Güvenlik Bilimleri Dergisi / Journal of Security Sciences

Jandarma ve Sahil Güvenlik Akademisi
Güvenlik Bilimleri Enstitüsü
Güvenlik Bilimleri Dergisi, Mayıs 2023,Cilt:12, Sayı:1, 69-96
doi:10.28956/gbd. 1264593

Gendarmerie and Coast Guard Academy
Institute of Security Sciences
Journal of Security Sciences, May 2023,Volume:12, Issue:1, 69-96
doi:10.28956/gbd. 1264593

Makale Türü ve Başlığı / Article Type and Title
Araştırma/ Research Article
İşletmelerin Maruz Kaldığı Siber Suçların Boyutu
The Size of Cyber Crimes That Businesses Are Exposed

Yazar(lar) / Writer(s)
Cem EROĞLU, Gazi Üniversitesi, Adli Bilişim Doktora Programı Öğrencisi, e-posta: cem.eroglu1@gazi.edu.tr. ORCID: https://orcid.org/0000-0001-8491-6398.

Bilgilendirme / Acknowledgement:
-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:
-Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur.
- Bu çalışma, yazarın "İşletmelerin Maruz Kaldığı Siber Suçların Boyutu ve İşletmelere Etkisi" başlıklı yüksek lisans tez çalışmasının bir bölümünden elde edilmiştir.
-Bu makalede araştırma ve yayın etiğine uyulmuştur.

Bu makale Turnitin tarafından kontrol edilmiştir.
This article was checked by Turnitin.

Makale Geliş Tarihi / First Received :13.03.2023
Makale Kabul Tarihi / Accepted :25.05.2023

Atıf Bilgisi / Citation:
Eroğlu C., (2023). İşletmelerin Maruz Kaldığı Siber Suçların Boyutu, *Güvenlik Bilimleri Dergisi, 12(1), ss 69-96. doi:10.28956/gbd. 1264593*

İŞLETMELERİN MARUZ KALDIĞI SİBER SUÇLARIN BOYUTU

Öz

İnsanlar teknolojik gelişmeler ve internetin yaygınlaşmasıyla birlikte alışveriş yapma, arkadaşlarıyla görüşme, bankacılık işlemleri gibi alışkanlıklarını değiştirmeye başlamıştır. Bu değişim ve siber ortam vasıtasıyla suç kavramı da dönüşüme uğramış ve siber suç kavramı insan hayatına girmiştir. Teknolojiye uyum sağlamaya çalışan işletmeler ise siber ortamın tehlikeleriyle karşılaşmıştır. Genel amacı işletmeleri bir siber suçun hedefi hâline getiren faktörleri araştırmak olan çalışmada Siber Güvenlik İhlalleri Anketi 2021'in veri setleri ikincil veri olarak kullanılmıştır. Türkiye'de işletmeler ve siber suç konularında yapılan az sayıdaki çalışma siber güvenlik ve siber risk üzerine yapılmıştır. Bu araştırmada ise işletmenin büyüklüğü, insan faktörü, dijital görünürlük, siber güvenlik önlemleri, siber farkındalık ve siber suçla mücadele eğitiminin siber suç mağduriyeti ile ilişkisi incelenmiştir. Araştırma sonucunda orta ve büyük işletmelerin daha fazla siber suça maruz kaldığı görülürken işletmelerin en yaygın maruz kaldığı siber suç oltalama suçu olmuştur. İnsan faktörünün oltalama suçu riskini artıran etken olarak çıktığı çalışmada, işletmelerin siber ortamdaki görünürlüğünün siber suç mağduriyetini artırdığı görülmüştür. Araştırmanın sonuç kısmında ise analiz sonuçları yorumlanarak bireylere, işletmelere ve siber güvenlikle ilgili politika üreten kurumlara öneriler sunulmuştur.

Anahtar Kelimeler*: Siber, siber suç, siber güvenlik, işletme.*

THE SIZE OF CYBER CRIMES THAT BUSINESSES ARE EXPOSED

Abstract

People have started to change their habits such as shopping, meeting with friends, banking transactions with the technological developments and the spread of the internet. Through this change and the cyber environment, the concept of crime has also transformed and the concept of cyber crime has entered human life. Businesses trying to adapt to technology have faced the dangers of the cyber environment. The datasets of the Cybersecurity Breaches Survey 2021 were used as secondary data in the study, the general purpose of which is to investigate the factors that make businesses the target of a cybercrime. Few studies on businesses and cybercrime in Türkiye have been conducted on cyber security and cyber risk. In this research, the relationship between the size of the business, the human factor, digital visibility, cyber security measures, cyber awareness and cybercrime training with cyber crime victimization has been examined. As a result of the research, it was seen that medium and large enterprises were exposed to cybercrime more, while the most common cybercrime that businesses were exposed to was phishing. In the study, where the human factor was found to be the factor that increased the risk of phishing crime, it was seen that the visibility of businesses in the cyber environment increased the victimization of cybercrime. In the conclusion part of the research, the results of the analysis were interpreted and suggestions were presented to the individuals, enterprises and the institutions that produce policies related to cyber security.

Keywords: *Cyber, cybercrime, cybersecurity, business.*

GİRİŞ

Kurum, kuruluş ve devletler; teknolojik gelişmelerin sonucunda sundukları kritik hizmetleri bilişim sistemleri altyapısı ile yazılım ve donanımlara dayandırmış, fiziksel bilgi alışverişi yerine bilgi ve iletişim teknolojisi (BİT) cihazlarını kullanarak elektronik bilgi alışverişini siber ortamda gerçekleştirmeye başlamıştır. İnternet ve BİT cihazlarının toplum hayatının bir parçası hâline gelmesi ile siber ortamda da yeni saldırı fırsatları ortaya çıkmış, suç da dijitalleşmeye başlamıştır. Bazı geleneksel suçlar siber ortamın mesafe ve sınır tanımazlığı sayesinde siber ortamda veya siber ortamın yardımıyla işlenmeye başlarken yeni suç çeşitleri de oluşmaya başlamıştır. Dolayısıyla faydalarını neredeyse herkesin bildiği internet ile BİT cihazlarının, faydalarının yanında bir takım riskler de taşıdığı ortaya çıkmıştır. Günümüzde doğal afetler, terör, savaş, göç gibi risklerin yanında siber risk kavramı da yer almaya başlamıştır.

İşletmelerin siber ortamı ve BİT cihazlarını kullanımı giderek artmakla beraber maruz kaldığı siber suç sayısı ile maddi kayıplarda büyük artışlar yaşanmaktadır. Literatürde işletmeler ile siber suç, siber risk veya siber güvenlik ilişkisini inceleyen bireysel araştırmacılar tarafından yapılan çalışmalar *(Anderson vd., 2012; Veenstra vd., 2016)*, kamu kuruluşları tarafından yapılan/yaptırılan çalışmalar *(Klahr vd., 2016; Klahr vd., 2017; Wang vd., 2018; Vaidya, 2019; Johns, 2020; Johns, 2021a)* ve özel şirketler tarafından yapılan/yaptırılan çalışmalar *(International Business Machines [IBM], 2014; IBM, 2015; Ponemon Institute, 2016; Willis Towers Watson, 2017; Lewis, 2018; Accenture Security & Ponemon Institute, 2019; Marsh & Microsoft, 2019; Lewis vd., 2020)* mevcuttur. Türkiye'de ise bu ilişkiyi inceleyen araştırma *(Abduladheem, 2017; Bozgeyik, 2018; Büyükkılıç, 2018; Marsh & TÜSİAD [Türk Sanayicileri ve İş İnsanları Derneği], 2020)* yok denecek kadar azdır. Bu kapsamda siber suçlar ile işletmeler arasındaki ilişkiye yeterli önemin verilmediği değerlendirilmiştir.

Ekonominin temelini işletmeler oluşturmasına karşın başta Türkiye'de olmak üzere tüm dünyada işletmelerin maruz kaldığı siber suçlarda bir anlayış eksikliği ve tedbirsizlik mevcuttur. Bu değerlendirmeye alanda yeterli çalışma yapılmamasından, işletmelerin maruz kaldığı siber suç sayısı ile maddi kayıplardaki artıştan, çalışanlara siber suçla mücadele eğitimi verilmemesinden, siber güvenlik uzmanlarından destek alınmamasından varılmıştır.

Genel amacı; işletmeleri bir siber suçun hedefi hâline getiren faktörleri araştırmak olan çalışmada üç temel araştırma sorusuna yanıt aranmıştır;

- İşletmelerin maruz kaldığı siber suç riskleri nelerdir?
- İşletmeleri siber suçlular için uygun bir hedef hâline getiren faktörler nelerdir?
- Siber suç mağduriyetinin işletmelerin siber güvenlik önlemleri üzerindeki etkileri nelerdir?

İşletmelerin en yaygın maruz kaldığı; fidye yazılımı, zararlı yazılım, bilgisayar korsanlığı ve oltalama saldırıları (Klahr vd., 2017; Wang vd., 2018; Vaidya, 2019; Johns, 2020; Johns, 2021a) araştırmada maruz kalınan siber suç çeşitleri olarak işletimselleştirilmiştir.

