlulara odaklanarak değil, fiziksel ve

sosyal çevredeki suç fırsatlarını sürekli olarak azaltarak mümkün olduğunu savundu. Aslında Clarke, suçluların rehabilitasyonu ve topluma yeniden kazandırılmasından daha basit ve daha etkili bir yöntem önerdi. Clarke, suç işleme fırsatlarının bolluğunun suç oranlarının artmasına yol açtığını ve fırsatların suçluları motive ederek suç işlemelerini kolaylaştırdığını savundu (Clarke, 1997).

Durumsal suç önleme yaklaşımı, klasik ve neoklasik kriminolojinin ilkelerine dayanır ancak bu kriminolojik ilkelerin ötesine geçerek yeni bir yaklaşım sunar. Suç literatürü çok sayıda teori içermesine rağmen, tüm bu teorilerin başlangıç noktası olarak kabul edilen klasik okulun ilkelerinin net bir şekilde anlaşılması, durumsal suç önleme yaklaşımını anlamak için çok önemlidir (Erbuğa, 2020).

Durumsal suç önleme yaklaşımı, politikalar, idari kararlar, çevresel düzenlemeler vb. yoluyla suçun oluşma fırsatlarının azaltılması yoluyla suçun önlenebileceğini ileri sürer. Suç fırsatlarını azaltma hedefi, durumsal suç önleme yaklaşımının temelini oluşturur. Bu hedefe ulaşmak için suçluları yakalama olasılığı artırılmalı ve suçun faydaları azaltılmalıdır (Dolu, 2009).

Benson ve Madensen (2007), durumsal suç önleme teorilerini, potansiyel suçluların kullanımına açık fırsat yapılarının çeşitli boyutlarını değiştirerek suçun azaltılabileceği, hatta tamamen önlenebileceği varsayımına dayandırırlar. Durumsal suç önleme, rasyonel seçim teorisi ve rutin etkinlik teorisi ile yakından ilişkilidir. Suç işlemenin temeli risk değerlendirmesi, fayda ve zararların analizi, etkili kontrol mekanizmalarının varlığı ve mağdurun savunmasız olup olmadığı sorusudur. Önleme tedbirleri suç fırsatlarını azaltmaya, kontrol ve korumayı iyileştirmeye ve mağdur sayısını düşürmeye dayanır.

Suç önleme iki şekilde sağlanabilir: (ı) suçluların rehabilitasyonu yoluyla, (ıı) suç fırsatlarını azaltarak. Ancak suç önleme araştırmalarında, suç azaltma fırsatlarını azaltmayı amaçlayan tedbirlerin suçluların rehabilitasyonundan daha etkili ve hızlı bir şekilde suç azaltmaya katkıda bulunduğuna dair genel bir inanç vardır. Bu tedbirler arasında gözetim ve kontrol, mağdura karşı artırılmış koruyucu tedbirler (yani, mağdura karşı suçları daha zor hale getirme) ve son olarak çevresel ve durumsal tedbirler yer alır (Clarke, 1997).

1.2. Bilgi Güvenliği Farkındalığı Kavramı

Bilgi güvenliği farkındalığı, bilgi güvenliğini riske atan faktörlerden ve söz konusu faktörlere karşı alınabilecek tedbirlerden haberdar olma durumunu kapsar. Dolayısıyla, kurumsal düzeyde bilgi güvenliği farkındalığının artırılması, kurumsal faaliyetlerin amaca uygun ve sorunsuz bir şekilde yürütülmesi için hayati öneme sahiptir (Öztemiz ve Yılmaz, 2013:87-100).

Khando ve diğerleri (2021:1) tarafından ifade edildiği üzere, bilgi güvenliği farkındalığı; bireylerin güvenli bilgi uygulamalarına yönelik algılarını, değerlerini, tutumlarını, davranışlarını, normlarını, çalışma alışkanlıklarını ve örgütsel kültür ve yapılarını değiştirmeyi amaçlayan bir süreçtir. Küresel ölçekte işletmelerin, bilgi güvenliği konusunda teknolojik önlemlere önemli yatırımlar yapmalarına rağmen, birçoğunun hala yetersiz teknik çözümlere güvendiği ve bu nedenle bilgi varlıklarını korumada başarısız olduğu belirtilmektedir. Bu bağlamda, bilgi güvenliği farkındalığının artırılması, kuruluşların ve bireylerin bilgi güvenliği konusunda daha bilinçli ve hazırlıklı olmalarını sağlayarak, potansiyel risklere karşı daha etkili bir şekilde savunmalarını mümkün kılar.

Günümüzde dijitalleşme ile birlikte işletmelerin kendi bilgi varlıklarını koruma ihtiyacı önemli bir boyut kazanmıştır. Bu sebeple, işletmelerin bilgi güvenliği farkındalığını sürdürülebilir kılabilmesi için önemli unsurları içeren temel stratejilere ihtiyaç duyulmaktadır. Maurer ve ekibi (2011) yaptıkları çalışmada, başarılı bir bilgi güvenliği stratejisinin bilgi kaynaklarının korunduğu bir ortam oluşturmaktan geçtiğini vurgulamışlardır. Dolayısıyla, başarılı bilgi güvenliği programlarının genellikle önemli bazı temel unsurlardan oluştuğu bilinmektedir (Page, 2017: 1-8):

- Teknik Kontroller: Bu unsurlar, sistemlere ve ilgili kurumsal verilere yetkisiz erişime ve kötüye kullanıma karşı otomatik koruma sağlayan donanım veya yazılım çözümlerini içerir.
- Yönetim Süreci Kontrolleri: Kullanıcı davranışını yönlendirmek ve uygun olduğunda değiştirmek için tasarlanmış politikalar ve yaptırımları kapsar. Bu kontroller, kullanıcı davranışını değiştirmek için tasarlanmış politikalar ve yaptırımları içerir.

- Eğitim Programları: Bilgi güvenliğini destekleyen bir kültür oluşturmanın temel unsurlarından biridir. Kullanıcıları bilgi güvenliği riskleri ve sorumlulukları konusunda eğitmek, bilgi güvenliği kültürünün oluşturulması için esastır.
- Yönetişim Programları: Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından tanımlanan bu programlar, bilgi güvenliği stratejilerinin iş hedefleriyle uyumlu olduğuna, bunları desteklediğine ve politikalara bağlı kalarak geçerli yasa ve yönetmeliklerle tutarlı olduğuna dair güvence sağlamak için bir çerçeve oluşturma ve sürdürme sürecini içerir.

Bilgi güvenliğine yönelik farkındalığı artırmak için, daha bütüncül bir yaklaşım benimsenmesi gerekmektedir, ki bu insanların, süreçlerin ve teknolojinin önemli rollerini kabul eder. Örneğin, genel bir güvenlik mimarisi oluşturmak için gerekli olan teknolojiyi dağıtmak için gerekli kaynaklar sağlanmalıdır. Yönetim, gerekli kaynakların sağlanmasının yanı sıra, firma içinde çalışanların güvenlik politikalarına ve prosedürlerine bağlılığını artırmaya yardımcı olacak bir güvenlik kültürü oluşturmalıdır. Her çalışanın bilgi güvenliği tehditlerini önleme ve azaltmadaki rolünün farkında olması önemlidir. Çalışanlar, güvenlik tehditlerini azaltmak ve bunlara yanıt vermek için mevcut politikalar ve prosedürlerle güncel kalmaya kararlı olmalıdırlar, özellikle de ön saflarda bulunmaları dikkate alındığında. Bu nedenle, herhangi bir güvenlik açığını kapatmak için bu politikaların ve prosedürlerin periyodik olarak gözden geçirilmesi gerekmektedir (Saban vd., 2021:263-264). Bu şekilde, bilgi güvenliğine yönelik kapsamlı bir yaklaşım benimsemek, işletmelerin güvenlik açıklarını kapatma ve risklere karşı daha etkin bir şekilde önlem alma kapasitelerini artırabilir.

1.2.1. Bilgi Güvenliği Farkındalığının Önemi

Bilgi güvenliği farkındalığının amacı, kurum içindeki çalışanların ve paydaşların paylaştıkları bilgileri koruma sorumluluklarının farkında olmalarını sağlamaktır. Her kurum bu farkındalığa sahip çalışanlarla çalışmalıdır. Aynı zamanda bilgi güvenliği ile ilgili rol ve sorumlulukların atanması ve sürece dahil edilmesi farkındalığa katkıda bulunur. Bilgi güvenliği farkındalığı, kurumların bilgi güvenliği risklerini uygun seviyeye düşürmek için büyük önem taşımaktadır. Temel amaç, bilgi güvenliği sürecindeki en

zayıf halka olan insan faktörünün kötüye kullanılmasından kaynaklanan hataları ve riskleri azaltmak ve çalışanları bilgili ve bilinçli hale getirmektir (Özbey, 2024).

Bilgi güvenliği farkındalığı, günümüzün dijital çağında hayati öneme sahiptir ve geniş kapsamlı ve derin etkileri vardır. Bu farkındalık, bireylerin ve kurumların dijital tehditlerin farkına varmalarını ve bunlara karşı koruyucu stratejiler geliştirmelerini sağlar. Kullanıcılar siber suçlara, veri ihlallerine ve diğer dijital tehditlere karşı daha iyi hazırlanır ve daha etkili bir şekilde savunma yapar (Takemura vd., 2011).

Aynı şekilde kurumsal düzeyde bilgi güvenliği farkındalığı, şirketlerin dijital varlıklarını koruma çabalarını güçlendirir. Çalışan eğitimi ve farkındalık eğitimleri, şirketlerin siber saldırılara karşı daha sağlam savunmalar geliştirmesine yardımcı olur. Japonya kurumlarında yapılan bir çalışmada, kişisel özelliklerin çalışanların bilgi güvenliği farkındalığını etkilediği bulunmuştur. Ayrıca, bilgi güvenliği farkındalık eğitiminin önemi vurgulanmıştır (Takemura vd., 2011).

Bilgi güvenliği farkındalık eğitimine ek olarak, aşağıdaki yöntemler kullanılabilir (Şahinaslan vd., 2009):

- Kullanıcıların bilgi güvenliği farkındalığını artırmak için animasyonlar ve çizgi filmler oluşturulabilir.
- Çalışanların sürece katkıları değerlendirilebilir ve ödüllendirilebilir.
- Bilgi güvenliği oyunları düzenlenebilir.
- Bireyler için sanal eğitim oturumları düzenlenebilir.
- E-bültenler oluşturulabilir ve düzenli aralıklarla kullanıcılara gönderilebilir.
- Kullanıcıların sürekli bulunduğu ortamlarda broşürler ve posterler sergilenebilir.

1.2.1. Bilgi Güvenliğini Tehdit Eden Unsurlar

Bilgisayar sistemlerindeki yeni teknolojilerin ortaya çıkması, kişilere ve kurumlara birçok kolaylık sağlarken aynı zamanda bilgi güvenliği konusunda da ciddi tehditler oluşturmuştur. Tehdit, bir sistemin veya kurumun zarar görmesine sebep olan, istenmeyen bir olayın arka planında gizli neden olarak tanımlanabilir (Vural, 2007). Bilginin elektronik ortamda anlık olarak paylaşılması, e-uygulamalarının günlük ve iş hayatında yaygınlaşması, bilgiye erişimde mekân kavramının genişlemesi ve elektronik

ortamda işlenen organize suçların artması, bilgi güvenliğindeki tehditlerin sayısının artmasına neden olmuştur (Gülmüş, 2010). Teknolojik ilerlemelerin sağladığı avantajlardan tam olarak yararlanırken, aynı zamanda güvenlik açıklarını minimize etmek için sürekli olarak yeni tehditlere karşı hazırlıklı olmak önemlidir.

Bilgi güvenliğine yönelik tehditler, bilgi sistemlerindeki açıkları kullanarak etkili olurlar. Bu tehditlerin zarar vermesini engellemek için uygun ortam şartları yok edilmelidir. Bilgi güvenliğine yönelik tehditleri aşağıdaki gibi sıralamak mümkündür:

- Doğal Afetlere Dayalı Tehditler: Deprem, sel, yangın gibi doğal afetler, bilgi güvenliğini tehdit eden unsurlar arasındadır. Bu tür tehditler önceden bilinmesi ve gerekli önlemlerin alınması gereken doğal olaylardır. Ancak bu tür tehditlere karşı önceden planlama yapılması ve gerekli önlemlerin alınması, olası zararların minimize edilmesini sağlayabilir (Vural, 2007).
- Prosedürel Eksikliklere Dayalı Tehditler: Prosedürel eksikliklerden kaynaklanan olaylar, kurum ve kuruluşlar için ciddi kayıplara neden olabilir. Bu tür tehditlerin önlenebilmesi için, bilgi güvenliği konusunda izlenecek süreçler modellenmeli, çalışanların görev ve sorumlulukları belirlenmeli ve uymaları gereken prosedürler, standartlar ve politikalar tanımlanmalıdır (Aslan-Öztezcan, 2017).
- Zararlı Yazılımlara Dayalı Tehditler: Zararlı yazılımlar, saldırganların yazılım ve donanım açıklarını kullanarak istedikleri bilgiye erişmelerini sağlayan tehditlerdir. Bu yazılımlar, kullanıcıların bilgisi olmadan veya dikkatsizliklerinden faydalanarak bilgisayarlarına yerleşerek önemli verileri ele geçirebilirler (Şahinaslan, 2013).
- İnsan Faktörüne Dayalı Tehditler: Bilgi güvenliği konusunda teknolojik önlemler alınsa da insan faktörü göz ardı edilirse, alınan tedbirler etkisiz kalabilir. Bilgi güvenliği bilinci olmayan veya farkındalığı düşük bireyler, güvenlik sürecini tehlikeye atabilirler (Yılmaz vd., 2016). Dolayısıyla, bireylerin doğru davranışları sergilemesi ve bilgi güvenliği konusunda eğitilmesi önemlidir (Gökçearslan vd., 2021). Saldırganlar insanların zafiyetini kullanarak sistemlere erişmekte ve zarar vermektedir (Şekil 2).

