DİJİTAL DÖNÜŞÜM ÇAĞINDA
SİBER GÜVENLİK VE MAHREMİYET

Murat ZARALI

MART 2022

DİJİTAL DÖNÜŞÜM ÇAĞINDA SİBER GÜVENLİK VE MAHREMİYET

BAHÇEŞEHİR ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
YÜKSEK LİSANS TEZİ

MURAT ZARALI

İŞLETME DALINDA
YÜKSEK LİSANS DERECESİ İÇİN GEREKLİ ÇALIŞMALAR
YERİNE GETİRİLMİŞTİR

MART 2022

BAHÇEŞEHİR ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

...../...../.....

YÜKSEK LİSANS TEZ ONAY FORMU

Program Adı:	
Öğrencinin Adı Soyadı:	
Tezin Adı:	
Tez Savunma Tarihi:	

Bu tezin Yüksek Lisans tezi olarak gerekli şartları yerine getirmiş olduğu Lisansüstü Eğitim Enstitüsü tarafından onaylanmıştır.

Prof. Dr. Ahmet ÖNCÜ
Enstitü Müdürü

Bu Tez tarafımızca okunmuş, nitelik ve içerik açısından bir Yüksek Lisans tezi olarak yeterli görülmüş ve kabul edilmiştir.

	Ünvanı, Adı Soyadı	**İmza**
Tez Danışmanı:		
2. Üye :		
3. Üye :		

Bu tezdeki tüm bilgilerin akademik kurallara ve etik ilkelere uygun olarak elde edildiğini ve sunulduğunu; ayrıca bu kuralların ve ilkelerin gerektirdiği şekilde, bu çalışmadan kaynaklanmayan bütün atıfları yaptığımı beyan ederim.

Ad, Soyad :

İmza :

ÖZET

DİJİTAL DÖNÜŞÜM ÇAĞINDA SİBER GÜVENLİK VE MAHREMİYET

Zaralı, Murat

İşletme Yüksek Lisans Programı (Türkçe)

Danışman: Dr. Öğr. Üyesi Görkem Kar

Eş Danışman: Prof. Dr. Çağatay Çatal

Ocak 2022, 67 Sayfa

Günümüzde şirketler işlerini büyütmek, rekabette fark yaratmak, müşterinin değişen ve gelişen ihtiyaçlarına daha iyi, kaliteli ve hızlı cevap vermek için yüksek seviyede dijital dönüşüm yatırımı yapmaktadır. Ancak getirdiği faydaların yanında, dijital dönüşümün doğası gereği yüksek miktarda veri toplanması ve işlenmesi, bu süreçlerin web, mobil ve bulut platformlarında gerçekleşmesi nedeniyle ciddi seviyede artan siber güvenlik ve mahremiyet riskleri, dünya genelinde Covid-19 pandemisi etkisiyle artan dijitalleşme ile beklenenin de çok üzerine çıkmaktadır. Bu riskleri azaltmak için yapılan siber güvenlik ve mahremiyet koruma çalışmaları ve ayrılan bütçeler aynı oranda artmazsa, önümüzdeki dönemlerde şirketlerin başına gelecek ihlal olayları kaçınılmaz olacaktır.

Bu çalışmada, Türkiye'de, farklı sektörlerde faaliyet gösteren firmaların Genel Müdür ve Bilgi Teknolojileri (BT) Müdürü seviyesindeki 44 yöneticisiyle anket çalışması yapılmıştır. Yapılan anket çalışmasıyla, firmaların dijital dönüşüme yaptıkları yatırımlar ile siber güvenlik ve mahremiyet koruma konusunda yaptıkları yatırımlar arasındaki ilişkiler incelenmiştir. Ayrıca, şirketlerin üst düzey yöneticilerinin dijital dönüşümün getirdiği riskler konusundaki farkındalıkları değerlendirilmiştir. Araştırma sonuçlarına göre; üst yöneticileri en çok endişelendiren teknolojilerin başında 3. partilerle olan entegrasyonlar gelmektedir. En çok endişelendikleri güvenlik konularının başında ise şirket ve müşteri verilerinin çalınması bulunuyor. Bu çalışmanın sonunda; elde edilen tüm bulgular kullanılarak, dijital dönüşüm projelerinin daha güvenli hale getirilmesi için üst düzey yöneticilere düşen görevlerin neler olması gerektiği ortaya konulmuştur.