Araştırmanın birinci temel araştırma sorusu olan; işletmelerin maruz kaldığı siber suç riskleri, aşağıdaki araştırma sorusu ile araştırılmıştır:

Soru 1: İşletmelerin maruz kaldığı siber saldırıların (fidye yazılımı, zararlı yazılım, oltalama, bilgisayar korsanlığı) ve uğranılan zararın boyutları nelerdir?

Araştırmanın ikinci temel araştırma sorusu olan; bir işletmeyi uygun bir hedef hâline getiren faktörler ise *işletmenin büyüklüğü*, *insan faktörü* ve *dijital görünürlük* ile işletimselleştirilmiş ve çeşitli hipotezler ile araştırılmıştır.

İşletmenin büyüklüğü: Araştırmada işletmeler çalışan sayısına göre mikro, küçük, orta ve büyük olarak dört sınıfa ayrılmıştır. Büyük işletmeler sınıfına giren işletmelerde çalışan sayısı, değerli veri ve mali kaynaklar daha fazla olduğu için büyük işletmelerin siber suça maruz kalma olasılığının diğer işletmelere nazaran daha yüksek olduğu değerlendirilmiştir.

H_1: İşletmenin büyüklüğü ile uğranılan zararın büyüklüğü arasında istatistiksel olarak anlamlı bir ilişki vardır.

H_2: İşletmenin büyüklüğü ile siber suç mağduru olma olasılığı arasında istatistiksel olarak anlamlı bir ilişki vardır.

İnsan faktörü: Siber suçlarla mücadele edecek unsurlar bir futbol metaforu ile betimlenirse son savunma hattı oyuncuları, bilgisayar kullanıcılarıdır (Jansen, 2017, s. 55). İnsan faktöründe insandan kaynaklı davranışlar esas alınmıştır. Önceki araştırmalarda da insan faktörünün siber suç mağduriyetinde en büyük paya sahip olduğu ortaya çıkmıştır (IBM, 2015; Willis Towers Watson, 2017; Tessian, 2020; Akdemir & Lawless, 2020; Karsperky, 2021c).

H_3: İnsan faktörü ile işletmelerin siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki vardır.

Dijital görünürlük: Bir işletmenin siber ortamdaki genel varlığıdır. Yapılan çalışmada dijital görünürlüğün siber suç mağduriyeti üzerindeki etkisi Cohen ve Felson'un (1979) bir hedefin suça maruz kalma riskini açıkladığı *VIVA (*value [değer], inertia [hareket kabiliyeti], visibility [görünürlük], access [ulaşılabilirlik]) kuramı ile açıklanmıştır. Bu kapsamda dijital görünürlük; değer, görünürlük ve ulaşılabilirlik ile işletimselleştirilmiştir. Hareket kabiliyeti hedefin taşınabilirliği ile ilgili olup taşınabilirlik siber suçta hedefteki verinin boyutu olarak değerlendirilebileceğinden araştırma kapsamından hariç tutulmuştur.

H_4: Siber ortamda işletmelerin değeri ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki vardır.

H_5: Siber ortamda işletmelerin görünürlüğü ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki vardır.

H_6: Siber ortamda işletmelerin ulaşılabilirliği ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki vardır.

Araştırmadaki üçüncü temel araştırma sorusunda siber suç mağduriyetinin işletmelerin güvenlik önlemleri üzerindeki etkileri araştırılmıştır. Siber ortamda bilgi teknolojileri uzmanları ya da siber güvenlik uzmanları gibi fiziksel koruyucuların yanı sıra antivirüs programı, istenmeyen mesaj (spam) filtresi, casus yazılım önleme programı, güvenlik duvarı gibi teknolojik koruyucular vardır (Yar, 2005, s. 423). Siber güvenlik önlemlerinin yanı sıra siber güvenlik farkındalığı ve siber suçla mücadele eğitimi de siber güvenlikte önem arz eden iki önemli unsurdur. Siber farkındalık bireylere siber ortamı, siber suç çeşitlerini, siber suçların işlenme şekillerini ve olası sonuçlarını anlatıp siber ortamın risklerini temel seviyede kazandırmaktır. Yapılan araştırma ve anketlerde siber güvenlik eğitimi veren işletmelerin siber suç mağduriyetinin daha düşük olduğu görülmüştür (Willis Towers Watson, 2017; Johns, 2021a).

H_7: Siber suç mağduriyeti ile işletmelerin uygulamış olduğu siber güvenlik önlemleri arasında istatistiksel olarak anlamlı bir ilişki vardır.

H_8: Siber suç mağduriyeti ile siber farkındalık arasında istatistiksel olarak anlamlı bir ilişki vardır.

H_9: Siber suç mağduriyeti ile siber suçla mücadele eğitimi arasında istatistiksel olarak anlamlı bir ilişki vardır.

Yapılan araştırma ile siber suçlar neticesinde ciddi kayıplar yaşayan başta işletmeler ve suçun önlenmesiyle ilgili politika yapıcılar olmak üzere birey, kurum ve kuruluşlar için önemli bilgilere ulaşıldığı değerlendirilmiştir.

1. SİBER SUÇ ve İŞLETME

Araştırma; işletme ve siber suç olmak üzere iki temel kavramdan oluşmaktadır. Bu konuda çalışmanın daha iyi anlaşılması bakımından kavramsal bir bakış açısıyla siber suçun tanımı, siber suç çeşitleri, işletmenin tanımı ve işletme türlerinin açıklanmasıyla araştırmaya başlamanın daha faydalı olacağı değerlendirilmiştir.

1.1. Siber Suç Kavramı ve Tanımı

Siber suç kavramı yeni bir kavram olmasa da literatürde kavramın genel kabul görmüş bir tanımı yoktur (Gordon & Ford, 2006, s. 13). Google Akademik'te siber suç ile ilgili en çok atıf alan bazı eserler incelendiğinde; Wall (2004, s. 2) bilgisayar içeren her suçu siber suç olarak adlandırmanın yanlış olacağını, siber suçun ağ bağlantılı teknolojiler ile internetin sağlamış olduğu küresel yetenekle internet üzerinden işlenen suç olduğunu ifade etmiştir ve siber suçu, ağ bağlantılı cihazlarla aracılık edilen ve siber ortamda işlenen suç olarak tanımlamıştır (Wall, 2007, ss. 10-11).

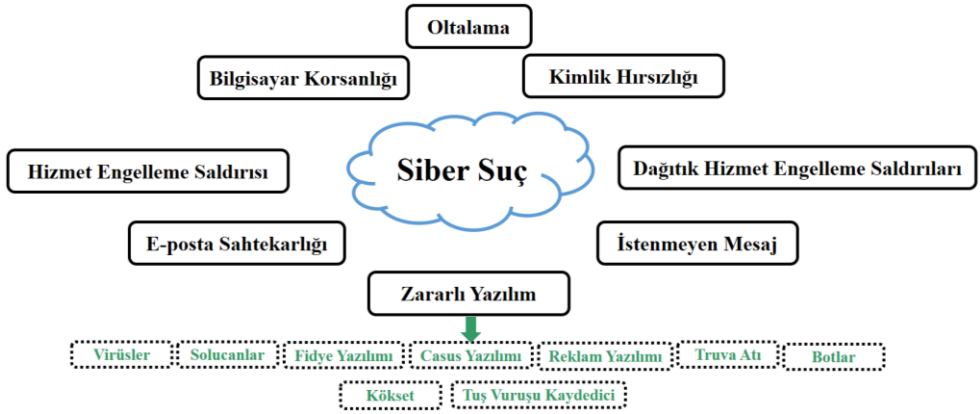
Gordon ve Ford'un (2006, s. 14) siber suç tanımında bilgisayar veya bilişim cihazlarını, Thomas ve Loader'ın (2000, s. 3) ise bilgisayar ve ağ kavramlarını ön plana çıkardığı görülmüştür. Wall (2007), Thomas ve Loader (2000) ile Gordon ve Ford'un (2006) siber suç tanımlarında siber ortam ön plana çıkmasa da suçun bilgisayar veya ağ teknolojili cihazlar vasıtasıyla icra edileceği ifade edilmiştir. Bu tanımlardan yola çıkarak siber suç; *BİT cihazlarının hedef, fail veya kolaylaştırıcı olarak kullanıldığı, genellikle internet veya ağ üzerinden işlenen suç* olarak tanımlanmıştır.

Sonuç olarak etkileriyle mekan ve sınır tanımayan (Grabosky, 2001, s. 243), bu yüzden de mevzuatta birliktelik gerektiren siber suç kavramında (Jakankhani vd., 2014, s. 152) tam bir küresel birliktelik yoktur. Ancak teknolojideki hızlı gelişmeler nedeniyle literatürde bilgisayar ve ağ teknolojisinin yardımıyla işlenen suçlar için bilgisayar suçu, yüksek teknoloji suçu, sanal suç gibi farklı kavramlar kullanılmış, siber suç da "*çok çeşitli suçları ve davranışları içeren bir şemsiye terim*" hâline gelmiştir (Marion ve Twede, 2020, s. xi). Literatürde siber suç kavramı genel kabul gören bir terim olmaya başlarken araştırmamızda da bilgisayar

ve ağ teknolojisinin yardımıyla işlenen suçlar ile ilgili siber suç terimi kullanılmıştır.