Şekil 1: Sıkça Kullanılan Zararlı Yazılım Türleri

Kaynak: Burlu, 2015.

Şekil 2: İnsan Faktörüne Dayalı Tehditler

Kaynak: Gökçearslan vd., 2021.

İnsan faktörüne dayalı tehditler, ayrıntılı olarak şu şekilde açıklanabilir:

- **Oltalama (Phishing):** Sazan avlama olarak da bilinen bu yöntem, insan zafiyetlerinden faydalanır. Kullanıcıları kandırmak veya ikna etmek suretiyle gerçek olmayan e-postalarla kişisel ve kredi kartı gibi önemli verilerin elde

edilmesini sağlayan bir dolandırıcılık yöntemidir. Kullanıcı, sahte web sayfasına yönlendiren bir linki tıkladığında, bu sayfa genellikle kendi bankası veya önceden alışveriş yaptığı bir site gibi görünür ve bilgi girişi yapılırken kullanıcılar yanıltılır (Ateş, 2023).

- **Sosyal Mühendislik (Social Engineering):** Sosyal mühendislik, düşük teknoloji ve insan zafiyetlerine dayalı teknikler kullanarak önemli verilere ve ağ sistemlerine erişmeyi planlayan saldırganlar tarafından kullanılan bir yöntemdir. Bu tekniklerle saldırganlar, bireylerin gizli bilgilerini ele geçirmek için psikolojik manipülasyon yöntemlerini kullanırlar. Saldırganlar, kandırma sanatını ve ikna tekniklerini ustalıkla kullanarak hedeflerine ulaşmaya çalışırlar (Gündüz ve Daş, 2016).

- **Spam:** Spam, kişilerin isteği olmadan gönderilen, genellikle reklam içerikli e-postalardır. İstem dışı olarak gönderilen bu e-postalar, ticari reklam yapmayı amaçlar ve sahtekarlık, dolandırıcılık ve zararlı yazılımların yayılmasında rol oynarlar (Öztürk, 2009).

- **Hoax:** Hoax, insanların ilgisini çeken duygusal içerikli e-postaları alıcılarının kendi tanıdıklarıyla paylaşmalarını isteyen e-postalardır. İnternet aldatmacası ise kişi veya kuruluşlar hakkında sahte haberler yaparak bu kişi veya kuruluşa zarar vermeyi amaçlayan e-postalardır. Kullanıcılar, bu tür e-postaları güvenilir bir kaynaktan geldiğini düşünerek inanmakta ve paylaşmaktadırlar. Bu süreçte, e-postaya dâhil olan kullanıcıların e-posta adres bilgileri toplanabilir (Mart, 2012).

Bu şekilde, insan faktörüne dayalı tehditler, bilgi güvenliği açısından önemli bir risk oluşturur ve bu tür tehditlerle başa çıkmak için dikkatli olunmalıdır.

1.2.2. Kurumsal Bilgi Güvenliği Farkındalığı ve İnsan Faktörü

Bilgi güvenliği ve kurumsal bilgi güvenliği farkındalığında insan faktörünün belirleyici bir rol oynaması göz ardı edilemez. Bilgi güvenliği farkındalığının sağlanmasında, insanların güvenlik politikalarına uyum göstermesi ve bu politikaların uygulanması temel bir öneme sahiptir. Doğru planlama, etkili güvenlik önlemleri ve çalışanların yüksek farkındalık düzeyi, bilgi güvenliğinin sağlanmasında kritik bir rol oynamaktadır. İnsanlar,

gerçek yaşam ile siber uzay arasında bir köprü vazifesi gördükleri için kurumsal bilgi güvenliği farkındalığının oluşturulması da büyük ölçüde insan faktörüne bağlıdır (Nezgitli, 2021).

İnsan faktörü, güvenlik sistemlerindeki en zayıf halka olarak kabul edildiğinden, saldırganlar genellikle güvenlik açıklarını bu noktadan tespit etmeye çalışmaktadır. Özellikle, saldırı yöntemleri ve teknikleri, bireylerin bilgi güvenliği konusunda sahip oldukları farkındalık düzeyine bağlı olarak şekillenmektedir. Bilgi güvenliği ihlallerinin büyük bir kısmı, çalışanların siber tehditler konusundaki bilinç eksikliğinden kaynaklanmaktadır. Bu nedenle, kurumların bilgi güvenliği stratejilerini oluştururken insan faktörüne öncelik vermesi ve çalışanların farkındalık düzeyini artırmaya yönelik sistematik çalışmalar yürütmesi büyük önem taşımaktadır. Bu farkındalık seviyesinin artırılması, çeşitli eğitim programları, seminerler ve bilinçlendirme çalışmalarıyla sağlanmalı, aynı zamanda çalışanlara, sistemlerdeki yetkili erişimlerinin ne derece kritik olduğu anlatılmalıdır (Kraus, 2018). Bu bağlamda, bilgi güvenliğini sağlamaya yönelik gerçekleştirilecek yatırımların yalnızca teknolojik altyapıyı güçlendirmeye yönelik değil, aynı zamanda insan kaynağının bilinç düzeyini yükseltmeye odaklanması gerekmektedir. Kurumsal bilgi güvenliğinin sürdürülebilir bir şekilde korunabilmesi için çalışanların tehditleri tanıma ve bu tehditlere karşı önlem alma yetkinliklerinin artırılması kritik bir gereklilik olarak öne çıkmaktadır (Doğan, 2021).

Kurumsal bilgi güvenliği farkındalığı, çalışanların dikkatsiz ve bilinçsiz davranışlarının kuruma maddi ve manevi olarak geri dönüşü olmayan zararlar verebileceği gerçeği göz önünde bulundurularak büyük önem taşımaktadır. Bu sebeple, insan faktörüne odaklanarak farkındalık düzeyini artırmak için belirli yöntemlerin uygulanması gerekmektedir. Bu yöntemlerin temel amaçları şu şekildedir (Şahinaslan ve diğerleri, 2009; Al Mindeel ve Martins, 2020):

- Tüm çalışanlara yönelik bilgi güvenliği eğitim ve farkındalık programları, kurumun ihtiyaçları doğrultusunda düzenlenmelidir.
- Eğitim ve program içerikleri, çalışanların ihtiyaçları ve teknolojideki değişimler göz önünde bulundurularak düzenli olarak güncellenmelidir.

- Eğitim ve programlar, yüz yüze veya çevrim içi olarak gerçekleştirilebileceği gibi, el kitapçıkları, etkinlikler ve bilinçlendirme çalışmaları gibi farklı formatlarda da sunulabilir.
- Çalışanların günlük iş temposundaki yoğunlukları nedeniyle dikkat dağınıklığı yaşayabilecekleri göz önünde bulundurularak, ekran koruyucular aracılığıyla düzenli aralıklarla bilgi güvenliği farkındalığı mesajları iletilmelidir.
- Kurum içi iletişim portalı üzerinden düzenli olarak bilgi notları ve önemli bilgi güvenliği uyarıları yayınlanarak çalışanların bilinçlenmesi sağlanabilir.
- Verilen eğitimlerin etkinliğini ölçmek ve çalışanların farkındalık düzeyini değerlendirmek için geri bildirim alabilecekleri bir değerlendirme mekanizması oluşturulmalıdır.

Tüm bu adımlar, kurum çalışanlarının bilgi güvenliği konusunda daha bilinçli olmalarını sağlayarak, yüksek düzeyde bilgi güvenliği farkındalığına sahip bireylerin yetişmesine katkıda bulunacaktır.

1.2.3. Bilgi Güvenliği Farkındalığı Oluşturma Önerileri

Günümüzde, kurumların en değerli varlığının insan kaynağı olduğu kabul edilmektedir. Dolayısıyla, kurum politikası olarak insan kaynaklarına yapılan yatırımlar, aslında kuruma yapılan bir yatırımı temsil etmektedir. Bilgi güvenliği farkındalığının kurum çalışanları arasında sağlanması için öncelikle yöneticilerin bu konudaki farkındalık çalışmalarını benimsemesi ve önemini kavraması gerekmektedir. Ardından, bilgi güvenliği eğitimleri konusunda personelin ihtiyaçlarına ve beklentilerine uygun olarak değişen farkındalık programları hazırlanmalıdır. (Özdemir, 2019: 48):

Bu çerçevede, bilgi güvenliği farkındalık eğitimleri, üst yöneticilerden çalışanlara kadar tüm görev ve pozisyonlara özel olarak tasarlanmalıdır. Özellikle yeni başlayan personeller için farkındalık eğitimleri, oryantasyon programlarının önemli bir parçası haline getirilmelidir. Ayrıca, kurum personeline düzenli aralıklarla güncellenen ve gelişmelere adapte edilen eğitim programları sunularak bilgi güvenliği konusundaki farkındalık sürekli olarak taze tutulmalıdır. Eğer kurum içerisindeki bilgi güvenliği personeli bu konuda yeterli donanıma sahip değilse, dışarıdan danışmanlık hizmeti

alınması da bir seçenek olabilir. Bu sayede kurum, bilgi güvenliği alanında uzman kişilerden destek alarak daha etkili ve güncel bir farkındalık programı oluşturabilir.

Farkındalık eğitimlerinde, geleneksel sınıf içi uygulamalar yerine daha esnek ve etkili alternatif yöntemler kullanılarak çalışanların bilgi güvenliği konusundaki bilinç düzeyleri artırılabilir. Bu tür eğitimlerin, bireylerin günlük iş akışlarına entegre edilebilmesi ve tekrarlayan öğrenme süreçleriyle desteklenmesi, bilgi güvenliği farkındalığının kalıcılığını güçlendirmektedir. Bu bağlamda, aşağıda belirtilen yöntemler, çalışanların bilgi güvenliği konusunda daha bilinçli hareket etmelerini sağlamak amacıyla kullanılabilir (Özdemir, 2019: 48):

- Düzenli Güvenlik Analizleri ve Değerlendirmeler: Kurum içerisindeki farklı birimlerin bilgi güvenliği konusundaki eksiklikleri belirlenerek, alınması gereken önlemler çalışanlarla paylaşılabilir. Böylece, hem mevcut güvenlik açıkları kapatılmış olur hem de personelin farkındalığı artırılır.

- Dijital ve İnteraktif Eğitimler: Geleneksel eğitim modellerinin ötesine geçerek, sanal eğitimler, simülasyonlar ve kısa animasyon videolar ile çalışanlara bilgi güvenliği konusunda pratik bilgiler sunulabilir. Bu yöntem, öğrenmeyi daha ilgi çekici ve akılda kalıcı hale getirebilir.

- Görsel Destekleyici Materyallerin Kullanımı: Çalışanlara yönelik bilgi güvenliği el kitapçıkları, broşürler ve posterler hazırlanarak, kritik güvenlik konuları vurgulanabilir. Özellikle, günlük iş ortamında sık görülen alanlarda bu materyallerin bulundurulması, bilinç seviyesini artırmada etkili olabilir.

- Dijital Ekranlarda Animasyon ve Bilgilendirme Mesajları: Kurum içindeki LED ekranlarda bilgi güvenliği konulu kısa animasyonlar gösterilerek, çalışanların dikkatleri bu önemli konuya yönlendirilebilir. Aynı zamanda, koridorlardaki dijital panolarda kısa bilgilendirme metinleri paylaşılabilir.

- E-Posta Bültenleri ve Güncellemeler: Çalışanların kurumsal e-posta adreslerine belirli aralıklarla bilgi güvenliğiyle ilgili güncellemeler ve hatırlatmalar içeren bültenler gönderilebilir. Bu sayede, çalışanlar en güncel tehditler ve korunma yöntemleri hakkında düzenli olarak bilgilendirilmiş olur.

- Ekran Koruyucu ve Açılış Mesajları: Çalışanların bilgisayar ekranlarında, bilgi güvenliği farkındalığını artırmaya yönelik uyarı mesajları içeren ekran koruyucular kullanılabilir. Ayrıca, bilgisayar açılış ekranlarında güvenlikle ilgili kısa hatırlatıcı mesajlar veya sloganlar yer alabilir.

Bu yöntemler, farklı öğrenme stillerine ve tercihlere uygun olarak bilgi güvenliği farkındalığını artırmak için kullanılabilir.

1.3. Kamuda Bilgi Güvenliği

1.3.1. Kamu Kurumlarında Uyulması Gereken Bilgi Güvenliği Kriterleri

"Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" ile "Kamu Bilgi Güvenliği Programı" çerçevesinde, bilgi ve iletişim sistemlerindeki güvenlik açıklarının önlenmesi ve kötüye kullanımın engellenmesi amacıyla Ulaştırma ve Altyapı Bakanlığı (UDHB) tarafından "Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri" adlı bir doküman hazırlanmıştır. Bu kriterler, Türkiye'deki tüm kamu kurumlarını kapsamakta olup, bilgi güvenliğinin kurumsal düzeyde sağlanmasına yönelik çeşitli düzenlemeler içermektedir. Kamu kurumlarının bilgi güvenliği politikalarını belirlerken bu kriterleri dikkate almaları zorunlu tutulmuş ve güvenlik açıklarının minimize edilmesi için sistematik bir yaklaşım benimsenmiştir. Kriterler kapsamında, bilgi güvenliğine dair temel önlemler, siber saldırılara karşı korunma mekanizmaları ve yetkilendirme süreçleri detaylı bir şekilde ele alınmıştır (UDHB, 2019; Özbilen ve Çağlar, 2020: 81). Bu kriterler, kamu kurumlarının bilgi güvenliği alanında etkin bir şekilde faaliyet göstermesini ve ulusal siber güvenliğin sağlanmasını amaçlamaktadır.

Şekil 3: Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri

Kaynak: UDHB, 2019; Özbilen ve Çağlar, 2020: 81.

