Makale Türü/Article Type: Araştırma Makalesi/Research Article

SİBER SALDIRILARA KARŞI KOBİLERİN FARKINDALIK DÜZEYLERİNİN İNCELENMESİ: ANKARA İLİ ÖRNEĞİ

Abdulhamit EŞ[1], Nurşah SERDAR[2]

Öz

Son yıllarda siber saldırı ve suçlarının internet teknolojisindeki gelişmeye paralel olarak büyük bir artışa geçtiği görülmektedir. Bu artış işletmeler açısından ciddi bir güvenlik riskine yol açmakta ve işletmeler için büyük bir tehdit oluşturmaktadır. İşletme yönetici ve yetkililerinin bu tehditlere karşı tedbir almaması işletmelerin sahip olduğu bilgi ve sermaye unsurlarını savunmasız bırakmaktadır. Türkiye'deki işletmelerin çoğunluğunu oluşturan KOBİ'lerin siber saldırılara daha çok maruz kaldığı KOBİ yöneticilerinin siber saldırılara karşı tedbir almaları kaçınılmazdır. Bu çalışmada KOBİ'lerin maruz kaldığı siber saldırılara kaşı çalışanların bilgi farkındalık düzeyleri analiz edilmiştir. Çalışmanın verileri Ankara'daki KOBİ çalışanlarının anket sorularına verdikleri cevaplardan elde edilmiştir. Çalışanların bilgi farkındalık düzeyleri çeşitli demografik özelliklerine göre T testi ve ANOVA testi ile analiz edilmiştir. Cinsiyete göre çalışanların bilgi farkındalık düzeyleri arasında anlamlı bir farklılık bulunmazken, orta ve üst düzey yöneticilerinin diğer pozisyondaki çalışanlara göre, yaşlıların gençlere göre, lisans mezunlarının diğer alt eğitim düzeylerine göre, yüksek gelir düzeyine sahip çalışanların daha az gelir düzeyine göre, karmaşık şifre belirleyenlerin basit şifreleme kullananlara göre daha yüksek bilgi farkındalığına sahip olduğu belirlenmiştir.

Anahtar Kelimeler: *Siber Saldırı, KOBİ, Siber Güvenlik, Bilgi Farkındalık Düzeyi*

INVESTIGATION THE AWARENESS LEVELS OF SMEs AGAINST CYBER ATTACKS: CASE OF ANKARA

Abstract

In recent years, it is seen that cyber attacks and crimes have increased in parallel with the development in internet technology. This increase leads to a serious security risk for businesses and poses a great threat to businesses. The fact that business managers and officials do not take precautions against these threats leaves the information and capital elements of businesses vulnerable. It is inevitable that SME managers, who make up the majority of businesses in Turkey, are more exposed to cyber attacks, to take precautions against cyber attacks. In this study, information awareness levels of employees against cyber attacks that SMEs are exposed to were analyzed. The data of the study were obtained from the answers given by the SME employees in Ankara to the survey questions. Employees' knowledge awareness levels were analyzed by T test and ANOVA test according to their various demographic characteristics. There was no significant difference between the knowledge awareness levels of the employees by gender. It has been determined that middle and senior managers compared to the employees in other positions, the elderly compared to the young, undergraduate graduates compared to other lower education levels, the employees with high income levels compared to have a lower income level and those who set complex passwords compared to those who use simple encryption have higher information awareness.

Keywords: Cyber Attacks, SME, Cyber Security, Information Awareness Level

[1] Dr. Öğr. Üyesi, Bolu Abant İzzet Baysal Üniversitesi, İşletme Bölümü, abdulhamit.es@gmail.com, orcid: 0000-0002-4120-0768

[2] Bolu Abant İzzet Baysal Üniversitesi, İşletme Anabilim Dalı, İşletme Tezli Yüksek Lisans, nursahserdar@gmail.com, orcid: 0000-0002-4576-523X

Bu Yayına Atıfta Bulunmak İçin/Cite as: Eş, A. ve Serdar, N. (2021). Siber saldırılara karşı kobi'lerin farkındalık düzeylerinin incelenmesi: Ankara ili örneği, *Düzce Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11*(1), 133-151.

Makale Geliş Tarihi:17/05/2021 Makale Kabul Tarihi:27/07/2021 Makale Yayın Tarihi:30/07/2021

1. Giriş

Bilgi ve iletişim teknolojilerinin son yüz yılda hayatın her alanında kullanılması birçok avantaj ve dezavantajı beraberinde getirmektedir. Teknolojik gelişmelere işletmeler arasındaki fiziksel mesafeler ortadan kaldırılmakla bilgi ve ihtiyaçların elde edilmesi çok daha kolay ve hızlı hale gelmektedir. Elektronik imza, e-posta, bulut teknolojisi vb. birçok bilgi teknolojileri işletmelerin siber güvenlik problemini ortaya çıkarmaktadır. Bilgi teknolojisi güvenliği veya elektronik bilgi güvenliği olarak da bilinen siber güvenlik, internet ortamında bilgisayarları, sunucuları, ağları ve verileri, kurum, kuruluş ve kullanıcıların karşılaşabilecekleri risklere karşı güvenliğini sağlamak için kullanılan bir uygulamadır. Temel hedefi, gizlilik, bütünlük ve erişilebilirliktir.

İşletmelerin internet, intranet ve ekstranet gibi teknolojileri kullanması ve çalışanların birçoğunun internete bağlantılı işlemler yürütmesi işletmeleri elektronik saldırıların hedefi haline getirmiştir(Özmen, 2013:489). Küresel risklerle ilgili en son yayınlanan Dünya Ekonomik Forumu (WEF) raporu, siber saldırıların hem etki hem de gerçekleşme olasılığı açısından büyük riskler arasında olduğunu doğrulamaktadır. Türkiye ekonomisinde önemli rollerden birini üstlenen küçük ve orta büyüklükteki işletmeler (KOBİ) tüm işletmelerin % 99.77'sini, toplam istihdamın % 78'ini, toplam katma değerin % 55'ini, toplam satışların % 65.5'ini, toplam yatırımların % 50'sini, toplam ihracatın % 60.1'ini, toplam kredilerin % 24'ünü gerçekleştirmektedir (Bilim, Sanayi ve Teknoloji Bakanlığı, 2016). Ülkelerin ekonomik ve sosyal kalkınmasının temel taşını oluşturan KOBİ'ler stratejik pazarlarda varlıklarını sürdürmek için teknolojiyi çok iyi kullanmaları ve siber saldırılar karşısında gerekli tedbirleri almak zorundadırlar. Büyük şirketlere göre daha az korunan ve risklerden habersiz olan KOBİ'ler, siber ortamda meydana gelen saldırının boyutunu çoğu zaman tespit edemezler. Bunun yanı sıra firma çalışanlarının, yöneticilerinin bilgi güvenliği konusunda yeteri kadar donanıma sahip olmaması ve KOBİ'lerin finansal kaynaklarının kısıtlı olması, yeterli teknik bilgiye ve deneyime sahip olmamaları nedeniyle her türlü siber saldırıya ve bu saldırılardan doğabilecek zararlara karşı savunmasız kalmaktadır.

Birleşik Krallık hükümeti tarafından yakın zamanda yapılan araştırmaya göre, KOBİ'lerin üçte ikisinden fazlasının hiçbir zaman siber suç mağduru olabileceklerini düşünmediğini ortaya koymuştur. Ancak Price waterhouse Coopers (PWC) tarafından yayınlanan rapor, KOBİ'lerin %60'ının bilgisayarlarının ihlal edildiğini ve siber saldırıların hafife alınmaması gerektiğini göstermektedir (Lecisotti, 2015:10).

İşletmelere yönelik yapılan siber saldırılarda sisteme yetkisiz erişim, sistemin bozulması veya engellenmesi, bilgilerin değiştirilmesi, yok edilmesi, ifşa edilmesi ve çalınması gibi çeşitli yollarla, KOBİ'lerin faaliyetlerinin kesintiye uğramasına, itibarına zarar vermesine ve varlığını tehlikeye atmanın yanı sıra gelir kaybı, müşteri ve yatırımcı güven kaybına neden olmak gibi birçok mali yükü beraberinde getirmektedir(Atalay, 2014). Oluşan bu mali yükün tespiti ve olayın ne kadar ciddi olduğunu gösteren çeşitli şirketlerin yapmış olduğu araştırmalar bulunmaktadır. Bunlardan bazıları veri ihlalini engellemek üzerine yapılan harcamaları ve siber saldırı oranlarını ön plana çıkarırken bazı araştırmalarda veri sızıntısı ve veri kaybından kaynaklanan maliyeti ön plana çıkarmaktadır(Çetin vd., 2015). KOBİ'lerin siber suçların neden olduğu zararı hafifletmek, farkındalık oluşturmak, gerekli yazılım ve donanım önlemlerini almak, çalışanlarını tehditler hakkında bilgilendirmek, güvenlik tehditleriyle ilgili gelişmeleri takip etmek ve güvenlik varlıklarını artırmak için desteğe ihtiyacı olduğu bulunmaktadır.

Bu çalışmada giriş bölümünden sonra literatür bölümünde KOBİ'lerin temel özellikleri, siber güvenlik ve siber saldırı kavramları açıklandıktan sonra siber güvenlik ve siber saldırı alanında literatürde yer alan çalışmalara yer verilmiştir. Yöntem kısmında çalışmanın amacı, anakütle

örneklemi, önemi ve kullanılan ölçekler hakkında bilgiler verilmiş, kullanılan analiz teknikleriyle elde edilen değerler bulgular kısmında yazılarak sonuç kısmında tartışılmıştır.