1.2. Siber Suç Çeşitleri

Siber suç; BİT cihazlarının hedef, fail veya kolaylaştırıcı olarak kullanıldığı, internet üzerinden işlenen suç olup kullanılan teknikler, hedefte istenen etki ve yayılma biçimi gibi etkenlere göre birçok çeşidi bulunmaktadır:



Şekil 1.1. Siber suç çeşitleri

Yapılan araştırmalarda işletmelerin en yaygın yaşadığı siber suçlar sırasıyla oltalama, zararlı yazılım *(fidye yazılımı hariç)*, bilgisayar korsanlığı ve fidye yazılımı saldırıları olarak ortaya çıkmıştır (Klahr vd., 2017; Wang vd., 2018; Vaidya, 2019; Johns, 2020; Johns, 2021a). Bu kapsamda dört siber suç çeşidinin tanımlarına yer verilmiştir:

1.2.1. Zararlı Yazılım

Zararlı yazılım, "özel bilgi veya verilere zarar vermek, bunlara erişmek veya bunları çalmak amacıyla, ağlara ve bilgisayarlara sızmak için kullanılan her türlü zararlı yazılım programı veya kodu" anlamına gelmektedir (Marion & Twede, 2020, s. 249). Zararlı yazılımların ortak yönü kullanıcı tarafından istenmemesi, bilinmemesi veya kullanıcıya düşman olmasıdır (Pecora, 2009, s. 121).

Zararlı yazılımlar genellikle e-posta, web tabanlı aktif içerikler, anlık mesajlaşma ve eşler arası (peer-to-peer) uygulamalar yoluyla bulaşmaktadır (Jackson, 2018, s. 619). Zararlı yazılımlar bulaştıkları cihazda verileri silme, çalma, yok etme, zarar verme, yeni siber saldırılara olanak sağlama, saldırı başlayana

kadar uykuda bekleme gibi özelliklere sahiptir. Birçok zararlı yazılım çeşidi bulunmaktadır. Bunlardan bazıları aşağıdaki gibidir:

- *Virüsler;* adını biyolojik virüsten almış olup konakçı olarak bir bilgisayar ile insan eylemine (virüslü e-postanın bir başkasına iletilmesi gibi) ihtiyaç duymakta ve insan eylemiyle ana bilgisayardan yayılmaktadır (Marion & Twede, 2020, ss. 431-432; Johansen, 2020).

- *Solucanlar;* virüslerin aksine yayılmak için de kullanıcı eylemine ihtiyaç duymadan ağlar üzerinden yayılabilen bir zararlı yazılım çeşididir (Marion & Twede, 2020, s. 450). Solucanlar bir ana bilgisayara bulaştıktan sonra güvenlik açığı olan bilgisayarları arayıp savunmasız olanlara kopyalarını yerleştirip hızlıca yayılabilme yeteneğine sahiptir (Ahmad, 2021, s. 987).

- *Fidye yazılımları;* kullanıcının bilgisayarını veya bazı dosyalarını kilitleyip kullanıcıdan fidye talep etmek amacıyla tasarlanmış bir zararlı yazılım çeşididir. Fidye yazılımcılar; kullanıcıları fidye ödenmediği takdirde bilgisayar sistemini bozma, verileri yok etme, zarar verme, dosyaları silme veya özel belgeleri ifşa etmekle tehdit etmektedir (Kharraz, 2018, s. 721).

1.2.2. Bilgisayar Korsanlığı

"Bilgisayar becerilerini başka bir kişinin veya kuruluşun bilgisayar sistemine veya ağına izinsiz veya yetkisiz olarak erişmek için kullanan kişi" *bilgisayar korsanı*, yaptığı iş de *bilgisayar korsanlığı* olarak tanımlanmıştır (Marion ve Twede, 2020, s. 205). Bilgisayar korsanları yetenekleri ile sisteme zararlı yazılım yükleyebilmekte, dosyaları silme, zarar verme, veri alma gibi işlemleri yapabilmekte, web sitelerinden kullanıcı bilgilerini çalabilmekte, bilgisayar sisteminin yazılım veya donanımını değiştirebilmekte, hatta sistemi tamamen kapatabilmektedir.

1.2.3. Oltalama

Oltalama, siber suçluların kendisini başka bir şahıs, işletme veya kurum gibi tanıtarak sahte web sitesi, sahte e-posta, sosyal medya aracılığıyla sosyal mühendislik gibi çeşitli teknikleri kullanarak kurbana ait kişisel bilgileri elde etmeye çalıştığı bir yazılım çeşididir **(**Woelk, 2009a, s. 140; Marion ve Twede, 2020, ss. 316-317). Burada siber saldırganın hedefi kurbanın kimlik ya da finansal bilgilerine erişmek olduğu hâlde yöntem olarak sosyal mühendislik, sahte e-posta, sahte web sitesi ya da başka teknikler kullanabilmektedir.

1.3. İşletme Kavramı ve Tanımı

"Tarım, sanayi, ticaret, bankacılık vb. iş alanlarında, kâr amacıyla bir sermaye yatırılarak kurulan kurum" (TDK, 2019) olarak tanımlanan işletmeler, bir ülkede sağlıklı ve güçlü bir ekonomiye sahip olmanın en önemli şartlarını oluşturmaktadır (Mucuk, 2011, s. 1). Ekonomiyi en basit tanımıyla kıt kaynakların verimli kullanımı olarak tanımlarsak işletmeler de bu kıt kaynakların üretiminden ve dağıtımından sorumlu olup ekonominin temel taşlarındandır.

İşletmelerin bir araya gelmesi ile ekonomi oluşmaktadır (Mucuk, 2011, s. 9). İşletmeler ürettikleri mal ve hizmetleri pazara sunarken aynı zamanda da yeni mal ve hizmet üretmek için de hammadde, iş gücüne ihtiyaç duymaktadır. İnsan da bir yandan işletmelerin ürettiği mal veya hizmetlerin tüketicisi konumundayken bir yandan da üreticisi konumundadır. İnsan ihtiyaçlarının sonsuz olduğu günümüzde işletmeler hem insanın mevcut ihtiyaçlarını ürettikleri mal ve hizmetler ile karşılarken hem de gelecekteki ihtiyaçları için mal ve hizmet üretmektedir (Ürper, 2018, ss. 3-4).

1.4. İşletme Türleri

Yapısı gereği işletmeler çeşitli sınıflara ayrılmaktadır. Literatürde işletmelerin ekonomik yapısı, sermaye sahipliği, büyüklükleri, faaliyet konusu, hukuki yapıları açılarından çeşitli sınıflandırmalara ayrıldığı görülmüştür. Ancak mevcut çalışmada işletmeler büyüklüklerine göre sınıflandırılıp analiz edildiğinden bu bölümde büyüklüklerine göre işletme çeşitleri açıklanmıştır.

1.4.1. Büyüklüklerine Göre İşletme Türleri

İşletmeleri büyüklüklerine göre sıralarken niteliksel ve niceliksel özellikler ön plana çıkmaktadır. "Yıllık satışlar, yıllık kârlar, varlıklar, öz sermaye miktarı, çalışanların sayısı, yatırımların toplamı" niceliksel (kantitatif) ölçütler iken, "sermaye koyanların sayısı, yönetim biçimi, bölgeye yönelik olup olmama, endüstri dalındaki nispi durum, hukuki şekil" niteliksel (kalitatif) ölçülerdir (Mucuk, 2011, ss. 94-98).

Araştırmada Türkiye'de bulunan mevzuatlar ele alınmış ve Türkiye İstatistik Kurumu (TÜİK) tarafından yapılan araştırmalarda da kullanılan *mikro, küçük, orta ve büyük ölçekli işletme* sınıflandırması kullanılmıştır.

Mikro, küçük ve orta işletmelerin tanımlarına 25997 sayılı Küçük ve Orta Büyüklükteki İşletmelerin Tanımı, Nitelikleri ve Sınıflandırılması Hakkında Yönetmelik'te (2005, md. 5) aşağıdaki gibi yer verilmiştir:

- *Mikro işletmeler*: "On kişiden az yıllık çalışan istihdam eden ve yıllık net satış hasılatı veya mali bilançosundan herhangi biri üç milyon Türk lirasını aşmayan işletmeler."

- *Küçük işletmeler*: "Elli kişiden az yıllık çalışan istihdam eden ve yıllık net satış hasılatı veya mali bilançosundan herhangi biri yirmi beş milyon Türk lirasını aşmayan işletmeler."

- *Orta işletmeler*: "İki yüz elli kişiden az yıllık çalışan istihdam eden ve yıllık net satış hasılatı veya mali bilançosundan herhangi biri yüz yirmi beş milyon Türk lirasını aşmayan işletmeler."

- *Büyük işletmeler* ise 29793 sayılı Perakende Ticarette Uygulanacak İlke ve Kurallar Hakkında Yönetmelik'te (2016, md. 3/d) orta ölçekli işletme sınırını aşan işletmeler olarak tanımlanmıştır.

2. ARAŞTIRMANIN METODOLOJİSİ

Araştırmada nicel araştırma deseni kullanılmıştır. Anket veri toplama yöntemi ile işletmelerden elde edilmiş olan veriler sosyal bilimler istatistik paketi (statistical package for the social sciences – SPSS) nicel analiz yazılımı aracılığı ile analize tabi tutulmuştur. Araştırmada ikincil veri olarak Birleşik Krallık Dijital, Kültür, Medya ve Spor Dairesi Başkanlığı tarafından yaptırılan Siber Güvenlik İhlalleri Anketi 2021'in veri setleri kullanılmıştır.