Anahtar Kelimeler: Dijital dönüşüm, Mahremiyet, Siber Güvenlik, Yatırım, Riskler

ABSTRACT

CYBER SECURITY AND PRIVACY
IN THE ERA OF DIGITAL TRANSFORMATION

Zaralı, Murat

Master Program in Management (Turkish)

Supervisor: Asst. Prof. Dr. Gorkem Kar

Co-Supervisor: Prof. Dr. Çağatay Çatal

January 2022, 67 Pages

Today, companies invest heavily in digital transformation to expand their businesses, make a difference in competition, respond better, faster, and with good quality to changing and developing customers' needs. However, in addition to the benefits it brings, the cyber security and privacy risks have increased significantly due to the nature of digital transformation, collection, and processing of high amounts of data including the fact that these processes take place on the web, mobile, and cloud platforms. Now it becomes higher than expected with the increasing digitalization under the effect of worldwide Covid-19 pandemic. If the cyber security and privacy protection efforts and allocated budgets for reducing these risks do not increase at the same rate, the breaches that will occur in the following terms will be inevitable for the companies.

In this study, a survey was conducted with 44 managers at the level of General Manager and Information Technology (IT) Manager of companies operating in different sectors in Turkey. With the survey study, the relationship between the investments made by companies in digital transformation and their investments in cyber security and privacy protection were investigated. In addition, the awareness of the senior managers of the companies about the risks brought by digital transformation was evaluated. Integration with third parties is one of the technologies that worries top managers the most. At the top of the security issues, they are most worried about the theft of company and customer data. At the end of this study, duties of senior managers to make digital transformation projects more secure have been presented by using all the findings obtained in this research.

Keywords: Digital Transformation, Privacy, Cyber Security, Investments, Risks

Canım kızlarım Aslı'm ve Ayça'ma

TEŞEKKÜR

Bu tez çalışmasının hazırlanmasında ve ortaya çıkabilmesinde değerli fikirleriyle beni yönlendiren ve yardımlarını hiçbir zaman esirgemeyen, çok kıymetli hocalarım ve danışmanlarım Sayın Dr. Öğr. Üyesi Görkem KAR ve Prof. Dr. Çağatay ÇATAL'a teşekkürü bir borç bilirim.

Ayrıca, değerli görüşleriyle katkıda bulunan Dr. Öğr. Üyesi Ahmet Anıl DİNDAR ve Dr. Selmin Danış ÖNCÜL'e bu süreçte sundukları desteklerden dolayı kendilerine çok teşekkür ederim.

İÇİNDEKİLER

TABLOLAR LİSTESİ

TABLOLAR

ŞEKİLLER LİSTESİ

ŞEKİLLER

KISALTMALAR LİSTESİ

BT	Bilgi Teknolojileri
CDO	Chief Digital Officer (Dijital Dönüşüm Lideri)
CEO	Chief Executive Officer (Genel Müdür/İcra Kurulu Başkanı)
CIA	Confidentiality, Integrity, Accesibility
CIO	Chief Information Officer (Bilişim Kurulu Başkanı)
CISO	Chief Information Security Officer (Bilgi Güvenliği Başkanı)
DPA	Data Protection Act (Veri Koruma Direktifi)
GBE	Gizlilik, Bütünlük, Erişilebilirlik
GDPR	General Data Protection Regulation (Genel Veri Koruma Tüzüğü)
IaaS	Infrastructure as a Service (Servis Olarak Altyapı)
IoT	Internet of Things (Nesnelerin İnterneti)
KVKK	Kişisel Verilerin Korunması Kanunu
MVP	Minimum Viable Product (Minimum Uygulanabilir Ürün)
OT	Operational Technology (Operasyonel Teknoloji)
PaaS	Platform as a Service (Servis Olarak Platform)
SaaS	Software as a Service (Servis Olarak Yazılım)
SCADA	Supervisory Control And Data Acquisition (Merkezi Kontrol ve Veri Toplama Sistemi)

