SAKARYA ÜNİVERSİTESİ

JOBS

İşletme Bilimi Dergisi
The Journal of Business Science

Sakarya Üniversitesi / Sakarya University
İşletme Fakültesi / Sakarya Business School

Cilt/Volume : 9
Sayı/Issue : 2
Yıl/Year :2021

ISSN: 2148-0737

DOI: 10.22139/jobs

İşletme Bilimi Dergisi
2021
Cilt:9 Sayı:2

İNDEKS BİLGİLERİ/ INDEXING INFORMATION

JOBS

İşletme Bilimi Dergisi
2021
Cilt:9 Sayı:2

İşletme Bilimi Dergisi
2021
Cilt:9 Sayı:2

Dergimize yayınlanmak üzere gönderilen makalelerin yazımında etik ilkelere uyulduğu ve yazarların ilgili etik kurulundan gerekli yasal onayları aldığı varsayılmaktadır. Bu konuda sorumluluk tamamen yazarlara aittir. İşletme Bilimi Dergisi'nde yer alan makalelerin bilimsel sorumluluğu yazara aittir. Yayınlanmış eserlerden kaynak gösterilmek suretiyle alıntı yapılabilir.

It is assumed that the articles submitted for publication in our journal are written in ethical principles and the authors have obtained the necessary legal approvals from the relevant ethics committee. The responsibility of this matter belongs to the authors. Scientific responsibility for the articles belongs to the authors themselves. Published articles could be cited in other publications provided that full reference is given.

İşletme Bilimi Dergisi; www.dergipark.gov.tr/jobs Sakarya Üniversitesi İşletme Fakültesi jobs@sakarya.edu.tr Esentepe Kampüsü 54187 Serdivan/SAKARYA

JOBS

Bu Sayıda Katkıda Bulunan Hakemler

Reviewers List of This Issue

Prof. Dr. Mehmet AYGÜN	Van Yüzüncü Yıl Üniversitesi
Prof. Dr. Mehmet Ünsal MEMİŞ	Çukurova Üniversitesi
Prof. Dr. Şakir SAKARYA	Balıkesir Üniversitesi
Prof. Dr.Ruziye COP	Bolu Abant İzzet Baysal Üniversitesi
Prof. Dr. Yaşar KABATAS	Marmara Üniversitesi
Doç. Dr. Emrah ÖZSOY	Sakarya Üniversitesi
Doç. Dr. Erkan ÖZTÜRK	Kırklareli Üniversitesi
Doç. Dr. Koray TUAN	Çukurova Üniversitesi
Doç. Dr. Metin Reyhanoğlu	Hatay Mustafa Kemal Üniversitesi
Doç. Dr. Oğuz IŞIK	Hacettepe Üniversitesi
Dr. Öğr. Üyesi Buket BORA SEMİZ	Bilecik Şeyh Edebali Üniversitesi
Dr. Öğr. Üyesi Ayhan CESUR	Van Yüzüncü Yıl Üniversitesi
Dr. Öğr. Üyesi Aynur İNCEKIRIK	Manisa Celâl Bayar Üniversitesi
Dr. Öğr. Üyesi Fatma MUMCU KÜÇÜKÇAYLI	Burdur Mehmet Akif Ersoy Üniversitesi
Dr. Öğr. Üyesi Şule Yıldız	Sakarya Üniversitesi
Dr. Öğr. Üyesi Semra Boğa	Adana Alparslan Türkeş Bilim ve Teknoloji Üniversitesi
Dr. Öğr. Üyesi Zülküf ÇEVİK	Sakarya Üniversitesi
Dr. Ahmet Karakiraz	Sakarya Üniversitesi

İşletme Bilimi Dergisi
2021
Cilt:9 Sayı:2

Değerli Bilim İnsanları,

İşletme Bilimi Dergisinin 9. Cilt 2. Sayısını farklı bilim dallarından dokuz makale ile sizlere sunmaktan onur ve mutluluk duyuyoruz. Dergimizin mevcut sayısında yayınlanan makaleler Yönetim ve Organizasyon, Uluslararası Ticaret, Yönetim Bilişim Sistemleri ve Muhasebe ve Finansman alanlarından gelmiştir. Dergimiz kurulduğu günden bu güne kadar İşletme Biliminin farklı disiplinlerinden çalışmalar yayınlamaya gayret göstermektedir. Bunu dergi politikası olarak benimsemiş olmamız nedeniyle bundan sonra da İşletme Biliminin farklı disiplinlerinden gelen makaleleri bilimsel etik ve yayın kalitesini göz önünde bulundurarak sizlere sunmaya gayret edeceğimizi ifade etmek isteriz.

Sayımızın ilk makalesi Eray ÇETİN ve Alpaslan YAŞAR tarafından hazırlanan "The Association Between Audit Quality And Earnings Management Using Classification Shifting" başlıklı makaledir. Bu makalenin amacı denetim firması büyüklüğü ile ölçülen denetim kalitesi ve sınıflandırma değiştirmesi yoluyla kâr yönetimi arasındaki ilişkinin ortaya konulmasıdır. Çalışmanın sonucu, şirketlerin tahakkukları yönetme fırsatlarının bağımsız denetim kalitesi ile kısıtlandığı durumda, alternatif kâr yönetimi aracı olarak sınıflandırma değiştirmesine yönelebileceklerini göstermesi açısından önem taşımaktadır.

Sayımızın ikinci makalesi Önder BÜBERKÖKÜ'nün kaleminden çıkan "Kripto Para Birimleri Arasındaki Frekans Alanı Nedensellik İlişkinin Analizi" başlıklı makaledir. Bu çalışmada günlük veriler kullanılarak Binance coin (BNB), Bitcoin cash (BCH), Stellar (XLM) ve Cardano'dan (ADA) oluşan dört kripto para birimi arasındaki nedensellik ilişkileri incelenmiştir. Günümüzde yaygın şekilde kullanılan ve önemli bir yatırım aracı olan kripto paralar üzerine yapılan bu araştırmanın literatüre katkı sağlayacağına inanmaktayız.

Sayımızda yer alan bir diğer makale "Sosyal Medyada Etkileşimi Etkileyen Faktörlerin İncelenmesi: Kuyumculuk Sektöründe Bir Örnek Olay İncelemesi" başlıklı makaledir. Makale Fatma İŞLER tarafından hazırlanmış olup, makalede bir altın ve saat firmasının Instagram'da paylaştığı içeriklerde müşteri etkileşimini etkileyen faktörlerin tespiti amaçlanmıştır. Çalışma sonuçlarının günümüzde önemli bir iletişim aracı olan sosyal medyanın pazarlama konusunda nasıl kullanılması gerektiği ile ilgili literatüre katkı sağlayacağı düşünülmektedir.

Sayımızın dördüncü makalesi Erol KÖYCÜ'nün hazırladığı "Borsa İstanbul'da Yerli Yatırımcı İle Toplam Yatırımcı Arasındaki Nedensellik İlişkisi" başlıklı makaledir. Bu makalenin amacı Borsa İstanbul'da toplam yatırımcı sayısında meydana gelebilecek bir değişikliğin toplam yerli yatırımcı sayısını etkileyip etkilemediğinin araştırılması amaçlanmıştır. Çalışma sonuçları Borsa İstanbul'da toplam yatırımcı sayısında yaşanan artışların yerli yatırımcıları cesaretlendirdiğini ve daha fazla yerli yatırımcının Borsa İstanbul'da işlem

yapmasına neden olduğunu ortaya koyması bakımından önem arz etmektedir.

Sayımızda yer alan bir diğer makale Barış AKSOY ve Necati Alp ERİLLİ tarafından hazırlanan "Siber Suçların Siber Saldırılara Maruz Kalan Şirketlerin Hisse Senedi Fiyatları Üzerindeki Etkileri" başlıklı makaledir. Bu makale siber suç tehdidinin halka açık şirketlerin hisse senedi fiyatları üzerindeki etkisini incelemeyi araştırmaktadır. Günümüzde önemli bir tehdit olan siber suçların şirketleri mali açıdan nasıl tehdit edebileceğini ortaya koyan bu makalenin literatüre katkı sağlayacağına inanmaktayız.

Sayımızın altıncı makalesi Zekeriya DEMİR'in kaleminden çıkan "Aile Şirketlerinde Sürdürülebilirlik Açısından Muhasebe Ve Raporlamanın Önemi: Örnek Olaylar" başlıklı makaledir. Aile şirketlerinde sürdürülebilirlik açısından muhasebe ve raporlamanın önemini örnek olaylarla ortaya koymayı amaçlayan bu makalenin sonuçları etkin bir muhasebe ve raporlama sistemi olmayan şirketlerin mali dengelerini gözetmekte zorlandıklarını ve uzun vadede borçlanarak battıkalrını ortaya koymaktadır. Bu açıdan makalenin literatüre katkı sağlayacağı düşünülmektedir.

Sayımızın yedinci makalesi Hatice İLHAN KÜÇÜK ve Kahraman ÇATI'nın hazırladığı "Çevrimiçi Satın Alma Kararına Tüketici Değerlendirmelerinin Etkisi" başlıklı makaledir. Bu makale tüketicilerin çevrimiçi satın alma kararında, yorumlara verdikleri önemin ve içerik oluşturmalarının etkisini incelemek amacıyla gerçekleştirilmiştir. Tüketici değerlendirme ve yorumlarının, satın alma kararı üzerinde etkili olması nedeniyle firmaların çevrimiçi kanallarda yorum ve değerlendirme imkânı oluşturması ve bu mecraları dikkate alması gerektiği sonucuna ulaşan makalenin pazarlama yönetimi literatürüne önemli katkı sağlayacağı düşünülmektedir.