2. Literatür

2.1 KOBİ'lerin Tanımı

2018 yılında Bilim, Sanayi ve Teknoloji Bakanlığı, Gümrük ve Ticaret Bakanlığı, Avrupa Birliği (AB) Bakanlığı, Kamu Gözetimi Kurumu (KGK), Türkiye Esnaf ve Sanatkarları Konfederasyonu (TESK), Türkiye İstatistik Kurumu (TÜİK), Küçük ve Orta Ölçekli İşletmeleri Geliştirme ve Destekleme İdaresi Başkanlığı (KOSGEB) katılımıyla oluşturulan yeni yönetmeliğe göre KOBİ, "250 kişiden az yıllık çalışan istihdam eden ve yıllık net satış hasılatı ya da mali bilançosu 125 milyon lirayı aşmayan ve yönetmelikte mikro işletme, küçük işletme ve orta büyüklükte işletme olarak sınıflandırılan ekonomik birimler"dir. 2018 yılı itibariyle KOSGEB veri tabanına kayıtlı işletme sayısı 1.417.995'e ulaşmıştır (KOSGEB, 2018).

Günümüz küresel ekonomik şartlarında KOBİ'ler büyük ölçüde internet ve bilgi teknolojilerine bağımlıdırlar. Ancak BT Güvenliği söz konusu olduğunda, çoğu KOBİ'nin genellikle sistemlerini siber tehditlere karşı koruyacak bilgi korumayla ilgili kurumsal politikalar ve görevler oluşturacak teknik uzmanlık ve bilgiye sahip olmadıklarını görülmektedir.

Son yapılan araştırmalara göre Türkiye'de gerçekleştirilen siber saldırıların %71'inin KOBİ'lere yönelik olduğu ortaya konmuştur. KOBİ'ler için siber saldırı riskinin ise %61'e yükseldiğini söyleyen uzmanlar, siber güvenlik okur-yazarlılığının düşük olduğu KOBİ'lere karşı tehditlerin giderek artacağını öngörüyor. Bu bağlamda bütçe kısıtlamaları veya personel eksikliği nedeniyle KOBİ'ler için siber saldırılara karşı güçlü güvenlik önlemleri uygulamak ve internet güvenliği ihlallerini kontrol etmek oldukça zordur.

Ponemon Enstitüsü tarafından yakın zamanda yapılan bir araştırma, KOBİ'lerin karşılaştığı siber güvenlik zorluklarına dair net bir çerçeve sunmaktadır. "KOBİ'lerde Küresel Siber Güvenlik Durumu" isimli raporda üst üste üç yıl, KOBİ'lerdeki güvenlik ihlallerinde önemli bir artış olduğu bildirilirken, aynı zamanda işletmelerin veri ihlallerini tespit etme süresinin de ortalama 197 gün sürdüğü belirtilmektedir(CyberMag, 2020). National Technology Security Coalition tarafından yapılan araştırmada 2019 yılında dünya çapındaki tüm işletmelerin %28'inin DDoS saldırılarına maruz kaldığı ve bu saldırıların başarılı olması fidye yazılımı gibi yıkıcı sonuçlara neden olabildiği belirtilmektedir. Aynı araştırmada global tüm kuruluşların %27'sinin mobil ve bulut platformlarına yönelik saldırılardan etkilendiği ve 2019 yılının çalışan ve müşteri bilgilerinin çalınmasına dair rekor sayıda veri ihlali olduğu raporlanmıştır (Ntsc, 2020: 22,23). Ayrıca yapılan araştırmalar işletmelerin uğradığı siber saldırıların her geçen gün daha da arttığını ve buna bağlı olarak marka ve imaj kayıplarının yanı sıra bir takım finansal kayıplarla da karşı karşıya kaldıklarını ortaya koymaktadır.

Zurich Insurance'nin 2019 yılında yayınladığı rapor hızlı dijitalleşmenin ve nesnelerin internetinin gelişmiş dünyanın ve altyapısının bağlantısını genişlettiğini ortaya koyarken (Mangat, M. 2020), ABD merkezli KOBİ'lere finansman desteği sağlayan Fundera'nın KOBİ'ler üzerinde gerçekleştirdiği siber güvenlik araştırmaları ise, siber saldırıların yarısının KOBİ'lere yönelik gerçekleştiğini ve büyük çoğunluğunun BT güvenliğinden sorumlu uzman çalışana sahip olmamasından kaynaklı olduğunu ortaya koymaktadır. Özellikle küresel ortamda KOBİ'lerin yılda 2.2 milyon dolarlık bir zarara uğramasının nedeni olan saldırganların yaptıkları saldırılarda başarıya ulaşma konusunda çok da zorlanmadıklarına dikkat çekilmiştir. Uzmanlar 2020 yılında işletmelerin neredeyse %25'inin IoT cihazları aracılığıyla veri ihlallerine yenik düştüğünü belirtilmiştir. Siber saldırılara uğrayan KOBİ'lerin %60'ının ABD'de 6 ay sonra iş faaliyetlerini sonlandırdığı da

düşünüldüğünde, finansal ve itibar kaybı yaşamak istemeyen KOBİ'lerin dikkat etmesi gereken siber güvenlik adımlarının olduğu belirtilmektedir (Hürriyet, 2020).

2.2 Siber Güvenlik ve Siber Saldırı

KOBİ ve Kurumların penceresinden siber güvenlik kavramına bakıldığında bilgi güvenliği kavramı sıkça karşımıza çıkmaktadır. Bilgi güvenliği, bilginin işlenirken, depolanırken ve taşınırken izinsiz veya yetkisiz bir biçimde erişimi, kullanımı, değiştirilme, yeni veriler ekleme, silinme, el değiştirme ve hasar verilmesini önlemek olarak tanımlanırken, "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç temel unsurdan oluşmaktadır. Başaranoğlu (2016), bu unsurları şu şekilde tanımlamaktadır:

- **Gizlilik:** Bilginin işlenirken, depolanırken ve taşınırken yetkisiz kişilerin eline geçmesinin engellenmesi ve yetkisiz erişimlerden korunmasıdır.
- **Bütünlük:** Bilginin yetkisiz kişiler tarafından bozulmasının, yeni veriler eklenmesinin, silinmesinin ve değiştirilmesinin engellenmesidir.
- **Erişilebilirlik:** Bilginin ihtiyaç duyulduğu zaman tam ve eksiksiz olarak ulaşılabilir ve kullanılabilir durumda olmasıdır.

Siber güvenlik; bilgi teknolojisi güvenliği olarak bilinen ve bireylerin, kurumların veya hükümetlerin bilgi işlem sistemlerini güvenilir bir şekilde sürdürebilmesini sağlamanın yanı sıra siber saldırılara ve izinsiz erişimlere karşı koruyan uygulama olarak bilinmektedir.

Ürünlerini pazarlamak ve potansiyel müşterilere ulaşmak için sosyal ağları aktif kullanan KOBİ'ler, Siber suçlardan etkilenme ihtimalleri oldukça yüksektir. Bilgisayar korsanları ve diğer siber suçluların saldırıları sonucunda KOBİ'ler yaşayacakları finansal kayıpların yanı sıra, KOBİ'lerin marka ve imaj kayıplarıyla birlikte müşterilerinin güvenini kaybetme riski ile de karşı karşıya kalmalarıdır. Başlıca siber saldırıları aşağıdaki şekilde sıralamak mümkündür;

- **Phishing (Oltalama) Saldırıları:** Rastgele kullanıcı hesaplarına e-mail gönderilerek şifreleri ve kredi kartı bilgilerini çalmaya yönelik yapılan bir tür çevrimiçi saldırıdır.
- **Kötü amaçlı yazılım:** Bir kullanıcının bilgisayarına zarar vermek üzere tasarlanmış bir program veya dosyadır.
- **DoS ve DDoS:** Bazı çevrimiçi hizmetlerin düzgün çalışmasını engellemeye çalışmak için yapılan saldırılardır. Yani başka bir deyişle, saldırganlar sistemi meşgul etmek amacıyla bir web sitesine veya bir veri tabanına çok sayıda istek yollarlar ve bu da sistemlerin durmasına neden olur.
- **SQL Injection:** Bu yöntemde SQL güvenlik açıklarından faydalanılarak veri tabanları kontrol altına alınır.

Siber Güvenlik ve siber saldırı alanında literatürde yer alan çalışmalara aşağıda değinilmiştir. Çalışmaların Siber saldırılara karşı kullanılacak program ve yazılımlara ve kurumların uğradığı finansal kayıplara odaklandığı görülürken, personellerin bilgi farkındalığına dair bir çalışma bulunmamaktadır.