Bölüm 1

Giriş

1.1 Teorik Çerçeve

Dijital dönüşüm, beraberinde siber güvenlik ve mahremiyet risklerini de getirdi. Teknolojik gelişmeler, şirketlerin yakın geçmişe kadar manuel ve analog yöntemlerle oldukça yavaş ve verimsiz yaptıkları birçok işlemi, otomatik ve dijital yapabilme kabiliyeti kazanmasını sağladı ancak çok kısa bir zaman içinde aynı teknolojiler saldırganlar tarafından da etkili ve etkin şekilde kullanılmaya başladı. Bu durum da siber güvenlik ve mahremiyet risklerindeki artışın en önemli nedeni oldu. Özellikle internet ve mobil teknolojilerin gelişimiyle birlikte şirketler insanlık tarihinde hiç olmadığı kadar çok veriyi toplama ve işleme kabiliyetine kavuştu. Şirketlerin veri tabanlarında biriken bu veriler saldırganların birinci hedefi haline geldi. Zaten çok hızlı geliştirilen dijital projeler dünya genelinde Covid-19 pandemisi etkisiyle daha da hızlandı. Hızlı geliştirme aktiviteleri, üretilen yazılım kaynak kodlarında daha fazla güvenlik açığı oluşmasına sebep oldu. Çok fazla sayıda tedarikçinin de bu sürece dahil olması ile birlikte, güvensiz geliştirilen şirket projeleri, aynı şekilde hızla dijitalleşmeye zorlanan tedarikçilerin güvensiz geliştirilmiş projeleri ile birleşerek, şirketlerin verilerini dış dünyaya daha fazla noktadan açık ve korunmasız hale getirdi. Yıllardır eylemlerini paraya dönüştürmenin yollarını arayan saldırganlar, dijital para platformları sayesinde (örneğin, Bitcoin veya Ethereum) geliştirdikleri fidye saldırıları (ransomware) ile tüm bu zayıflıkları kullanarak, her geçen gün daha fazla şirketin sistemini ele geçirerek siber suçlar üzerinden daha fazla para kazanabilir hale geldiler.

1.2 Problem Durumu

Üst yönetimlerin dijital dönüşüm için gerekli finansmanı ayırdıklarını, gerekli organizasyonel değişiklikleri yaptıklarını, belli bir stratejilerinin olduğunu, hatta kurum kültürlerinin bu yönde değişmesi için yoğun çaba harcadıklarını görüyoruz. Ancak aynı üst yönetimin, siber güvenlik ile ilgili algılarının, diğer şirketlerin yaşadığı saldırılardan ve karşı karşıya kaldıkları yasal ceza ve yaptırımlar nedeniyle oluşan büyük bir korkudan ibaret olduğunu değerlendirmekteyiz. Yapısı gereği yöneticiler, kendilerine fazla teknik ve karmaşık gelen bu konularla ilgili detaylı fikirlere sahip olmayıp bu konuda belli bir ajandaya da çoğu zaman sahip değillerdir, ek olarak, bu

konuyu teknik ekiplerin, hatta çoğu zaman şirkette bu konudaki görevli tek bir çalışanın, çözmesi gereken bir konu olarak değerlendirmektedirler. Birçok üst düzey yönetici, dijitalleşme ile büyüyen siber güvenlik risklerinin farkında olmadığı gibi bazı yöneticiler de dijitalleşme ile beraber şirketlerinin daha güvenli hale geldiğine dair yanlış bir algıya sahiptir. Farkındalık ve algıdaki bu tür eksiklikler, hızla dijitalleşen şirketlerde, siber güvenlik konularında gerekli bütçelerin ayrılmamasına, organizasyonel yapılanmada, siber güvenliğin olması gereken yerde konumlanamamasına ve bir strateji ve kurumsal kültür unsuru olmaktan uzak kalmasına neden olmaktadır.