1.3.2. Kamuda Teknik Açıdan Bilgi Güvenliği

Bilgi güvenliği, günümüzde hem bireyler hem de kurumlar için hayati önem taşıyan bir konudur. Teknolojinin hızla ilerlemesiyle birlikte bilgi ve verilerin güvenliği, her geçen gün daha da kritik hale gelmektedir. Kamuda bilgi güvenliği, devlet kurumları ve kamu hizmetlerinin yürütülmesi açısından son derece önemlidir (Özbilen ve Çağlar, 2020: 73).

Teknik açıdan, kamuda bilgi güvenliği, çeşitli teknolojik önlemler alınarak sağlanmaktadır. Bu önlemler, bilgi sistemlerinin güvenliğini sağlamak, veri bütünlüğünü korumak ve yetkisiz erişimleri engellemek için kullanılmaktadır. Kamuda bilgi

güvenliğinin sağlanmasında kullanılan teknik önlemler şunları içermektedir (Güler ve Arkın, 2019: 18; İleri, 2017: 56-57; Altıntaş ve Barkuş, 2023: 64):

- Güvenlik Duvarları (Firewalls): Kamu kurumlarında kullanılan bilgi sistemlerini dışarıdan gelebilecek saldırılara karşı korumak için güvenlik duvarları kullanılır. Bu duvarlar, yetkisiz erişimleri engellemek ve zararlı yazılımların sisteme girişini önlemek için trafiği filtreler.
- Şifreleme Teknolojileri: Hassas bilgilerin güvenliğini sağlamak için şifreleme teknolojileri kullanılır. Kamu kurumlarında iletilen verilerin şifrelenmesi, veri güvenliğini artırır ve yetkisiz erişimlere karşı koruma sağlar.
- Güvenlik Yazılımları: Kamu kurumlarında kullanılan bilgi sistemlerini korumak için antivirüs yazılımları, kötü amaçlı yazılımları algılamak ve engellemek için kullanılır. Ayrıca, kötü niyetli faaliyetleri izlemek ve tespit etmek için güvenlik bilgi ve olay yönetimi (SIEM) yazılımları da kullanılabilir.
- Güncelleme ve Yama Yönetimi: Bilgisayar sistemlerindeki güvenlik açıklarını gidermek için düzenli olarak güncelleme ve yamaların yapılması önemlidir. Kamu kurumları, sistemlerini güncel tutarak potansiyel saldırılara karşı daha dirençli hale getirebilirler.
- Erişim Kontrolü: Kamu kurumlarında, kullanıcıların yetkilerinin belirlenmesi ve sınırlı erişimlerin sağlanması önemlidir. Erişim kontrolleri, hassas bilgilere sadece yetkili kişilerin ulaşmasını sağlayarak veri güvenliğini artırır.

1.3.3. Kamuda Personel Açısından Bilgi Güvenliği

Personel açısından ise, kamuda bilgi güvenliğinin sağlanmasında insan faktörü büyük önem taşımaktadır. Personelin eğitilmesi, farkındalık oluşturulması ve doğru bilgi güvenliği politikalarının benimsenmesi gerekmektedir. Kamuda bilgi güvenliğinin personel açısından ele alınması şu şekilde olabilir (Özbilen ve Çağlar, 2020: 80-85; Özdemir ve Uluyol, 2021: 652; Ağdeniz, 2021: 526-527):

- Eğitim ve Farkındalık: Kamu çalışanlarına düzenli olarak bilgi güvenliği eğitimleri verilmelidir. Bu eğitimler, güvenli şifre kullanımı, zararlı e-postalara karşı dikkatli olma ve sosyal mühendislik saldırılarını tanıma gibi konuları

kapsamalıdır. Ayrıca, çalışanların bilgi güvenliği konusunda farkındalığının artırılması için periyodik olarak farkındalık kampanyaları düzenlenebilir.

- Güvenlik Politikalarının Uygulanması: Kamu kurumları, bilgi güvenliğini sağlamak için kapsamlı güvenlik politikaları geliştirmeli ve uygulamalıdır. Bu politikalar, şifreleme gereklilikleri, veri saklama ve imha prosedürleri ve güvenli internet kullanımı gibi konuları içermelidir. Çalışanlar, bu politikalara uygun şekilde hareket etmelidir.
- Bilgi Güvenliği Sorumluları: Kamu kurumlarında bilgi güvenliği sorumluları atanmalı ve bu kişiler, kurumun bilgi güvenliği politikalarının uygulanmasından sorumlu olmalıdır. Bilgi güvenliği sorumluları, güvenlikle ilgili konuları takip eder, güvenlik açıklarını belirler ve uygun önlemleri alır.
- İç Denetim ve İzleme: Kamu kurumları, iç denetim süreçleri ve izleme mekanizmaları kullanarak bilgi güvenliği önlemlerinin etkinliğini değerlendirmelidir. Bu süreçler, potansiyel güvenlik risklerini belirlemek ve uygun düzeltici önlemleri almak için önemlidir.
- Olay Müdahale Planları: Kamu kurumları, bilgisayar sistemlerinde meydana gelebilecek güvenlik ihlallerine karşı hazırlıklı olmalıdır. Olay müdahale planları oluşturulmalı ve bu planlar düzenli olarak test edilmelidir. Böylece, olası bir güvenlik olayında etkili bir şekilde müdahale edilebilir.

Kamuda bilgi güvenliği, teknik önlemlerin yanı sıra personelin eğitimi ve bilinçlendirilmesiyle sağlanabilir. Ancak, bu süreç sürekli bir çaba gerektirir ve teknolojik ve insan faktörlerinin her ikisinin de sürekli olarak güncel olayları takip etmesi ve kendini geliştirmesi gerekmektedir.

1.4. İlgili Araştırmalar

1.4.1. Konuyla İlgili Ulusal Araştırmalar

Mart (2012) tarafından gerçekleştirilen çalışmada, 2010-2012 yılları arasında farklı illerde ve çeşitli meslek gruplarında görev yapan toplam 501 katılımcıya yönelik bir anket uygulanmıştır. Araştırma kapsamında elde edilen veriler, t testi ve tek yönlü ANOVA testi ile analiz edilmiştir. Çalışmanın bulguları, katılımcıların yaş grupları ile bilgisayar kullanım süreleri arasında istatistiksel olarak anlamlı farklılıklar bulunduğunu ortaya

koymuştur. Bu sonuçlar, bireylerin yaşlarına bağlı olarak bilgi teknolojileriyle etkileşim düzeylerinin değiştiğini ve bilgisayar kullanım alışkanlıklarının yaş faktörüyle ilişkili olabileceğini göstermektedir. Çalışmanın önerisi, bilgi güvenliği farkındalığının küçük yaşlardan itibaren eğitilmesi gerektiğini vurgulamaktadır.

Tekerek ve Tekerek (2013) tarafından gerçekleştirilen çalışmada, Kahramanmaraş ilinde öğrenim gören ilk ve orta öğretim öğrencilerinin bilgi güvenliği farkındalık düzeylerini ölçmek amacıyla özel bir ölçek geliştirilmiştir. Araştırmanın bulguları, öğrencilerin etik konulara ilişkin farkındalıklarının yeterli seviyede olduğunu, ancak teknik konularda bilgi güvenliği farkındalıklarının yetersiz kaldığını ortaya koymuştur. Bu durumun temel nedenlerinden biri olarak, öğrencilere yönelik bilgi ve bilgisayar güvenliği farkındalık eğitimlerinin ve etkinliklerinin sınırlı olması gösterilmiştir. Çalışmada, bilgi güvenliği bilincinin artırılabilmesi için eğitim programlarının güçlendirilmesi ve daha kapsamlı farkındalık etkinliklerinin düzenlenmesi gerektiği vurgulanmıştır.

Öztemiz ve Yılmaz (2013) tarafından gerçekleştirilen bir çalışmada, Ankara ilinde bulunan on dört kütüphanedeki kütüphane ve dokümantasyon daire başkanları veya yardımcıları ile bilgi güvenliği farkındalığı hakkında nitel bir araştırma yapılmıştır. Araştırma sonuçları, kütüphanelerin çoğunluğunun bilgi güvenliğinin önemini vurguladığını, ancak bilgi güvenliği uygulamalarının içeriğinin yeterince bilinmediğini ve uygulamaların genellikle bilgi işlem daire başkanları tarafından yürütüldüğünü ortaya koymuştur. Bu nedenle, çalışmanın önerisi, kütüphanelerde çalışanlara farkındalık eğitimleri verilirken aynı zamanda görev ve sorumluluk bilincinin de aşılanması gerektiğidir.

Keser ve Güldüren (2015) tarafından yürütülen çalışmada, yükseköğretim kurumlarında görev yapan öğretim elemanlarının bilgi güvenliği farkındalık düzeylerini ölçmek amacıyla bir ölçek geliştirilmiştir. Araştırma sürecinde, katılımcılara uygulanan bilgi güvenliği farkındalık eğitimlerinin etkili olduğu gözlemlenmiş ve bu bulgu, çalışmanın en önemli sonuçlarından biri olarak öne çıkmıştır. Bu durum, yükseköğretim kurumlarında görev yapan akademik personelin bilgi güvenliği konusundaki bilinç düzeyinin artırılmasında eğitimlerin kritik bir rol oynadığını göstermektedir.

Çavuş ve Erçağ (2016) tarafından gerçekleştirilen bir diğer araştırmada, öğretmenlerin güvenli internet kullanımı konusundaki yeterlilikleri değerlendirilmiştir. Araştırma bulgularına göre, öğretmenlerin dijital veri güvenliği farkındalık düzeylerinin genel olarak yüksek olduğu belirlenmiştir. Bununla birlikte, farkındalık seviyelerinin cinsiyet, günlük bilgisayar kullanım süresi ve günlük internet kullanım süresi gibi değişkenlere bağlı olarak farklılık gösterdiği, ancak öğretmenlerin branşı, eğitim düzeyi, öğretim kademesi ve mesleki kıdemi gibi faktörlerden etkilenmediği tespit edilmiştir. Bu sonuçlar, dijital güvenlik farkındalığının bireysel kullanım alışkanlıklarıyla daha yakından ilişkili olduğunu ortaya koymaktadır.

Gökmen ve Akgün (2016) tarafından yürütülen başka bir çalışmada ise öğretmen adaylarının bilişim suçlarıyla ilgili deneyimlerini ve bilişim güvenliği dersi müfredatı hakkındaki görüşlerini incelemek amaçlanmıştır. Araştırma sonuçları, öğretmen adaylarının büyük bir kısmının bilişim güvenliği ile ilgili herhangi bir ders almadığını ve kendilerini bu konuda yeterli görmediklerini göstermektedir. Bu bulgu, bilişim güvenliği eğitiminin öğretmen yetiştirme programlarına daha fazla entegre edilmesi gerektiğini ortaya koymakta ve eğitim sisteminde bu alana yönelik daha kapsamlı düzenlemeler yapılmasının önemini vurgulamaktadır.

Kuru ve Ocak (2016) tarafından gerçekleştirilen çalışmada, kamu çalışanlarının siber güvenlik ve siber savaşlar konusunda yeterli bilgiye sahip oldukları belirtilmiştir. Çalışmanın sonuçlarına göre, kamu çalışanlarına çalışma hayatları boyunca düzenli eğitimler verilmesi ve üniversitelerde bu konuya yönelik derslerin müfredata eklenmesi gerektiği önerilmiştir. Ayrıca, siber savunma politikalarının diğer devlet kurumlarıyla iş birliği yaparak planlanması gerektiği vurgulanmıştır.

Yılmaz ve diğerleri (2016) tarafından yapılan araştırmada ise öğretmenlerin dijital veri güvenliği farkındalığı incelenmiş ve yüksek bir farkındalık düzeyine sahip oldukları tespit edilmiştir. Araştırmanın bulgularına göre, erkek öğretmenlerin kadınlara göre daha yüksek bir farkındalık düzeyine sahip olduğu görülmüştür. Ayrıca, ilkokul, ortaokul ve lise öğretmenleri arasında farkındalık düzeyleri açısından belirgin bir farklılık tespit edilmemiştir. Buna ek olarak, bilişim cihazlarına sahip olan ve günlük olarak daha fazla bilgisayar ve internet kullanan öğretmenlerin dijital veri güvenliği farkındalıklarının daha yüksek olduğu ortaya konmuştur.

Öztezcan (2017) tarafından Marmara Üniversitesi'nde gerçekleştirilen bir araştırmada, 414 idari ve akademik personele yönelik yapılan çalışma sonuçlarına göre, kadın personellerin bilgi güvenliği farkındalıklarının erkeklere kıyasla daha düşük olduğu tespit edilmiştir. Ayrıca, 19-27 yaş aralığındaki personelin bilgi güvenliği konusundaki farkındalık düzeyinin daha yüksek olduğu, yaş seviyesinin arttıkça ise hassasiyetin azaldığı görülmüştür. Eğitim seviyesinin kişisel verilerin korunması konusundaki farkındalığı etkilediği ve doktora seviyesindeki personelin lise mezunu personele göre daha yüksek bir farkındalığa sahip olduğu belirtilmiştir. Görev süresi ile bilgi güvenliği konusunda anlamlı bir farklılık görülmezken, interneti daha uzun süredir kullanan ve günlük olarak daha fazla internet kullanan personelin farkındalık düzeyinin daha yüksek olduğu ortaya konmuştur. Araştırmada, sosyo-kültürel farkların bilgi güvenliği konusunda önemli olduğuna vurgu yapılmış ve kurumsal politikaların belirlenirken bu özelliklerin dikkate alınması gerektiği vurgulanmıştır.

Okul ve diğerleri (2018) tarafından gerçekleştirilen çalışmada, Kuşadası'nda faaliyet gösteren beş yıldızlı konaklama işletmelerinde görev yapan 52 yöneticiye yönelik bir ölçek uygulanmıştır. Araştırmada, yöneticilerin bilgi güvenliği farkındalık seviyelerinin değerlendirilmesi amacıyla katılımcıların anket sorularına verdikleri yanıtların ortalamaları hesaplanmış ve elde edilen veriler üzerinde t testi ve tek yönlü ANOVA testi uygulanmıştır. Araştırma sonuçları, yöneticilerin bilgi güvenliği farkındalık seviyelerinin genel olarak yüksek olduğunu, ancak bazı kritik noktalarda bilgi eksikliği yaşadıklarını ortaya koymuştur. Bu eksikliklerin giderilmesi ve bilgi güvenliği bilincinin daha kapsamlı bir şekilde artırılması amacıyla, konaklama işletmelerinde düzenli bilgi güvenliği eğitimleri verilmesi gerektiği önerilmiştir.