Önder ve Ender Şahinaslan (2019: 494) ise, yaptığı araştırmalarda Symantec güvenlik firmasının 2012 yılında yapmış olduğu "Endpoint Security En İyi Uygulamalar Araştırması" sonucuna göre 2011 yılında araştırmaya katılan ülkelerden 1.425 kurumun %81'inin siber saldırılara maruz kaldığını belirtmiştir. Ortaya çıkan en belirgin kayıplar arasında kurumsal kimliğin ve marka imajının zarar gördüğü, motivasyon kaybının yaşandığı, müşterilere ya da personele ait veri ihlallerinin yaşandığı belirtilmiştir. Symantec tarafından 2012 yılında yapılan bu araştırmada,

siber saldırıların şirketlere verdiği zararlardan doğan finansal kaybın 470.000$ olduğu belirtilmektedir. 2011 yılında Britanya'da gerçekleşen siber saldırıların ülke ekonomisine maliyetinin 27 milyar pound olduğu, ABD'de ise gerçekleşen siber saldırılardan kaynaklı finansal kayıpların oldukça yüksek bir rakama ulaştığı raporlanmaktadır. Bu bağlam da işletmeler için başarılarının devamlılığını sürdürmeleri açısından cari sermayelerini korumak, veri ihlalleri karşısında depolanan verilerin türünü, nerede depolandığını, veri güvenliği ve kurtarma eylemlerini uygularken olası yükümlülüklerin neler olduğunu özetleyebilmek adına "iş sürekliliği planı" na sahip olmak, bunların yanı sıra marka ve imajlarını da korumaya çalışmak ve siber saldırıları kurumsal sistemleri ihlal etmeden önce önlemek stratejik zorunluluk olmalıdır.

Boateng ve Osei (2013), yaptıkları araştırmada güvenlik açıklarının çok sayıda tehdit tarafından istismar edildiğinden, KOBİ'lerin bu durumdan olumsuz etkilendiğini ve bunun da bazı durumlarda işletmenin kapanmasına neden olabileceğini belirtmişlerdir. Son zamanlarda siber saldırıların kapsamının artmasıyla uzmanlar, bu konuda hiçbir şey yapılmazsa gelecekteki saldırıların ciddiyetinin bugüne kadar gözlemlenenden çok daha büyük olabileceğine inanıyorlar. Ayrıca yapmış oldukları araştırmada, bu güvenlik açıklarının ortaya çıkma ve ele alınma hızının belirsiz olduğunu da vurgulamışlardır. Bu durum, KOBİ'lerin sık sık güvenlik açığı değerlendirmesine tabi tutulmasını gerekli kılmaktadır.

Dr. Göztepe ve diğerleri (2014), yaptıkları çalışmada Estonya'da 2007 yılında gerçekleşen siber saldırıların, siber tehdit kavramının dikkate alınması açısından dünyayı alarma geçirmesi hususunda dönüm noktası olması gerekirken, siber saldırılara maruz kalan ilk hedef ülkelerden biri olan Türkiye'nin, doğrudan veya dolaylı olarak bu saldırıların temeli haline geldiğini de belirtmişlerdir. İşletmelerde özellikle kullanıcı sayısının artmasının ve işletmenin büyümesinin bilgi güvenliği seviyesinde azalma meydana getireceğini vurgularlarken, dışarıdan gelecek saldırılara karşı önlem almanın yanında yerel alan ağ güvenliğinin de önemli bir husus olarak karşımıza çıktığını belirtmişlerdir. Ayrıca, çalışmada uygulama düzeyinde saldırıları önlemenin kullanıcı nedeniyle zor olduğu belirtilirken bu konuda fiziksel katmanda, ağda ve sistemde güvenliği sağlamaya yönelik geleneksel yaklaşımın, yazılım güvenliği ile tanımlanması gerektiği ve önümüzdeki on yıl içinde siber saldırıların, dünyadaki güvenlik için en büyük tehditlerden biri haline geleceği vurgulanmaktadır.

Nabila Amrin (2014), yaptığı çalışmada KOBİ veri güvenliğine yönelik en büyük 10 tehdidin bilinen bir güvenlik açığından otomatik olarak yararlanma, kötü amaçlı HTML e-posta, çalışanlar tarafından pervasız web sörfü, web sunucusu uzlaşması, taşınabilir bir cihazda veri kaybı, Wi-Fi etkin noktalarının dikkatsiz kullanımı, otel ağlarının ve kioskların dikkatsiz kullanımı, uzlaşmaya yol açan zayıf konfigürasyon, olasılık eksikliği, içeriden saldırılar olduğunu belirtirken güvenliği ihlal eden varlıkların ise bilgisayarların işletim sistemi, e-postayı görüntüleyen cihazlar, bilgisayarlar, dizüstü bilgisayarlar vb., web sitesi ve sunucu, Taşınabilir cihazlar ve veriler, Şirketin verileri, çalışanın cihazı, tüm internet ağı, tüm BT altyapısı, tüm BT altyapısı olduğunu vurgulamıştır.

İbrahim Kurnaz (2016), yaptığı çalışmada ağlara dayalı güvenlik kategorisinde bulunan siber saldırıların, dünya çapında sonuçları bakımından 21. yüzyılın önemli güvenlik tehditlerinden biri olduğunu belirtmiştir.

Kerem Yaylacı (2020), araştırmasında bir siber saldırı sonucunda oluşabilecek finansal kayıpların tam olarak hesaplanabilmesinin oldukça güç olmasının ötesinde şirketlerin çoğunlukla ağlarının siber saldırıya maruz kaldığını ve bunun sonucunda da oluşan bir takım hasarları müşteri, marka-imaj, güven kaybı ve yasal sorunlar gibi pek çok nedenlerden ötürü gizleme yoluna gittiğini belirtmiştir. Ayrıca buna ilişkin verilerin oldukça kısıtlı olduğunu da belirten Yaylacı, açıklanan bazı verilere bakıldığında maddi hasarın da oldukça yüksek olduğunu raporlamıştır.

Çetin vd. (2015), çalışmada siber güvenlik tehditleri ortaya konarak Türkiye'de ve Dünya'da e-ticaret üzerindeki etkileri incelenmiş ve siber saldırıların maliyetleri üzerinde durulmuştur.

Taner ve Kılıç (2019), Siirt'te görev yapan 404 emniyet personelinin bilgi güvenliği farkındalık düzeyleri anket çalışmasıyla belirlemiştir. Çalışmada personelleri saldırı ve tehditler alt faktöründe ve kişisel verileri koruma faktörlerinde elde edilen sonuçların yetersiz olduğu ve bilgi farkındalık düzeylerinin arttırılması için personele bu konular hakkında gerekli eğitimlerin verilerek tedbirlerin arttırılması gerektiği sonucuna ulaşılmıştır.

3. Yöntem

3.1 Araştırmanın Amacı

Siber güvenlik konusu özellikle son yıllarda birçok araştırmacının ilgi odağı haline gelmiş ve çalışmalara konu olmuştur. Yeni teknoloji sistemlerinin uygulanması, KOBİ'lerin işlerini yürütme şeklini değiştirmiştir. KOBİ'lerde hedeflere ulaşmak için kötü amaçlı yazılım, veri ihlalleri, güvenli olmayan ağ gibi açık riskleri dikkate almadan yeni teknolojiyi benimsemek iş dünyasında sorunlara yol açar. Bu çalışmanın temel amacı; Ankara'da faaliyet gösteren KOBİ'lerin siber güvenlik yönetimine ilişkin mevcut düzeylerinin analiz edilmesi ve siber güvenlik yönetimine ilişkin sorunlarının tespit edilmesidir.

3.2 Araştırmanın Önemi

National Technology Security Coalition tarafından yapılan araştırma da 2019 yılında dünya çapındaki tüm işletmelerin %28'inin DDoS saldırılarına maruz kaldığı belirtilmiştir. Bu tür bir saldırının başarılı olması fidye yazılımı gibi yıkıcı sonuçlara neden olabilmektedir. Aynı araştırmada global olarak tüm kuruluşların %27'sinin mobil ve bulut platformlarına yönelik saldırılardan etkilendiği ve 2019 yılının çalışan ve müşteri bilgilerinin çalınmasına dair rekor sayıda veri ihlali olduğu raporlanmıştır (Ntsc, 2020:22). Ayrıca yapılan araştırmalar işletmelerin uğradığı siber saldırıların her geçen gün daha da arttığını ve buna bağlı olarak marka ve imaj kayıplarının yanı sıra bir takım finansal kayıplarla da karşı karşıya kaldıklarını ortaya koymuştur. Dolayısıyla işletmeler bu tehditlere ve risklere karşı gereken önlemleri almak zorunda olsalar da çoğu işletme siber saldırıları önemsememektedir. Bu çalışma Ankara'da faaliyette bulunan KOBİ'lerin siber saldırılara yönelik bilgi güvenliği farkındalığının ve mevcut durumlarının analiz edilmesi açısından önem arz etmektedir.

3.3 Çalışmanın Evreni ve Örneklemi

Bu araştırmada Ankara ilinde varlığını sürdüren tüm KOBİ çalışanları ana kütle (evren) olarak kabul edilmiş ve örneklemin evreni daha iyi temsil edebilmesi için farklı sektörlerde faaliyet gösteren KOBİ çalışanlarına ulaşılmaya çalışılmıştır. Bu çalışma da kolayda örnekleme yöntemi tercih edilmiştir.

Araştırmada kullanılacak ana kütlenin büyüklüğü çalışmanın geçerliliği yönünde etkili olacaktır. Ölçek geliştirme çalışmaları incelendiğinde araştırmacılar örneklem büyüklüğü olarak 100 ve 200 ü zayıf, 300 ve 500 ü iyi olarak değerlendirirlerken 1000'i mükemmel olarak tanımlamışlardır (Çatuk, 2018:70). Bu nedenle bu çalışma da tek bir il üzerine odaklanılmasından dolayı toplam da 300-500 boyut aralığında bir veri seti kullanılmıştır.