1.3 Çalışmanın Amacı

Bu çalışmanın amacı, yapılan dijital dönüşüm projelerinin, şirketlerin siber güvenlik ve mahremiyet risklerini azaltıp azaltmadığını incelemek ve bu projelerin ele alınış yöntemleri ve kullanılan teknolojilerin doğası gereği veri güvenliğini ve mahremiyeti daha fazla risk altına atıp atmadığı konusunda değerlendirmeler yapmaktır. Bu amaca dönük olarak, dijital dönüşüm sürecindeki risklerin neler olduğu ve bilgi teknoloji liderlerinin rolleri arasında bulunan, dijital dönüşüm kaynaklı risklerin azaltılması konuları ayrıntılı olarak ele alınmış, şirketlerin dijital dönüşüm süreçlerinde müşterilerinin kendilerine verdikleri az ve kısıtlı veriyle yetinmeyerek, farklı teknolojiler kullanarak, müşterilerinin çoğu zaman farkında olmadan verdiği büyük miktarlarda verileri de kullanarak mahremiyet sınırlarını nasıl zorladığı ve bu konularda üst yönetimlere düşen görevler ortaya konulmuştur.

1.4 Araştırma Soruları

Bu çalışmada aşağıdaki sorulara cevaplar aranmıştır:

1. Şirketlerin dijital dönüşüm ile siber güvenlik ve mahremiyet konularına yaptıkları yatırımların değişimi ne düzeydedir?
2. Dijital dönüşüm projelerinin kurumlarda siber güvenlik ve mahremiyet risklerine etkisi nasıldır?
3. Dijital dönüşüm projelerinde siber güvenlik ve mahremiyet ile ilgili konular nasıl ele alınmaktadır?
4. Diğer firmaların karşılaştığı siber güvenlik ve mahremiyet olayları dijital dönüşüm projelerini nasıl etkilemektedir?

5. Dijital dönüşüm projelerinde yöneticileri siber güvenlik ve mahremiyet açısından en çok endişelendiren teknolojiler nelerdir?
6. Dijital dönüşüm projelerinde yöneticileri en çok endişelendiren siber güvenlik ve mahremiyet riskleri nelerdir?
7. Siber güvenlik ve mahremiyet konuları şirketlerde hangi seviyede ele alınmaktadır?

1.5 Çalışmanın Önemi

Bu çalışma, cevaplarını aradığı sorulara bulduğu yanıtlar sayesinde, kurumlarda üst düzey yöneticilerin dijital dönüşümün getirdiği riskler konusunda bilgilenmesini ve farkındalıklarının artmasını, bu sayede siber güvenlik ve mahremiyet koruma konularının dijital dönüşüm projelerinin önemli ve değişmez bir parçası olduğunun farkına varmalarını ve bu alana gerekli yatırım ve insan kaynağını ayırmalarını sağlayacak önemli bilgiler ve bulgular sunmaktadır. Bu sayede kurumların dijital dönüşüm ile ana amaçları olan rekabette avantaj sağlama ve öne çıkma hedefleri daha sürdürülebilir hale gelecek, benzer yatırımları yapmayan firmalar güvenlik ve mahremiyet konularında yaşadıkları olaylar neticesinde, prestij ve para kaybı yaşarken bu yatırımları yapan firmalar ise amaçlarına ulaşabileceklerdir.