Köktürk ve Avcı (2019) tarafından yürütülen çalışmada ise, bir kamu kurumunda çalışan 72 kişi üzerinde bilgi güvenliği farkındalık seviyelerini ölçmeye yönelik bir ölçek uygulanmıştır. Araştırma kapsamında toplanan veriler, frekans ve yüzde dağılımları temel alınarak analiz edilmiştir. Elde edilen bulgular, katılımcıların bilgi güvenliği farkındalık seviyelerinin genel olarak yüksek olduğunu göstermektedir. Bununla birlikte, çalışanların en az güvenlik duvarı yazılımları hakkında bilgi sahibi oldukları, buna karşın parola güvenliği konusundaki risklerin farkında oldukları belirlenmiştir. Çalışmanın sonucunda, kamu kurumlarında çalışan personelin bilgi güvenliği farkındalığının

sürdürülebilir bir şekilde artırılabilmesi için düzenli eğitim programlarının uygulanması önerilmiştir. Bu sayede, kurum çalışanlarının hem mevcut güvenlik riskleri hakkında daha bilinçli hale gelmeleri hem de bilgi güvenliği önlemlerini daha etkin bir şekilde uygulamaları sağlanabilecektir.

Ceylan (2019) tarafından yürütülen çalışmada, 200 bilişim çalışanına yönelik bir ölçek uygulanarak bilgi güvenliği farkındalık seviyeleri değerlendirilmiştir. Elde edilen verilerin analizinde t testi ve tek yönlü ANOVA testi kullanılmıştır. Araştırma sonuçları, katılımcıların bilgi güvenliği farkındalık seviyelerinin genel olarak yüksek olduğunu ortaya koymuştur. Çalışmanın bulgularına dayanarak, gelecekte daha geniş bir katılımcı kitlesiyle kapsamlı farkındalık analiz çalışmalarının gerçekleştirilmesinin faydalı olacağı öngörülmüştür. Bu durum, bilgi güvenliği farkındalığının sürdürülebilir bir şekilde ölçülmesi ve geliştirilmesi için daha geniş ölçekli araştırmalara olan ihtiyacı vurgulamaktadır.

Özdemir (2019) tarafından 501 kamu çalışanıyla gerçekleştirilen bir araştırmada, kadın ve erkek personelin bilgi güvenliği farkındalıklarının benzer olduğu tespit edilmiştir. Birim bazında incelendiğinde, teknik eğitim almış birimlerde ve 40 yaş altı personelin bilgi güvenliği farkındalıklarının diğer personellere göre daha yüksek olduğu görülmüştür. Araştırmacı, personelin ihtiyaçları, eğitimleri ve birikimleri dikkate alınarak bilgi güvenliği farkındalık eğitimlerinin yenilikler doğrultusunda belirli periyodlarla verilmesinin önemine vurgu yapmıştır.

Özdemir ve Uluyol (2021) tarafından gerçekleştirilen bir araştırmada, kamu çalışanlarının bilgi güvenliği farkındalıklarını ortaya koymayı amaçlanmıştır. Araştırma, 501 kişi ile gerçekleştirilmiştir. Elde edilen sonuçlara göre, kamu çalışanlarının genel olarak orta düzeyde bilgi güvenliği farkındalığına sahip oldukları belirlenmiştir. Cinsiyet ve yaş grupları arasında farklılıklar olmasına rağmen, erkek ve kadın katılımcıların benzer düzeyde farkındalığa sahip oldukları gözlemlenmiştir. Teknik eğitim almış olan bilgi teknolojileri çalışanlarının ve üniversite düzeyinde eğitim almış olan katılımcıların ise genel olarak daha yüksek düzeyde farkındalığa sahip oldukları saptanmıştır. Araştırmanın sonucunda, bilgi güvenliği farkındalığını artırmaya yönelik eğitim ve farkındalık programlarının öneminin vurgulanması önerilmiştir.

Keser ve Yayla (2021) tarafından yürütülen araştırmada, Fatih Projesi kapsamında yer alan okullarda görev yapan öğretmenlerin, diğer okullarda çalışan öğretmenlere kıyasla bilgi güvenliği farkındalık seviyelerinin daha yüksek olduğu belirlenmiştir. Araştırma sonuçları, erkek öğretmenlerin kadın öğretmenlere göre daha yüksek bilgi güvenliği farkındalığına sahip olduğunu göstermektedir. Ayrıca, bilgi güvenliği eğitimi almış öğretmenlerin, bu tür bir eğitim almayan meslektaşlarına kıyasla daha bilinçli olduğu gözlemlenmiştir. Çalışmanın bulguları arasında, bilişim teknolojileri öğretmenlerinin diğer branş öğretmenlerine göre daha yüksek bilgi güvenliği farkındalığına sahip olduğu öne çıkmaktadır. Bunun aksine, okul öncesi öğretmenlerinin bilgi güvenliği farkındalık seviyelerinin diğer öğretmen gruplarına göre daha düşük olduğu belirlenmiştir. Bu sonuçlar, bilgi güvenliği farkındalığının öğretmenlerin branşlarına ve aldıkları eğitime bağlı olarak farklılık gösterdiğini ortaya koymaktadır. Araştırma, özellikle okul öncesi öğretmenleri gibi düşük farkındalık seviyesine sahip gruplara yönelik bilgi güvenliği eğitimlerinin artırılması gerektiğini vurgulamaktadır.

1.4.2. Konuyla İlgili Uluslararası Araştırmalar

Vroom ve Von Solms'un (2004) araştırmasında, bilgi güvenliği farkındalığının oluşturulmasında bilgi güvenliği politikalarının, kurumsal bilgilendirme faaliyetlerinin ve kurum kültürünün, kişisel özellikler gibi faktörlerle birlikte etkili olduğu belirtilmektedir.

Kruger ve Kearney'in (2006) çalışmasında ise uluslararası bir maden şirketi için bilgi güvenliği farkındalığı konusunda bir prototip geliştirilmiştir. Otuz beş sorudan oluşan ölçek çalışmasında, şirket çalışanlarının genel bilgi güvenliği farkındalığı orta derecede (%65) olarak değerlendirilmiştir. Çalışmanın sonucunda, bu prototipin hayata geçirilmesi için ölçümlemenin bölgesel düzeylerden genel bir ölçümleme düzeyine taşınması gerektiği önerilmiştir.

Albrechtsen'in (2007) çalışmasında, çalışanların güvenlik önlemlerine karşı tutumları incelenmiş ve özellikle bilişim teknolojileri şirketleri ile Norveç'teki bankalar üzerinde bir değerlendirme yapılmıştır. Araştırma, bilgi güvenliğini sağlayan yöneticiler ile personel arasındaki iletişim eksikliğinin ciddi bir sorun teşkil ettiğini ortaya koymuştur. Elde edilen bulgular, güvenlik ihlallerinin büyük ölçüde çalışanların bilgi güvenliği farkındalığının yetersizliğinden kaynaklandığını göstermektedir. Bu durum,

organizasyonlarda bilgi güvenliğini sağlamak için yalnızca teknik önlemler almanın yeterli olmayacağını, aynı zamanda çalışanların bilinç düzeylerinin artırılması gerektiğini vurgulamaktadır.

Kruger ve diğerleri (2010) tarafından yürütülen bir başka araştırmada ise üniversite öğrencilerinin bilgi güvenliği farkındalık seviyelerini ölçmeye yönelik özel bir değerlendirme aracı geliştirilmiştir. Bu ölçme aracı, farkındalık eğitimlerinde ele alınabilecek temel konuların belirlenmesine yardımcı olabilecek bir "bilgi güvenliği sözcük testi" içermektedir. Çalışma kapsamında, geliştirilen testin geçerliliğini ve güvenilirliğini değerlendirmek amacıyla iki aşamalı bir anket uygulanmıştır. İlk aşamada katılımcılara bilgi güvenliği ile ilgili temel kavramları içeren sözcük testi sunulurken, ikinci aşamada ise katılımcıların güvenlik farkındalık düzeylerine bağlı olarak gösterdikleri davranışlar analiz edilmiştir. Araştırma sonuçları, bu testin bilgi güvenliği farkındalığını ölçmek ve geliştirmek için kullanılabilecek etkili bir araç olabileceğini ortaya koymuştur.

Kaur ve Mustafa (2013) tarafından gerçekleştirilen çalışmada, Malezya'daki bir küçük ve orta ölçekli işletmenin (KOBİ) 110 çalışanı üzerinde bilgi güvenliği farkındalığına yönelik bir ölçek uygulanmıştır. Bu ölçek kapsamında, katılımcıların bilgi güvenliğinin temel unsurları olan gizlilik, bütünlük ve kullanılabilirlik ilkelerine yönelik tutumları ölçülmüştür. Araştırmanın temel amacı, KOBİ çalışanlarının bilgi güvenliği farkındalık seviyelerini belirlemek ve bu farkındalık düzeylerinin kurumsal güvenlik politikaları açısından ne derece yeterli olduğunu değerlendirmektir. Bulgular, çalışanların işyerindeki bilgi kaynaklarının gizliliği konusunda yüksek bir farkındalık düzeyine sahip olduğunu, ancak kimlik avı içeren e-postalar konusunda farkındalık düzeylerinin düşük olduğunu göstermektedir. Bu nedenle, çalışmanın sonucunda katılımcılara bu konuda eğitim verilmesi gerektiği önerilmektedir.

Kınay ve diğerleri (2014) tarafından geliştirilen Bilgi Güvenliği Farkındalığı Ölçeği, İstanbul ilindeki bir özel üniversitenin öğrencileri üzerinde uygulanmıştır. Ölçek, eğitim, bilgi ve davranış düzeylerini ölçen 32 sorudan oluşmaktadır. Elde edilen puanlar 100-80 arası "yüksek", 79-60 arası "orta" ve 60 ve altı ise "düşük" olarak değerlendirilmiştir. Her farkındalık seviyesi için alınması gereken kararlar tartışılmıştır.

Hadlington ve Chivers (2020) tarafından yürütülen bir araştırmada, 18 ile 84 yaş arasındaki 1054 katılımcının siber suç duyarlılığının, bilgi güvenliği farkındalığı ve kişilik faktörleri arasındaki ilişkiye etkisi incelenmiştir. Ölçek, 26 sorudan oluşan 11'li Likert tipinde hazırlanmış ve katılımcılara uygulanmıştır. Araştırma sonuçlarına göre, katılımcıların %60'ının siber suça yatkınlık konusunda yüksek risk kategorisinde olduğu tespit edilmiştir. Ancak bilgi güvenliği farkındalığı düzeyinin düşük olduğu, ancak dürtüsellik konusunda yüksek düzeyde oldukları belirlenmiştir. Çalışmanın önerisi, siber suça karşı duyarlılığın anlaşılması için ele alınan segmentasyonun farkındalık düzeyinin daha genişletilmesi gerektiği yönündedir.

Bağlam temelli mikro eğitim ve oyun tabanlı eğitimin bilgi güvenliği farkındalık eğitimlerine katkısı Kavrestad ve diğerleri (2022) tarafından incelenmiştir. Araştırma sonuçlarına göre, kullanıcıların kimlik avı e-postalarını tespit etme ve güvenli davranışlar sergileme konularında mikro eğitimin ve oyun tabanlı eğitimin her ikisinin de fayda sağladığı ancak tek başına yeterli olmadığı belirtilmiştir. Bu bulgular, bilgi güvenliği farkındalık eğitimlerinin çeşitli yöntemlerin bir araya getirilmesiyle daha etkili hale getirilebileceğini göstermektedir.

Subagyo ve Ramli (2022) tarafından gerçekleştirilen araştırmada, insan faktörünün siber güvenlik açısından en zayıf halka olduğu vurgulanmıştır. Bu bağlamda, bilgi güvenliği farkındalık eğitiminin XYZ telekomünikasyon şirketi çalışanları üzerindeki etkisini incelemişlerdir. Araştırma sonuçları, eğitimin şirket çalışanlarının bilgi güvenliği farkındalık düzeylerinde olumlu bir artış sağladığını göstermektedir. Eğitim öncesinde kimlik avı saldırılarından etkilenen çalışan sayısının %24 olduğu ancak eğitimden sonra bu oranın %4'e düştüğü belirlenmiştir. Teknik pozisyonlarda çalışanların diğer çalışanlara göre daha yüksek bir farkındalık düzeyine sahip olduğu da araştırmanın bir diğer bulgusudur. Araştırmacılar, farkındalık düzeylerini korumak için bu tür eğitimlerin periyodik olarak tekrarlanmasının önemine vurgu yapmışlardır.

Uzaktan çalışma ortamında bilgi güvenliği farkındalığını etkileyen faktörleri inceleyen Zhen ve diğerleri (2022) adlı çalışmada, uzaktan çalışma deneyimi olan 420 kişi üzerinde bir araştırma yürütülmüştür. Araştırma sonuçlarına göre, bilgi, davranış ve öğrenme ataletinin bilgi güvenliği farkındalığı ile pozitif yönde ilişkili olduğu tespit edilmiştir. Ancak deneyim ataleti ile tutum arasında farkındalık üzerinde bir etkinin olmadığı

görülmüştür. Bu bulgular, uzaktan çalışma ortamında bilgi güvenliği farkındalığını artırmak için özellikle bilgi, davranış ve öğrenme ataletiyle mücadele edilmesi gerektiğini ortaya koymaktadır.