3.4 Veri Setinin Toplanması

Araştırmaları yürütebilmek adına genellikle nitel, nicel ve karma olarak üç yöntem kullanılır. Araştırmada birincil veri toplama aracı olarak kullanılan anket, Google form da hazırlanarak katılımcılara internet ortamında ulaştırılmıştır.

Araştırmada nicel verilerin toplanması için iki kısımdan oluşan bir anket formu oluşturulmuştur. Birinci kısımda katılımcıların özelliklerini belirlemeye yönelik demografik soruların yanı sıra KOBİ'lerin bilgi güvenliklerine yönelik siber saldırılara karşı uyguladıkları yöntem ve teknikleri belirlemeye yönelik sorular sorulurken, ikinci kısımda çalışanların bilgi güvenliği farkındalığını belirlemeye yönelik 5'li likert tipi sorularla beraber şirket yöneticilerinin ve çalışanların olası bir siber saldırı da firmalarının yaşayacağı kayıpların farkında olup olmadıklarının ve herhangi bir siber saldırıya maruz kalıp kalmadıklarını, eğer maruz kaldılarsa bunun hem finansal hem de finansal olmayan açılardan işleri üzerindeki etkilerinin neler olabileceğine dair farkındalıklarını ölçmek adına açık uçlu sorular sorulmuştur ve açık uçlu soruların cevapları temalara bölünmüştür.

Elde edilen ham veri kümesinin istatistiksel analizinden önce, anketin KOBİ çalışanları tarafından eksiksiz bir şekilde doldurulup doldurulmadığı, sorulara bilinçli bir şekilde cevap verilip verilmediğini belirlemek amacı ile güvenilirlik ve küresellik çalışması yapılmıştır. Güvenilirlik Cronbach alpha, küresellik ise Barlett testi ve Kaiser Mayer Olkin(KMO) ölçütü ile saptanmıştır (Nunnally, 1967), (Barlett, 1950). Bu kapsam da verilen cevaplar incelenmiş ve eksik veya uç değer olmadığı saptanmıştır. Tablo 1 hesaplanan test sonuçlarını belirtmektedir.

Tablo1
Veri Seti Güvenilirlik ve Küresellik Değerleri

Ölçekler	N	KMO	Bartlett Test	Cronbach Alpha
Bilgi Güvenliği Farkındalığı	365	0,962	0,000	0,966

Tabloda görüldüğü üzere hesaplanan güvenilirlik istatistiği (Cronbach alpha) 0.96 olarak tespit edilmiştir. İdeal güvenilirlik seviyesinin %70'ten büyük olması verinin güvenilir ve yansız olduğunu ifade etmektedir (Nunnally, 1967). Bunun yanı sıra, Bartlett test istatistiği de korelasyonun yeterli olduğunu göstermektedir(0,00<0,05). Ayrıca, KMO ölçütü de "mükemmel" değer aralığında (1,00 ≤ KMO ≤ 0,90) çıkmıştır. Bu durum bize verilerin faktör analitik modeli ile modellenebileceğini göstermektedir (Field, 2000).

3.5 Veri Çözümleme Yöntemleri

Bu çalışmada, 365 kişinin anket sorularına vermiş olduğu cevaplardan açık uçlu sorular için temalar belirlenerek kodlanmış örüntüler ortaya çıkarılmıştır. Açık uçlu soruların temaları aşağıdaki gibidir:

- Olası bir siber saldırıda firmanızın yaşayacağı kayıplardan kaçınmak için alınacak önlemler:
  - Sistem ile ilgili önlemler: 1
  - Yedekleme ile ilgili önlemler: 2
  - Eğitim ile ilgili önlemler: 3
  - Kontrol ile ilgili önlemler: 4
- Siber saldırıya maruz kalındıktan sonra yaşanan kayıplar:
  - Veri kayıpları: 1
  - İmaj/Müşteri/Prestij kayıpları: 2
  - Finansal kayıplar: 3
  - İş aksaması ile ilgili kayıplar: 4

Kapalı uçlu sorular da numerik etiketler ve puanlama kullanılmıştır. Demografik veriler (cinsiyet, yaş, vb.) kategorik olarak belirlenirken, çoktan seçmeli sorular da pozitif negatif

puanlama yapılmıştır. Bu puanlar toplanarak her bir bireyin farkındalık seviyesi tespit edilmiş ve çözümlenmiştir.

Araştırmada kullanılan 5'li Likert tipi ölçeği kapsamında katılımcılardan değişkenlere ait her bir soru için 1= Kesinlikle katılmıyorum, 2= Katılmıyorum, 3= Kararsızım, 4= Katılıyorum, 5= Kesinlikle katılıyorum seçeneklerinden birisini tercih etmeleri istenmiş ve ölçek maddeleri olarak da "gizlilik", "tamlık", "erişilebilirlik" ve "güvenilirlik" maddeleri kullanılmıştır. Bu analizde de, kapalı uçlu sorulara benzer şekilde ölçekler puanlara çevrilerek her bir bireyin bilgi farkındalığı değişkenlerine verdiği cevaplar puan olarak hesaplanmıştır.

Demografik özelliklerin bilgi farkındalığına dayalı karşılaştırılmaları T-Test ve ANOVA kullanılarak yapılmıştır. Elde edilen farklılığın hangi gruplar arasında olduğunu belirlemek amacıyla Tukey HSD testi uygulanmış ve çoklu karşılaştırma tabloları elde edilmiştir.

Melnick (2020), "En yaygın 10 Siber Saldırı Türü" adlı yaptığı araştırmada, parola ile ilgili saldırıların ilk 5 içinde yer aldığını belirtmiştir. Arezina (2019), yaptığı çalışmada şifrelerin (%32) tarayıcıya kaydedildiğini ve %26'sının ise şifrelerini deftere veya yapışkanlı notlara yazdıklarını raporlamıştır. Ayrıca aynı raporda çalışanların %57'sinin parola yönetimini işlerini yapmaktan alıkoyan bir sıkıntı olarak gördüklerini belirtmiştir. Michael (2017) ise, yaptığı araştırmada, dünya çapındaki şirketlerin CEO'larının %30'unun iş e-postalarını kullanabilmek adına bir çevrimiçi hizmete kaydettikleri şifrelerinin sızdırıldığını raporlamıştır. Bu bilgiler ışığında, yönetici pozisyonlarının şifrelere yönelik tutumu arasında ilişki olup olmadığını tespit etmek için "Firmadaki pozisyonunuz" ve "Şifrelerinizi ne sıklıkla değiştirirsiniz" anket soruları için Ki-Kare (Chi-square) analizi kullanılmıştır.

Bu araştırmada kullanılan anket soruları, Çatuk (2018) tarafından yapılan bir çalışmadan referans alınarak hazırlanmıştır. Bu çalışma, kullanılacak istatistiksel yöntemlerin sonuçlarına göre değerlendirilmiştir ve analiz için SPSS Statistics 26 programı kullanılmıştır.

4. Çalışma Bulguları

4.1 Tanımlayıcı İstatistikler

Bu bölümde toplanan verilerin istatistiksel analizleri, testleri yapılmış ve sonuçlar yorumlanmıştır. Araştırmada öncelikle demografik verilerle betimleyici istatistikler tanımlanmıştır.

Tablo 2
Ankete Katılanların Demografik Özelliklerinin Frekans Dağılımı

Cinsiyet	**N**	**%**	**Firmadaki Pozisyon**	**N**	**%**
Kadın	178	48,8	İdari çalışan	60	16,4
Erkek	187	51,2	Teknik çalışan	90	24,6
Yaş			Alt düzey yönetici	75	20,5
18-24	60	16,4	Orta düzey yönetici	80	22,1
25-31	91	24,9	Üst düzey yönetici	60	16,4
32-38	90	24,7	**Gelir Düzeyi**		
39-45	71	19,5	0-2500 TL	57	15,6
46 ve üzeri	53	14,5	2501-4000 TL	113	31,0
Eğitim			4001-6000 TL	90	24,7
İlköğretim	45	12,3	6001-8000 TL	60	16,4
Lise	83	22,7	8001 ve üzeri	45	12,3
Önlisans	71	19,5	**Toplam**	**365**	**100**
Lisans	113	31,0			
Lisansüstü	53	14,5			
Toplam	**365**	**100**			

Tablo 2'de görüldüğü üzere araştırmaya katılan bireylerin 187 (%51,2) sini erkekler oluştururken 178 (%48,8) katılımcı cinsiyetini kadın olarak belirtmiştir. Buna ek olarak ankete cevap veren katılımcıların çoğunluğunun 25-31(%24,9) ve 32-38(%24,7) yaş grubu aralığında olduğu görülmektedir. Katılımcıların yaş grubu dağılımının da homojen olduğu tablodaki frekans değerlerinden anlaşılmaktadır. Ayrıca görüldüğü üzere anketi cevaplayan katılımcıların çoğunluğunu 90 kişi(%24,6) ile teknik çalışanlar oluşturmaktadır. Katılımcıların eğitim seviyelerine bakıldığında ise, büyük çoğunluğun(%31) lisans mezunu olduğu görülmektedir. 2501-4000 TL arası gelir düzeyine sahip katılımcıların ankette çoğunluk olduğu(%31) tespit edilmiştir.