1.6 Çalışmanın Literatüre Katkısı

Bu çalışma, Türkiye'de üst düzey yöneticilerin dijitalleşmeye yoğun bir şekilde odaklanırken bu çalışmaların doğası gereği ortaya çıkan siber güvenlik ve mahremiyet riskleri konusundaki farkındalıklarını ortaya çıkarmaya ve bu konuda üst düzey yöneticilerin şirketlerini daha iyi hale getirmek için neler yapılabileceği konusunda kritik bilgiler sunmaya yönelik öncü nitelikte bir araştırma niteliğindedir. Ulaşılması ve bilgi edinilmesi kolay olmayan bir alanda, üst yöneticilerden, oluşturulan anket çalışması için önemli girdiler sağlanmış ve durum değerlendirilmesi gerçekleştirilmiştir. Ulusal düzeyde bu konuları ele alan ve kritik gözlemler ortaya koyan bir çalışma gerçekleştirildiği değerlendirilmektedir. Literatürdeki bilgilerden farklı olarak, Covid-19 andemisinin etkisi de dikkate alınarak, mevcut durum değerlendirilmesi gerçekleştirilmiş ve şirketlere farklı önerilerde bulunulmuştur. Bu yönleriyle literatürdeki çalışmalardan ayrıldığı ve elde ettiği bulgulara bağlı olarak sunduğu somut önerilerle literatüre katkı sunduğu değerlendirilmektedir.

1.7 Tanımlar

Dijital dönüşüm: Günümüzde şirketler işlerini büyütmek, rekabette fark yaratmak, müşterilerinin değişen ve gelişen ihtiyaçlarına daha iyi, kaliteli ve hızlı cevap vermek için yoğun şekilde dijital dönüşüm yatırımları yapmaktadır. İlk dijital dönüşüm projeleri, şirket içindeki verilerin analog formattan dijital formata dönüştürülmesi olarak ortaya çıktı ve daha çok, kağıtlara basılı verilerin bilgisayara aktarılması ve bu veriler ile takip edilen iş süreçlerinin bilgisayarlar yardımıyla takip edilmesine olanak sağladı. Şirketler dijitalleşen süreçleri sayesinde daha hızlı ve daha verimli çalıştıklarını keşfettiler ve yeni projeler, dönüşümden daha ziyade tamamen dijital olarak tasarlanmaya başladı.

Dijital dönüşüm, getirdiği faydaların yanında, doğası gereği yüksek miktarda veri toplanması, işlenmesi ve bu süreçlerin tamamının ağırlıklı olarak web, mobil ve bulut platformlarında gerçekleşmesi nedeniyle, ciddi seviyede artan siber güvenlik ve mahremiyet riskleri taşımaktadır. Bu riskler dijitalleşmenin Covid-19 pandemisi ile beklenenin çok üzerinde gerçekleşmesiyle katlanarak artmıştır. Literatürde, bu anlamda yer alan görüşler, geleceğe dönük bazı fikirler sunmaktadır. Bunlardan aşağıda iki tanesi öne çıkmaktadır:

“Dijital dönüşüm sadece teknolojiyle değil, stratejiyle ve yeni düşünme biçimleriyle de ilgili. Dijital çağ için dönüşüm, şirketlerin BT altyapısından daha çok, stratejik düşünce biçimlerini yenilemelerini gerektiriyor” (Rogers, 2016).

“Dijital dönüşüm, üretkenliği, değeri ve sosyal refahı artırmak için yıkıcı teknolojileri benimsemekle ilgilidir. Ulusal hükümetler, çok uluslu kuruluşlar ve endüstri temsilcileri dijital dönüşüm ile ilgili uzun vadeli politikalarını temele koyan stratejik öngörü çalışmaları üretiyorlar. Tüm bu gruplar, dijital dönüşüm ile ilgili politikaların uygulanması ile Tablo 1'de listelenen hedeflere ulaşmayı amaçlamaktalar” (Ebert, 2018).

Bu araştırmaya konu olan güvenlik ve mahremiyet başlığı Tablo 1’de Sosyal perspektif altında yer almaktadır. Ebert’e göre dijital dönüşümün amaçlarından biri de “dijital veri güvenliğini, şeffaflığı, özerkliği ve güvenilirliği güçlendirmektir” (Ebert, 2018).