Yapılan ulusal ve uluslararası araştırmalar, bilgi güvenliği farkındalığının bireylerin demografik özelliklerine, mesleki konumlarına, eğitim geçmişlerine ve dijital araçlarla etkileşim düzeylerine bağlı olarak anlamlı farklılıklar gösterdiğini ortaya koymaktadır. Eğitim düzeyi ve teknik bilgiye sahip olma, genel olarak bilgi güvenliği farkındalığını artıran temel etkenler arasında yer almaktadır. Ayrıca, birçok çalışmada farkındalık düzeylerinin artırılmasında yapılandırılmış eğitim programlarının ve kurumsal politika uygulamalarının belirleyici bir rol oynadığı görülmektedir. Özellikle öğretmenler, kamu çalışanları ve özel sektör personeli gibi farklı gruplar üzerinde yapılan araştırmalarda, bilgi güvenliği eğitimi alan bireylerin farkındalık düzeylerinin anlamlı biçimde yükseldiği saptanmıştır. Bununla birlikte, yalnızca teknik önlemlerin yeterli olmadığı; bireylerin davranışsal ve bilişsel düzeyde eğitilerek sürdürülebilir bir güvenlik kültürünün oluşturulması gerektiği vurgulanmaktadır.

2.BÖLÜM: YÖNTEM

2.1. Araştırmanın Yöntemi

Bu araştırmada, nicel araştırma yöntemlerinden ilişkisel tarama yöntemi kullanılmıştır. Bu yöntem kapsamında, öğretmenlerin bilgi güvenliği farkındalık seviyelerini değerlendirmek amacıyla anket formu oluşturulmuş ve katılımcılardan veri toplanmıştır. İlişkisel tarama yöntemi, değişkenler arasındaki ilişkileri incelemek için kullanılan bir yöntem olup, bu çalışmada öğretmenlerin bilgi güvenliği farkındalığının çeşitli değişkenlere göre farklılık gösterip göstermediğini belirlemek amacıyla uygulanmıştır.

2.2. Araştırmanın Örneklemi ve Örnekleme Yöntemi

Çalışma Karaman Sosyal Güvenlik İl Müdürlüğü örnekleminde gerçekleştirilmiştir. Yönetim biriminin en altında bulunan hizmetli kadrosundan başlamak üzere birimlerde görev yapan tüm personeller çalışmamızın örneklemini teşkil etmektedirler. Bu bağlamda kurumda çalışan 102 kişiye anket uygulanmıştır. Bu araştırmada kolayda örnekleme yönteminden yararlanılmıştır.

2.3. Araştırmanın Hipotezleri

Bu araştırma kapsamında test edilen ana hipotezler aşağıdaki gibidir:

- Hipotez 1: Kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeyleri cinsiyet açısından farklılık göstermektedir.
- Hipotez 2: Kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeyleri medeni durum açısından farklılık göstermektedir.
- Hipotez 3: Kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeyleri yaş açısından farklılık göstermektedir.
- Hipotez 4: Kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeyleri öğrenim durumu açısından farklılık göstermektedir.
- Hipotez 5: Kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeyleri meslekte toplam hizmet süresi açısından farklılık göstermektedir.

- Hipotez 6: Kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeyleri çalışma sınıfı açısından farklılık göstermektedir.
- Hipotez 7: Kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeyleri iş yerindeki pozisyon açısından farklılık göstermektedir.

2.4. Veri Toplama Yöntemi

Bu araştırmada veri toplama yöntemi olarak araştırmacı tarafından hazırlanan demografik form ve "Bilgi Güvenliği Farkındalık Ölçeği" kullanılmıştır. Ölçek, Keser ve Güldüren (2014) tarafından geliştirilmiş olup, 5'li Likert tipi bir ölçektir. Ölçek, toplam 34 maddeden oluşmakta ve katılımcıların bilgi güvenliği farkındalık düzeylerini değerlendirmek amacıyla tasarlanmıştır. Yanıt seçenekleri "hiç katılmıyorum", "katılmıyorum", "kararsızım", "katılıyorum" ve "tamamen katılıyorum" şeklinde derecelendirilmiş olup, ölçek içerisinde hem olumlu hem de olumsuz ifadeler yer almaktadır. Ölçek, "Saldırı ve Tehditler" ile "Kişisel Verileri Koruma" olmak üzere iki alt boyuttan oluşmaktadır. 16 sorudan oluşan Saldırı ve Tehditler alt boyutu, bireylerin bilgi güvenliği tehditlerine karşı bilinç düzeylerini değerlendirirken, 18 sorudan oluşan Kişisel Verileri Koruma alt boyutu, kişisel ve kurumsal verilerin güvenliği konusunda katılımcıların farkındalık seviyelerini ölçmeyi amaçlamaktadır. Bu yapı, ölçeğin bilgi güvenliği farkındalığını farklı açılardan ele alarak kapsamlı bir değerlendirme yapmasını sağlamaktadır.

2.5. Araştırmanın Varsayımları ve Kısıtları

Kamu çalışanlarının bilgi güvenliği algılarının cinsiyete, yaşa, eğitim düzeyinde, deneyimine ve çalışılan birime göre değişiklik göstereceği ön kabul olarak ele alınmaktadır. Araştırmada anket yöntemi veri toplanmış olup, ölçekler ve bunların geçerlilik ve güvenilirliği yöntemin özellikleri ile sınırlıdır. Çalışmanın diğer bir kısıtı ise yalnızca Karaman Sosyal Güvenlik İl Müdürlüğü bünyesinde, dar bir alanda çalışılmış olmasıdır.

2.6. Verilerin Analizi

Araştırmada veriler, Google Formlar aracılığıyla çevrimiçi ortamda toplanmış ve analiz sürecinde SPSS 23 programı kullanılmıştır. Verilerin normal dağılım gösterip

göstermediğini belirlemek amacıyla çarpıklık ve basıklık testleri uygulanmıştır. Yapılan analizler sonucunda, ölçek ve alt boyutlarının normal dağılım gösterdiği tespit edilmiştir. Bu nedenle, veri analiz sürecinde parametrik testler tercih edilerek istatistiksel değerlendirmeler gerçekleştirilmiştir. Parametrik yöntemlerin kullanılması, veri setinin normal dağılım göstermesi durumunda daha güçlü ve güvenilir sonuçlar elde edilmesine olanak sağlamaktadır. Katılımcıların demografik özellikleri ölçek ve alt boyut puanlarının karşılaştırılmasında, T-Testi ve tek yönlü ANOVA Testi yapılmıştır.

2.7. Güvenilirlik Analizi

Cronbach's alfa katsayısı, ölçeğin iç tutarlılığını değerlendiren bir güvenilirlik ölçütüdür ve 0 ile 1 arasında değişmektedir. Ölçeğin güvenilirlik düzeyi, hesaplanan alfa katsayısına bağlı olarak aşağıdaki şekilde yorumlanmaktadır (Tavşancıl, 2005):

- 0,00- 0,40: Ölçek güvenilir değildir, ölçme aracı güvenilirlik açısından yetersizdir.
- 0,40- 0,60: Ölçek düşük düzeyde güvenirlik göstermektedir, güvenilirliği artırmak için gözden geçirilmesi gerekebilir.
- 0,60- 0,80: Ölçek oldukça güvenilir olup, kabul edilebilir bir iç tutarlılığa sahiptir.
- 0,80- 1,00: Ölçek yüksek derecede güvenilir olup, güçlü bir iç tutarlılığa sahiptir ve güvenilirlik açısından üst düzeyde değerlendirilmektedir; bu sınıflandırma, ölçeklerin bilimsel araştırmalarda kullanım amacına uygun olup olmadığını belirlemek için kritik bir referans noktasıdır (Tavşancıl, 2005).

Tablo 1’de Bilgi Güvenliği Farkındalık Ölçeğinin güvenilirlik analizi sonucunda elde edilen Cronbach Alfa katsayısı verilmiştir. Cronbach Alfa değerine göre ölçek yüksek derecede güvenilirdir.

Tablo 1: Güvenilirlik Analizi

	Madde Sayısı	Cronbach's Alfa
Bilgi Güvenliği Farkındalık Ölçeği	34	0,984

2.8. Faktör Analizi

Bu çalışmada değerlendirilen ölçeğin faktör analizi için uygunluğunu belirlemek amacıyla KMO değeri (Kaiser-Meyer-Olkin) ve Bartlett testi sonuçları değerlendirilmiştir. 0 ile 1,00 arasında değişen KMO değerinin faktör analizi için uygunluk açısından en az 0,5 olması gerekmektedir (Field, 2009).

Tablo 2’de Bilgi Güvenliği Farkındalık ölçeğine ilişkin KMO değeri ve Bartlett Testi sonucu verilmiştir. Elde edilen değerlere göre Bartlett testi anlamlı ve KMO değeri 0,5’in üzerinde bulunmuştur.

Tablo 2: Faktör Analizi Özet Tablo

	KMO	$\chi 2$	p
Bilgi Güvenliği Farkındalık Ölçeği	0,939	5040,894	0,000

Tablo 3’de, Bilgi Güvenliği Farkındalık Ölçeği’ne ilişkin faktör analizi sonuçları verilmiş olup, maddelerin faktör yüklerinin dağılımı incelenmiştir. Yapılan analiz sonucunda, ölçeğin iki faktörlü bir yapı sergilediği belirlenmiştir.

Tablo 3: Bilgi Güvenliği Farkındalık Ölçeği Faktör Analizi ve Boyutların Dağılımı

	Faktör 1	Faktör 2	Açıklanan Varyans
BG1		0,691	
BG2		0,761	
BG3		0,724	
BG4		0,640	
BG5		0,800	
BG6		0,868	
BG7		0,580	
BG8		0,777	66,36
BG9		0,801	
BG10		0,743	
BG11		0,649	
BG12		0,819	
BG13		0,827	
BG14		0,553	
BG15		0,697	
BG16		0,673	
BG17	0,845		
BG18	0,818		
BG19	0,836		
BG20	0,602		
BG21	0,565		
BG22	0,636		
BG23	0,877		
BG24	0,911		
BG25	0,690		8,21
BG26	0,859		
BG27	0,648		
BG28	0,760		
BG29	0,817		
BG30	0,751		
BG31	0,760		
BG32	0,884		
BG33	0,843		
BG34	0,831		

- Birinci faktör, 0,553 ile 0,868 arasında değişen faktör yüklerine sahip 16 maddeden oluşmaktadır. Bu faktör, toplam varyansın %66,36'sını açıklamaktadır ve ölçeğin büyük bir bölümünü temsil etmektedir.
- İkinci faktör, 0,565 ile 0,911 arasında değişen faktör yüklerine sahip 18 maddeden meydana gelmektedir ve toplam varyansın %8,21'ini açıklamaktadır.

Bu bulgular, ölçeğin faktör yapısının açıklayıcı faktör analizi (AFA) sonucunda belirlenen iki temel boyuttan oluştuğunu göstermektedir. Birinci faktör, ölçeğin büyük bir kısmını oluşturduğu için bilgi güvenliği farkındalığının ana bileşeni olarak değerlendirilebilirken, ikinci faktör ise farkındalığın daha spesifik bir yönüne işaret

etmektedir. Elde edilen sonuçlar, ölçeğin geçerli ve güvenilir bir yapıya sahip olduğunu desteklemektedir.

Analiz sonucunda elde edilen sonuçlara bakıldığında elde edilen faktör dağılımları orijinal ölçekte yer alan boyutlar ile birebir uyum göstermektedir. Buna göre 1 numaralı faktör “Saldırı ve Tehdit” 2 numaralı faktör ise “Kişisel Verileri Koruma” boyutlarına karşılık gelmektedir.

3.BÖLÜM: BULGULAR

Tablo 4'de katılımcıların kişisel bilgilerinin dağılımı verilmiştir.

Tablo 4: Demografik Değişkenlere İlişkin Bulgular

		n	%
Cinsiyet	Kadın	39	38,2
	Erkek	63	61,8
Medeni Durum	Bekar	17	16,7
	Evli	85	83,3
Yaş	20-29	17	16,7
	30-39	42	41,2
	40-49	32	31,4
	50 ve üzeri	11	10,8
Öğrenim durumu	İlköğretim ve Lise	10	9,8
	Ön lisans	14	13,7
	Lisans	62	60,8
	Lisansüstü	16	15,7
Meslekte toplam hizmet süresi	1-5 yıl	17	16,7
	6-10 yıl	18	17,6
	11-15 yıl	38	37,3
	16 yıl ve üzeri	29	28,4
Çalışma sınıfı	Memur	68	66,7
	İşçi	34	33,3
İş yerindeki pozisyon	Personel	80	78,4
	Yönetici	22	21,6

Buna göre katılımcıların %38,2'si kadın ve %61,8'i erkektir. Katılımcıların %41,2'si 30-39 yaş aralığındadır. Ankete katılanların %60,8'i lisans mezunudur. Katılımcıların %37,3'ü meslekte toplamda 11-15 yıldır çalışmaktadır. Ankete katılanların %66,7'si memur, %33,3'ü ise işçidir. Katılımcıların %78,4'ü personel, %21,6'sı ise yöneticidir.

Bilgi Güvenliği Farkındalık Ölçeği ile alt boyutlarının normal dağılıma uygunluğunu değerlendirmek amacıyla çarpıklık (skewness) ve basıklık (kurtosis) katsayıları analiz edilmiş olup Tablo 5'de verilmiştir. Yapılan değerlendirmede, ilgili literatüre göre çarpıklık ve basıklık değerlerinin -3 ile +3 aralığında yer alması, verilerin normal dağılım gösterdiğini kabul etmek için yeterli görülmektedir (De Carlo, 1997). Yapılan analizler sonucunda, Bilgi Güvenliği Farkındalık Ölçeği ve alt boyutlarının normal dağılım gösterdiği belirlenmiştir. Normal dağılım varsayımının sağlanması nedeniyle, araştırmada parametrik analiz yöntemleri tercih edilmiştir. Bu bağlamda, t testi ve tek yönlü ANOVA gibi parametrik testler kullanılarak değişkenler arasındaki ilişkiler ve farklılıklar istatistiksel olarak değerlendirilmiştir. Normal dağılım gösteren veri setlerinde parametrik yöntemlerin kullanılması, analizlerin daha güçlü ve güvenilir sonuçlar ortaya koymasını sağlamaktadır

Tablo 5: Betimleyici İstatistikler

	ort.	ss.	min.	maks.	çarpıklık	basıklık
Saldırı ve Tehditler	2,75	1,18	1	5	0,012	-1,134
Kişisel Verileri Koruma	3,32	1,28	1	5	-0,699	-0,856
Bilgi Güvenliği Farkındalık Ölçeği	3,06	1,17	1	5	-0,42	-0,933

Araştırma kapsamındaki hipotezlerin test edilmesi için fark testleri uygulanmıştır. Bu kapsamda kamu çalışanlarının bilgi güvenliği konusundaki farkındalık düzeylerinin cinsiyet, medeni durum, yaş, öğrenim durumu, meslekte toplam hizmet süresi, çalışma sınıfı ve iş yerindeki pozisyon açısından fark gösterip göstermediği test edilmiştir.