Yukarıda bahsedilen tanımlayıcı istatistiklere ek olarak ilgili demografik değişkenlerle çapraz analizler gerçekleştirilmiştir. Bu analizlerin sonucunda, şu sonuçlara varılmıştır:

- Katılımcılardan erkek çalışanların çoğunluğunun 25 ila 31 yaş arası grubunda olduğu tespit edilmiştir.
- Katılımcılardan üst düzey pozisyona sahip çalışanların %33'ünün kadın olduğu görülmüştür.
- Erkek katılımcıların çoğunluğunun pozisyonunun teknik sorumlu(%29,7) olduğu saptanmıştır.
- Orta düzey çalışanların %43,5'inin 38-45 yaş aralığında olduğu tespit edilmiştir.
- 46 ve üzeri yaş grubunun %60'ının üst düzey yönetici pozisyonunda görev aldığı saptanmıştır.
- 18-24 yaş grubu çalışanlarının büyük bir çoğunluğunun(%56) idari çalışan olduğu görülmüştür.

Demografik verilerin tanımlayıcı istatistiklerinden sonra güvenlik politikası ile alakalı çoktan seçmeli anket sorusunun da tanımlayıcı istatistiği hesaplanmıştır. Aralığı -3 puan ve 6 puan arasında değişmekte olup, ortalaması 1,78'dir. Bu gösteriyor ki güvenlik politikası uygulamaları her ne kadar pozitif bir ortalama çıkarmış olsa da yeterli farkındalık mevcut değildir.

Açık uçlu sorularda tespit edilen temalar için yeni değişkenler atanmış ve tanımlayıcı istatistikleri hesaplanmıştır. 51 katılımcının olası bir siber saldırıdan kaçınmak için alacağı önlemlere ait teması ve sıklığı aşağıdaki gibidir:

Tablo 3
Önlemlere Ait Tema Frekans Dağılımı

Tema	N	%
Sistem Güvenlik Önlemleri	15	29,4
Yedekleme Önlemleri	13	25,5
Eğitim Önlemleri	12	23,5
Kalite Kontrol Önlemleri	11	21,6
Toplam	**51**	**100,0**

Tablo 3'te görüldüğü üzere katılımcıların çoğunluğu sistem koruması(%29,4) ve yedeklemenin(%25,5) firmanın olası bir siber saldırıya karşı alacağı önlemler arasında daha etkin olacağını düşünmektedir.

36 katılımcının siber saldırıya maruz kalındıktan sonra firmanın yaşadığı kayıpları belirttiği tema ve sıklığı aşağıdaki gibidir:

Tablo 4
Siber Saldırı Sonrası Yaşanılan Kayıpların Tema Frekans Dağılımı

Tema	N	%
Veri kayıpları	10	27,8
İmaj/Müşteri/Prestij kayıpları	12	33,3
Finansal kayıplar	9	25,0
İş akması ile ilgili kayıplar	5	13,9
Toplam	**36**	**100,0**

Tablo 4'te görüldüğü üzere katılımcılar siber saldırıya maruz kaldıktan sonra şirketlerinde gördükleri en büyük kaybın imaj/müşteri/prestij kayıpları(%33,3) olduğunu belirtmişlerdir.

Likert tipi ölçüm sorusundan hesaplanan anket puanlarında katılımcılar en düşük 9 puan almışken en yüksek 45 puan almışlardır. Puan ortalaması ise, 29,47 olup, katılımcı şirketlerde bilgi farkındalığının mevcut olup yeterli olmadığı yorumlanmıştır.

4.2 Bilgi Farkındalığı Analizleri

Araştırmanın bu aşamasında katılımcıların 5'li Likert tipi ölçeği kapsamında yaptığı seçimler puana çevrilerek her bir birey için ortalama puanları yeni bir değişken olarak(farkındalık puanı) tanımlanmıştır. Daha sonra bu demografik değişkenlerin farkındalık değişkeni üzerinde etkisi olup olmadığına dair hipotezler kurularak T-Test ve ANOVA gerçekleştirilmiştir. Bu testler için anlamlılık düzeyini gösteren α değeri, 0,05 olarak alınmıştır.

Yapılan ilk analizde firmadaki pozisyonun bilgi farkındalığı ile anlamlı bir ilişkisinin olup olmadığının analizi yapılmış olup test istatistiği 0,001 olarak hesaplanmıştır. Bunun sonucunda, %95 güven aralığında firmadaki pozisyonun bilgi farkındalığı açısından anlamlı bir farklılık olduğunu göstermektedir.

Tablo 5
Firmadaki Pozisyona Göre Bilgi Farkındalığı Farklılık Test Sonucu

Firmadaki Pozisyon	Ortalama	Standart Sapma	Sig. (P)
İdari çalışan	2,73	1,31	0,001
Teknik çalışan	3,21	1,12	
Alt düzey yönetici	3,26	1,07	
Orta düzey yönetici	3,60	1,13	
Üst düzey yönetici	3,48	1,45	

Firmadaki pozisyona göre farkındalık değerleri arasında elde edilen farklılığın hangi gruplar arasında olduğunu belirlemek amacıyla post hoc testlerinden Tukey testi uygulanmış ve elde edilen çoklu karşılaştırma sonuçları aşağıdaki tabloda verilmiştir.

Tablo 6
Firmadaki Pozisyona Göre Tukey Karşılaştırma Sonuçları

Firmadaki Pozisyon	Sig. (P)				
	İdari çalışan	Teknik çalışan	Alt düzey yönetici	Orta düzey yönetici	Üst düzey yönetici
İdari çalışan	-	0,151	0,092	0,00*	0,007*
Teknik çalışan	0,151	-	0,997	0,184	0,616
Alt düzey yönetici	0,092	0,997	-	0,383	0,821
Orta düzey yönetici	0,000*	0,184	0,383	-	0,976
Üst düzey yönetici	0,007*	0,616	0,821	0,976	-

Tablo 6'da hesaplanan istatistiklere göre idari çalışanların farkındalık düzeyleri ile orta düzey yöneticiler ve üst düzey yöneticilerin bilgi farkındalık düzeyleri arasında anlamlı bir farklılık bulunmaktadır. Bu grupların ortalama değerlerine bakıldığında orta ve üst düzey yöneticilerin farkındalık değerlerinin idari çalışanlara göre yüksek olduğu görülmektedir.

Katılımcıların yaş değerlerine göre bilgi farkındalık değerleri arasında anlamlı bir fark olup olmadığını belirleme amacıyla ANOVA testi kullanılmış ve elde edilen sonuçlar Tablo 7'de verilmiştir.

Tablo 7
Yaşa Göre Bilgi Farkındalığı Farklılık Test Sonucu

Yaş Grupları	Ortalama	Standart Sapma	Sig. (P)
18-24	2,73	1,32	0,001
25-31	3,46	1,13	
32-38	3,32	1,01	
39-45	3,55	1,14	
46 ve üzeri	3,05	1,54	

Elde edilen p değerinin(0,001) 0,05'ten küçük olması yaş grupları arasında farkındalık düzeyleri bakımından anlamlı bir farklılık bulunduğunu göstermektedir. Bu farklılığın hangi gruplar arasında olduğunu belirlemek amacıyla post hoc testlerinden Tukey testi uygulanmış ve elde edilen çoklu karşılaştırma sonuçları aşağıdaki tabloda verilmiştir.

Tablo 8
Yaşa göre Tukey Karşılaştırma Sonuçları

Yaş Grupları	Sig. (P)				
	18-24	25-31	32-38	39-45	46 ve üzeri
18-24	-	0,003*	0,029*	0,001*	0,612
25-31	0,003*	-	0,928	0,993	0,283
32-38	0,029*	0,928	-	0,761	0,708
39-45	0,001*	0,993	0,761	-	0,164
46 ve üzeri	0,612	0,283	0,708	0,164	-

Elde edilen Tukey test sonuçlarına göre 18-24 yaş grubu farkındalık değerleri ile 25-31, 32-38 ve 39-45 yaş grupları arasında anlamlı bir farklılık bulunmaktadır($p \leq 0,05$). Bu yaş gruplarının ortalama değerlerine bakıldığında 18-24 yaş grubunun farkındalık değerinin diğer gruplardan daha düşük olduğu görülmektedir. Diğer grupların birbirleri arasındaki farkındalık değerlerinin birbirinden farklı olamadığı anlaşılmaktadır.

Katılımcıların eğitim düzeyi değerlerine göre bilgi farkındalık değerleri arasında anlamlı bir fark olup olmadığını belirleme amacıyla Anova testi kullanılmış ve elde edilen sonuçlar Tablo 9'da verilmiştir.

Tablo 9
Eğitim Durumuna Göre Bilgi Farkındalığı Farklılık Test Sonucu

Eğitim Düzeyi	Ortalama	Standart Sapma	Sig. (P)
İlköğretim	1,77	0,74	0,000
Lise	3,08	1,09	
Önlisans	3,09	0,98	
Lisans	3,83	1,08	
Lisansüstü	3,83	1,21	

Elde edilen p değerinin(0,000) 0,05'ten küçük olması Eğitim düzeyi grupları arasında farkındalık düzeyleri bakımından anlamlı bir farklılık bulunduğunu göstermektedir. Bu farklılığın hangi gruplar arasında olduğunu belirlemek amacıyla post hoc testlerinden Tukey testi uygulanmış ve elde edilen çoklu karşılaştırma sonuçları aşağıdaki tabloda verilmiştir.