Tablo 1

Dijital Dönüşüm Hedefleri (Ebert, 2018)

Perspektif	Amaç
Sosyal	• Endüstride ve toplumda daha yenilikçi ve işbirlikçi bir kültürün gelişimini teşvik etmek • Dijital çalışma ve toplumda mükemmelliğe ulaşmaları için kişilere yeni beceriler ve geleceğe yönelik olarak eğitim sistemini değiştirmek • Dijital iletişim altyapıları oluşturup, devamlılığını sağlayarak bunların yönetişim, erişilebilirlik, servis kalitesi ve satın alına bilirliğini sağlamak • Dijital veri güvenliğini, şeffaflığı, özerkliği ve güvenilirliği güçlendirmek • Nüfusa sunulan dijital hizmetlerin erişilebilirliğini ve kalitesini iyileştirmek
Ekonomik	• Yeni ve yenilikçi iş modelleri uygulamak • Ekonomide gelir, verimlilik ve katma değer yaratmak • Düzenleyici yapıyı ve teknik standartları iyileştirmek

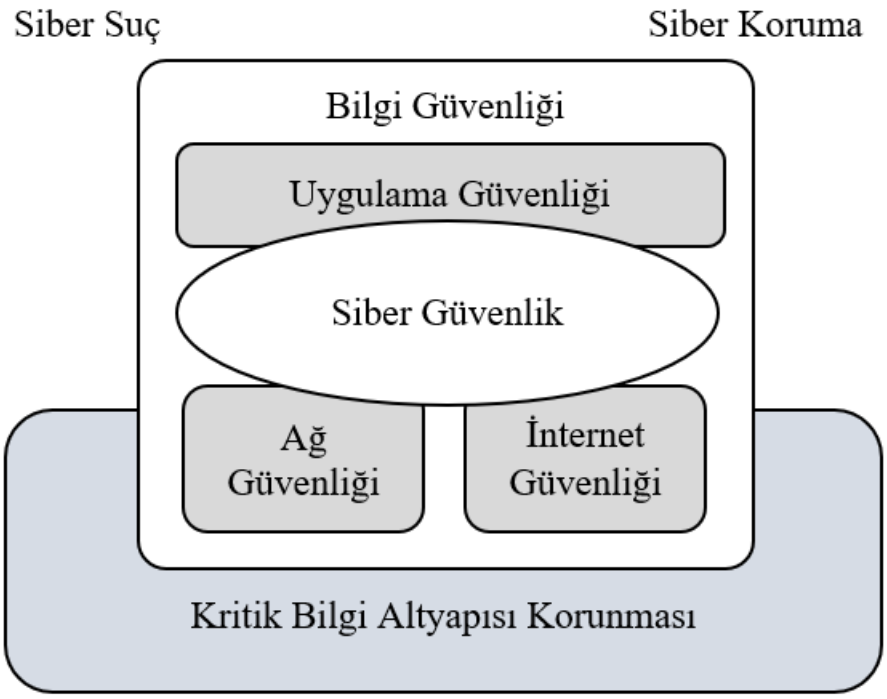
Bilgi güvenliği: Bilgi güvenliği, sistemlerin, ağların ve uygulamaların her türlü saldırıya karşı korunmasıdır. Saldırılara karşı korunurken amaç, verilerin ihtiyaç duyulduğu anda erişilebilir olması, art niyetli kişilerin eline geçmemesi ve bozulmamış olmasıdır. Literatürde bu husus "Bilgi güvenliğinin üç temel ilkesi, Gizlilik, Bütünlük ve Erişilebilirlik (GBE) Üçlüsü (CIA Triad - Confidentiality, Integrity, Accesibility)" olarak açıklanmaktadır (Möller, 2020).

Ağ güvenliği: Ağ güvenliği, sistemlere ve ağ üzerinden geçen verilere içeriden veya dışarıdan gelebilecek izinsiz erişimleri ve devre dışı bırakma saldırılarını önlemeyi amaçlar. Bunu başarmak için yetkisiz ağ saldırılarını izlemek, önlemek ve bunlara yanıt vermek için tasarlanmış güvenlik araçları, taktikleri ve güvenlik politikalarını kullanır.