Tablo 6'da katılımcıların cinsiyet gruplarına göre Bilgi Güvenliği Farkındalık Ölçeği ve alt boyut puanlarının bağımsız örneklem t testi sonuçları görülmektedir. Analiz sonuçlarına göre; erkek katılımcıların hem ölçek puanları hem de alt boyutlara ilişkin puanları kadın katılımcılara kıyasla daha yüksek düzeydedir. Bundan dolayı, Hipotez 1 kabul edilmiştir.

Tablo 6: Ölçek Puanlarının Katılımcıların Cinsiyetleri Bakımından Karşılaştırılması

	Grup	ort.	ss.	t	p
Saldırı ve Tehditler	Kadın	2,25	1,20	-3,573	0,001*
	Erkek	3,06	1,06		
Kişisel Verileri Koruma	Kadın	2,90	1,48	-2,525	0,014*
	Erkek	3,59	1,08		
Bilgi Güvenliği Farkındalık Ölçeği	Kadın	2,60	1,27	-3,094	0,003*
	Erkek	3,34	1,02		

Tablo 7'de, katılımcıların medeni durumlarına göre Bilgi Güvenliği Farkındalık Ölçeği ve alt boyut puanlarının bağımsız örneklem t testi sonuçları yer almaktadır. Analiz bulgularına göre; evli ve bekar bireylerin ölçek ve alt boyut puanları arasında istatistiksel olarak anlamlı bir fark bulunmamaktadır (p> 0,05). Bu bulgu, medeni durumun bilgi güvenliği farkındalığı üzerinde belirleyici bir değişken olmadığını göstermektedir. Bundan dolayı, Hipotez 2 reddedilmiştir.

Tablo 7: Ölçek Puanlarının Katılımcıların Medeni Durumları Bakımından Karşılaştırılması

	Grup	ort.	ss.	t	p
Saldırı ve Tehditler	Bekar	2,64	1,16	-0,441	0,660
	Evli	2,78	1,18		
Kişisel Verileri Koruma	Bekar	3,40	1,01	0,308	0,761
	Evli	3,31	1,33		
Bilgi Güvenliği Farkındalık Ölçeği	Bekar	3,04	0,97	-0,060	0,953
	Evli	3,06	1,22		

Tablo 8'de katılımcıların yaşlarına göre Bilgi Güvenliği Farkındalık Ölçeği ve alt boyut puanlarının ANOVA testi sonuçları görülmektedir. Analiz sonuçlarına göre yaş grupları arasında Bilgi Güvenliği Farkındalık Ölçeği ve alt boyut puanları bakımından istatistiksel olarak anlamlı fark bulunmamaktadır (p>0.05).

Tablo 8: Ölçek Puanlarının Katılımcıların Yaşları Bakımından Karşılaştırılması

	Grup	ort.	ss.	t	p
Saldırı ve Tehditler	20-29	2,38	1,33	2,323	0,080
	30-39	2,85	1,14		
	40-49	3,04	1,12		
	50 ve üzeri	2,16	0,99		
Kişisel Verileri Koruma	20-29	2,74	1,47	2,037	0,114
	30-39	3,48	1,22		
	40-49	3,55	1,23		
	50 ve üzeri	2,97	1,14		
Bilgi Güvenliği Farkındalık Ölçeği	20-29	2,57	1,35	2,291	0,083
	30-39	3,18	1,13		
	40-49	3,31	1,11		
	50 ve üzeri	2,59	0,99		

Tablo 9'da, katılımcıların öğrenim durumlarına göre Bilgi Güvenliği Farkındalık Ölçeği ve alt boyut puanlarının ANOVA testi sonuçları yer almaktadır. Analiz sonuçlarına göre; farklı öğrenim düzeylerine sahip katılımcılar arasında ölçek ve alt boyut puanları bakımından istatistiksel olarak anlamlı bir fark tespit edilmemiştir (p> 0,05). Bu bulgu, bireylerin eğitim seviyelerinin bilgi güvenliği farkındalık düzeyleri üzerinde belirleyici bir etkiye sahip olmadığını göstermektedir.

Tablo 9: Ölçek Puanlarının Katılımcıların Öğrenim Durumları Bakımından Karşılaştırılması

	Grup	ort.	ss.	t	p
Saldırı ve Tehditler	İlköğretim ve Lise	2,98	1,36	0,127	0,944
	Ön lisans	2,68	1,44		
	Lisans	2,72	1,13		
	Lisansüstü	2,88	1,16		
Kişisel Verileri Koruma	İlköğretim ve Lise	2,92	1,35	0,396	0,756
	Ön lisans	3,25	1,47		
	Lisans	3,39	1,28		
	Lisansüstü	3,37	1,13		
Bilgi Güvenliği Farkındalık Ölçeği	İlköğretim ve Lise	2,90	1,29	0,102	0,959
	Ön lisans	2,99	1,38		
	Lisans	3,07	1,14		
	Lisansüstü	3,14	1,12		

Tablo 10'da, katılımcıların meslekteki toplam hizmet sürelerine göre Bilgi Güvenliği Farkındalık Ölçeği ve alt boyutlarına ilişkin ANOVA testi sonuçları sunulmaktadır.

Yapılan analizler doğrultusunda, farklı hizmet süresi grupları arasında ölçek ve alt boyut puanları açısından anlamlı bir farklılık ortaya çıkmamıştır (p> 0,05). Bu bulgu, bireylerin meslekte geçirdikleri toplam sürenin, bilgi güvenliği farkındalık düzeyleri üzerinde belirleyici bir faktör olmadığını göstermektedir.

Tablo 10: Ölçek Puanlarının Katılımcıların Meslekte Toplam Hizmet Süreleri Bakımından Karşılaştırılması

	Grup	ort.	ss.	t	p
Saldırı ve Tehditler	1-5 yıl	2,79	1,32	0,387	0,763
	6-10 yıl	2,50	1,21		
	11-15 yıl	2,86	1,17		
	16 yıl ve üzeri	2,75	1,11		
Kişisel Verileri Koruma	1-5 yıl	3,35	1,41	1,374	0,255
	6-10 yıl	2,88	1,42		
	11-15 yıl	3,60	1,29		
	16 yıl ve üzeri	3,22	1,07		
Bilgi Güvenliği Farkındalık Ölçeği	1-5 yıl	3,09	1,31	0,924	0,432
	6-10 yıl	2,70	1,28		
	11-15 yıl	3,25	1,17		
	16 yıl ve üzeri	3,00	1,02		

Tablo 11'de, katılımcıların çalışma sınıflarına göre Bilgi Güvenliği Farkındalık Ölçeği ve alt boyut puanlarına ilişkin bağımsız örneklem t testi sonuçları yer almaktadır. Elde edilen analiz bulgularına göre; farklı çalışma sınıflarına mensup katılımcılar arasında ölçek ve alt boyut puanları açısından anlamlı bir farklılık görülmemiştir (p> 0,05). Bu bulgu, bireylerin çalıştıkları sınıfların bilgi güvenliği farkındalığı üzerinde belirleyici bir değişken olmadığını göstermektedir.

Tablo 11: Ölçek Puanlarının Katılımcıların Çalışma Sınıfları Bakımından Karşılaştırılması

	Grup	ort.	ss.	t	p
Saldırı ve Tehditler	Memur	2,64	1,20	-1,407	0,163
	İşçi	2,99	1,10		
Kişisel Verileri Koruma	Memur	3,19	1,28	-1,518	0,132
	İşçi	3,59	1,26		
Bilgi Güvenliği Farkındalık Ölçeği	Memur	2,93	1,19	-1,542	0,126
	İşçi	3,31	1,12		

Tablo 12'de, katılımcıların iş yerindeki pozisyonlarına göre Bilgi Güvenliği Farkındalık Ölçeği ve alt boyut puanlarının bağımsız örneklem t testi sonuçları yer almaktadır. Analiz

sonuçlarına göre, iş yerindeki pozisyon grupları arasında Bilgi Güvenliği Farkındalık Ölçeği ve alt boyut puanları açısından istatistiksel olarak anlamlı bir fark bulunmamaktadır (p> 0,05). Bu bulgu, çalışanların iş yerindeki pozisyonlarının bilgi güvenliği farkındalık seviyeleri üzerinde belirleyici bir etkiye sahip olmadığını göstermektedir.

Tablo 12: Ölçek Puanlarının Katılımcıların İş Yerindeki Pozisyonları Bakımından Karşılaştırılması

	Grup	ort.	ss.	t	p
Saldırı ve Tehditler	Personel	2,70	1,18	-0,899	0,371
	Yönetici	2,95	1,15		
Kişisel Verileri Koruma	Personel	3,28	1,28	-0,701	0,485
	Yönetici	3,49	1,31		
Bilgi Güvenliği Farkındalık Ölçeği	Personel	3,00	1,17	-0,829	0,409
	Yönetici	3,24	1,20		

SONUÇ VE ÖNERİLER

Bu araştırmada kamu sektöründe görev yapan kişilerin bilgi güvenliği konusundaki farkındalık düzeyleri incelenmiştir. Elde edilen sonuçlar bu bölümde yer almaktadır.

Bilgi Güvenliği Farkındalığı kapsamında yapılan analiz neticesinde, çalışanların genel bilgi güvenliği farkındalığının orta derecede olduğu belirlenmiştir. Özdemir ve Uluyol (2021), Çelikçöp ve Yarar (2019), Kaur ve Mustafa (2013) ve Kruger ve Kearney'da (2006) çalışmalarında şirket çalışanlarının genel bilgi güvenliği farkındalığının orta derecede olduğu sonucuna ulaşmışlardır. Keser ve Yayla (2021), Ceylan (2019), Köktürk ve Avcı (2019), Okul ve diğerleri (2018), Yılmaz ve diğerleri (2016), Çavuş ve Erçağ (2016) ve Keser ve Güldüren (2015) ise araştırmalarında çalışanlarının genel bilgi güvenliği farkındalığının yüksek olduğu sonucuna ulaşmışlardır. Hadlington ve Chivers (2020) araştırmalarında çalışanlarının genel bilgi güvenliği farkındalığının düşük olduğu sonucuna ulaşmışlardır. Bu çalışmada elde edilen orta düzeydeki bilgi güvenliği farkındalığı sonucu, literatürde yer alan düşük, orta ve yüksek düzeyde farkındalık belirten farklı araştırma bulgularıyla örtüşmekte ve konunun bağlama göre değişkenlik gösterdiğini ortaya koymaktadır.

Erkeklerin Bilgi Güvenliği Farkındalık Ölçeği ve alt boyut puanları kadınlara göre daha yüksektir. Keser ve Yayla (2021), Öztezcan (2017), Yılmaz ve diğerleri (2016) ve Çavuş ve Erçağ (2016)'da araştırmamıza benzer şekilde erkeklerin Bilgi Güvenliği Farkındalık Ölçek puanlarının kadınlardan yüksek olduğu sonucuna ulaşmışlardır. Özdemir ve Uluyol (2021) ve Özdemir (2019) ise Bilgi Güvenliği Farkındalık ölçek puanlarının cinsiyete göre değişmediği sonucuna ulaşmışlardır.

Analiz sonuçlarına göre medeni durum grupları arasında Bilgi Güvenliği Farkındalık Ölçeği ve alt boyut puanları bakımından istatistiksel olarak anlamlı fark bulunmamaktadır. Analiz sonuçlarına göre çalışma sınıfı grupları arasında Bilgi Güvenliği Farkındalık Ölçeği ve alt boyut puanları bakımından istatistiksel olarak anlamlı fark bulunmamaktadır. Elde edilen verilere göre iş yerindeki pozisyon grupları arasında Bilgi Güvenliği Farkındalık Ölçeği ve alt boyut puanları bakımından istatistiksel olarak anlamlı fark bulunmamaktadır.

Elde edilen verilere göre yaş grupları arasında Bilgi Güvenliği Farkındalık Ölçeği ve alt boyut puanları bakımından istatistiksel olarak anlamlı fark bulunmamaktadır. Mart (2012) katılımcıların yaş grubu ile bilgi güvenliği farkındalıkları arasında anlamlı fark olduğunu belirlemiştir. Buna göre, bilgi güvenliği farkındalığının küçük yaşlardan itibaren eğitilmesi gerektiği sonucuna erişmiştir. Öztezcan (2017) 19-27 yaş aralığındaki personelin bilgi güvenliği konusundaki farkındalık düzeyinin daha yüksek olduğu, yaş seviyesinin arttıkça ise hassasiyetin azaldığını belirlemiştir. Özdemir (2019) 30 yaş altı personelin bilgi güvenliği farkındalıklarının diğer personellere göre daha yüksek olduğu sonucuna erişmiştir.