Tablo 10
Eğitim Düzeyine Göre Tukey Karşılaştırma Sonuçları

Eğitim Durumu	**Sig. (P)**				
	İlköğretim	**Lise**	**Önlisans**	**Lisans**	**Lisansüstü**
İlköğretim	-	0,000	0,000	0,000	0,000
Lise	0,00	-	*1,000*	0,000	0,001
Önlisans	0,000	*1,000*	-	0,000	0,001
Lisans	0,000	0,000	0,000	-	*1,000*
Lisansüstü	0,000	0,001	0,001	*1,000*	-

Elde edilen Tukey test sonuçlarına göre ilköğretim mezunlarının farkındalık düzeyi ile diğer tüm gruplar arasında anlamlı bir farklılık bulunmaktadır. Buna göre ilköğretim mezunlarının farkındalık düzeyi diğer tüm grupların farkındalık düzeyinden düşüktür. Ayrıca Lisans mezunlarının farkındalık değeri de lise ve ön lisans mezunlarından yüksek iken lisans üstü mezunlarıyla anlamlı bir farklılık bulunmamaktadır. Lisansüstü mezunlarının bilgi farkındalık düzeyleri lisans mezunları hariç tüm gruplardan daha yüksek çıkmıştır.

Katılımcıların gelir düzeyi değerlerine göre bilgi farkındalık değerleri arasında anlamlı bir fark olup olmadığını belirleme amacıyla Anova testi kullanılmış ve elde edilen sonuçlar tablo 11'de verilmiştir.

Tablo 11
Gelir Düzeyine Göre Bilgi Farkındalığı Farklılık Test Sonucu

Gelir Düzeyi	**Ortalama**	**Standart Sapma**	**Sig. (P)**
0-2500 TL	2,32	1,16	0,000
2501-4000 TL	3,22	1,04	
4001- 6000 TL	3,49	1,15	
6001-8000 TL	3,64	1,22	
8001 ve üzeri	3,60	1,37	

Elde edilen p değerinin(0,000) 0,05'ten küçük olması gelir düzeyi grupları arasında farkındalık düzeyleri bakımından anlamlı bir farklılık bulunduğunu göstermektedir. Bu farklılığın hangi gruplar arasında olduğunu belirlemek amacıyla post hoc testlerinden Tukey testi uygulanmış ve elde edilen çoklu karşılaştırma sonuçları aşağıdaki tabloda verilmiştir.

Tablo 12
Gelir Düzeyine Göre Tukey Karşılaştırma Sonuçları

Gelir Düzeyi	**Sig. (P)**				
	0-2500 TL	**2501-4000 TL**	**4001-6000 TL**	**6001-8000 TL**	**8001 ve üzeri**
0-2500 TL	-	0,000*	0,000*	0,000*	0,000*
2501-4000 TL	0,000*	-	0,477	0,163	0,333
4001- 6000 TL	0,000*	0,477	-	0,937	0,982
6001-8000 TL	0,000*	0,163	0,937	-	1,000
8001 ve üzeri	0,000*	0,333	0,982	1,000	-

Elde edilen Tukey test sonuçlarına göre gelir düzeyi 0-2500 aralığında olan katılımcıların farkındalık düzeyi ile diğer tüm gelir grupları arasında anlamlı bir r farklılık bulunmaktadır. Elde edilen ortalama değerlere bakıldığında 0-2500 gelir düzeyindeki bireylerin farkındalık değerleri

diğer grupların farkındalığından düşük olduğu görülmektedir. Diğer gelir düzeylerinin farkındalık değerleri arasındaki farklılık p değerlerinin 0,05'ten büyük olması bu gruplar arasında anlamlı bir farklılık olmadığını göstermektedir.

Bilgi farkındalığının cinsiyete ve firmadaki çalışan sayısına göre anlamlı bir farkı olup olmadığını belirlemek amacıyla yapılan t-testi ve Anova testi yapılmıştır. Elde edilen p değerlerinin 0,05'ten büyük olması cinsiyet ve çalışan sayısına göre farkındalık değerleri arasında anlamlı bir farkılılık olmadığını göstermektedir.

Tablo 13
Cinsiyete ve Çalışan Sayısına Göre Bilgi Farkındalığı Farklılık Test Sonucu

Cinsiyet	**Ortalama**	**Standart Sapma**	**Sig. (P)**
Kadın	3,17	1,23	0,170
Erkek	3,35	1,23	
Çalışan Sayısı			
1-10	2,96	1,29	0,094
11-49	3,16	1,11	
50-100	3,33	1,15	
101-250	3,44	1,35	

Katılımcıların firmada çalışma yılı değerlerine göre bilgi farkındalık değerleri arasında anlamlı bir fark olup olmadığını belirleme amacıyla Anova testi kullanılmış ve elde edilen sonuçlar Tablo 14'te verilmiştir.

Tablo 14
Firmada Çalışma Yılına Göre Bilgi Farkındalığı Anova Test Sonucu

Çalışma Yılı	**Ortalama**	**Standart Sapma**	**Sig. (P)**
0-5	3,37	1,24	0,001
6-10	3,33	1,06	
11-15	3,43	1,31	
16-20	3,06	1,38	
21 ve üstü	2,37	1,19	

Elde edilen p değerinin(0,001) 0,05'ten küçük olması çalışma yılı grupları arasında bilgi farkındalık düzeyleri bakımından anlamlı bir farklılık bulunduğunu göstermektedir. Bu farklılığın hangi gruplar arasında olduğunu belirlemek amacıyla post hoc testlerinden Tukey testi uygulanmış ve elde edilen çoklu karşılaştırma sonuçları aşağıdaki tabloda verilmiştir.

Tablo 15
Firmada Çalışma Yılına Göre Tukey Karşılaştırma Sonuçları

Çalışma Yılı	**Sig. (P)**				
	0-5	**6-10**	**11-15**	**16-20**	**21+**
0-5	-	0,999	0,998	0,680	0,001*
6-10	,998	-	0,982	0,800	0,002*
11-15	,998	0,982	-	0,615	0,002*
16-20	,680	0,800	0,615	-	0,169
21 ve üstü	,001*	0,002*	0,002*	0,169	-

Elde edilen Tukey test sonuçlarına göre çalışma yılı 21 ve üstü olan bireylerin bilgi farkındalık düzeyi ile 0-5, 6-10 ve 11-15 yılları grupları arasında anlamlı bir farklılık bulunmaktadır. Buna göre çalışma yılı 21 ve üstü olan bireylerin bilgi farkındalık düzeyleri belirtilen gruplara göre daha düşüktür. Diğer grupların bilgi farkındalık düzeylerinin arasında anlamlı bir farklılık bulunmamaktadır.

Katılımcıların şifre belirleme yöntemine göre bilgi farkındalık değerleri arasında anlamlı bir fark olup olmadığını belirleme amacıyla Anova testi kullanılmış ve elde edilen sonuçlar Tablo 16'da verilmiştir.

Tablo 16
Şifre Belirleme Yöntemine Göre Bilgi Farkındalığı Anova Test Sonucu

Şifre Belirleme Yöntemi	Ortalama	Standart Sapma	Sig. (P)
İlk Şifre	2,36	1,09	0,000
Kısa Şifre	2,99	1,06	
En Az 6 Karakterli	3,45	1,11	
Kişisel Anlamlı	3,51	1,15	
Karmaşık	3,45	1,35	

Elde edilen p değerinin(0,000) 0,05'ten küçük olması şifre belirleme yöntemleri arasında bilgi farkındalık düzeyleri bakımından anlamlı bir farklılık bulunduğunu göstermektedir. Bu farklılığın hangi gruplar arasında olduğunu belirlemek amacıyla post hoc testlerinden Tukey testi uygulanmış ve elde edilen çoklu karşılaştırma sonuçları aşağıdaki tabloda verilmiştir.

Tablo 17
Şifre Belirleme Yöntemine Göre Tukey Karşılaştırma Sonuçları

Şifre Belirleme Yöntemi	Sig. (P)				
	İlk Şifre	Kısa Şifre	En Az 6 Karakterli	Kişisel Anlamlı	Karmaşık
İlk Şifre	-	0,068	0,000*	0,000*	0,000*
Kısa Şifre	,068	-	0,167	0,073	0,140
En Az 6 Karakterli	,000*	0,167	-	0,997	1,000
Kişisel Anlamlı	,000*	0,073	0,997	-	0,997
Karmaşık	,000*	0,140	1,000	0,997	-

Elde edilen Tukey test sonuçlarına göre ilk şifreyi kullanan bireylerin bilgi farkındalık düzeyleri ile kısa şifre grubu hariç diğer grupların bilgi farkındalık düzeyleri arasında anlamlı bir farklılık bulunmaktadır. Grupların bilgi farkındalık değerlerine bakıldığında bu grubun farkındalık düzeyi 2,36 değeri diğer tüm gruplardan daha düşüktür. Diğer grupların farkındalık değerleri arasında anlamlı bir farklılık bulunmamaktadır.

Katılımcıların şifre değiştirme sıklığına göre bilgi farkındalık değerleri arasında anlamlı bir fark olup olmadığını belirleme amacıyla Anova testi kullanılmış ve elde edilen sonuçlar Tablo 18'de verilmiştir.

Tablo 18
Şifre değiştirme Sıklığına Göre Bilgi Farkındalığı Anova Test Sonucu

Şifre Değiştirme Sıklığı	Ortalama	Standart Sapma	Sig. (P)
Hiç değiştirmem	2,94	1,17	0,000
Biriyle Paylaştığımda	3,55	1,13	
Çok Sık	3,31	1,17	
6 ayda bir	3,59	1,21	
Yılda 1 kez	2,97	1,34	

Elde edilen p değerinin(0,000) 0,05'ten küçük olması şifre değiştirme sıklığına göre bilgi farkındalık düzeyleri bakımından anlamlı bir farklılık bulunduğunu göstermektedir. Bu farklılığın hangi gruplar arasında olduğunu belirlemek amacıyla post hoc testlerinden Tukey testi uygulanmış ve elde edilen çoklu karşılaştırma sonuçları aşağıdaki tabloda verilmiştir.