Araştırmanın ilk örneklem grubu 89372 işletmeden oluşmakta iken işletmenin telefonuna ulaşılamaması, yanlış numara gibi operasyonel nedenlerden dolayı 29074 işletmeye ulaşılmıştır. Araştırmada rastgele olasılıklı olarak örnekleme seçilen 29074 işletmeden 17947 işletmeye anket uygulanmıştır. Ancak çeşitli operasyonel nedenlerle 1419 işletme anketi tamamlamıştır (Johns, 2021b, s. 15). Bu sonuç da veri toplamının zorluğunu göz önüne sermektedir.

Araştırmada, Birleşik Krallık'ın son beş yıldaki Siber Güvenlik İhlalleri Anketi araştırmaları incelenmiş ve işletmelerin en yaygın maruz kaldığı siber suç çeşitleri belirlenmiştir. Bunlar araştırmanın bağımlı değişkenlerini *(bilgisayar korsanlığı, zararlı yazılım, fidye yazılımı, oltalama saldırısı)* oluşturmuştur. Sonrasında ise işletmeleri bir siber suçun hedefi hâline getiren unsurlar literatürde taranmış ve araştırmanın bağımsız değişkenleri *(insan faktörü, dijital görünürlük, siber güvenlik önlemleri, siber farkındalık)* oluşturulmuştur.

Araştırmada öncelikle araştırma verilerinin daha kolay anlaşılmasını sağlamak maksadıyla sıklık, yüzde ve ortalamasının grafik veya tablolar ile ifade edildiği

betimsel analiz (Yıldız, 2019, s. 172) kullanılmıştır. Sonrasında ise değişkenler arasındaki ilişkilerin varlığını, gücünü ve yönünü incelemek için Pearson Ki-kare testi, çapraz tablolamalar ve değişkenler arası ilişkinin gücünü artırmak için Phi testi kullanılmıştır.

3. ARAŞTIRMANIN BULGULARI

Araştırmanın bu bölümünde Siber Güvenlik İhlalleri Anketi 2021'in nicel analiz sonuçları sunulmuştur. Bu amaçla öncelikle tanımlayıcı istatistiksel veriler açıklanacak, sonrasında ise hipotezler test edilecektir.

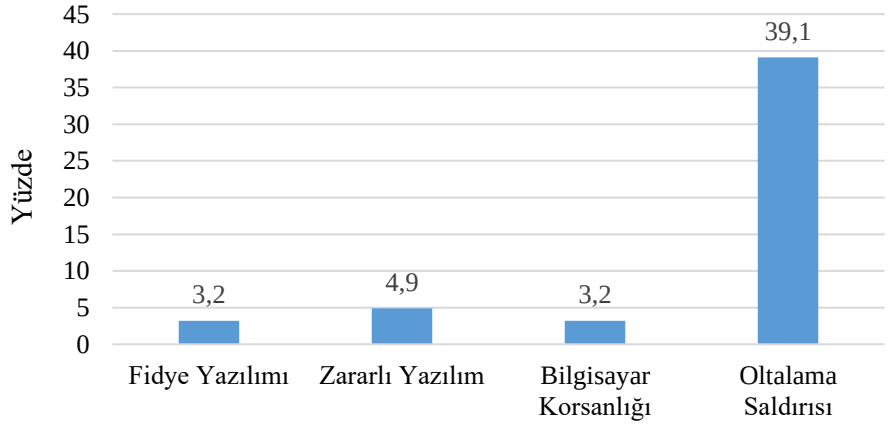
3.1. Betimsel İstatistiklerin Analizi

Örneklemdeki yapıların sıklığı hakkında bilgi sunmak amacıyla nicel analizde kullanılan değişkenlerin temel tanımlayıcı istatistiklerinin analizi bu bölümde sunulmuştur.

3.1.1. Bağımlı Değişken

Bu bölümde araştırmanın bağımlı değişkenleri olan *fidye yazılımı, zararlı yazılım, bilgisayar korsanlığı ve oltalama saldırısı* suçlarına maruz kalan işletmeler analiz edilmiştir.

Yapılan incelemede işletmelerin maruz kaldığı siber suçlarda fidye yazılımı, zararlı yazılım, bilgisayar korsanlığına maruz kalma oranlarının yakın olduğu, oltalama saldırısının ise diğer siber suç türlerine göre çok daha yaygın olduğu görülmüştür.



Şekil 3.1. Bağımlı değişkenlerin siber suça maruz kalma oranlarının karşılaştırılması

3.1.2. Bağımsız Değişken

Araştırmanın bağımsız değişkenleri insan faktörü, dijital görünürlük, siber güvenlik önlemleri ve siber farkındalık olarak dört başlıkta incelenmiştir:

- *İnsan faktörü*; siber suç açısından uzaktan veya mobil çalışma, çalışanların BT cihazlarını kullanması, fiziksel belleklerde bilgi saklama ve kişisel cihazların ticari faaliyetler için kullanılması olarak işletimselleştirilmiştir.

- *Dijital görünürlük*; bir işletmenin siber ortamdaki genel varlığı olup Felson ve Clarke'ın (1998, s. 5) VIVA (değer, hareket kabiliyeti, görünürlük, ulaşılabilirlik) kuramı ile açıklanmıştır.

- *Siber güvenlik önlemleri*; siber saldırılara karşı kişiler, kuruluşlar ya da devletler tarafından alınan tedbirler siber güvenlik önlemleridir. Siber güvenlik önlemleri; elektronik cihazların güvenliğini koruma, kurumsal verileri koruma ve çalışanlara yönelik koruma önlemleri olarak üç başlıkta incelenmiştir.

- *Siber farkındalık*; bireylerin siber ortam, siber güvenlik, siber suç ve siber suçların nasıl gerçekleştiği konusunda bilgisinin var olmasıdır (Marion ve Twede, 2020, s. 20). Bu kapsamda siber farkındalık siber suçlarla mücadele eğitimi ve siber farkındalık ile işletimselleştirilmiştir.

3.2. İki Değişkenli Analizler

İki değişkenli analizde bağımsız değişkenler ile bağımlı değişkenler arasındaki ilişki çapraz tablolar yapılarak analiz edilmiştir. Analizlerini test etmek amacıyla yapılan çapraz tablolarda H_0 (boş hipotez) bağımsız değişkenler ile bağımlı değişkenler arasında ilişkinin olmadığını ifade ederken H_a (alternatif hipotez) ilişkinin varlığına atıfta bulunmaktadır.

3.2.1. İşletmelerin Büyüklüğü ile Uğranılan Siber Suç Zararı İlişkisi

Ki-kare testi sonuçları, işletmenin büyüklüğü ile uğranılan siber suç zararı arasında istatistiksel olarak anlamlı bir şekilde ilişkili olduğunu ($\chi 2$=50,939, $p\leq$ 0,05) göstermiştir. Phi değeri ise 0,286 olup değişenler arası orta seviyede bir ilişkinin olduğu sonucu ortaya çıkmıştır. İki değişkenli analizin sonucunda P değeri 0.05'ten küçük olduğu için $H1_o$ hipotezi reddedilmiş ve alternatif hipotez kabul edilmiştir. Sonuç olarak; $H1_a$ *(işletmenin büyüklüğü ile uğranılan zararın büyüklüğü arasında istatistiksel olarak anlamlı bir ilişki vardır)* hipotezi kabul edilmiştir.

Araştırmada siber suç mağduriyeti dört siber suç için ele alınmıştır. Bu bağlamda işletmenin büyüklüğü ile fidye yazılımı, zararlı yazılım, bilgisayar korsanlığı ve oltalama saldırısı mağduriyeti arasındaki ilişki iki değişkenli çapraz tablo analizleri ile teker teker incelenmiştir.

Fidye yazılım ve *bilgisayar korsanlığı* mağduru olmada p değeri 0,05'ten büyük olduğu için işletmenin büyüklüğü ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki olmadığı sonucu ortaya çıkmıştır. Ki kare test sonuçları *zararlı yazılım* ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir şekilde ilişki olduğunu ($\chi2$=13,722, $p\leq$0,05) göstermiştir. Phi değeri 0,098 olup değişenler arası ilişki zayıftır. Zararlı yazılım ve siber suç mağduru olma oranları incelendiğinde işletmenin büyüklüğü arttıkça siber suç mağduriyetinin arttığı görülmüştür.

O*ltalama saldırısı* ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki olduğu ($\chi2$=93,293, $p\leq$0,001) görülmüştür. Phi değeri 0,256 olup değişenler arası orta seviyede bir ilişki olduğu sonucu ortaya çıkmıştır.

Siber suç mağduru olmanın ölçüldüğü dört siber suç çeşidinden sadece ikisinin değişkenler arasındaki ilişkisi istatistiksel olarak anlamlı olduğu için $H2_0$ *(işletmelerin büyüklüğü ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki yoktur)* kabul edilmiştir.