İnternet güvenliği: İnternet güvenliği, internet üzerinden gerçekleşebilecek saldırılara karşı kurumu korumayı amaçlar. Çevrimiçi erişim ve internet kullanımı kaynaklı tehditlere ve güvenlik açıklarına odaklanır.

Uygulama güvenliği: Uygulama güvenliği, uygulamaların saldırılara karşı güvenli tasarlanması, kodlanması ve uygulamanın saldırılara karşı dayanıklı hale getirilmesini amaçlar. Bu amaca ulaşmak için geliştirme ekiplerinin yazılım geliştirme yaşam döngüsüne güvenlik unsurlarını ekleyerek uygulamalardaki güvenlik sorunlarını bulmayı, düzeltmeyi ve oluşmadan önlemeyi hedefler.

Siber güvenlik: Siber güvenlik, siber dünyadaki dijital varlıkların korunmasını hedefler. Bilgi güvenliği prensiplerinin; ağ güvenliği, internet güvenliği ve uygulama güvenliği kuralları ile birlikte işletilmesi ile sağlanır. Siber güvenliğin amacı, kritik bilgi altyapısını ve bilgiyi yetkisiz ve izinsiz erişimlere ve saldırılara karşı korumaktır. Şekil 1'de bu alanlar ve siber güvenlik ilişkisi resmedilmiştir.



Şekil 1. Siber güvenlik ve diğer güvenlik alanları arasındaki ilişki (ISO/IEC 27032)

Mahremiyet: Mahremiyet, bilgi güvenliğin üç unsurundan biri olan gizlilik konusu ile çoğu zaman karıştırılabilmektedir. Yüksel (2003) tarafından aşağıda yapılan tanıma bakıldığında, bu ayrım daha açık şekilde görülmekte ve günümüzde bazı şirketlerin dijital dönüşüm projelerinde kişilerin mahrem verilerini işleme iştahları göz önünde bulundurulduğunda çıkabilecek olası riskler daha görünür hale gelmektedir.

"Toplumsal yaşamda mahremiyete duyulan ihtiyaç, farklı görünümlerde ortaya çıkar. Yalnız kalma veya tek başına olma isteği, bu görünümlerden en yaygın olandır. İkinci bir görünümü ise, arkadaşlar, yakın tanıdıklar ve sevgililer gibi kimselerle, diğer kimselerin müdahalesinden ve gözetiminden uzak şekilde ilişki ve iletişim kurma arzusu olarak ortaya çıkar. Üçüncü olarak, kişisel olarak tanınmadan, yani dikkatleri üzerine çekmeden, kamu yaşamına katılma talebini ifade eder" (Yüksel, 2003).

Mahremiyet tanımının tam tersi olarak, sosyal medyanın yaygın şekilde kullanımı ile beraber, herkes tarafından tanınmak ve takip edilmek ve tüm dikkatleri üzerinde toplamak birçok birey acısından ilgi çekici bir hale geldi. İlk çıkış amacı kişilerin arkadaşlarıyla ve yakın çevresi ile iletişim kurmak olan bu platformlar, daha sonra kişileri, paylaşımlarını herkese açma konusunda cesaretlendirmiş ve hatta bu verileri ticari amaçlarla şirketlerin de kullanımına açmıştır (Mosquera, Odunowo, McNamara, Guo ve Petrie, 2020). İlk amaçlarından farklı olarak bu yönde evrilen bu tür sosyal ağ uygulamaları, mahremiyet alanında birçok problemi de beraberinde getirmiştir.

Bölüm 2

Dijital Dönüşümün Getirdiği Riskler

Dijital dönüşüm; şirketlere rekabet avantajı, rakiplerden ayrışma, daha büyük ve küresel pazarlara ve daha fazla müşteriye kolay erişim avantajları sağlamaktadır. Tüketiciler ise şirketlerin dijital dönüşümü kullanarak sundukları ürün ve hizmetler sayesinde, daha geniş ürün ve hizmet yelpazesine, küresel kalitede ve rekabetçi fiyatlarla erişme şansına sahip olmaktadırlar.