Sayımızda yer alan bir diğer makale Özen AKÇAKANAT ve Oğuzhan ÇARIKÇI tarafından kaleme alınan "Bağımsız Denetim Sürecinin İç Ve Dış Denetçi İş Birliği Açısından Değerlendirilmesi" başlıklı makaledir. Bu çalışmada, iç ve dış denetçiler arasındaki iş birliğine ve dış denetçilerin iç denetim çalışmasına olan güvenine özellikle vurgu yaparak, iç ve dış denetçiler arasındaki ilişkiyi incelemek amaçlanmıştır. Çalışmada bağımsız denetçilerin, denetçiler arası iş birliği seviyesine yönelik algılamalarının tam orta düzeyde olduğu tespit edilmiştir.

Sayımızın son makalesi "Dış Ticaret Sermaye Şirketlerinin Misyon Ve Vizyon Beyanlarına Yönelik Bir İçerik Analizi" başlıklı Ömer Faruk COŞKUN tarafından kaleme alınan makaledir. Bu araştırmanın amacı; Türkiye'de faaliyet gösteren Dış Ticaret Sermaye Şirketlerinin kurumsal internet sitelerinde yer alan vizyon ve misyon beyanlarını sistematik bir şekilde ele alarak öne çıkan kavramları tespit etmek ve bu beyanları unsurları ve özellikleri açısından değerlendirmektir. Çalışmadan elde edilen sonuçların misyon ve vizyon belirleme noktasında şirketlere fikir

İşletme Bilimi Dergisi
2021
Cilt:9 Sayı:2

verebilecek nitelikte olması çalışmanın önemini arttırdığına inanılmaktadır.

Dergimiz yayın hayatına başladığı 2013 senesinde itibaren İşletme Biliminin farklı disiplenlerinden bir çok makaleyi siz değerli bilim insanlarının ve ilgili literatürün hizmetine sunmuştur. Mevcut sayıda da bu politikamızı devam ettirerek sizlere zengin bir içerik sunmaktan kıvanç duymaktayız. Bu sayımızda göndermiş oldukları makaleler ile dergimize katkı sağlayan tüm yazarlarımıza, dergimize gönderilen makalelerin değerlendirilmesi için kıymetli vakitlerini ayıran saygıdeğer hakemlerimize ve makalelerin dergide yayınlanmaya hazır hale gelmesi için yoğun bir gayret gösteren editör kurulumuz ve dergi sekretaryamıza teşekkürlerimi sunarım. Dergimizin okurlarımız ve bilim insanlarına faydalı olması dileklerimle sonraki sayılarımızda işletmeciliğin güncel çalışmalarını bilim dünyasının hizmetine sunmak için siz değerli bilim insanları ve araştırmacıların katkılarını bekliyoruz.

Saygılarımızla…

Prof. Dr. Mahmut AKBOLAT
Editör

JOBS

İÇİNDEKİLER/*CONTENTS*

Yıl (Year) 2021 Cilt (Vol.) 9 Sayı (No) 2

Araştırma Makaleleri/Research Articles

JOBS

Araştırma Makalesi/Research Article

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

SİBER SUÇLARIN SİBER SALDIRILARA MARUZ KALAN ŞİRKETLERİN HİSSE SENEDİ FİYATLARI ÜZERİNDEKİ ETKİLERİ

Barış AKSOY

Dr. Öğr. Üyesi, Sivas Cumhuriyet Üniversitesi, İİBF, Finans ve Bankacılık Bölümü
baksoy@cumhuriyet.edu.tr,

***ORCID:** 0000-0002-1090-5693*

Necati Alp ERİLLİ

Doç. Dr., Sivas Cumhuriyet Üniversitesi, İİBF, Ekonometri Bölümü
aerilli@cumhuriyet.edu.tr,

***ORCID:** 0000-0001-6948-0880*

ÖZ

Amaç: İnternet ve diğer dijital teknolojileri kullanarak işlenen yasa dışı faaliyetler, siber suç olarak adlandırılmaktadır. Siber suçlar, kullanıcıların gizli verilerine yetkisiz erişim, DOS saldırıları, virüs yayma, çevrimiçi dolandırıcılık ve bilgisayar korsanlığı gibi çeşitli çevrimiçi suçları içermektedir. Siber saldırıların şirketlere olan maliyetleriyle ilgili önemli araştırmalar yapılmış olsa da, bir şirketin hissedarlarına doğrudan maliyeti, yani siber suçun bir şirketin hisse senedi fiyatı üzerindeki etkisini ele alan çok az araştırma yapılmıştır. Bu araştırma siber suç tehdidinin halka açık şirketlerin hisse senedi fiyatları üzerindeki etkisini incelemeyi araştırmaktadır. Araştırmada 2012-2020 döneminde yurtiçi ve yurt dışında siber saldırılara maruz kalan 17 halka açık şirket hakkındaki siber saldırı duyurularının hisse senedi fiyatları üzerindeki etkisi araştırılmış ve siber suç haberlerinin halka açık şirketlerin hisse senedi fiyatları üzerinde istatistiksel olarak önemli etkilere yol açıp açmadığı belirlenmiştir.

Yöntem: Çalışmada hisse senetlerinin fiyatları ve getirilerinin ayrı ayrı 5'er ve 7'şer günlük siber saldırı sonrası ve öncesi dönemler arasında istatistiksel fark olup olmadıkları ve korelasyon katsayıları araştırılmıştır. Hisse senetlerinin fiyatları günlük bazda birbirlerini etkilediklerinden eşleştirilmiş t-testi ile, hisse senedi getirileri birbirlerinden bağımsız olduklarından 2 grup için bağımsız değişkenler arası t-testi ile değerlendirilmiştir.

Makale Geliş Tarihi/Received for Publication : 30/06/2021
Revizyon Tarihi/ 1th Revision Received : 07/08/2021
Kabul Tarihi/Accepted : 16/08/2021

Atıfta Bulunmak İçin:
Aksoy, B. & Erilli, N.A. (2021). Siber Suçların Siber Saldırılara Maruz Kalan Şirketlerin Hisse Senedi Fiyatları Üzerindeki Etkileri İşletme *Bilimi Dergisi*, *9*(2), *239-259*.

JOBS

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

Bulgular: Analiz sonuçlarına göre yedi günlük dönemler için 10, beş günlük dönemler için 9 firmanın hisse senetlerinin, saldırı öncesi ve sonrası dönemlerdeki değişimleri istatistiksel olarak anlamlı bulunmuştur. Hisse senedi getirilerinde altı firmanın hisse senedi getirileri beş ve yedi günlük periyotlarda ters yönlü hareket ederken, 10 firmanın getirilerinde 5'er ve 7'şer günlük periyotlarda farklı yönlerde eğilim gösterdiği belirlenmiştir.

Sonuç: Araştırmanın sonucuna göre siber saldırılara uğrayan firmaların saldırı zamanı sonrası, hisse senedi fiyat ve getirilerinde istatistiksel olarak farklılıklar olduğu belirlenmiştir. Siber saldırıların firmaları direkt olarak etkilediği söylenebilir.

Anahtar Kelimeler: Siber Suç, Siber Saldırı, Bilgisayar Güvenliği, Şirket Hisse Senedi Fiyatı

THE EFFECTS OF CYBERCRIME ON THE STOCK PRICES OF COMPANIES EXPOSED TO CYBER ATTACKS

ABSTRACT

Aim: Illegal activities committed using the Internet and other digital technologies are called cybercrime. Cybercrime includes a variety of online crimes, including unauthorized access to users' confidential data, DoS attacks, virus spread, online fraud and computer hacking. While important research has been done on the costs of cyber-attacks to companies, there has been little research that addresses the direct cost of a company to its shareholders, namely the impact of cybercrime on a company's stock price. This research explores the impact of the cybercrime threat on the stock prices of publicly traded companies. The study investigated the impact of cyberattack announcements about 17 publicly traded companies on stock prices. It was determined whether cyber crime news had statistically significant effects on the stock prices of publicly traded companies in the period 2012-2020.

Method: This study investigated whether the prices and returns of stocks were statistically different and correlation coefficients between the periods after and before the 5-and 7-day cyberattacks decisively. Since stock prices affect each other on a daily basis, they were investigated by a paired t-test, and stock returns were investigated by indenependet sample t-test for 2 groups, since they are independent of each other.

JOBS

Findings: According to the results of the analysis, the changes in the shares of 10 companies for seven-day periods and 9 companies for five-day periods in the periods before and after the attack were statistically significant. In stock returns, it was determined that the stock returns of six firms moved inversely in five-and seven-day periods, while the returns of 10 firms trended in different directions in 5-and 7-day periods.

Results: According to the results of the study, it was determined that there were statistical differences in stock prices and returns after the time of the attack of companies that were subjected to cyber attacks. It can be said that cyber attacks directly affect firms.