Tablo 19
Şifre Değiştirme Sıkılığına Göre Tukey Karşılaştırma Sonuçları

Şifre Değiştirme Sıklığı	Sig. (P)				
	Hiç değiştirmem	Biriyle Paylaştığımda	Çok Sık	6 ayda bir	Yılda 1 kez
Hiç değiştirmem	-	0,009*	0,373	0,011*	0,822
Biriyle Paylaştığımda	,009*	-	0,706	0,999	0,000*
Çok Sık	,373	0,706	-	0,633	0,055
6 ayda bir	,011*	0,999	0,633	-	0,001*
Yılda 1 kez	,822	0,000*	,055	0,001*	-

Elde edilen Tukey test sonuçlarına göre şifresini hiç değiştirmeyenler ile yılda bir kez şifre değiştirenlerin bilgi farkındalık düzeyleri ile şifresini biriyle paylaştığında değiştiren ve 6 ayda bir değiştiren bilgi farkındalık düzeyleri arasında anlamlı bir farklılık bulunmaktadır. Buna göre grupların ortalama değerlerine bakıldığında, şifresini 6 ayda bir değiştiren ve biriyle paylaştığında değiştirenlerin bilgi farkındalık düzeyleri şifresini hiç değiştirmeyen ve yılda bir kez değiştirenlerden daha yüksek olduğu görülmektedir. Ayrıca çok sık şifre değiştirenlerin bilgi farkındalık düzeyi ile diğer tüm gruplar arasında anlamlı bir farklılık bulunmamaktadır.

Firmadaki pozisyon ve şifre değiştirme sıklığı arasında bir ilişki olup olmadığını belirlemek amacıyla Ki-Kare ilişki testi kullanılmış ve elde edilen p değerinin 0,05'ten küçük çıkmasıyla iki değişken arasında pozitif yönlü anlamlı bir ilişki bulunduğu görülmüştür. Buna göre bireylerin firmadaki pozisyonu yükseldikçe şifre değiştirme sıklığı da artmaktadır.

Tablo 20
Şifre Değiştirme Sıklığı İle Firmadaki Pozisyon Arasındaki İlişki Testi

Ölçüt	Pearson Ki-Kare Değeri	Sig.(P)
Firmadaki Pozisyon* Şifre Değiştirme Sıklığı	178,66	0,001

5. Tartışma ve Sonuç

Ankara ilinde bulunan KOBİ çalışanlarının bilgi güvenliği ve siber saldırılara karşı farkındalığı karşı bir çalışma yapılmış ve elde edilen veri seti test edilmiştir. Bu çalışma için, 365 çalışanın bilgi farkındalığı ve demografik bilgilerine dayalı çevrimiçi anket uygulaması kullanılmıştır. Elde edilen veri setinde güvenilirlik ve küresellik testlerinin sonuçları anlamlı çıkmış olup, veri seti üzerinde analizler gerçekleştirilmiştir. Tanımlayıcı istatistiklerde katılımcıların demografik olarak homojen bir dağılım sergilediği görülmüştür. Değişken gruplarındaki farklılıklar için yapılan analizlerde T-Test, ANOVA ve Ki-Kare testleri gerçekleştirilmiştir. İstatistiksel analizler sonucu bazı demografik verilerin farkındalık kazanma ile ilgili anlamlı etkileşimlerin varlığı tespit edilmiştir. Bilgi farkındalığı konusunda idari çalışanların diğerlerine göre bilgi farkındalığı düzeyinin daha yüksek olduğu görülmüştür. Bunun nedeni, kurumlardaki kalite sistemlerinin olgunlaşmış olması ve ilgili bilgi güvenliği standartlarının (ISO 27001 gibi) sistemde oturmuş olmasından kaynaklı olabilir. Bunun yanı sıra, düşük gelir düzeyine sahip çalışanları Tukey HSD test sonucunun diğer gelir düzeylerine sahip katılımcılar ile anlamlı bir farklılığa sahip olup en düşük ortalama puana sahip olduğu görülmüştür. Dolayısıyla bu grubun, siber saldırılara ve bilgi güvenliği farkındalığına önem vermediği sonucunu yorumlamak mümkündür. Eğitim düzeyi ve yaş gruplarında da çıkan bilgi güvenliği farkındalığı testi de anlamlı çıkmıştır. Bu sebeple, bu değişkenler için en az bir grubun diğerlerinden farklı olduğu hipotezi kabul edilmiş olup çoklu karşılaştırma tabloları incelenmiştir. İlköğretim mezunu katılımcıların gelir düzeyinde olduğu gibi diğerleriyle anlamlı bir farklılığa sahip olduğu görülmekte olup en düşük puan ortalamasını yapmakta olduğu tespit edilmiştir. TÜİK (2019) verilerine göre eğitim seviyesi ilköğretim ve lise olan çalışanların yıllık ortalama brüt kazancı 9 bin 640 lira iken lisans ve lisansüstü mezunlarının

kazancı 27 bin 310 liradır. Dolayısıyla düşük gelir düzeyine sahip katılımcıların çoğunluğunu düşük eğitim düzeyi grubu olarak yorumlayabilir ve bilgi farkındalığına önem verilmediği bu analiz için de yapılabilir. Yaş grubunda da en dikkate değer yaş grubunun 18-24 yaş grubu arası olduğu görülmektedir. Bu durum, bu kuşağın bilişim ve teknoloji konusunda daha bilinçli, daha etkin ve daha bilgili olduğuyla açıklanabilir. Bu demografik değişkenlerin yanı sıra, bu çalışmada cinsiyet ve firmadaki çalışan sayısında farklılık olup olmadığının testleri de yapılmış ancak anlamlı bir değer kaydedilmemiştir. Ertuğrul ve Keskin (2012: 81) bilişim çağının hüküm sürdüğü sanal ortamda cinsiyet, ırk, kültür vb. gibi gerçek dünyada önemli olabilecek değişkenlerinin önemini yitirdiğini vurgulamaktadır. Haliyle, bu çalışmada cinsiyetin bu ortamdaki güvenlik farkındalığı testinin anlamlı bir değer tespit etmemesi Ertuğrul ve Keskin 'in (2012: 81) bu savıyla yorumlanabilir.

Araştırmada bu çalışmalara ek olarak, açık uçlu sorularla, atak yaşanan KOBİ'lerde çalışanların şirketin en çok zarar gördüğü alanın imaj ve prestij kaybı dolaylı olarak da müşteri kaybı olduğu tespit edilmiştir. Ayrıca çalışanların çoğu bu ataklara karşı önlem olarak sistemin güçlendirilmesini ve yedekleme eylemlerini önermişlerdir. Yapılan anket çalışmasında, bilgi farkındalığına dayalı puanlamanın ortalaması 29,47 çıkmıştır. Bu durum KOBİ'ler de bilgi farkındalığının mevcut ancak yeterli olmadığını göstermektedir.

Son olarak, çalışanların çoğunluğu, bir siber saldırının işletme imajları üzerinde olumsuz etkilere neden olacağını belirtmişlerdir. Bu durum, işletmelerin imajlarının olumsuz etkilenmemesi için, işletmelerin genel güvenlik stratejilerine ve planına, siber güvenlik ihlali raporlamalarına sahip olmaları, siber güvenlik konusunda farkındalık çalışmalarının yapılması ve çalışanların siber riskler konusunda bilinçlenmeleri gibi önlemlere daha fazla önem vermeleri gerektiği sonucunu doğurmuştur.

Çalışanların siber güvenlik ve siber saldırılara karşı bilgi farkındalık düzeylerinin belirlenmesine yönelik literatürde benzer çalışmaların bulunmaması elde edilen sonuçların kurum ve yıllara göre karşılaştırma imkanını ortadan kaldırmaktadır. Çalışanların bilgi farkındalık düzeyleri hakkında özellikle eğitim ve askeriye gibi önem arz eden farklı kurumlarda yapılacak çalışmalarla alan literatürü zenginleştirilecek ve kullanılacak ek değişken ve yöntemlerle konunun farklı boyutları ortaya çıkarılacaktır.

Kaynaklar

Acılar, A. (2009). KOBİ'lerde Bilişim Teknolojileri Güvenliği Sorunu: Tehditler ve Önlemler, Afyon Kocatepe Üniversitesi, İ.İ.B.F. Dergisi, (C.X I,S I, 2009).

Allan, C.Annear, J. , Beck, J. Beveren, J. V. (2003). A Framework for The Adoption of Ict and Security Technologies by SME's, A paper for the Small Enterprise Association of Australia and New Zealand 16th annual Conference, Ballarat, 28 Eylül-1 Ekim 2003. http://www.africres.org/SMME%20Research/SMME%20Research%20General/Reports/Adoption%20of%20ICT%20by%20SMES.pdf , (Erişim Tarihi: 25.11.2020).

Amrin, N. (2014). The Impact of Cyber Security on SMEs, University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science, 2014. https://essay.utwente.nl/65851/1/Amrin_MA_EEMCS.pdf , (Erişim Tarihi: 09.02.2021).