3.2.2. İnsan Faktörü Siber Suç Mağduru Olma İlişkisi

Analiz sonucunda insan faktörü ile işletimselleştirilen dört özelliğin sadece oltalama saldırısı mağduriyeti ile istatistiksel olarak anlamlı bir ilişkide olduğu görülmüştür. Bu kapsamda;

- Uzaktan veya mobil çalışma ile oltalama saldırısı mağduriyeti arasındaki ilişkinin ($\chi2$=9,964, p≤0.001) istatistiksel olarak anlamlı olduğu, phi değerinin 0,12 olup değişkenler arasında orta seviyede ilişki olduğu,

- Çalışanların BT cihazlarını kullanması ile oltalama saldırısı mağduriyeti arasındaki ilişkinin ($\chi2$=16,769, p≤0.001) istatistiksel olarak anlamlı olduğu, phi değerinin 0,155 olup değişkenler arasında orta seviyede ilişki olduğu,

- Kişisel cihazların ticari faaliyetler için kullanılması ile oltalama saldırısı mağduriyeti arasındaki ilişkinin ($\chi2$=5,902, p≤0.001) istatistiksel olarak anlamlı olduğu, phi değerinin 0,092 olup değişkenler arasında zayıf seviyede ilişki olduğu,

- Fiziksel belleklerde bilgi saklama ile oltalama saldırısı mağduriyeti arasındaki ilişkinin ($\chi 2=0,176$ $p\leq 0.001$) istatistiksel olarak anlamlı olduğu, phi değerinin 0,016 olup değişkenler arasında zayıf seviyede ilişki olduğu görülmüştür.

Sonuç olarak; insan faktörü sadece oltalama saldırısının mağduru olmada istatistiksel olarak anlamlı olduğu için, diğer siber suç çeşitlerinde istatistiksel olarak anlamlı görülmediği için $H3_0$ *(insan faktörü ile işletmelerin siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki yoktur)* kabul edilmiştir.

3.2.3. Dijital Görünürlük ile Siber Suç Mağduru Olma İlişkisi

Dijital görünürlük Felson ve Clark'ın (1998) VIVA kuramının *değer* (value), *görünürlük* (visibility) ve *ulaşılabilirlik* (accessibility) unsurları ile üç kategoride işletimselleştirilmiştir. *Hareket kabiliyeti* (inertia) hedefin taşınabilirliği ile ilgilidir, bu da siber suçta hedefteki verinin boyutu olarak değerlendirilebilecek olup araştırma kapsamından hariç tutulmuştur.

- Hedefin değeri ile siber suç mağduru olma ilişkisi

Değer, bir hedefin kolayca elden çıkarılıp çabucak maddi kazanç getirecek olmasıdır. Araştırmada hedefin değeri teknolojinin gelişmesiyle beraber işletmelerin sahip olma ihtiyacı duyacağı iki yetenek ile ölçülmüştür. Birincisi; *müşterileriniz/lehtarlarınız, hizmet kullanıcıları veya bağışçılarınız hakkında elektronik ortamda kişisel bilgi tutma* olup sadece oltalama suçu mağduriyeti ile aralarında ($\chi 2=28,378$, $p\leq 0.001$) istatistiksel olarak anlamlı bir ilişki olduğu sonucu ortaya çıkmıştır. Phi değeri ise 0,143 değişkenler arasında orta seviyede bir ilişki vardır. Diğer üç siber suç mağduriyetinde p değeri 0,05'ten büyük olduğu için istatistiksel olarak anlamlı bir ilişki bulunamamıştır.

İkincisi; *kuruluşunuzun veya müşterilerinizin ödeme yaptığı bir çevrim içi banka hesabı kullanımı* olup herhangi bir siber suç mağduriyeti çeşidi ile aralarında istatistiksel olarak anlamlı bir ilişki bulunamamıştır.

Sonuç olarak; hedefin değerinin işletimselleştirildiği iki değişkenden sadece birinin bir siber suç türü ile istatistiksel olarak anlamlı olduğu için $H4_0$ *(Siber ortamda işletmelerin değeri ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki yoktur)* kabul edilmiştir.

- Hedefin görünürlüğü ile siber suç mağduru olma ilişkisi

Hedefin görünürlüğü işletmelerin günümüzde kullanacağı iki özellik ile ölçülmüştür. Birincisi, *sosyal medya sitelerindeki hesap veya sayfa (ör. Facebook veya Twitter) kullanımıdır*. Değişkenler arasındaki ilişki; fidye yazılımı mağduru olmada ($\chi2$=3,825, p≤0.05), bilgisayar korsanlığı mağduru olmada ($\chi2$=0,452, p≤0.05) ve oltalama saldırısı mağduru olmada ($\chi2$=27,089, p≤0.001) istatistiksel olarak anlamlıdır. Phi değerleri ise sırasıyla 0,052, 0,018, 0,138'dir. Zararlı yazılım mağduriyetinde ($\chi2$=3,825, p≥0.05) ise değişkenler arasında istatistiksel bir anlamlı bir ilişki bulunamamıştır.

Hedefin görünürlüğü ile işletimselleştirilen ikinci özellik; *müşterilerin çevrim içi ürün veya hizmetler için sipariş verme, rezervasyon yapma veya ödeme yapma yeteneğidir*. Değişkenler arasındaki ilişki fidye yazılımı mağduriyetinde ($\chi2$=7,478, p≤0.05), zararlı yazılım mağduriyetinde ($\chi2$=6,012, p≤0.05) ve bilgisayar korsanlığı mağduriyetinde ($\chi2$=11,439, p≤0.001) olup istatistiksel olarak anlamlıdır. Phi değerleri sırasıyla 0,073, 0,064, 0,090'dır. Oltalama saldırısı mağduriyetinde p değeri 0,05'ten büyük olduğu için istatistiksel olarak anlamlı bir ilişki bulunamamıştır.

Sonuç olarak siber ortamda hedefin görünürlüğünün siber suç mağduru olmayı artırdığını ifade eden $H5_a$ *(siber ortamda işletmelerin görünürlüğü ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki vardır)* kabul edilmiştir.

- Hedefin ulaşılabilirliği ile siber suç mağduru olma ilişkisi

Ulaşılabilirlik; suçlunun hedefe ulaşması ve sonrasında suç mahallinden uzaklaşma yeteneği olup iki özellik ile işletimselleştirilmiştir.

Windows'un eski sürümlerinin yüklü olduğu bilgisayarlar (ör. Windows 7 veya 8) kullanımı ile zararlı yazılım mağduriyeti ($\chi2$=4,549, p ≤0.05) arasında istatistiksel olarak anlamlı bir ilişki bulunduğu, phi değerinin 0,057 olduğu için değişkenler arasında zayıf bir ilişki olduğu görülmüştür. Fidye yazılımı mağduriyeti, oltalama saldırısı mağduriyeti ve bilgisayar korsanlığı mağduriyeti ile arasındaki ilişkide p değeri 0,05'ten büyük olduğu için istatistiksel olarak anlamlı bir ilişki bulunmamıştır.

Bazen akıllı cihazlar olarak adlandırılan televizyonlar, bina kontrolleri, alarmlar, hoparlörler vb. gibi ağa bağlı cihazların kullanımı ile fidye yazılımı mağduriyeti, zararlı yazılım mağduriyeti ve bilgisayar korsanlığı mağduriyeti

arasında p değeri 0,05'ten büyük olduğu için istatistiksel olarak anlamlı bir ilişki bulunamamıştır. Oltalama saldırısı mağduriyeti ile arasında ise ($\chi 2$=14,802, $p \leq 0.001$) istatistiksel olarak anlamlı bir ilişki olup phi değeri 0,102 olduğundan orta seviyede ilişki mevcuttur.

Sonuç olarak hedefin ulaşılabilirliğini ifade eden özelliklerden ikisi ile siber suç mağduru olma arasında istatistiksel anlamda ilişki olmadığından $H6_0$ *(siber ortamda işletmelerin ulaşılabilirliği ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki yoktur)* kabul edilmiştir.

3.2.4. Siber Suç Mağduriyeti ile Siber Güvenlik Önlemleri Arasındaki İlişki

Siber güvenlik önlemleri elektronik cihazların güvenliğini koruma, kurumsal verileri koruma ve çalışanlara yönelik koruma önlemleri esas alınarak işletimselleştirilmiş ve on dört siber güvenlik önlemiyle işletmelerin almış oldukları siber güvenlik önlemleri ile siber suç mağduriyeti arasındaki ilişki analiz edilmiştir. Analiz sonucunda altı siber güvenlik tedbiri ile siber mağduriyet arasında istatistiksel olarak anlamlı ilişki olduğu görülmüştür.

Elektronik cihazların güvenliğini koruma;

- Personel ve ziyaretçiler için ayrı wi-fi ağları *(istatistiksel olarak anlamlı)*,
- Yazılım güvenlik güncellemelerini 14 gün içinde uygulamaya yönelik bir politika *(istatistiksel olarak anlamlı değil)*,
- Uzaktan bağlanan personel için sanal özel ağ tedbirleri *(istatistiksel olarak anlamlı)*,
- Şirkete ait cihazlarda (örneğin dizüstü bilgisayarlar) güvenlik kontrolleri *(istatistiksel olarak anlamlı)*,
- Tüm BT ağınızı ve ayrıca bireysel cihazları kapsayan güvenlik duvarları *(istatistiksel olarak anlamlı değil)*,
- Güncel zararlı yazılım koruması *(istatistiksel olarak anlamlı değil)*,
- Yalnızca şirkete ait cihazlar aracılığıyla erişime izin verilmesi *(istatistiksel olarak anlamlı)*.