Keywords: Cybercrime, Cyber attack, Computer security, Company stock price

I. GİRİŞ

İnternet ve bilgisayar aracılı iletişim (CMC'ler), bireylerin dünya genelinde iletişim kurma ve bilgi paylaşma şeklini büyük ölçüde değiştirmiştir. Bilişim teknolojilerinin insanlara sağladığı kolaylıklar arttıkça elektronik ortamların kullanımı yaygınlaşmış, her türlü bilginin işlendiği, taşındığı veya saklandığı ortamlara ulaşmak zaman veya mekân gözetmeksizin çok kolay bir hale gelmiştir. Bilgisayar teknolojileri, her türlü teknolojinin suçun kolaylaştırılmasında merkezi bir rol oynadığı siber suçların gelişimini de teşvik etmiştir. Suçlu ve sapkın gruplar artık forumlar ve haber grupları gibi bilgisayar aracılı iletişim teknolojilerini büyük mesafeler arasında bilgi paylaşmak için kullanabilmektedirler. Ayrıca, bilgisayar korsanları, güvenli kaynaklara erişim elde etmek ve bilgi çalmak için neredeyse her tür bilgisayar yazılımı ve donanımından yararlanmanın yollarını bulmuşlardır (Holt, 2012). Bilişim suçları konusunda en çok benimsenen tanım "Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış" olarak belirtilebilir (Altunok & Vural, 2011). "Siber", bilgisayar veya bilgisayar ağlarını ilgilendiren bir kavramı tanımlamak için kullanılmaktadır. "Siber alan" da birbiriyle bağlantılı donanım, yazılım, sistem ve insanların etkileşimde bulundukları soyut veya somut alanı ifade etmektedir (Hekim & Başıbüyük, 2013).

Siber suç, halka açık şirketlerin ticari faaliyetlerine yönelik artan bir şekilde ve yaygın bir tehdit oluşturmaktadır. Siber suç, önleme çabaları, çalınan varlıklar, iş kaybı ve bir şirketin itibarına zarar verme açısından işletmelere her yıl milyarlarca dolara mal olmakta ve şirketlerin borsa

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

değerini etkileyebilmektedir. Müşteriler, kişisel bilgilerinin ve işlemlerinin güvende olmadığını düşündüklerinde işletmelere olan güvenlerini kaybetmektedirler. Siber suç, siber saldırılara karşı savunmasızlık ticari faaliyetlerin uygulanabilirliğini ve dolayısıyla şirketin gelecekteki kârlılığını tehdit ettiğinden, hissedarlar için bir endişe kaynağıdır. Yatırımcılar şirketin hisse senedi değerini düşürerek piyasa değerinin düşmesine neden olabilmektedirler (Smith et. al.., 2019).

Siber saldırıların şirketlere olan maliyetleriyle ilgili önemli araştırmalar yapılmış olsa da, bir şirketin hissedarlarına doğrudan maliyeti, yani siber suçun bir şirketin hisse senedi fiyatı üzerindeki etkisini ele alan çok az araştırma yapılmıştır. Bu araştırma siber suç tehdidinin halka açık şirketlerin hisse senedi fiyatları üzerindeki etkisini incelemektedir. Araştırmada 2012-2020 döneminde yurtiçi ve yurt dışında siber saldırılara maruz kalan 17 halka açık şirket hakkındaki siber saldırı duyurularının hisse senedi fiyatları üzerindeki etkisi araştırılmış ve siber suç haberlerinin halka açık şirketlerin hisse senedi fiyatları üzerinde istatistiksel olarak önemli etkilere yol açıp açmadığı belirlenmiştir. Bu çalışma konusu üzerine yurt içinde çalışılmamış olması, yurt dışında ise sınırlı çalışma yapılmış olması araştırmanın en önemli motivasyonunu oluşturmaktadır. Çalışmada siber saldırılar, siber suç türleri, maliyetleri, siber güvenliğe yönelik tehditler incelenmiş ve siber suç duyurusunun şirketin hisse senedi fiyatı üzerindeki etkisi analiz edilmiştir. Bu çalışma beş bölümden oluşmaktadır. Birinci bölümde siber, siber alan, siber suç kavramsal yönden ele alınmış ve araştırma genel hatları ile özetlenmiştir. İkinci bölümde siber suç kavramı başlığı altında siber suçların ortaya çıkışını sağlayan etmenler, siber saldırıların şirketlere olan maliyetleri, siber saldırı türleri, siber saldırıların şirketler ve ülkeler açısından sonuçları ele alınmıştır. Üçüncü bölümde literatür incelemesi, dördüncü bölümde yöntem, veri seti, araştırmanın kısıtları, analiz ve bulgular, beşinci bölümde ise sonuç ve tartışma yer almaktadır.

II. SİBER SUÇ KAVRAMI

20. yüzyılın son dönemlerinden itibaren, insanların bilgisayar teknolojilerini kullanma biçimlerinde büyük bir değişim meydana gelmiştir. İnternet ağlarının yaygınlaşması, bilgisayar donanımı ve yazılımlarının geliştirilmesi, insanların iletişim kurma ve ticari işlemlere katılma biçiminde devrim yaratmıştır. Hücresel telefonun, kablosuz internet bağlantısının, tablet PC'lerin ve mobil cihazların geliştirilmesi, bireylerin herhangi bir zamanda herhangi bir yerden çevrim içi iletişim kurmasını giderek daha

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

kolay hale getirmiştir. Sonuç olarak, artık bireylerin sapkınlık ve suç eylemlerinde bulunmak için bu cihazları kötüye kullanmaları için sayısız fırsat bulunmaktadır (Holt & Bossler, 2014). Bilgisayar korsanları bilgisayarlara yetkisiz erişim sağlamaya çalışan kişiler olarak tanımlanabilir. Bilgisayar korsanları, bir bilgisayara erişmek için doğru olanı bulmak için milyarlarca parolayı deneyen parola kırma yazılımını kullanarak kaynaklara erişmeye çalışmaktadır. Bilgisayar ağlarında bilgisayar korsanlığı, ağ bağlantılarının ve bağlı sistemlerin normal davranışını değiştirmeye yönelik herhangi bir teknik çabadır (Gandhi, 2012).

Bilişim teknolojileri yeni tip suçların ortaya çıkmasını sağlamıştır. Günümüzde İnternet sayesinde siber suç işlemek eskisi kadar teknik bilgi ve beceriyi gerektirmemektedir. Bilişim teknolojilerine olan bağımlılığın giderek artması, bireylerin suç mağduru olma riskini artırmaktadır. (Hekim & Başıbüyük, 2013). Dünya'da özel ve kamu kurumlarının bilgisayar sistemlerine saldırılar yapılırken ülkemizde siber saldırı tehditleri altındadır. Birçok sektörde Internet kullanımının artmasına rağmen, siber saldırılar hakkında yeterli bilgi sahibi olunmaması tehlikenin önemini daha da artırmaktadır. Kamu ve özel sektördeki bilişim güvenlik uzmanları, siber-terör eylemler konusunda tedbirli davranmaktadırlar. Herhangi bir siber saldırı esnasında ülkemiz ekonomisinde birçok sektörün faaliyetlerinin ve dolayısıyla hizmetlerinin aksaması muhtemeldir (Hatipoğlu, 2017).

Nesnelerin Internet'i (Internet of Things, IoT) kavramı ile birlikte internete bağlı cihaz sayısındaki artış bu cihazların güvenlik ihlallerine maruz kalma riskini de artırmaktadır. Birbiriyle bağlantılı donanım, yazılım, sistem ve insanların etkileşimde bulundukları soyut veya somut alanı tanımlayan siber uzay içerisinde alınan güvenlik tedbirleri hakkında son kullanıcı haberdar edilerek farkındalık artırılabilir (Aslay, 2017). Küresel pazar araştırma şirketi Vanson Bourne'nun yaptığı araştırmada dünya genelindeki şirketler veri ihlalini engellemek için aylık ortalama 4129 Euro harcama yapmaktayken bu tutar Türk şirketleri için 3220 Euro olduğu belirtilmiştir. Rapordaki bir diğer önemli husus 2020 yılında günümüzdeki tutarın 50 katı daha fazla verinin siber saldırıdan korunması gerekmesi üzerinedir. Son birkaç yıldır, Türk şirketleri ve kamu kurumlarının siber saldırıların hedefinde olmaları bu problemin çözümü için daha fazla kaynak ayırması gerektiğini göstermektedir. Siber güvenlik harcama tutarlarının siber tehditlerin verebileceği zararlardan daha az olduğu göz önüne alındığında siber savunmaya ayrılan bütçenin önemi ortaya çıkmaktadır (Aslay, 2017).

Çevrimiçi bilgisayar korsanlığı, virüs saldırıları ve diğer bilgi güvenliği ihlallerinin potansiyel riskleri, internete bağımlılığın artmasıyla

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

hızla artmıştır. Siber suçlar kullanıcıların gizli verilerine yetkisiz erişim, DOS saldırıları, virüs yayma, çevrimiçi dolandırıcılık ve iletişimin yanlış yönlendirilmesi, fikri mülkiyet hırsızlığı, sistem kesintisi veya müdahalesi, kara para aklama ve bilgisayar korsanlığı gibi çeşitli çevrimiçi suçları içermektedir. Suçlu, kullanıcının gizli bilgilerine veya kişinin kimlik bilgilerine yasa dışı erişim veya saldırı gerçekleştirdiğinde (ör. parola ve PIN kodu) bu tür siber suçlar, gizli verilere yetkisiz erişim olarak adlandırılır (Malik & Islam, 2019).

Bir siber suçlu saldırı gerçekleştirmek için herhangi bir sisteme girdiğinde çok sayıda ihtimal bulunmaktadır. Örneğin sistemi erişilemez hale getirebilir, bilgiler çalınabilir, değiştirilebilir veya tahrip edilebilir. Sisteme yetkisiz olarak giren kişi uzmanlığına bağlı olarak varlığından kimseyi haberdar etmeksizin verileri değiştirip fark edilmeden sistemden çıkabilir. Bu durumda sistemdeki verinin bütünlüğü ile ilgili herhangi bir şüphe oluşmayacak ve işletme rutin bir şekilde ancak bütünlüğü bozulmuş veriyle günlük işlemlerine devam edecektir (Hekim & Başıbüyük, 2013).