Analiz sonuçlarına göre öğrenim durumu grupları arasında Bilgi Güvenliği Farkındalık Ölçeği ve alt boyut puanları bakımından istatistiksel olarak anlamlı fark bulunmamaktadır. Çavuş ve Erçağ (2016) Bilgi Güvenliği Farkındalık ölçek puanlarının öğrenim durumuna göre değişmediği sonucuna ulaşmışlardır. Öztezcan (2017) eğitim seviyesinin kişisel verilerin korunması konusundaki farkındalığı etkilediği ve doktora seviyesindeki personelin lise mezunu personele göre daha yüksek bir farkındalığa sahip olduğu sonucuna erişmiştir. Özdemir ve Uluyol (2021) teknik eğitim almış olan bilgi teknolojileri çalışanlarının ve üniversite düzeyinde eğitim almış olan katılımcıların genel olarak daha yüksek düzeyde farkındalığa sahip olduklarını saptamışlardır.

Elde edilen verilere göre meslekte toplam hizmet süresi grupları arasında Bilgi Güvenliği Farkındalık Ölçeği ve alt boyut puanları bakımından istatistiksel olarak anlamlı fark bulunmamaktadır. Öztezcan (2017) ve Çavuş ve Erçağ (2016) Bilgi Güvenliği Farkındalık ölçek puanlarının hizmet süresine göre değişmediği sonucuna ulaşmışlardır.

Bu araştırmanın sonuçlarına dayalı olarak, bilgi güvenliği farkındalığının çeşitli değişkenlerle ilişkisinin istatistiksel olarak farklılaşması veya farklılaşmaması dikkate alınarak aşağıdaki öneriler geliştirilmiştir:

- Araştırma sonuçları, bilgi güvenliği farkındalığının genel olarak orta düzeyde olduğunu göstermektedir. Kamu sektöründeki bilgi güvenliği farkındalığını artırmak amacıyla, düzenli ve kapsamlı eğitim programları ile farkındalık kampanyaları düzenlenmelidir. Bu eğitimler, siber tehditler, veri koruma ve güvenliğe ilişkin en iyi uygulamalar gibi temel konuları kapsamalıdır. Eğitim

programları, farklı öğrenme tarzlarına uygun çeşitli formatlarda (örneğin, atölyeler, e-öğrenme modülleri, interaktif eğitimler) sunulmalıdır.

- Kamu sektöründeki bilgi güvenliği politikaları, çalışanların farkındalığını artıracak şekilde güçlendirilmelidir. Bu politikalar, bilgi güvenliği uygulamalarının önemi ve çalışanların uyması gereken standartları net bir şekilde belirtmelidir. Ayrıca, bilgi güvenliği politikalarının düzenli olarak gözden geçirilmesi ve güncellenmesi önerilmektedir.
- Teknolojik araçlar, bilgi güvenliği farkındalığını artırmada etkili olabilir. Kamu sektörü kurumları, siber güvenlik tehditlerini tespit etmeye yardımcı olacak yazılımlar ve sistemler kullanarak çalışanların bilgi güvenliği farkındalığını artırabilir. Bu teknolojik çözümler, siber tehditleri gerçek zamanlı olarak izleme ve çalışanları potansiyel riskler konusunda uyarma yeteneğine sahip olmalıdır.
- Bilgi güvenliği farkındalığını artırmak için, kamu sektöründe bilgi güvenliği kültürünün geliştirilmesi önemlidir. Bu kültür, üst yönetimin bilgi güvenliğine olan taahhüdünü ve çalışanların bilgi güvenliğini teşvik etmesini içerir. Bilgi güvenliği kültürü, çalışanların bilgi güvenliği ile ilgili olumlu davranışlar sergilemesine ve güvenlik önlemlerine sadık kalmasına yardımcı olabilir.

KAYNAKÇA

Ağdeniz, Ş. (2021). Bilgi ve iletişim güvenliği denetiminde kamu iç denetçilerinin rolü ve yetkinliklerine ilişkin bir araştırma. *Alanya Akademik Bakış*, *5*(2), 525-545.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*, 179-211.

Ajzen, I., & Madden, T. J. (1986). Prediction of goal-directed behavior: Attitude, intentions, and perceived behavioral control. *Journal of Experimental Social Psychology*, *22*, 453-474.

Akıncan, E. (2022). *Ortaokul öğretmenlerinin dijital okuryazarlık dijital bağımlılık ve bilgi güvenliği farkındalık düzeylerinin incelenmesi* [Yüksek Lisans Tezi, Amasya Üniversitesi], Amasya.

Aktan, C. C., & Vural, İ. Y. (2016). Bilgi çağında bilginin yönetimi. *Yeni Türkiye*, *88*(1), Bilim ve Teknoloji Özel Sayısı, 1-15.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & security*, *26*(4), 276-289.

AlMindeel, R., & Martins, J. T. (2020). Information security awareness in a developing country context: insights from the government sector in Saudi Arabia. *Information Technology ve People*, *34*(2), 770-788.

Alshaikh, M., Maynard, S., Ahmad, A., & Chang, S. (2015). Information security policy: A management practice perspective. *Australasian Conference on Information Systems*. Adelaide, South Australia.

Altıntaş, S., & Barkuş, F. (2023). Dijital ortamlarda kişisel veri güvenliği kavramı üzerine bir derleme çalışması. *Ejovoc (Electronic Journal of Vocational Colleges)*, *13*(1), 46-69.

Aslan-Öztezcan, B. (2017). *Bilgi güvenliği farkındalığı üzerine bir araştırma: Marmara Üniversitesi örneği* [Yüksek Lisans Tezi, Marmara Üniversitesi]. İstanbul.

Ateş, S. (2023). *Öğretmenlerin bilgi güvenliği farkındalık ve dijital okuryazarlık düzeylerinin çeşitli değişkenler açısından incelenmesi* [Yüksek Lisans Tezi, T.C. Atatürk Üniversitesi]. Erzurum.

Bellinger, G., Castro, D., & Mills, A. (2004). Data, information, knowledge, and wisdom. https://homepages.dcc.ufmg.br/~amendes/SistemasInformacaoTP/TextosBasicos/Data-InformationKnowledge.pdf (Erişim tarihi: 23.05.2025).

Benson, M. L., & Madensen, T. D. (2007). Situational crime prevention and white-collar crime. In H. N. Pontell & G. Geis (Eds.), *International handbook of white-collar and corporate crime* (ss. 609-626). Springer, Boston, MA.

Bhaharin, S., Mokhtar, U., Sulaiman, R., & Yusof, M. (2019). Issues and trends in information security policy compliance. *2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)*. Malaysia.

Boisot, M., & Canals, A. (2004). Data, information and knowledge: Have we got it right? *Journal of Evolutionary Economics, 14*(1), 43-67.

Brown, K. M. (1999). Antecedents of culturally significant tourist behavior. *Annals of Tourism Research, 26*(3), 676-700.

Burlu, K. (2015). *Bilişimin karanlık yüzü* (4. baskı). Nirvana.

Butler, J. T. (2001). *Principles of health education & health promotion* (3rd ed.). USA: Wadsworth Thomson Learning.

Calder, A. (2018). *NIST cybersecurity framework: A pocket guide*. IT Governance Publishing Ltd.

Can, Ö., & Akbaş, M. F. (2014). Kurumsal ağ ve sistem güvenliği politikalarının önemi ve bir durum çalışması. *Türk Bilim Araştırma Vakfı TUBAV Bilim Dergisi, 7*(2), 16-31.

Can, Ö., & Ünalır, M. O. (2010). Ontoloji tabanlı bilgi sistemlerinde politika yönetimi. *Gazi Üniversitesi Bilişim Enstitüsü Bilişim Teknolojileri Dergisi, 3*(2), 3.

Ceylan, H. (2019). *Türkiye'de bilgi güvenliği algısının istatistiksel analizi* [Yüksek Lisans Tezi, İstanbul Üniversitesi]. İstanbul.

Clarke, R. V. G. (1997). A revised classification of situational crime prevention techniques. *Crime Prevention at a Crossroads*, Cincinnati.

Coştan, U. (2014). *Suç ve suç önleme stratejileri doğrultusunda Ankara ili örneğinde suçu önleyici yaklaşımlar* [Yüksek Lisans Tezi, Kırıkkale Üniversitesi]. Kırıkkale.

Çakır, H., & Tuygun, M. (2019). ISO27001 bilgi güvenliği yönetim sistemi standardının kamu kurumlarına uygulanabilirliğinin araştırılması: Ankara ili örneği. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 3*(2), 59-78.

Çavuş, N., & Erçağ, E. (2016). The scale for the self-efficacy and perceptions in the safe use of the Internet for teachers: The validity and reliability studies. *British Journal of Educational Technology, 47*(1), 76–90.

Çek, E. (2017). *Kurumsal bilgi güvenliği yönetişimi ve bilgi güvenliği için insan faktörünün önemi* [Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi]. İstanbul.

Çelikçöp, Ç., & Yarar, Y. (2019). Kalite yönetim direktörlerinin bilgi güvenliği farkındalığı: İstanbul ili örneği. *Sağlıkta Performans ve Kalite Dergisi, 17*(2), 29-48.

Darsono, L. I. (2005). Examining information technology acceptance by individual professionals. *[Dergi adı eksik]*, *7*(2), 155-178. **Not:** Dergi adı belirtilmemiştir. İsterseniz ekleyebilirsiniz.

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* [Doktora Tezi, MIT Sloan School of Management]. Cambridge, MA.

Davis, F., Bagozzi, R., & Warshaw, P. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982–1003.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Department of Business Administration and Computer Science, University of Applied Sciences and Arts*, 92-100.

Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2008). Information security: The moving target. *Computers & security, 28*(3-4), 189-198

Doğan, M. (2021, 7 Şubat). Bilgi güvenliğinde farkındalık ve insan faktörü. https://www.rskveri.com/bilgi-guvenliginde-farkindalik-ve-insan-faktoru/

Doğru, M. (2023). *Bilgi güvenliği farkındalığı ve teknolojik okuryazarlık arasındaki ilişki* [Yüksek Lisans Tezi, İstanbul Topkapı Üniversitesi]. İstanbul.

Dolu, O. (2009). Bir fırsat olarak suç: Suçun durumsal belirleyicileri, suç fırsatları ve rutin faaliyetler teorisi. *Polis Bilimleri Dergisi*, *11*(2), 1-30.

Erbuğa, G. S. (2020). Durumsal suç önleme yaklaşımı çerçevesinde beyaz yakalı suçların önlenmesi. *İzmir İktisat Dergisi*, *35*(3), 593-609.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407-429.

Gökçearslan, Ş., Günbatar, M. S., & Sarıtepeci, M. (2021). Ortaöğretim öğrencilerinin bilgi güvenliği farkındalıklarının incelenmesi. *YYÜ Eğitim Fakültesi Dergisi, 18*(1), 354- 373.

Gökmen, Ö.F., & Akgün, Ö.E. (2016). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği bilgilerinin çeşitli değişkenlere göre incelenmesi. *Çukurova Üniversitesi Eğitim Fakültesi Dergisi, 44*(1), Adana.

Guo, L., & Congdon, P. (2021). IEEE 802 NENDICA report: Intelligent lossless data center networks. *IEEE SA Industry Connections – IEEE 802 NENDICA Report: Intelligent Lossless Data Center Networks*, 1-44.

Gurteen, D. (1999). Creating a knowledge sharing culture. *Knowledge Management Magazine, 2*(5), 1-4.

Güler, A., & Arkin, A. K. (2019). Siber Hijyenin Sağlanmasında İç Denetimin Rolü. *Denetişim*, (19), 17-40.

Gülmüş, M. (2010). *Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği.* [Yayınlanmamış Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi]. İstanbul.

Gündüz, M. Z., & Daş, R. (2016). Sosyal mühendislik: yaygın ataklar ve güvenlik önlemleri. *9.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*, Ankara.

Güngör, M. (2015). *Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma*. T.C. Kalkınma Bakanlığı Bilgi Toplumu Daire Başkanlığı, Yayın, (2919).

Hadlington, L., & Chivers, S. (2020). Segmentation analysis of susceptibility to cybercrime: exploring individual differences in information security awareness and personality factors. *Policing: A Journal of Policy and Practice, 14*(2), 479-492.

Henkoğlu, T., & Yılmaz, B. (2013). Avrupa Birliği (AB) bilgi güvenliği politikaları. *Türk Kütüphaneciliği Dergisi, 27*(3), 451-471.

Instant Security Policy. (2010). *IT security policy guide*. Durham: InstantSecurityPolicy.

ISACA. (2018). *COBIT 2019 framework: Introduction and methodology*. Schaumburg, USA: ISACA.

ISACA. (2019). *COBIT 5 implementation – Supplemental tools and materials*. USA: ISACA.

ISACA. (2022). ISO/IEC, (2022). *IT audit framework (ITAF)* (4th ed.). https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko91EAC

ISO 27001 vs. ISO 27002. (t.y.). *ISO 27001 vs. ISO 27002: Understanding the difference içinde*. https://www.nemko.com/iso-27001-vs-iso-27002

İleri, Y. Y. (2017). Örgütlerde bilgi güvenliği yönetimi, kurumsal entegrasyon süreci ve örnek bir uygulama. *Anadolu Üniversitesi Sosyal Bilimler Dergisi, 17*(4), 55-72.

Kalman, S. (2003). *Web security field guide*. Indianapolis: Cisco Press, 36-37.

Kaur, J., & Mustafa, N. (2013). Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. In 2013 *International Conference on Research and Innovation in Information Systems (ICRIIS)*, 286-290.

Kävrestad, J., Hagberg, A., Nohlberg, M., Rambusch, J., Roos, R., & Furnell, S. (2022). Evaluation of contextual and game-based training for phishing detection. *Future Internet, 14*(4), 104.

Keser, H., & Güldüren, C. (2015). Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) geliştirme çalışması. *Kastamonu Üniversitesi Kastamonu Eğitim Dergisi, 23*(3), 1167-1184, Kastamonu.

Keser, H., & Yayla, H. G. (2021). Fatih projesi uygulanan okullardaki öğretmenlerin bilgi güvenliği farkındalık düzeylerinin incelenmesi. *Milli Eğitim Dergisi, 50*(229), 9-40.

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security, 106*, 102267.