Arezina, L. (2019). Password statistics for 2020 – 'iloveyou' and 'sunshine' are most common, Dataprot, Kasım 2019. https://dataprot.net/statistics/password-statistics/ , (Erişim Tarihi: 07.01.2021).

Atalay, A. H. (2014). Siber Güvenlik ve Siber Suçlar. Erişim Tarihi: 08.04.2015. http://www.slideshare.net/ahatalay/sber-gvenlk-ve-sbersularahaaralk2014-43135183

Barlett, M. S. (1950). Test of Sigficance in Factor Analysis. British Journal of Psychology, Statistical Section, 3, 77-85.

Başaranoğlu, E. (2016). Bilgi Güvenliği Unsurları (CIA ve Diğerleri), Siberportal, Ocak 2016. https://www.siberportal.org/blue-team/securing-information/bilgi-guvenligi-unsurlari-cia-ve-digerleri/ , (Erişim Tarihi: 15.12.2020).

Berqnet, (2018). Siber Güvenlik Nedir? Veri Güvenliğini Nasıl Sağlarız?, Berqnet Blog, Aralık 2018. https://berqnet.com/blog/siber-guvenlik-nedir , (Erişim Tarihi: 23.11.2020).

Boateng, Y. , Osei, E. (2013). Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity ve Availability (CIA), Institut for Elektroniske Systemer, Aalborg Universitet, 2013.

https://vbn.aau.dk/ws/portalfiles/portal/316448052/PhD_Thesis_Boateng_Final_for_print.pdf , (Erişim Tarihi: 09.02.2021).

Bozgeyik, A. (2018). Gaziantep'te Faaliyet Gösteren Orta ve Büyük Ölçekli İşletmelerin Siber Güvenlik Yönetim Yaklaşımlarının Analizi, Hasan Kalyoncu Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı İşletme Doktora Programı Doktora Tezi, 2018.

Çatuk, C. (2018). Siber Riskler Karşısında KOBİ'lerin Bilgi Güvenliği Farkındalıklarını Ölçen Bir Ölçek Geliştirme: Gaziantep Örneklemi, Hasan Kalyoncu Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı İşletme Doktora Programı Doktora Tezi, 2018.

Digitalage, (2018). KOBİ'lerin cevaplaması gereken 10 siber güvenlik sorusu, Digitalege İş Dünyası Platformu, Nisan 2018. https://digitalage.com.tr/kobilerin-cevaplamasi-gereken-10-siber-guvenlik-sorusu/ , (Erişim Tarihi: 23.11.2020).

Chepken, C. (2015). The Effects of Cyber-crime on E-commerce; a model for SMEs in Kenya, University of Nairobi School of Computing and Informatics, 2015.

http://erepository.uonbi.ac.ke/bitstream/handle/11295/95232/Wekunda_%20The%20Effects%20of%20Cybercrime%20on%20E-Commerce%20a%20Model%20for%20SMEs%20in%20Kenya.pdf?sequence=1&isAllowed=y , (Erişim Tarihi: 23.11.2020).

Çetin H., Gundak İ. ve Çetin H.H. (2015). E-İşletme Güvenliği ve Siber Saldırılar Üzerine Bir Araştırma, Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 6(2): 223-240

Göztepe, K. , Kılıç, R. , Dr. Kayaalp, A. (2014). Cyber Defense In Depth: Desıgnıng Cyber Securıty Agency Organızatıon for Turkey, Journal of Naval Science and Engineering 2014, Vol.10, No.1, pp.1-24, 2014.

https://www.researchgate.net/profile/Kerim_Goztepe/publication/274733863_Cyber_Defense_In_Depth_Designing_Cyber_Security_Agency_Organization_For_Turkey/links/55290b710cf2779ab78e45a4/Cyber-Defense-In-Depth-Designing-Cyber-Security-Agency-Organization-For-Turkey.pdf , (Erişim Tarihi: 09.02.2021).

kaynakçada unvan kullanımı?) Leccisotti, F. Z. (2015). Guidelines for IT Security in SMEs, United Nations Interregional Crime and Justice Research Institute (UNICRI), 2015.

https://www.combattingcybercrime.org/files/virtual-library/phenomena-challenges-cybercrime/guidelines-for-it-security-in-smes.pdf , (Erişim Tarihi: 27.11.2020).

Ertuğrul, İ. ve Keskin, N. (2012). İnternet'İn Türkçenin Kullanımında Ve Toplum Birey Yapısının Değişimindeki Rolü. Doğu Akdeniz Üniversitesi, Bilgisayar ve Teknoloji Yüksek Okulu, Mesleki Eğitim Sempozyumu, 3(2), 80-88.

https://dergipark.org.tr/tr/download/article-file/402505, (Erişim Tarihi: 11.02.2021)

Field, A. (2000). Discovering Statistics using SPSS for Windows. London- Thousand Oaks New Delhi: Sage Publications. https://dergipark.org.tr/en/download/article-file/156632, (Erişim Tarihi: 20.01.2021).

Her iki KOBİ'den biri siber saldırıya uğruyor, Hürriyet Teknoloji, Eylül 2019. https://www.hurriyet.com.tr/teknoloji/her-2-kobiden-biri-siber-saldiriya-ugruyor-41337601 , (Erişim Tarihi: 23.11.2020).

Ilgaz, B. (2018). Küçük ve Orta Büyüklükteki İşletmeler için Veri Güvenliği ve Standartları, KTO Karatay Üniversitesi Fen Bilimleri Enstitüsü Adli Bilişim Ana Bilim Dalı Yüksek Lisans Programı Yüksek Lisans Tezi, Temmuz 2018.

KOBİ'lerin sıkça karşılaştığı siber güvenlik sorunlarına 5 etkili çözüm, Hürriyet Teknoloji, Ekim 2020. https://www.hurriyet.com.tr/teknoloji/her-2-kobiden-biri-siber-saldiriya-ugruyor-41337601 , (Erişim Tarihi: 23.11.2020).

Kurnaz, İ. (2016). Siber Güvenlik Ve İlintili Kavramsal Çerçeve, Cyberpolitik Journal Vol. 1, No. 1, 2016. http://cyberpolitikjournal.org/index.php/main/article/view/91/89, (Erişim Tarihi: 25.12.2020).

Mangat, M. (2020). 81 Eye-Opening Data Breach Statistics for 2020, PhoenixNap Global IT Services, 2020. https://phoenixnap.com/blog/data-breach-statistics , (Erişim Tarihi: 25.12.2020).

Melnick, J. (2020). Top 10 Most Common Types of Cyber Attacks, Netwrix Blog, Ekim 2020. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/ , (Erişim Tarihi: 07.01.2021).

Michael, M. (2017). 1 in 3 CEOs Have Had Passwords Leaked in Breaches, F-Secure Blog, Ekim 2017. https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf , (Erişim Tarihi: 07.01.2021).

Ntsc (2020). Cyber Security Report 2020, National Technology Security Coalition, 2020. https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf , (Erişim Tarihi: 25.12.2020).

Nunnally, J. C. (1967). Psychometric Theory, New York, NY: McGraw-Hill.

Osborn, E. (2014). Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMEs, University of Oxford Centre for Doctoral Training in Cyber Security CDT Technical Paper 1/15, Eylül 2015.

Özmen, Ş. (2013). Ağ Ekonomisinde Yeni Ticaret Yolu: E-Ticaret, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

Ponsard, C. , Grandclaudon, J. , Dallons, G. (2018). Towards a Cyber Security Label for SMEs: A European Perspective, CETIC Research Centre, Charleroi, Belgium, 2018.

https://www.scitepress.org/Papers/2018/66576/66576.pdf , (Erişim Tarihi: 16.12 2020).

Shojaifar, A. , Fricker, S. A. , Gwerder, M. (2018). Elicitation of SME Requirements for Cybersecurity Solutions by Studying Adherence to Recommendations, FHNW, IIT and IMVS, 5210 Windisch, Switzerland 2018. https://arxiv.org/ftp/arxiv/papers/2007/2007.08177.pdf , (Erişim Tarihi: 17.12.2020).

Şahinaslan, Ö. , Şahinaslan, E. (2019). Siber Tehditlerin Toplum Üzerindeki Olumsuz Etkileri, Proceedings of the International Congress on Business and Marketing, 2019 Maltepe University, Istanbul, 13.06.2019-14.06.2019.

Taner E. Ve Kılıç İ. (2019). Güvenlik Güçlerinin Bilgi Güvenliği Farkındalığını Belirlemeye Yönelik Bir Araştırma, Güvenlik Bilimleri Dergisi, 8(2), 253-269

TÜİK (2019). Kazanç Yapısı Araştırması, 2018. Türkiye İstatistik Kurumu Haber Bülteni, Sayı: 30580. https://tuikweb.tuik.gov.tr/PreHaberBultenleri.do?id (Erişim Tarihi: 11.02.2021)

Valli, C. , Martinus, I. C. , Jhonstone, M, N. (2014). Small to Medium Enterprise Cyber Security Awareness: An Initial Survey of Western A estern Australian Business alian Business, Security Research Institute Edith Cowan University, 2014.

Yaşar, H. , Çakır, H. (2015). Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri, Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 3, s.488-507, 2015.

Yaylacı, K. (2020). Siber Suçların Kurumsal ve Ekonomik Etkileri, Cahit Cengizhan Bilişim Etiği, Şubat 2020. https://cahitcengizhan.com/siber-suclarin-kurumsal-ve-ekonomik-etkisi-2/ , (Erişim Tarihi: 15.12.2020).