Büyük siber saldırıların (ör. Fidye yazılımı veya dağıtılmış hizmet reddi saldırıları (DDoS)) ve siber suçların oluşturduğu tehdit büyüdükçe, bireyler, kuruluşlar ve hükümetler bunlarla mücadele etmiş ve bunlara karşı savunma yolları açmışlardır. Siber suçların artan etkisi, hükümetleri siber güvenlik bütçelerini artırmaları için baskı oluşturmuştur. Küresel siber saldırılar son derece organize suç grupları tarafından yürütülmekte ve son zamanlarda yapılan birçok saldırının arkasında organize veya ulusal düzeydeki suç grupları bulunmaktadır. Tipik olarak, suç grupları siber suç karaborsasında bilgisayar korsanlığı araçlarını ve hizmetlerini satın alıp satmakta, burada saldırganlar korsanlıkla ilgili bir dizi bilgiyi paylaşmaktadırlar. Bu çevrimiçi yeraltı pazarı, saldırgan gruplar tarafından işletilmektedir ve karşılığında yeraltı siber suç ekonomisi desteklenmektedir (An & Kim, 2018). Birçok siber suç türü yüksek derecede organizasyon ve uzmanlaşma gerektirse de siber suçta artık organize suç gruplarının hakim olup olmadığını ve böyle bir biçim veya yapının ne olduğunu tespit etmek için yeterli ampirik kanıt yoktur. Siber suç çoğu zaman sınır ötesi bir durumdur. Bu gerçek, suçluları tespit etme, bulma ve tanımlamadaki zorluğu artırmaktadır (Broadhead, 2018).

Bankacılık, perakende, imalat sanayi ve lojistik dâhil olmak üzere tüm sektörlerde dijitalleşen süreçler tehditleri de beraberinde getirmiştir. Fabrikaların akıllı hale gelmesi, nesnelerin interneti ve Endüstri 4.0 gibi teknolojiler, veri güvenliği ihtiyaçlarını artırmaktadır. Türkiye'nin Amerika ve Brezilya'nın ardından Dünya'da en fazla siber saldırıya maruz kalan üçüncü ülke olması dikkat çekmektedir. Türkiye, 2018 yılında toplamda 25

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

milyon siber saldırıya maruz kalmıştır (Savunma Sanayi Dergisi, 2021). Trend Micro tarafından yayımlanan 2016 yılı verilerine göre, dünya genelinde fidye yazılım saldırılarının %172 oranında arttığı ve ülkemizin Avrupa bölgesinde en fazla fidye yazılım saldırıları yaşayan ülke olduğunu, dünyada ise ABD ve Brezilya'dan sonra üçüncü sırada yer aldığı belirtilmiştir (Aslay, 2017).

Muhtemel suçlular, uygun bir hedef oluşturan organizasyonlara veya ürünlere saldırmaya motive olmuş saldırganlardır. Ancak bu tür hedeflere saldırılırsa, hem hedefler hem de siber güvenlik ürünlerini tedarik edenler, saldırıyı mümkün kılan güvenlik açıklarının farkına vararak yazılımlarına güvenlik güncellemelerini gerçekleştirmektedirler. Bununla birlikte, saldırganlar daha sonra koruyucularla savaşmak için siber saldırı araçlarının yeni versiyonlarını geliştirip satacaklardır. Saldırganlar, kuruluşlarda veya ürünlerde güvenlik açıkları bulabildiği sürece bu döngü devam edecektir. Bu açıdan bakıldığında, siber suçların yeraltı karaborsası, esasen arz ve talep tarafından yönetilen bir piyasa ekonomisidir ve kuruluşlar tarafından alınan önleyici tedbirler talebin ana itici gücüdür. İronik olarak saldırganlar, karaborsayı daha canlı hale getirmeye hizmet eden hedef kuruluşlarının devam eden önleyici tedbirleri nedeniyle yalnızca yeni araçlar satabilmektedirler (An & Kim, 2018).

III. LİTERATÜR İNCELEMESİ

Shelley (1998) yüksek teknolojinin büyümesiyle suçun değişen doğasını örnekleyen üç soruna odaklanmaktadır: finansal piyasalarda yolsuzluk, internette şifreleme ve çocuk pornografisidir. Bu üç alan, virüslerin bilgisayar sistemlerine girmesi, dosyaların değiştirilmesi ve sistem çökmeleri yoluyla kasıtlı sabotaj gibi doğrudan teknolojinin kendisiyle bağlantılı olan önceki sorunlardan temelde farklı olduğunu belirtmişlerdir. Hem yasal hem de yasadışı çok uluslu işletmeler, giderek daha önemli hale gelen devlet dışı aktörler haline geldikçe, vurguladıkları sorunlar 21. yüzyılda merkezi bir endişe haline geleceği sonucuna ulaşmışlardır.

Johnston & Nedelescu (2006) finansal piyasaların doğrudan veya dolaylı olarak terörist eylemlerin kurbanı olduğu vakaları, bu eylemlerin finansal piyasalar üzerindeki sonuçlarını, politika ve düzenleyici tepkileri incelemişlerdir. Bu araştırmada çeşitlendirilmiş, akışkan ve sağlam finansal piyasaların terörist saldırıların şoklarını emmede etkili olduğu sonucuna ulaşılmıştır. Sistemik olarak önemli olan finansal kurumlar ve sistemler, büyük operasyon yerlerinde veya geniş çaplı faaliyetlerin ardından kilit personel ve sistemlerin kaybolması veya erişilemezliği sonrasında kritik

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

operasyonların hızlı bir şekilde ve zamanında yeniden başlatılmasını sağlayabilmesi gerektiği belirtilmiştir.

Holt (2012), siber terörü fiziksel terör ve siber suçlardan tanımlamanın ve ayırmanın doğasında bulunan konuları ele almıştır. İkinci olarak, aşırılık yanlısı grupların ve terör gruplarının bilgi toplamak, yaymak ve yeni üyeler almak için mevcut teknolojiyi kullanma yolları araştırılmış ve ardından aşırılık yanlısı ideolojileri desteklemek için siber saldırı tekniklerinin uygulanması üzerine bir tartışma yapılmıştır. Son olarak, siber terörizmin geleceği ve bu faaliyetlerin hükümet politika yapıcıları, güvenlik kuruluşları ve kanun uygulayıcı kurumlar için yarattığı zorluklar tartışılmıştır.

Kshetri (2013) siber suç örgütlerinin, potansiyel faillerin işleyiş biçimini, yapılarını, profillerini ve kişisel özelliklerini, siber suçların hedeflerini, doğasını, suç gruplarının geçmişleri, suç eylemleri için potansiyel hedeflerin özellikleri, mağdurlara verilen zararın niteliği ve kapsamını incelemiştir. Analiz sonucuna göre Çin'in küresel hırsının, rejim meşruiyetinin temelindeki Marksizm'den ekonomik büyümeye geçişin, güçlü devletin ve zayıf sivil toplumun, ülkenin siber saldırı ve siber güvenlik konusunda ayırt edici modeli açıkladığı sonucuna ulaşmıştır.

Broadhurst ve arkadaşları (2014) siber suçla uğraşan grupların doğasını araştırmıştır. Devlet aktörleri de dahil olmak üzere, bireysel, grup davranışlarını ve tipik suçluların motivasyonlarını gösteren bilinen vakalara örnekler vermişlerdir. İşletme veya kâr odaklı faaliyetler ve özellikle devlet aktörleri tarafından işlenen siber suçlar, liderlik, yapı ve uzmanlaşma gerektiriyor gibi görünmekte olduğu sonucuna ulaşmışlardır.

Holt & Bossler (2014) dört kategorili siber suç tipolojisi kullanılarak çeşitli teknoloji-etkin suç biçimleri hakkındaki literatürü değerlendirmişlerdir. Bunlar; siber ihlal, siber aldatma-hırsızlık, siber porno-müstehcenlik ve siber şiddettir. Her kategoriyi ayrıntılı olarak incelemişler ve açıklama alanlarını göstermek için her kategori içinde gelecekteki araştırmalara yol göstermesi amacıyla öneriler sunmuşlardır.

Broadhead (2018) çağdaş siber suç ekosistemine ve gelişmelerine çok disiplinli bir genel bakış sunmaktadır. Bunu, siber güvenlik, hukuk ve kriminoloji gibi alanlardan son siber suç araştırmalarını gözden geçirip sentezleyerek yapmıştır. Dahası, ekosistemdeki üç önemli tehdit vektörünü (kötü amaçlı yazılım, Darknet ve Bitcoin ve diğer kripto para birimleri) inceleyerek özelliklerini, tarihçesini, işlevlerini ve ekosistemdeki beklenen gelişme durumlarını araştırmıştır.

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

An & Kim (2018) araştırmacılara ve uygulayıcılara rehberlik etmek üzere yeraltındaki siber suçları analiz etmek için bir veri analizi çerçevesi önermişlerdir. Eğitim ve test veri setleri sırasıyla 300 ve 700 örnekten oluşmaktadır. CaaS ve suç yazılımları ile ilgili mesajların oluşturduğu örnekler % 95 güven aralığı (% 70,74, % 81,24) ile % 82,60 doğruluk verdiği belirtilmiştir. 2008 -2010, 2011- 2013, 2014 -2017/10 ve 2008 -2017/10 olmak üzere dört zaman aralığını değerlendirmişlerdir. En yaygın potansiyel hedef organizasyonlar teknoloji şirketleri (% 28), bunu finans (% 20), e-ticaret (% 12) ve telekomünikasyon (% 10) şirketlerinin takip ettiği bulunmuştur.