Çalışanlara yönelik koruma;

- Personelin sahte bir e-posta veya kötü amaçlı bir web sitesi belirlediklerinde izlemesi için üzerinde anlaşmaya varılan bir süreç *(istatistiksel olarak anlamlı)*,

- Kullanıcı etkinliğinin herhangi bir şekilde izlenmesi *(istatistiksel olarak anlamlı)*,
- Kullanıcıların güçlü parolalar belirlemesini sağlayan bir parola ilkesi *(istatistiksel olarak anlamlı değil)*,
- BT yöneticisini ve belirli kullanıcılara erişim haklarını kısıtlama *(istatistiksel olarak anlamlı değil)*,

Kurumsal verileri koruma;

- Bir bulut hizmeti aracılığıyla verileri güvenli bir şekilde yedekleme *(istatistiksel olarak anlamlı değil)*,
- Verileri başka yollarla güvenli bir şekilde yedekleme *(istatistiksel olarak anlamlı değil)*,
- Kişisel veri dosyalarının güvenli bir şekilde saklanması ve taşınması için özel kurallar *(istatistiksel olarak anlamlı değil)*.

Sonuç olarak on dört siber güvenlik önleminden sadece altısı ile istatistiksel olarak anlamlı çıktığı için $H7_0$ *(siber suç mağduriyeti ile işletmelerin uygulamış olduğu siber güvenlik önlemleri arasında istatistiksel olarak anlamlı bir ilişki yoktur)* kabul edilmiştir.

Ancak işletmelerin en yaygın siber suç mağduru olduğu oltalama suçu mağduriyetinin 14 siber güvenlik önlemi ile istatistiksel olarak anlamlı bir ilişkide olduğu, ayrıca değişkenler arasında orta derecede bir ilişki ortaya çıkmıştır. Bu yüzden "*oltalama suçu mağduriyeti ile siber güvenlik mağduriyeti arasında istatistiksel olarak anlamlı bir ilişki vardır"* sonucuna da erişilmiştir.

3.2.5. Siber Suç Mağduriyeti ile Siber Farkındalık Arasındaki İlişki

Siber farkındalık siber suçlarla mücadele eğitimi ve siber farkındalık ile işletimselleştirilmiştir. Siber suç mağduriyeti ve siber farkındalık ilişkisinin analizi sonucunda sadece oltalama saldırısı mağduriyeti ile siber farkındalık arasında istatistiksel olarak anlamlı ($\chi 2=30{,}562$, $p\leq 0.001$) bir ilişki olduğu görülmüştür. Phi değeri ise -0,147 olup değişkenler arasında orta seviyede negatif bir ilişki olduğu görülmüştür. Sonuç olarak dört siber suç mağduriyetinden sadece oltalama suçu ile siber farkındalık arasında istatistiksel olarak anlamlı bir ilişki olduğu için $H8_0$ *(Siber suç mağduriyeti ile işletmelerin siber farkındalığı arasında istatistiksel olarak anlamlı bir ilişki yoktur)* kabul edilmiştir.

Siber suçla mücadele eğitimi alma eğilimi ile fidye yazılımı mağduriyeti ($\chi2=3,991$ $p\leq0.05$), bilgisayar korsanlığı mağduriyeti ($\chi2=13,721$ $p\leq0.001$) ve oltalama saldırısı mağduriyeti ($\chi2=49,135$ $p\leq0.001$) arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmüştür. Phi değerleri ise sırasıyla -0,053, -0,098, -0,186'dır. Buna göre değişkenler arasındaki ilişki ile fidye yazılımı ve bilgisayar korsanlığı mağduriyeti için negatif zayıf seviyede olup oltalama suçu için negatif orta seviyededir. Zararlı yazılım mağduriyetinde ise p değeri 0,05'ten büyük olduğu için istatistiksel olarak anlamlı bir ilişki görülmemiştir. Siber suç mağduriyeti ile siber suçla mücadele eğitimi alma oranları incelendiğinde ise siber suç mağdurlarının daha az siber suçla mücadele eğitimi aldığı görülmüştür.

Sonuç olarak; dört siber suç mağduriyetinden üçü siber suçla mücadele eğitimi ile istatistiksel olarak anlamlı bir ilişkide olduğu için $H9_a$ *(Siber suç mağduriyeti ile işletmelerin siber suçlarla mücadele eğitimi alma eğilimi arasında istatistiksel olarak anlamlı bir ilişki vardır)* kabul edilmiştir.

4. SONUÇ VE ÖNERİLER

İşletmeleri bir siber suçun hedefi haline getiren faktörleri belirlemek amacıyla gerçekleştirilen bu çalışmada; işletmelerin büyüklükleri açısından siber suç mağduru olması ve yaşadığı siber suç zararının karşılaştırılması yapılmış, siber suç mağduriyeti ile insan faktörü, dijital görünürlük, siber güvenlik önlemleri ve siber farkındalık ilişkisi ölçülmüştür.

Gelişen teknoloji ile değerli veri ve mali kaynakları artan ve belli bir sayının üstünde çalışana sahip olan orta ve büyük işletmeler bir yandan BİT cihazları ve interneti daha yoğun kullanıp dijitalleşirken diğer yandan daha fazla siber suça maruz kalmaktadır. Siber suçun işletmeleri iflasa kadar sürükleyen etkileri de değerlendirildiğinde işletmelerin büyürken siber güvenlik önlemlerine daha fazla dikkat etmeleri gerektiği değerlendirilmiştir. Yapılan çalışmada işletmenin büyüklüğü ile maruz kalınan siber suç zararı arasında istatistiksel olarak anlamlı bir ilişki olduğu sonucu da ortaya çıkmıştır.

Bir diğer önemli sonuç ise oltalama suç mağduriyetinin işletmeler arasında diğer suç türlerine göre kayda değer şekilde daha yaygın olduğudur. Araştırma kapsamında işletmelerin %39,1'inin oltalama suçuna maruz kaldığı sonucu ortaya çıkmıştır. Bu oran zararlı yazılımlar için %4,9, bilgisayar korsanlığı ve fidye yazılımında %3,2'dir. Oltalama suçu mağduriyeti işletmelerin yaşadığı siber suç mağduriyetinde büyük bir paya sahip olmakla beraber oltalama suçu

mağduriyetinin insan faktörü, dijital görünürlük, siber güvenlik önlemleri ve siber farkındalık ile istatistiksel olarak anlamlı ilişkide olduğu görülmüştür.

Oltalama suçunu diğer üç siber suçtan ayıran en önemli özellik ise oltalama suçunun sosyal mühendisliğe, yani temelinde aldatmaya dayalı bir siber suç olmasıdır. Diğer üç siber suçta aldatma tekniği kullanılsa bile öncelikli yöntem değildir. Sosyal mühendisliğin öne çıktığı oltalama suçunda ise "kişisel yetenekli vesayet" kavramı ön plana çıkmaktadır. Siber suçta yetenekli koruyucu sadece siber güvenlik önlemleri değildir, BİT cihazı kullanıcısı da kendisinin koruyucusudur.

Sosyal mühendislikte insanı kandırmak esas olduğu için işletmelerdeki insan faktörünün siber suç mağduriyetine etkisi araştırılmış olup insan faktörü ile siber suç mağduriyeti arasında güçlü bir pozitif ilişki olduğu sonucu ortaya çıkmıştır. İşletmelerin siber güvenlik konusundaki en zayıf kullanıcısı kadar kuvvetli olduğu gerçeğinden yola çıkarak işletmeler tarafından BİT cihazlarının ve internetin kullanım esaslarının belirlenmesi, kullanıcı etkinliğinin izlenmesi, çalışanlara siber suçla mücadele eğitimi verilmesi gibi tedbirlerin oltalama suçu mağduriyetini azaltacağı değerlendirilmiştir.

Araştırma kapsamında siber suç mağduriyeti ile siber güvenlik önlemleri alma arasındaki ilişki incelenmiştir. Siber güvenlik önlemlerinin işletimselleştirildiği elektronik cihazların güvenliğini koruma, kurumsal verileri koruma ve çalışanlara yönelik koruma açısından ele alındığında kurumsal verileri koruma tedbirleri ile siber suç mağduriyetinin istatistiksel olarak anlamlı çıkmadığı görülmüştür. Bunun sebebinin de siber suçluların ilk önce insan hatasına, sonrasında ise elektronik cihazların güvenliğini kırmaya yönelik çabalarının olması olarak değerlendirilmiştir.

Çalışmanın bir diğer önemli bulgusu da işletmelerin siber ortamdaki görünürlüklerinin siber suç mağduriyetini artırdığıdır. İnternet kullanımı ve internet üzerinden alışveriş yapma gibi alışkanlıkların yaygınlaştığı dönemde işletmelerin görünürlüğü önem kazanırken işletmelerin siber suç mağduru olma riski de artmaktadır. Bu sonuç siber saldırganların hedef seçiminde rasyonel davrandıklarını ve daha görünür hedeflere yöneldiklerini göstermiştir.