Kınay, H., Sözcü, Ö. F., Taşkın, E., & İpek, İ. (2014). Bilgi güvenliği farkındalığı ölçeğinin ilk bulguları. *8. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu*, 18-20 Eylül 2014, Trakya Üniversitesi, Edirne.

Köktürk, E., & Avcı, Ü. (2019). Kurumsal bilgi güvenliği farkındalığı üzerine bir çalışma. 7th International Instructional Technologies and Teacher Education Symposium ITTES 2019 Abstract Book.

Kraus, A. (2018). *Developing an information security strategy* [Yüksek Lisans Tezi, St Pölten Üniversitesi]. Avusturya.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296.

Kruger, H., Drevin, L., Steyn, T. (2010) A vocabulary test to assess information security awareness. *Information Management & Computer Security, 18*(5), 316-327.

Kuru, H., & Ocak, M.A., (2016). Determination of Cyber Security Awareness of Public Employees and Consciousness-rising Suggestions, *Journal of Learning and Teaching in Digital Age, 1*(2), 57-65.

Lin, H. F. (2007). Predicting consumer intentions to shop online: An empirical test of competing theories. *Electronic Commerce Research and Applications*.

Luma, A., & Abazi, B. (2019). The importance of integration of information security management systems (ISMS) to the organization's enterprise information systems (EIS). *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1.

Ma, Q., & Liu, L. (2005). The technology acceptance model: A meta-analysis of empirical findings. *Journal of Organizational and End User Computing (JOEUC), 16*(1), 59-72.

Maden, B. (2024). *Enerji sektöründe bilgi güvenliği yönetim sistemlerinin etki analizi ve sonuçları* [Yüksek Lisans Tezi, Gazi Üniversitesi]. Ankara.

Marikyan, D., & Papagiannidis, S. (2023). Protection motivation theory: A review. In S. Papagiannidis (Ed.), *TheoryHub Book*. https://open.ncl.ac.uk / ISBN: 9781739604400

Mart, İ. (2012). *Bilişim kültüründe bilgi güvenliği farkındalığı* [Yüksek lisans tezi, Kahramanmanraş Sütçü İmam Üniversitesi]. Kahramanmaraş.

Maurer, C. C., Bansal, P., & Crossan, M. M. (2011). Creating economic value through social values: Introducing a culturally informed resource-based view. *Organization Science, 22*(2), 432-448.

Meral, S. (2022). *Kamu kurumlarının bilgi güvenliği politikalarının kurumsal bilgi güvenliğinin sağlanması açısından etkinliğinin analiz edilmesi* [Yüksek Lisans Tezi, Gazi Üniversitesi]. Ankara.

Nezgitli, S. (2021), *İngiltere ve Türkiye'nin siber güvenlik politikalarının karşılaştırılması.* [Uzmanlık Tezi, Radyo ve Televizyon Üst Kurulu Strateji Geliştirme Dairesi Başkanlığı]. Ankara.

Okul, T., Şimşek, G., Hafçı, B., & Barış, Z. (2018). Bilgi güvenliği farkındalığı: Kuşadası'ndaki konaklama işletmesi yöneticileri üzerine bir uygulama. *Uluslararası Türk Dünyası Turizm Araştırmaları Dergisi, 3*(2), 189-201.

Özbey, K. M. (2024). *Bilgi güvenliği farkındalıklarının incelenmesi: Teknopark örneği* [Yüksek Lisans Tezi, Bahçeşehir Üniversitesi]. İstanbul.

Özbilen, T., & Çağlar, A. (2020). Türk kamu sektöründe bilgi ve bilişim güvenliği. *Kamu Yönetimi ve Teknoloji Dergisi, 2*(1), 72-93.

Özbilen, T., & Çağlar, A. (2020). Türk kamu sektöründe bilgi ve bilişim güvenliği. *Kamu Yönetimi ve Teknoloji Dergisi*, *2*(1), 72-94.

Özdemir, A. (2019). *Kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı*. [Yüksek Lisans Tezi]. Ankara.

Özdemir, A., & Uluyol, Ç. (2021). Kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı. *Türkiye Sosyal Araştırmalar Dergisi*, *25*(3), 649-666.

Özkan, Y., & Tuncer, G (2021). Bilgi güvenliği ve yönetim standartlarına üzerine bir inceleme. *Bilgi Güvenliği Dergisi*, 9 (2), 45-57.

Öztemiz, S. & Yılmaz, B. (2013). Bilgi merkezlerinde bilgi güvenliği farkındalığı: Ankara'daki üniversite kütüphaneleri örneği (Awareness of information security in information centers: sample of academic libraries in Ankara). *Bilgi Dünyası, 14*(1), 87-100.

Öztezcan, B.A. (2017). *Bilgi güvenliği farkındalığı üzerine bir araştırma: Marmara Üniversitesi örneği.* [Yayınlanmamış Yüksek Lisans Tezi. Marmara Üniversitesi]. İstanbul.

Öztürk, G. (2008). *Bilgi güvenliği politikası oluşturma kılavuzu*. Kocaeli: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü.

Öztürk, Ö. (2009*). E-postalarda spam sorunu ve çözüm önerileri* [Uzmanlık tezi, Bilgi Teknolojileri ve İletişim Kurumu]. Ankara.

Page, B. B. (2017). Exploring organizational culture for information security in healthcare organizations: A literature review. In 2017 *Portland International Conference on Management of Engineering and Technology (PICMET),* 1- 8. IEEE.

Privia. (2023, 12 Şubat). Bilgi güvenliği farkındalık eğitiminin faydaları. https://www.priviasecurity.com/bilgi-guvenligi-farkindalik-egitimininfaydalari/

Rogers, R. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93-114.

Saban, K. A., Rau, S., & Wood, C. A. (2021). SME executives' perceptions and the information security preparedness model. *Information & Computer Security, 29*(2), 263-282.

Seyhan, B. G. (2013). *Okulöncesine devam eden çocukların sağlık algılarının incelenmesi* [Yüksek Lisans Tezi, Ege Üniversitesi Sosyal Bilimler Enstitüsü]. İzmir.

Subagyo, E. P., & Ramli, K. (2022). Analyzing the Impact of Information Security Awareness Training to the Employees of Telco Company XYZ. *Budapest International Research and Critics Institute (BIRCI-Journal): Humanities and Social Sciences, 5*(2), 8799-8808.

Şahinaslan Ö. (2013). *Siber saldırılara karşı kurumsal ağlarda oluşan güvenlik sorunu ve çözümü üzerine bir çalışma* [Doktora tezi, Trakya Üniversitesi]. Edirne.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., & Borandağ, E. (2009). Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri. *Akademik Bilişim, 9*, 11-13.

Takemura, T., Tanaka, H., & Matsuura, K. (2011). Analysis of awareness gap between security managers and workers in an organization with regard to the effectiveness of the information security measures. *Journal of Information Processing, 19*, 253-262.

Tekerek, M., & Tekerek, A. (2013) A research on students' information security awareness, *Turkish Journal of Education, 2*(3), Kahramanmaraş.

Turan, A. H. (2011). İnternet alışverişi tüketici davranışını belirleyen etmenler: Planlı Davranış Teorisi (TPB) ile ampirik bir test. *Doğuş Üniversitesi Dergisi, 12*(1), 128-143.

TÜBİTAK BİLGEM YTE. (2021). *Bilgi güvenliği ve yönetimi rehberi: İşletim ve bakım*. Dijital Kabiliyet Rehberleri. Kocaeli: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu, Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi, Siber Güvenlik Enstitüsü.

UDHB (2019, 17 Mart). http://ulk.ist/destekleyen-kuruluslar/tc-ulastirma-denizcilik-vehaberlesme-bakanligi/

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198.

Vural, Y. (2007). *Kurumsal bilgi güvenliği ve sızma penetrasyon testleri* [Yüksek Lisans Tezi, Gazi Üniversitesi]. Ankara.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security.* Cengage Learning.

Whitman, M. E., & Mattord, H. J. (2019). *Management of information security*. Boston: Cengage.

Xu, J., Wang, X., & Yan, L. (2021). The moderating effect of abusive supervision on information security policy compliance: Evidence from the hospitality industry. *Computers & Security, 111,* 102455. https://doi.org/10.1016/j.cose.2021.102455.

Yıldız, M. (2014). *Siber suçlar ve kurum güvenliği*. [Yayınlanmamış Uzmanlık Tezi, Ulaştırma Denizcilik ve Haberleşme Bakanlığı Bilgi İşlem Dairesi Başkanlığı]. Ankara.

Yılmaz, E., Şahin, Y. L. & Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya University Journal of Education, 6*(2), 26-45. DOI: 10.19126/suje.29650

Zhen, J., Dong, K., Xie, Z., & Chen, L. (2022). Factors Influencing Employees' Information Security Awareness in the Telework Environment. *Electronics, 11*(21), 34-58. DOI: https://doi.org/10.21203/rs.3.rs-1544020/v2

EK

Ek 1: Anket Formu

(BİLGİ GÜVENLİĞİ FARKINDALIK DÜZEYİ ANKETİ)

Sayın Katılımcı;

Bu anket bireylerin bilgi güvenliklerindeki farkındalıklarını ölçmeye yöneliktir. Bu anketle toplanan veriler sadece akademik çalışmalarda kullanılacaktır. Sizden kurum veya isim bilgileriniz istenmeyecektir. Lütfen soruları içtenlikle cevaplayınız. Anket ile ilgili soru, görüş ve düşünceleriniz için bizimle iletişime geçebilirsiniz.

Mehmet KÖSE

Danışman: Prof. Dr. Serkan ADA

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.

1. Cinsiyetiniz	: Erkek ( ) Kadın ( )
2. Medeni durumunuz	: Bekar ( ) Evli ( )
3. Yaşınız	: 18-25 ( ) 26-33 ( ) 34-41 ( ) 42-49 ( ) 50 ve üzeri ( )
4. Öğrenim Durumunuz	: İlköğretim ( ) Lise ( ) Ön lisans ( ) Lisans ( )Lisansüstü ( )
5. Meslekteki Toplam Hizmet Süreniz	: 1-5 yıl ( ) 6-10 yıl ( ) 11-15 yıl ( ) 16 ve üzeri yıl ( )
6. Çalışma Sınıfınız	: Memur ( ) İşçi ( )
7. **İş Yerindeki Pozisyonunuz**	: Personel ( ) Yönetici ( )

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

BG 19	Kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum.					
BG 20	Bilgi sistemlerinde kullanılan virüs koruma yazılımını nasıl kullanacağımı biliyorum.					
BG 21	Bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (realtime protection) özelliğini kullanmaktayım.					
BG 22	Bilgisayarımdaki virüs koruma yazılımının otomatik güncelleştirme yapmasını sağlayabilirim.					
BG 23	Dijital imza (digital signature) nedir biliyorum.					
BG 24	Şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum.					
BG 25	E-posta gönderirken "Gizli" (BCC) alanının sağladığı avantajları biliyorum.					
BG 26	İstenmeyen elektronik posta (spam) nedir biliyorum.					
BG 27	İstenmeyen elektronik posta miktarını azaltmak için gerekli bilgiye sahibim.					
BG 28	Sosyal ağ sitelerini (social networking sites) güvenli olarak nasıl kullanacağımı biliyorum.					
BG 29	USB sürücülerini (USB drives) kullanırken dikkat edilmesi gereken hususları biliyorum.					
BG 30	Taşınabilir cihazlara (portable devices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum.					
BG 31	Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.					
BG 32	Kişisel mahremiyet nedir biliyorum.					
BG 33	Çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum.					
BG 34	Mavidiş (Bluetooth) teknolojisi ile veri aktarımı konusunda bilgi sahibiyim.					

ÖZGEÇMİŞ

Ad Soyad: Mehmet KÖSE	
Eğitim Bilgileri	
Lisans	
Üniversite	Anadolu Üniversitesi
Fakülte	İşletme Fakültesi
Bölümü	İşletme
Makale ve Bildiriler	
1. SOCIAL SCIENCES STUDIES International Refereed & Index ISSN:2587-1587 2019-49 Yeşil Tedarik Zinciri Uygulamalarının İşletme Performansı ve Rekabet Edebilirliğe Etkisi- İmalat Sanayisinde Bir Firma Analizi ve Uygulaması	

T.C.

KARAMANOĞLU MEHMETBEY ÜNİVERSİTESİ

SOSYAL ve BEŞERİ BİLİMLER

BİLİMSEL ARAŞTIRMA VE YAYIN ETİK KURULU KARARLARI

Toplantı Tarihi	Toplantı Sayısı	Karar Sayısı
07.08.2023	**13**	**215-221**

Üniversitemiz Sosyal ve Beşeri Bilimler Bilimsel Araştırma Yayın Etik Kurulu Prof. Dr. İbrahim COŞKUN başkanlığında 07.08.2023 günü saat 10.00'da toplanarak aşağıdaki kararları almıştır.

KARAR 13-2023/217. Üniversitemiz Sosyal Bilimler Enstitüsü Yönetim Bilişim Sistemleri Anabilim Dalı yüksek lisans öğrencisi Mehmet KÖSE'nin, Prof. Dr. Serkan ADA danışmanlığında yapacağı **"Kamu Çalışanlarının Bilgi Güvenliği Konusundaki Farkındalık Düzeyleri Üzerine Bir Araştırma"** başlıklı çalışmaya ait uygulayacakları yönteme ilişkin gerekli izinlerin alınması kaydıyla fikri, hukuki ve telif hakları bakımından sorumluluğu başvuran kişiye ait olmak üzere etik olarak uygun olduğuna oy birliği ile karar verildi.

(e-imza)
Prof. Dr. İbrahim COŞKUN
Başkan

(e-imza)
Prof. Dr. Ercan OKTAY
Üye

(e-imza)
Prof. Dr. Özlem SADİ
Üye

(e-imza)
Prof. Dr. Mehmet MERCAN
Üye

(e-imza)
Prof. Dr. Murat TEKİN
Üye

(e-imza)
Prof. Dr. Mehmet KURT
Üye

Ferdane YAŞAR

Raportör