Smith ve arkadaşları (2019) siber suçların halka açık bir şirket örneğinin hisse senedi fiyatları üzerindeki etkisini incelemeyi amaçlamaktadırlar. Hisse senedi fiyatındaki yüzde değişimi, piyasanın geri kalanıyla birlikte hisse senedi fiyatının artıp artmadığını belirlemek için Dow Jones Industrial ortalamasındaki değişimle karşılaştırılmıştır. Şirket hisse senedi fiyatlarındaki değişim, Standard and Poor'un 500 borsa endeksindeki yüzde değişikliklerle karşılaştırılmaktadır. Ölçüm günleri için (67, 63 ve 61) yüzde değişimi, siber suç saldırısının duyurulduğu gün olan 0. günden itibaren değişim miktarını yansıtmaktadır. Sonuçlar, siber suç duyurulduktan sonra hisse senedi fiyatlarının piyasa değeri üzerinde olumsuz ama önemli olmayan bir etki olduğunu göstermektedir. Bu nedenle, şirketlerin ortalama hisse senedi fiyatlarının siber suç haberinden sonraki günlerde düştüğü ve aynı günlerde DJI'nin sürekli olarak arttığı bulgusu, siber suçların bir şirketin hisselerini nasıl olumsuz etkilediğini vurgulamaktadır.

Tsakalidis & Vergidis (2019) siber suç olaylarının özelliklerini, ilgili unsurlarını incelemekte ve tanımlamaktadırlar. Araştırmada siber suçla ilgili suçların kapsamlı bir listesi ortaya konmuştur. Çalışmada siber suç olaylarının özelliklerini, ilgili suçlar için bir sınıflandırma sistemini ve çeşitli unsurları birbirine bağlayan ve karşılık gelen eylemleri, önlemleri ve politikaları daha iyi önermek için birbirleriyle ilişkileri incelemişlerdir.

Malik & Islam (2019) Pakistan bankacılık sektörlerinde siber suç olaylarının örgütsel performans üzerindeki olumsuz etkisini ve bilgi güvenliği farkındalığının siber suçlar ve örgütsel performans ilişkisi üzerindeki etkisini incelemişlerdir. Analiz sonucunda ilk olarak siber suç olaylarının örgütsel performans üzerinde önemli olumsuz etkiye sahip olduğunu belirtmişlerdir. İkinci adımda, bilgi güvenliği bilincinin organizasyonel performansa etkisini kontrol etmişlerdir. Bilgi güvenliği farkındalığının, örgütsel performans üzerinde önemli bir olumlu etkisi olduğu sonucuna ulaşmışlardır. Çalışma ayrıca siber suçların kurumsal

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

performans üzerindeki etkisinin bilgi güvenliği farkındalığına bağlı olarak değişebileceğini ortaya koymuştur.

Buil-Gil ve arkadaşları (2020) suç fırsatlarının fiziksel ortamlardan çevrimiçi ortamlara kaydırılmasının bir etkisi olarak, en katı kapanma kısıtlamalarının olduğu aylarda (Mayıs 2019 ve Mayıs 2020) siber suçlarda bir artış yaşanıp yaşanmadığını incelemişlerdir. Sonuçlar, COVID-19 salgını sırasında siber suç raporlarının arttığını ve bunların en katı kapanma politikaları ve önlemleriyle iki ay boyunca dikkate değer ölçüde yüksek olduğunu göstermektedir. Siber-bağımlı ve siber-etkin suçların çoğunun her iki yıl arasında bir artış yaşadığı gözlenmiştir. Bu nedenle, toplam siber suç sayısının Mayıs 2020'de Mayıs 2019'dan önemli ölçüde daha fazla olduğunu gözlemlemişlerdir.

IV. YÖNTEM VE VERİ SETİ

Siber suç, halka açık şirketler için yaygın ve ciddi bir tehdittir. Şirket bilgi sistemlerini siber suçtan korumak, teknoloji yönetiminin en önemli görevlerinden biridir. Siber suç genellikle yalnızca çalınan varlıklara ve iş kaybına neden olmakla kalmaz, aynı zamanda bir şirketin itibarına da zarar vermekte, bu da şirketin borsa değerini etkileyebilmektedir. Bu durum şirket yöneticileri, finansal analistler, yatırımcılar ve alacaklılar yönünden ciddi bir endişe kaynağıdır (Smith et. al., 2019). Finansal araçların fiyatları zaman içindeki taahhütleri içermekte ve bu nedenle belirsizliğe karşı bir koruma sağlamaktadır. Herhangi bir büyük krizin ilk etkisi, yüksek belirsizlik seviyeleri nedeniyle bir finansal piyasanın aşırı tepkisini içerebilirken, yeni bilgiler alınarak krizin uzun vadeli etkisi değerlendirildiğinde, piyasalar kriz öncesi dönemlerine geri dönmektedir. Bundan sonra finansal piyasalar, yatırımcıların krizin nasıl çözüleceğine ilişkin algılarına göre yukarı veya aşağı kaymaktadır (Johnston & Nedelescu, 2006).

Bu çalışmada siber suçlar üç kategoride toplanmaktadır: Kimlik avı, DDos saldırısı ve Fidye yazılımıdır. Kimlik avı, failin alıcılardan kişisel ve mali bilgi toplamak amacıyla yasal görünen e-posta gönderdiği bir e-posta dolandırıcılığı yöntemidir. Tipik olarak, mesajlar iyi bilinen ve güvenilir Web sitelerinden geliyormuş gibi görünmektedir. Kimlik avcıları yemle karşılaşan avlardan en az birkaçını kandırmayı umarak kurbanlarını kandırmak için bir dizi farklı sosyal mühendislik ve e-posta hilesi kullanmaktadır (Gandhi, 2012). Kimlik avcıları alışveriş sitelerinin veya finansal kurumlara ait internet sitelerinin tıpatıp benzerlerini yaparak internet üzerinden yayımlamakta ve rastgele değişik mazeretlerle gönderilen e-postalarda olası mağdurları bu sahte web sitelerine

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

yönlendirmektedirler. Mağdurlar sahte sitelere girerek kullanıcı adı, şifre gibi kişisel verilerini girdiğinde bu bilgiler kötü niyetli kişilerin eline geçmektedir (Hekim & Başıbüyük, 2013).

DDoS (hizmeti engelleme, Denial of Service) saldırısı, iş uygulamaları literatüründe, "dünya çapında bir hedef sunucuya sahip olan çok sayıda bilgisayardan çok sayıda sahte istek içeren bir saldırı" şeklinde tanımlanmaktadır. DDoS saldırıları "birden fazla güvenliği ihlal edilmiş kaynaktan gelen trafikle doldurarak hizmeti kullanılamaz hale getirme olarak" tanımlanabilir (An & Kim, 2018). DDoS saldırıları, sunucu bilgisayarla kurulan fazla sayıda sahte bağlantı sonucunda sunucuya aşırı iş yükü yüklenmekte ve böylece gerçekten bağlantı kurmaya çalışan kullanıcılara cevap veremeyecek hale getirmektedir. DDoS saldırıları bazen binlerce bilgisayar kullanılarak yapılmakta ve yönetici talimatı doğrultusunda yazılımın bulaştığı bilgisayarlar tarafından hedefteki internet adresleriyle kurulan bağlantılar sunucuyu meşgul etmektedir (Hekim & Başıbüyük, 2013).

Fidye yazılımında bir kişi ya da kurumun ifşa edildiği taktirde itibarının zedeleneceği veya rakipleri karşısında dezavantajlı duruma düşeceği nitelikteki bilgileri saldırgan tarafından ele geçirilmekte ve daha sonra saldırgan bu bilgileri ifşa etmemesi karşılığında mağdurdan menfaat elde etmeye çalışmaktadır (Hekim & Başıbüyük, 2013).

4.1.Veri Seti ve Araştırmanın Kısıtları

Bu çalışmada 2012-2020 yılları arasında siber saldırıya maruz kalmış 3 yerli ve 14 yurtdışı borsalarında hisse senetleri işlem gören şirketlerle ilgili siber saldırı duyurularının hisse senedi fiyatı üzerindeki etkisi incelenmiştir. Örneklemi oluşturan şirketlere yönelik siber saldırı türü DDos Saldırısı, Fidye yazılımı ve veri ihlalinden oluşmaktadır. Siber saldırılara uğrayan şirketler ile ilgili bilgiler finans, bilişim, ekonomi ve genel konularda haber yapan internet sitelerinden, elde edilmiştir. Aynı konuda farklı internet sitesinde ve farklı zamanlarda yapılan haberlerde ilk haberin verildiği tarih çalışmada siber saldırı ile ilgili duyuru tarihi olarak alınmıştır. Siber saldırıya uğrayan şirketler ile ilgili saldırıya uğrama tarihi, saldırı türü, muhtemel zarar ile ilgili bilgilerin düzenli olarak kamuya duyurulduğu yurt içi ve yurt dışında resmi ya da özel bir kaynak bulunmamaktadır. Bu nedenle ilgili saldırılar internet haber kaynakları taranarak elde edilmektedir. Bu şekilde 2012-2020 yılları arasında 73 şirketin farklı türde siber saldırılara uğradığı bilgisine ulaşılmıştır. Bu çalışmada hisse senedi fiyat bilgisine ulaşmak için ilgili şirketin hisse senetlerinin borsada işlem görmesi şartının