İşletmelerin dijital görünürlüğünde değer kuramı ile işletimselleştirilen özelliklerin siber suç mağduriyeti ile istatistiksel olarak anlamlı çıkmadığı görülmüştür. Bu sonuç da her ne kadar siber suçlular değerli verileri hedeflese de öncelikli hedeflerinin insan hatasından, sonrasında elektronik cihazlardaki güvenlik

eksikliklerden yararlanarak siber saldırıyı gerçekleştirmek olduğunu gösterdiği değerlendirilmiştir. Bu kapsamda işletmeler çalışanlarına ve elektronik cihazlarına yönelik tedbirleri yeniden gözden geçirmeli ve eksiklikleri gidermelidir.

Araştırma kapsamında ele alınan dört siber suçtan üçü ile siber suçla mücadele eğitimi arasında istatistiksel olarak anlamlı bir ilişki ortaya çıkmıştır. İşletmeler siber suçla mücadele konusunda alabilecekleri tedbirleri belirlemeli, çalışanlarına bilmesi gereken prensibine göre eğitim vermelidir. İşletmeler tarafından çalışanlara siber güvenlik konularında eğitim verilerek siber suç mağduriyetinin azaltılacağı değerlendirilmiştir.

Araştırmada siber suç mağduriyeti yaşayan işletmelerin siber suç mağduriyeti ile siber farkındalıkları arasında istatistiksel olarak anlamlı bir ilişki olup olmadığı incelenmiş, sadece oltalama suçu mağduriyeti ile siber farkındalık arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmüştür. Siber farkındalık; bireylerin siber ortam, siber güvenlik, siber suç gibi konularda ve siber suçların nasıl gerçekleştiği konusunda bilgi sahibi olması (Marion ve Twede, 2020, s. 20) şeklinde tanımlanmıştır. Siber farkındalık siber suçla mücadele eğitimine göre daha temel seviyededir. Siber suç mağduriyeti ile siber suçla mücadele eğitimi arasında ise istatistiksel olarak anlamlı bir ilişki olduğu sonucu ortaya çıkmıştır. Siber farkındalığın sadece oltalama suçu ile anlamlı ilişkide olmasının nedeninin oltalama suçunun araştırmada ele alınan diğer üç siber suç türüne göre, insanı aldatmaya yönelik daha basit tekniklerle işlenmekte olması olarak değerlendirilmiştir. Ancak oltalama suçunun işletmelerin maruz kaldığı en yaygın suç olması ve siber farkındalığın kolayca kazandırılabilir olması sebepleriyle işletmeler tarafından siber farkındalığı artırıcı tedbirlerin hızlı bir şekilde alınması gerektiği değerlendirilmiştir.

4.1. İşletmelere Öneriler

İşletmeler açısından etkili önleyici stratejiler geliştirmek ve uygulamak elzem hâle gelmiştir. Araştırma neticesinde büyüklükleri açısından tüm işletme çeşitlerinin siber suç zararına maruz kaldığı, orta ve büyük işletmelerin ise daha fazla siber suç zararı yaşadığı sonucu ortaya çıkmıştır. Bu kapsamda üretim, satış, tanıtım gibi süreçlerde, müşteri, tedarikçi gibi paydaşları ile ilişkide interneti ve BİT cihazlarını kullanmaya başlayan mikro, küçük, orta ve büyük işletmeler, faaliyet konularına göre ihtiyaç duydukları alanlarda makine mühendisi, fizik mühendisi çalıştırdığı gibi siber güvenlik uzmanı edinmeli veya siber güvenlik danışmanlığı hizmeti almalıdır.

Siber ortamdaki görünürlük; teknolojinin gelişmesi ve hayatın dijitalleşmesi ile beraber işletmeler için adeta zorunluluk hâline gelse de görünürlük artarken güdülenmiş siber suçlularla daha çok karşılaşılacağı için işletmeler tarafından gerekli siber güvenlik önlemleri alınmalıdır.

İşletmelerdeki siber suç mağduriyetinin büyük bir kısmının insan hatasından kaynaklanan oltalama suçu olduğu unutulmamalı, siber farkındalık ve siber suçla mücadele eğitimlerine ağırlık verilmelidir. Dış dünyaya kapalı olacak şekilde tasarlanan İran'ın Natanz Uranyum Zenginleştirme Tesisine bir çalışanın fiziksel belleğine virüs bulaştırmak vasıtasıyla gerçekleştirilen Stuxnet saldırısı, insan hatasının nelere yol açabileceğinin tarihteki sadece bir örneği olmuştur.

4.2. Birey Açısından Alınması Gereken Siber Güvenlik Önlemleri

Teknolojinin ilerlemesi ile internet ticarette araç olarak kullanılmaya başlamıştır. Artan siber suçlarda sorumluluk devlet yetkilileri veya siber güvenlik uzmanlarında olduğu kadar bireysel kullanıcıda da olduğu değerlendirilmektedir. *"İki bin yıl önce karasal uzayda olduğu gibi, bugün siber ortamda, ilk savunma hattı kendini savunma olacaktır*" (Grabosky, 2001, s. 248) sözü de bu savı desteklemektedir. Bu kapsamda bireysel kullanıcıların alması gereken siber güvenlik önlemleri hakkında Avast (2021), Kaspersky (2021b) ve Norton (2021) tarafından yapılan öneriler aşağıdaki gibidir;

- Güçlü parola kullanılmalıdır.
- Orijinal antivirüs yazılımları, güvenlik yazılımları ve güvenlik duvarı kullanılmalıdır.
- Teknolojinin gelişmesi ile beraber değişen siber suçlara karşı bilgi edinilmelidir.
- Sosyal medya hesaplarında paylaşılan kişisel veriler sınırlandırılmalıdır.
- Ebeveynleri tarafından çocuklar siber zorbalık, siber taciz, kimlik hırsızlığı gibi konularda bilgilendirilmelidir.
- Tanınmayan kişilerden gelen veya şüpheli e-postalar açılmamalı, linklere giriş yapılmamalıdır.
- Topluma açık hâlde bulunan kablosuz internet ağlarına giriş yapılmamalıdır.
- Önemli veriler fiziksel bir bellek veya bulutta yedeklenmelidir.

4.3. Politika Yapıcılara Öneriler

Siber suçu geleneksel suçtan ayıran en önemli özellikler; siber suçun mesafe ve sınır tanımazlığı, maddi olmayan dijital kanıtlar içermesi, failin tespit edilmesinin veya yakalanmasının zorluğu, siber suçun otomatik olarak binlerce, hatta milyonlarca insanı etkileyebilmesi (Ngo, 2018, s. 133) olarak değerlendirilmektedir. Bu kapsamda siber suçla mücadele edecek unsurlar için mevzuatta küresel birliktelik gerekmektedir. Birleşmiş Milletler Ticaret ve Kalkınma Konferansı'nın (United Nations Conference on Trade and Development – UNCTAD) (2022) yaptığı bir araştırmaya göre dünyadaki ülkelerin sadece %80'inde siber suç mevzuatı oluşturulmuştur. Oran yüksek gibi gözükse de bu sonuç dünyadaki ülkelerin %20'sini oluşturan ülkelerde siber suçun suç olarak tasnif edilmediği anlamına da gelebilmektedir. Siber suçun suç olmadığı bir ülkeden siber saldırı gerçekleştiren bir siber suçlu, ülkeler arasında ikili anlaşma yoksa tespit edilse dahi herhangi bir cezai yaptırımla karşılaşmayabilecektir. Dolayısıyla siber suçla mücadelede küresel mevzuatta birliktelik ve uluslararası iş birliği gerekmektedir.

Siber suç mağduru olunmaması için siber suçla mücadele eğitimi alınması gerekmektedir. Bu bağlamda okullarda siber güvenlik konusu eğitim programına dâhil edilmeli ve eğitimlere ağırlık verilmelidir.

Teknolojinin hızlı gelişmesiyle beraber hayatın her alanında dijitalleşme devam etmektedir. Şu an gelişmekte olan teknolojik gelişmeler zamanla toplum hayatına daha fazla girecektir. Bu bağlamda ceza adalet sisteminde siber suç yeniden gözden geçirilmelidir.

Siber suç konusunda gerekli güvenlik önlemlerini almayan işletmeler kimi zaman büyük zararlar yaşamakta, bazen de kapanmak zorunda kaldığından belirlenecek kriterlere göre işletmeler tarafından siber güvenlik sigortası yaptırılmasının zorunlu hâle getirilmesi değerlendirilmelidir.

4.4. Sonuç

Teknolojinin insan hayatını kolaylaştırdığı bir dönemde, bilgi ve yeteneklerini geliştiren siber suçlular sayesinde siber tehditler her geçen gün artmaktadır. Bu husus Felson ve Clarke'ın (1998) Suç Fırsatı Perspektifinin "sosyal ve teknolojik değişimler yeni suç fırsatları yaratır" varsayımı ile örtüşmektedir. İnsanların hem üretici hem de tüketici olarak iş birliği içinde bulunduğu, ekonominin temelini

oluşturan işletmeler için risk her geçen gün artmaktadır. İşletmelerin siber suçtan korunabilmesi için suça sebebiyet veren fırsatların önlenmesi gerekmektedir.