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

gerçekleşmesi gerekmektedir. Bu nedenle anakütleyi oluşturan 73 şirket içerisinde hisse senedi borsada işlem gören 17 şirket örneği elde edilmiş ve örneklemi oluşturan 17 şirketin siber saldırı duyurusundan önceki ve sonraki yedi günlük fiyat verileri alınmıştır. Örnek kapsamındaki şirketlerin fiyat verileri iki farklı borsa-yatırım internet sitesinden elde edilmiştir (Investing Borsa, 2021; yahoo finans, 2021). Garanti BBVA Türkiye'de faaliyet gösteren finansal kuruluştur. Türk Telekom ve Vodafone Türkiye'nin bilgi, iletişim ve teknoloji şirketleridir. Diebold Nixdorf merkezi Almanya'da olan bir atm makinesi üreticisidir. Adobe ve PumpUp merkezi ABD'de yazılım ve teknoloji şirketleridir. eBay ve HauteLook merkezi ABD'de internet üzerinde açık artırma usulü ile satış yapan alışveriş siteleridir. Equifax ABD'de kurulmuş bireylerin mali durumunu değerlendiren kredi raporlama kurumudur. Heartland Payment Systems ABD'de kredi kartı ödeme işlemcisidir. LinkedIn, merkezi ABD'de iş dünyasında bireylerin birbirleriyle iletişim kurma ve bilgi alışverişini sağlayan profesyonel sosyal iş ağı platformudur. Marriott International merkezi ABD'de bulunan oteller zinciridir. Sina Weibo merkezi Çin'de bulunan Twitter ve Facebook sitelerinin karması olan bir mikroblog şirketidir. Zynga ve OMGPop merkezi ABD'de bulunan oyun şirketleridir. EyeEm merkezi Almanya'da bulunan bir teknoloji şirketidir. ClassPass belirli bir aylık sabit ücret karşılığında aboneleri tarafından sağlık kulüplerinin kullanımını sağlayan bir ABD merkezli şirkettir. Örneği oluşturan şirketlerin faaliyet gösterdiği sektörler yönünden bakıldığında An & Kim (2018) çalışmasında belirtildiği gibi en fazla siber saldırıya maruz kalan şirketler teknoloji şirketleri, finans, e-ticaret ve telekomünikasyon şirketleridir. Siber saldırıya uğrayan şirketler, siber saldırı tarihi, siber saldırının duyurulduğu internet sitesi ve siber saldırı türü bilgisi Tablo 1'de verilmiştir.

Tablo 1.
Siber Saldırılara Maruz Kalan Şirket Bilgileri

No	Siber Saldırıya Maruz Kalan Şirketler	Siber Saldırı Duyuru Tarihi	Siber Saldırı Türü
1	Garanti BBVA	28.10.2019	DDos Saldırısı
2	Türk Telekom	29.10.2019	DDos Saldırısı
3	Vodafone	30.10.2019	DDos Saldırısı
4	Diebold Nixdorf (ATM Manufacturer & Retailer)	25.04.2020	Fidye yazılımı siber saldırısı
5	Adobe	30.10.2013	Veri ihlali
6	eBay	21.05.2014	Veri ihlali
7	Equifax	07.09.2017	Veri ihlali
8	Heartland Payment Systems	08.05.2015	Veri ihlali

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

Tablo 1. Devamı

No	Siber Saldırıya Maruz Kalan Şirketler	Siber Saldırı Duyuru Tarihi	Siber Saldırı Türü
9	LinkedIn	05.06.2012	Veri ihlali
10	Marriott International	08.09.2018	Veri ihlali
11	Sina Weibo	24.03.2020	Veri ihlali
12	Zynga	19.12.2019	Veri ihlali
13	HauteLook	11.02.2019	Veri ihlali
14	EyeEm	12.02.2019	Veri ihlali
15	OMGPop	30.09.2019	Veri ihlali
16	PumpUp	31.05.2018	Veri ihlali
17	ClassPass	18.02.2019	Veri ihlali

Kaynak: Yazarlar tarafından oluşturulmuştur.

4.2.Yöntem

Haberin ilk yayınlandığı tarih, "0. Gün" olarak belirlenen "etkinlik günü" dür. Kısa bir süre önceki ve sonraki günler için hisse senedi fiyatları elde edilmektedir. Smith ve arkadaşları (2019) çalışması takip edilerek pay senedinin piyasa fiyatı olay günü (0. Gün), 7 gün öncesi ve sonrası için kaydedilmiştir. Ölçüm günleri için yüzde değişimi, siber suç saldırısının duyurulduğu gün olan 0. günden itibaren değişim miktarını yansıtmaktadır. Olaya yakın tarihler kullanılarak -bu durumda siber suç haberi- siber suç duyurusu dışındaki faktörlerin etkileri en aza indirilir. Bu diğer faktörler arasında faiz oranları, ekonomik görünüm, enflasyon, deflasyon, ekonomik-politik şok ve ekonomi politikasındaki değişiklikler gibi konular yer almaktadır.

Çalışmada hisse senetlerinin fiyatları ve getirilerinin ayrı ayrı 5'er ve 7'şer günlük siber saldırı sonrası ve öncesi dönemler arasında istatistiksel fark olup olmadıkları ve korelasyon katsayıları araştırılmıştır. Hisse senetlerinin fiyatları günlük bazda birbirlerini etkilediklerinden eşleştirilmiş t-testi ile, hisse senedi getirileri birbirlerinden bağımsız olduklarından iki grup için bağımsız değişkenler arası t-testi ile değerlendirilmişlerdir. Analizlerde SPSS.22 paket programı kullanılmış ve tüm istatistiksel testlerde önem seviyesi 0,05 olarak alınmıştır.

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

4.3.Bulgular

Tablo 2'de araştırma örneklemini oluşturan 17 firmanın hisse senedi fiyatlarının ve getirilerinin 14 günlük, siber saldırı öncesi ve sonrası 7 günlük ortalama ve standart sapma değerleri verilmiştir.

Tablo 2.
Hisse Senetleri Fiyatları ve Getirilerinin Tanımlayıcı İstatistikleri

	Hisse Senetlerinin Fiyatları						Hisse Senetlerinin Getirileri					
	14 Günlük		Siber Saldırı Öncesi 7 Gün		Siber Saldırı Sonrası 7 Gün		14 Günlük		Siber Saldırı Öncesi 7 Gün		Siber Saldırı Sonrası 7 Gün	
Firma Adı	**Ort**	**ss.**	**Ort**	**ss.**	**Ort**	**ss.**	**Ort**	**ss.**	**Ort**	**ss.**	**Ort**	**ss.**
Garanti	9,36	0,26	9,32	0,33	9,41	0,19	0,00	0,02	0,01	0,02	0,00	0,01
Telekom	5,91	0,32	5,69	0,12	6,14	0,29	0,01	0,01	0,01	0,01	0,01	0,01
Vodafone	20,64	0,19	20,61	0,19	20,67	0,20	0,00	0,00	-0,0	0,01	0,00	0,00
Diebold	4,23	0,75	3,61	0,15	4,84	0,55	0,02	0,10	-0,0	0,04	0,05	0,14
Adobe	54,14	0,78	53,73	0,67	54,55	0,70	0,00	0,01	0,00	0,01	0,00	0,02
eBay	20,93	0,27	21,08	0,14	20,78	0,30	0	0,01	0,00	0,00	-0,00	0,01
Equifax	123,19	20,55	141,34	0,60	105,05	12,1	-0,02	0,05	0,00	0,00	-0,05	0,06
Heartland	52,31	0,69	51,84	0,54	52,79	0,45	0,00	0,01	-0,01	0,01	0,00	0,00
LinkedIn	95,72	2,77	96,29	3,60	95,14	1,72	-0,00	0,02	-0,01	0,02	0,01	0,01
Marriott	127,5	1,76	126,11	0,79	128,88	1,29	0,00	0,00	0,00	0,01	0,00	0,00
SinaWeibo	30,36	1,67	29,06	1,33	31,66	0,60	0,00	0,04	0,00	0,05	0,01	0,03
Zynga	6,22	0,06	6,21	0,06	6,24	0,07	-0,00	0,00	0,00	0,00	-0,00	0,00
HauteLok	45,40	0,83	46,02	0,49	44,77	0,60	-0,00	0,01	0,00	0,01	-0,00	0,01
EyeEm	32,71	1,01	31,79	0,35	33,64	0,33	0,00	0,02	0,00	0,01	0,00	0,025
OMGPop	5,98	0,14	6,05	0,11	5,91	0,14	0,00	0,01	-0,00	0,01	0,00	0,01
PumpUp	16,73	2,088	18,64	0,89	14,83	0,45	-0,02	0,04	-0,01	0,02	-0,03	0,05
ClassPass	47,41	0,97	46,63	0,73	48,20	0,29	0,00	0,00	0,005	0,01	0,001	0,005

Hisse senetleri fiyatlarına bakıldığında siber saldırı sonrası en büyük fiyat değişiminin (ortalama ranj değeri yani Saldırı Öncesi-Saldırı Sonrası (36,29) değeri en büyük olan) Equifax firmasına ait olduğu görülmektedir.İkinci en büyük değişim ise 3,81 ile PumpUp firmasında gerçekleşmiştir. Diğer firmaların fiyat değişimlerinin oynaklığı nispeten benzer yapıda olmuştur. Hisse senedi getirilerinin siber saldırı sonrası yedi günlük dönemlerine bakıldığında beş firmanın negatif getirisi olduğu diğer firmaların ise pozitif getirilerinin olduğu görülmektedir. Ayrıca beş firmanın siber saldırı öncesi negatif getirilerinin siber saldırı sonrasında pozitif getiriye dönüştüğü belirlenmiştir.

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

Tablo 3'de 17 firmanın hisse senedi fiyatlarının ve getirilerinin siber saldırı öncesi ve sonrası beş ve yedi günlük dönemler için korelasyon katsayıları ve iki dönem arasındaki istatistiksel karşılaştırmalar verilmiştir.

Çalışmanın ana konusu siber saldırı öncesi ve sonrası yedi günlük periyotlar için değişimlerin olup olmadığı araştırılsa da zaman aralığının daraltılması ile sonuçlarda ne gibi farklılık oluşup oluşmadığı da araştırılmıştır.

Tablo 3.
Hisse Senetleri Fiyatları ve Getirilerinin İlgili Dönemlere Göre Korelasyon Katsayıları ve İstatistiksel Karşılaştırma Sonuçları

	Hisse Senetlerinin Fiyatları		Hisse Senetlerinin Getirileri	
Firma Adı	**7 Gün**	**5 Gün**	**7 Gün**	**5 Gün**
Garanti	0,665	0,734	-0,342	0,577
Telekom	**0,983 ***	**0,867 ***	-0,615	-0,528
Vodafone	-0,334	-0,724	-0,012	0,543
Diebold_Nixdorf	**0,405 ***	**-0,804 ***	0,465	-0,812
Adobe	-0,066	**0,414 ***	0,081	0,132
eBay	-0,413	-0,735	0,348	-0,541
Equifax	**-0,524 ***	**0,361 ***	-0,233 **	-0,355 **
Heartland	**0,268 ***	-0,779	0,302	-0,088
LinkedIn	-0,618	-0,289	**0,148 ***	0,727
Marriott	**-0,584 ***	**0,005 ***	0,107	0,248
Sina_Weibo	**0,24 ***	**-0,186 ***	0,249	-0,245
Zynga	-0,594	0,436	0,295	0,628
HauteLook	**0,416 ***	-0,532	0,438	-0,409
EyeEm	**0,503 ***	**-0,092 ***	0,511	0,724
OMGPop	-0,947 *	-0,73	-0,877	0,257
PumpUp	**0,509 ***	**0,313 ***	-0,241	0,258
ClassPass	**0,783 ***	**0,876 ***	0,501	-0,244

*p<0,05; ** p<0,10

Tablo 3'teki sonuçlar incelendiğinde fiyatlarda yedi günlük dönemler için 10, beş günlük periyotlar için de 9 firmanın hisse senetlerinin, saldırı öncesi ve sonrası dönemlerdeki değişimleri istatistiksel olarak anlamlı bulunmuştur (p<0,05). Getirilere bakıldığında sadece bir firmanın yedi günlük periyotlarda anlamlı olduğu görülmektedir. Equifax firmasının getirileri ise her iki periyot için %10 seviyesinde anlamlı olarak kabul edilebilir.

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

Tablo 3'teki korelasyon değerlerine bakıldığında Telekom, Garanti ve ClassPass firmalarının hisse senetleri fiyatlarında hem yedi hem de beş günlük dönemler için aynı yönlü yüksek ilişkili olduğunu söyleyebiliriz. Benzer şekilde OMGPop her iki dönem için ters yönlü yüksek ilişkili bulunmuştur. Hisse senetleri fiyatları arasında beş günlük periyotlarda aynı yönlü ilişki bulunan dört firmanın 7 günlük periyotlarda ters yönlü ilişkiye, benzer şekilde beş günlük periyotlarda ters yönlü ilişki bulunan dört firmanın yedi günlük periyotlarda aynı yönlü ilişkiye döndükleri bulunmuştur.

Hisse senedi getirilerinin ilişki katsayılarına bakıldığında ise hisse senedi fiyatlarında olduğu gibi benzerlikler görülmemektedir. 6 firmanın hisse senedi getirileri beş ve yedi günlük periyotlarda ters yönlü hareket ederken, 10 firmanın getirilerinde 5'er ve 7'şer günlük periyotlarda farklı yönlerde eğilim göstermiştir.

Örneği oluşturan şirketlerin faaliyet gösterdiği sektörler yönünden bakıldığında An & Kim (2018) çalışmasında belirtildiği gibi en fazla siber saldırıya maruz kalan şirketler teknoloji şirketleri, finans, e-ticaret ve telekomünikasyon şirketleri bu araştırmada da en fazla siber saldırıya maruz kalan şirketler oldukları görülmüştür.

Smith ve arkadaşları (2019) Ölçüm günleri için (67, 63 ve 61) yüzde değişimi, siber suç saldırısının duyurulduğu gün olan 0. günden itibaren değişim miktarını yansıtmaktadır. Sonuçlar, siber suç duyurulduktan sonra hisse senedi fiyatlarının piyasa değeri üzerinde olumsuz ama önemli olmayan bir etki olduğunu göstermektedir. Bu nedenle, şirketlerin ortalama hisse senedi fiyatlarının siber suç haberinden sonraki günlerde düştüğü sonucuna ulaşmışlardır. Bu çalışmadan elde edilen bulgulara göre desiber saldırılara uğrayan firmaların saldırı zamanı sonrası, hisse senedi fiyat ve getirilerinde istatistiksel olarak farklılıklar olduğu, saldırıların firmaları direkt olarak etkilediği söylenebilir.

V. SONUÇ

Bir şirketin siber saldırıya uğramış olması sonucunda işlemlerinde güvenlik ve istikrar eksikliği nedeniyle potansiyel hissedarlar şirkete yatırım yapmaktan vazgeçebilmektedirler. Bu kırılganlık, finansal analistlerin, yatırımcıların ve alacaklıların endişelerinden dolayı şirketin piyasa değerinin düşmesine neden olabilmektedir. Siber suç, bir şirket için bir iç kontrol meselesidir. Başarılı bir işletme olmak için, şirketlerin iş bilgilerini ve işlemlerini korumak için güçlü dahili kontrollere ihtiyacı vardır.

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

Müşteriler kendilerine ait bilgilerin gizliliğini sağlayan şirketlere güvenmekte ve şirketlerden yeterli düzeyde koruma beklemektedirler. Şirketler, müşteri verilerini güvende tutmak için önleyici tedbirlere sahip olmalıdır. Bazen siber suçların failleri şirkette çalışanlar olabilmektedir. Bu nedenle şirketler, güvenli erişim ve gizli bilgilerle çalışan personelleri işe alırken son derece seçici olmalıdır. Bazı kişiler, siber suçlular tarafından kullanılmak ve karaborsada satış yapmak üzere siber suç programları oluşturmaktadırlar.

Şirketler, saldırılar meydana geldiğinde siber suçları yönetmek için bir eylem planı oluşturmalıdır. Şirketler onarımlar, geri ödemeler ve gelecekteki koruma için bütçe ayırmalıdır. Bunu yaparak bir şirket, hissedarlar, borç verenler, alacaklılar, satıcılar, müşteriler, çalışanlar ve diğerleri dâhil olmak üzere pek çok paydaşın çıkarlarını daha iyi koruyabilmektedir. Şirket çalışanlarının bilgi güvenliği farkındalığının siber suçların olumsuz etkilerini en aza indirdiği, bu nedenle şirketlerin, çalışanların bilgi güvenliği farkındalığını artırmak için güvenlik eğitim programları yürütmesinin gerekli olduğu belirtilebilir. Şirket çalışanları bilgisayar korsanlığı araçlarının satıldığı yeraltı siber suç pazarları olduğunun farkında olmalıdırlar. Daha da önemlisi, bu araçlar kuruluşlarındaki, ürünlerindeki ve hizmetlerindeki güvenlik açıklarına dayalı olabilir. Bu nedenle hükümetler ve kuruluşlar için konu, farklı türlerdeki büyük ölçekli veri kümelerini analiz etmeye geldiğinde teknik yeteneklerini artırmalıdırlar.

Çevrimiçi veri kaynakları, aşırılık yanlısı grupların kritik altyapılara ve diğer hedeflere yönelik saldırılara girişmek için bilgisayar korsanı topluluğundan gelen araçları ve taktikleri uyarlama yöntemlerini belirlemek için de kullanılabilir. Örneğin, kötü amaçlı yazılımlar ve çalınan veriler için dünya çapında pazar araştırmaları, aşırılık yanlısı bir grup tarafından kullanılabilecek saldırı araçları ve vektörlerdeki olası eğilimleri belirlemek için yararlı olabilir. Siber suçluların faaliyetlerinin araştırılması, aşırılık yanlılarının bu kaynakları nasıl kullanabileceğine dair anlayışımızı genişletmek için kullanılabilir.

Örneği oluşturan şirketlerin faaliyet gösterdiği sektörler yönünden bakıldığında An & Kim (2018) çalışmasında belirtildiği gibi en fazla siber saldırıya maruz kalan şirketler teknoloji şirketleri, finans, e-ticaret ve telekomünikasyon şirketleri bu araştırmada da en fazla siber saldırıya maruz kalan şirketler oldukları görülmüştür. Örneği oluşturan şirketlerin faaliyet gösterdiği sektörler yönünden bakıldığında An & Kim (2018) çalışmasında belirtildiği gibi en fazla siber saldırıya maruz kalan şirketler teknoloji

şirketleri, finans, e-ticaret ve telekomünikasyon şirketleri bu araştırmada da en fazla siber saldırıya maruz kalan şirketler oldukları görülmüştür.