Araştırmada işletmeleri bir siber suçun hedefi hâline getiren unsurlar; işletmelerin siber suç mağduriyetine en çok maruz kalınan siber suç çeşitleri açısından ele alınarak farklı bir bakış açısı sunulmak istenmiştir. Ancak bu unsurlar siber suça neden olan tüm unsurlar olamayacağı gibi, önerilen çözümler de tüm güvenlik çözümleri değildir. Burada işletmelere genel bir çerçeve sunulmak istenmiştir. Sonrasında yapılacak çalışmalar ve işletmeler tarafından alınacak tedbirlerle bu çerçeve genişletilebilir. Ayrıca teknolojinin gelişmesi ile siber suçta yeni türler ortaya çıkmaktadır. Dolayısıyla siber suç, yaşayan bir organizma gibi evrim geçirebilen bir suç olup devamlı gözlem altında tutulmalı ve siber suç konulu çalışmalar devam ettirilmelidir.

KAYNAKÇA

Abduladheem, M. S. (2017). Farklı işletmelerin ortak siber güvenlik politikalarının karşılaştırmalı araştırması [Yayınlanmamış yüksek lisans tezi]. Atılım Üniversitesi, Ankara.

Accenture Security, & Ponemon Institute. (2019). The cost of cybercrime. Erişim tarihi: 21.08.2021, https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.

Ahmad, M. A. (2021). Worms. B. Warf. (Ed.). The sage encylopedia of the internet içinde (ss. 987-992). Sage Publications.

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. Internet Research, 30(6), 1665-1687. Erişim tarihi: 30.09.2021, https://doi.org/10.1108/INTR-10-2019-0400.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Eeten, M., Levi, M., Moore, T., & Savage, S. (2012). Measuring the cost of cybercrime. Erişim tarihi: 18.09.2021, https://doi.10.1007/978-3-642-39498-0_12.

Avast. (2021). What is cyber security? Erişim tarihi: 18.10.2021, https://www.avast.com/c-b-what-is-cybersecurity.

Birleşmiş Milletler Ticaret ve Kalkınma Konferansı. (2021). Cybercrime legislation worldwide. Erişim tarihi: 23.08.2021, https://unctad.org/page/cybercrime-legislation-worldwide.

Bozgeyik, A. (2018). Gaziantep'te faaliyet gösteren orta ve büyük ölçekli işletmelerin siber güvenlik yönetim yaklaşımlarının analizi [Yayınlanmamış doktora tezi]. Hasan Kalyoncu Üniversitesi Sosyal Bilimler Enstitüsü, Gaziantep.

Büyükkılıç, M. (2018). Cybersecurity framework for small and medium size enterprises [Yayınlanmamış yüksek lisans tezi]. Bahçeşehir Üniversitesi, İstanbul.

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review. 44.

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief. Police research series, paper, 98 (1-36).

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journel in Computer Virology, 2(1). 13-20.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? Social & Legal Studies, 10(2), 243-249.

IBM. (2014). IBM security services 2014 cyber security intelligence index. Erişim tarihi: 07.10.2021, https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF.

IBM. (2015). IBM security services 2015 cyber security intelligence index. Erişim tarihi: 07.10.2021, https://securityintelligence.com/media/cyber-security-intelligence-index-2015/.

Jackson, L. A. (2018). Malware. B. Warf. (Ed.). The sage encylopedia of the internet içinde (ss. 619-624). Sage Publications.

Jakankhani H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. Akhgar, B., Staniforth, A., & Bosco, F. (Ed.). Cyber crime and cyber terrorism investigator's handbook içinde (ss. 149-164). Elseviar.

Johns, E. (2020). Cyber security breaches survey 2020: Main report. London: Department for Digital, Culture, Media & Sport. Erişim tarihi: 12.12.2021, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020.

Johns, E. (2021a). Cyber security breaches survey 2021: Main report. London: Department for Digital, Culture, Media & Sport. Erişim tarihi: 13.12.2021, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021.

Johns, E. (2021b). Cyber security breaches survey 2021: Technical annex. London: Department for Digital, Culture, Media and Sport. Erişim tarihi: 13.12.2021, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021.

Kharraz, A. (2018). Ransomware. B. Warf. (Ed.). The sage encylopedia of the internet içinde (ss. 720-724). Sage Publications.

Klahr, R., Amili, S., Shah, J., Wang, V., & Button, M. (2016). Cyber security breaches survey 2016: Main report. Erişim tarihi: 16.12.2021, https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016.

Kaspersky. (2021b). Siber güvenlik nedir? Erişim tarihi: 17.08.2021, https://www.kaspersky.com.tr/resource-center/definitions/what-is-cyber-security.

Kaspersky. (2021c). The human factor in IT security: How employees are making businesses vulnerable from within. Erişim tarihi: 18.09.2021, https://www.kaspersky.com/blog/the-human-factor-in-it-security/.

Klahr, R., Shah, J., Sheriffs, P., Tossington, T., Pestell, G., Button, M., & Wang, V. (2017). Cyber security breaches survey 2017: Main report. Erişim tarihi: 15.12.2021, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017.

Küçük ve Orta Büyüklükteki İşletmelerin Tanımı, Nitelikleri ve Sınıflandırılması Hakkında Yönetmelik. (2005, 18 Kasım). Resmi Gazete (Sayı: 25997). Erişim tarihi: 15.10.2021, https://www.resmigazete.gov.tr/eskiler/2018/06/20180624-7.pdf.

Lewis, J. A. (2018). Economic impact of cybercrime. McAffee. Erişim tarihi: 11.11.2021, https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf.

Lewis, J. A., Smith, Z. M., & Lostri, E. (2020). The hidden costs of cybercrime. McAffee. Erişim tarihi: 10.11.2021, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

Marion, N. E., & Twede, J. (2020). Cybercrime: An encyclopedia of digital crime. ABC-CLIO.

Marsh, & Microsoft. (2019). 2019 global cyber risk perception survey. Erişim tarihi: 15.02.2022, https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf.

Marsh, & TÜSİAD. (2020). 2020 Türkiye siber risk algı araştırması. Erişim tarihi: 17.02.2022, https://tusiad.org/tr/yayinlar/raporlar/item/10602-2020-turkiye-siber-risk-algi-arastirmasi.

Mucuk, İ. (2011). Modern işletmecilik (17nci basım). Türkmen Kitabevi. (Orijinal çalışma basım tarihi 1983).

Ngo, F. T. (2018). Cybercrime. B. Warf. (Ed.). The sage encylopedia of the internet içinde (ss. 128-134). Sage Publications.

Norton. (2022). Bot and botnet. Erişim tarihi: 27.07.2022, https://www.nortonlifelockpartner.com/security-center/bots.html.

Pecora, D. (2009). Malware. Mcquade, S. C. (Ed.). Encyclopedia of cybercrime içinde (ss. 121-123). Greenwood Press.

Ponemon Institute. (2016). 2016 cost of cyber crime study & the risk of business innovation. Erişim tarihi: 07.02.2022, https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf.

Prakende Ticarette Uygulanacak İlke ve Kurallar Hakkında Yönetmelik. (2016, 6 Ağustos). Resmi Gazete (Sayı: 29793). Erişim tarihi: 02.09.2021, https://www.resmigazete.gov.tr/eskiler/2016/08/20160806-4.html.

TDK. (2019). İşletme. Sozluk.gov.tr sözlüğü içinde. Erişim tarihi: 02.08.2021, https://sozluk.gov.tr/.

Tessian. (2020). Psychology of human error. Erişim tarihi: 29.10.2021, https://www.tessian.com/research/the-psychology-of-human-error/.

Thomas, D., & Loader, B. (2000). Cybercrime: Law enforcement, security and surveillance in the information age. D. Thomas, & B. Loader. (Ed.). Cybercrime: Law enforcement, security and surveillance in the information age içinde (ss. 1-13). Routledge.

Ürper, Y. (2018). İşletmeler ve özellikleri. Z. Erdoğan, & A. Hepkul (Ed.). Genel işletme içinde (ss. 2-33). Anadolu Üniversitesi Yayınevi.

Vaidya, R. (2019). Cyber security breaches survey 2019: Main report. Department for Digital, Culture, Media and Sport, 66. Erişim tarihi: 19.12.2021, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019.

Veenstra, S., Zuurveen, R., & Stol, W. (2016). Cybercrime among companies: Research into cybercrime victimisation among small- and medium-sized enterprises and one-man businesses in the Netherlands. Eleven International Publishing.

Yıldız, A. (2019). İşletme alanında nicel araştırma yöntemleri ve yayın etiği. Gazi Kitabevi.

Wall, D. S. (2004). What are cybercrimes. The Centre for Crime and Justice Studies, 58(4). Erişim tarihi: 02.07.2021, https://www.crimeandjustice.org.uk/publications/cjm/article/what-are-cybercrimes.

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity.

Wang, V., Button, M., Finnerty, K., Motha, H., Shah, J. Y., & White, Y. F. (2018). Cyber security breaches survey 2018: Main report. Erişim tarihi: 18.12.2021, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018.

Willis Towers Watson. (2017). 2017 siber risk anketi. Erişim tarihi: 14.10.2021, https://www.willistowerswatson.com/-/media/WTW/Insights/2017/06/WTW-Cyber-Risk-Survey-US-2017.pdf?modified=20170609193130.

Woelk, B. (2009b). Preventing cybercrime. Mcquade III, S.C. (Ed.). Encyclopedia of cybercrime içinde (ss. 144-150). Greenwood Press.

Yar, M. (2005). The novelty of cybercrime: An assessment in light of routine activity theory. European Journal of Criminology 2(4), 407–427.