Siber suçların siber saldırılara maruz kalan şirketlerin hisse senedi fiyatlarını nasıl etkilediğine yönelik bir araştırmaya yurt içerisinde rastlanmamış yurt dışında ise çok sınırlı sayıda çalışma yapılmıştır. Bu husus araştırmanın en önemli motivasyonunu oluşturmaktadır. Siber saldırılara maruz kalan şirket bilgilerinin kamuoyu ile paylaşılması konusunda resmi veya özel herhangi bir kurumun bulunmaması araştırmacıların ilgili bilgiye ulaşılabilmesi için internet haberlerini tek tek incelemesine neden olmaktadır. Siber saldırıya uğrayan şirketlerin tümünün borsada işlem görmemesi örnek sayısının sınırlı sayıda olmasına neden olmaktadır. Örnek sayısının sınırlı sayıda olması aynı zamanda çalışmanın en önemli kısıtını da oluşturmaktadır. Çalışmada siber saldırılar, siber suç türleri, maliyetleri, siber güvenliğe yönelik tehditler incelenmiş ve siber suç duyurusunun şirketin hisse senedi fiyatı üzerindeki etkisi analiz edilmiştir. Bu yönüyle çalışmanın literatüre katkısının olacağı beklenmektedir. Gelecekte yapılacak çalışmalarda araştırma döneminin artırılması ile daha fazla sayıda örneğin daha uzun sürelerdeki fiyat ve getiri hareketleri uluslararası borsa endeks hareketleri karşılaştırılarak yapılacak çalışmaların literatüre değer katacağı beklenmektedir.

MAKALE BİLGİ FORMU

Yazar Katkıları

Fikir/Kavram: Barış AKSOY

Araştırma Tasarımı: Barış AKSOY ve Necati Alp ERİLLİ

Makale Yazımı: Barış AKSOY ve Necati Alp ERİLLİ

Veri Toplama: Barış AKSOY ve Necati Alp ERİLLİ

Analiz: Barış AKSOY ve Necati Alp ERİLLİ

Eleştirel Okuma: Barış AKSOY ve Necati Alp ERİLLİ

Çıkar Çatışması Bildirimi

Bu araştırma için herhangi bir kamu kuruluşundan, özel veya kâr amacı gütmeyen sektörlerden hibe alınmamıştır.

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

KAYNAKÇA

Altunok, E., & Vural, A. F. (2011). Bilişim Suçları. *Denetişim*, (8), 74-84.

An, J., & Kim, H.-W. (2018). A Data Analytics Approach to the Cybercrime Underground Economy. *IEEE Access, 6,* 26636-26652. DOI: 10.1109/ACCESS.2018.2831667

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies*, *1* (1), 24-28.

Broadhead, S. (2018). The Contemporary Cybercrime Ecosystem: A Multi-Disciplinary Overview of the State Of Affairs and Developments. *Computer Law & Security Review*, *34* (6), 1180-1196.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B. & Chon, S. (2014). Organizations and Cybercrime. *International Journal of Cyber Criminology*, *8* (1), 1-20.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S. & Díaz-Castaño, N. (2020). Cybercrime and Shifts in Opportunities During COVID-19: A Preliminary Analysis in the UK. *European Societies*, *23,* 1-13.

Friedrichs, D. O., & Friedrichs, J. (2002). The World Bank and Crimes of Globalization: A Case Study. *Social Justice*, *29* (1-2), 13-36.

Gandhi, V. (2012). An Overview Study on Cyber Crimes in Internet. *Journal of Information Engineering and Applications*, *2* (1), 1-5.

Hatipoğlu, C. (2017). *Teknolojik Savaşlar: Siber Terörizm Tehditleri.* 3nd International Congress on Political, Economic and Social Studies (157-168). İstanbul.

Hekim, H., & Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*, *4* (2), 135-158.

Holt, T. J. (2012). Exploring the Intersections of Technology, Crime, and Terror. *Terrorism and Political Violence*, *24* (2), 337-354.

Holt, T. J., & Bossler, A. M. (2014). An Assessment of The Current State of Cybercrime Scholarship. *Deviant Behavior*, *35* (1), 20-40.

Investing Borsa. https://www.investing.com (16/04/2021).

Johnston, R. B., & Nedelescu, O. M. (2006). The Impact of Terrorism on Financial Markets. *Journal of Financial Crime*, *13* (1), 7-25.

Kshetri, N. (2013). Cybercrime and Cyber-Security Issues Associated with China: Some Economic and Institutional Considerations. *Electron Commer Research*, *13*, 41-69.

Malik, M. S., & Islam, U. (2019). Cybercrime: An Emerging Threat to the Banking Sector of Pakistan. *Journal of Financial Crime*, *26* (1), 50-60.

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

Savunma Sanayi Dergisi. https://www.savunmasanayiidergilik.com/tr (27/01/2021).

Shelley, L. I. (1998). Crime and Corruption in the Digital Age. *Crime and Corruption in the Digital Age*, *51* (2), 605-620.

Smith, K. T., Johnson, A. J. & Smith, L. M. (2019). Examination of Cybercrime and its Effects on Corporate Stock Value. *Journal of Information, Communication and Ethics in Society*, *17* (1), 42-60.

Tsakalidis, G., & Vergidis, K. (2019). A Systematic Approach toward Description and Classification of Cybercrime Incidents. *IEEE Transactions Systems, Man and Cybernetics: Systems*, *49* (4), 710-729.

Yahoo Finans. https://finance.yahoo.com (16/04/2021).

JOBS

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

THE EFFECTS OF CYBERCRIME ON THE STOCK PRICES OF COMPANIES EXPOSED TO CYBER ATTACKS

EXTENDED SUMMARY

Illegal activities committed using the Internet and other digital technologies are called cybercrime. Cybercrime includes a variety of online crimes, including unauthorized access to users' confidential data, DoS attacks, virus spread, online fraud, and computer hacking.

This research examines the impact of the threat of cybercrime on the stock prices of publicly traded companies. In the study, data on 3 domestic and 14 foreign publicly traded companies whose shares were traded on exchanges that were subjected to cyber-attacks at home and abroad in the period 2012-2020 were used. Thus, the impact of a cyber-attack and cybercrime news announcements on stock prices of public companies researched leads to it is determined whether statistically significant effects on stock prices. A study of how cybercrime affects the stock prices of companies subjected to cyber-attacks has not been found at home, but a very limited number of studies have been conducted abroad. The study examined cyber-attacks, types of cybercrime, their costs, cybersecurity threats, and analyzed the impact of cybercrime announcements on the company's stock price. The type of cyber-attack against companies that make up the sample consists of a DDoS attack, ransomware, and a data breach. Information about companies that have been subjected to cyber-attacks has been obtained from websites that make news on finance, IT, economics, and general issues. Since the news was encountered on different websites and at different times on the same subject, the date of the first news was taken as the date of the announcement about the cyber-attack. There are no official or private sources at home and abroad, where information about the date of the attack, type of attack, possible damage related to companies that have been attacked by cyber is regularly released to the public. For this reason, related attacks are obtained by scanning internet news sources. In this way, it was reported that 73 companies were subjected to different types of cyber-attacks between 2012-2020. In this study, to obtain stock price information, it is necessary to meet the requirement that the shares of the related company be traded on the stock exchange. For this reason, price data for the seven days before and after the cyber-attack announcement was taken from 17 companies whose shares were traded on the stock exchange. Price data of the companies that make up the example (https://www.investing.com) and (https://finance.yahoo.com) obtained from websites. The date of the first

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

publication of the news for use in the analysis was determined as the day of the event. Stock prices were obtained for days shortly before and after that date and statistical analysis was applied.

The study investigated whether the prices and returns of stocks were statistically different and correlation coefficients between the periods after and before the 5-and 7-day cyber-attacks decisively. Since stock prices affect each other daily, they were tested by paired t-test, and since stock returns are independent of each other, they were tested by independence t-test for two groups. For seven-day periods, 10 firms 'pre-and post-attack changes were statistically significant, while for five-day periods, 9 firms' stock changes were found significant ($p<0.05$). Looking at benefits, it seems that only one firm is significant in 7-day periods. Equifax's benefits can be considered significant at 10% for both periods. Looking at the correlation coefficients, we can say that Telecom, Garanti and ClassPass companies have the same directional with high correlation in stock prices for both 7 and 5-day periods. Similarly, OMGPop has a high but negative direction correlation for both periods. Four firms with a positive relationship between share prices over five-day periods were found to have a negative relationship over seven-day periods. Similarly, it was found that four firms with a negative relationship in five-day periods returned to the positive relationship in seven-day periods. Looking at the relationship coefficients of stock returns, there are no similarities, as in stock prices. The stock returns of the six firms moved in the opposite direction in the five-and seven-day periods. Similarly, 10 firms showed a trend in different directions in the five-and seven-day periods.

According to the results of the study, it can be said that firms that have been subjected to cyber-attacks have significant differences in stock prices and benefits before and after the time of the attack. The results are similar as in the An & Kim (2018) stated that the companies most exposed to cyber-attacks were technology, finance, e-commerce, and telecommunications companies.

Smith et al., (2019) show that there is a negative but not significant impact on the market value of stock prices after cybercrime is announced. So, they concluded that the average share prices of companies fell in the days after the cybercrime news. According to the results of this study, the changes in the shares of 10 firms for seven-day periods and 9 firms for five-day periods in the periods before and after the attack were statistically significant. In stock returns, it was determined that six firms moved inversely in five-and seven-day periods, while the returns of 10 firms trended in different directions in 5-and 7-day periods.

İşletme Bilimi Dergisi (JOBS), 2021; 9(2): 239-259. DOI: 10.22139/jobs. 960181

While important research have been done on the costs of cyber-attacks to companies, there has been little research to address the impact of cyber-attacks on a company's stock price. This part is the most important motivation of this research. The absence of any official or private institution for sharing company information exposed to cyber-attacks with the public causes researchers to examine internet news one by one to access the relevant information. Not all the companies that have been attacked by cyber are listed on the stock market, causing the number of examples to be limited. The limited number of samples is also the most important limitation of the study. The study examined cyber-attacks, types of cybercrime, their costs, cybersecurity threats, and analyzed the impact of cybercrime announcements on the company's stock price. In this aspect, it is expected that the study will contribute to the literature.