Dünya genelindeki Covid-19 pandemisi ile beraber dijital dönüşümün gerçek gücünü daha önce göremeyen şirketler de, geç de olsa, zor yollardan farkına vararak pandemi döneminin öngörülemeyen kaotik ortamında, şirketlerini hayatta tutabilmek için hızlı bir şekilde bu sürece girdiler. Bu sürecin kendisi de bir o kadar kaotik ve zorluydu, zira bu sürece hazırlıksız yakalanan şirketler, pandeminin getirdiği belirsiz ortamında, daha önce hiç uzaktan çalışma deneyimi olmayan çalışanlarını, uzaktan çalışma yöntemleriyle yönetmeye çalışırken, bir yandan da hazırlıklı olmadıkları dijital dönüşüm süreçlerini hayata geçirmek için büyük mücadeleler vermek zorunda kaldılar. Şirketlerin içine girdiği bu mücadelenin bir de finansal riskleri vardı.

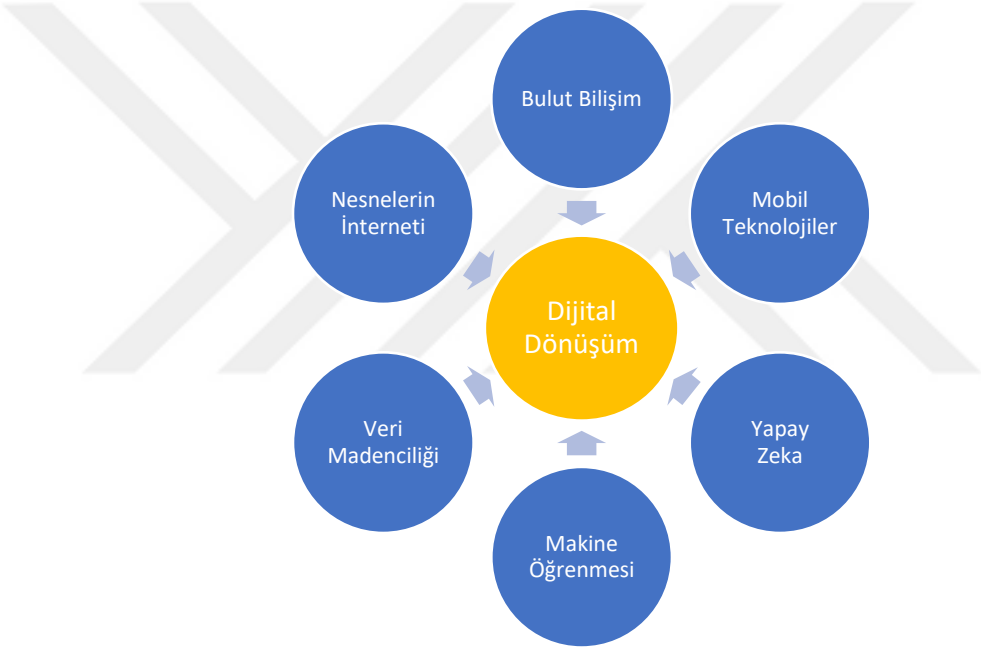
Pandeminin ne zaman biteceği, tüketicinin pandemi döneminde nasıl bir tüketim davranışı sergileyeceği, şirketlerin çalışanlarını ücretsiz izne çıkarması veya tamamen işten çıkarması gibi başka faktörlerle birleştiğinde, yapılan yatırımın geri dönüşü olacak mı ya da ne kadar zamanda olacak gibi sorular tüm dünya için cevaplanması çok güç sorulardı. Covid-19 döneminde dijital dönüşüm, çalışanlar açısından da çok farklı deneyimlerin yaşanmasına sebep oldu. Tüm dünyada insanların evlere kapandığı ve birçok sektörde işlerin durma noktasına geldiği bir dönemde, teknolojiye çok aşina olmayan çalışanlar dahil, daha önce hiç deneyimlemediği uzaktan çalışma teknolojilerini kullanarak, işlerini evlerinden devam ettirmek zorunda kaldılar.

Bu dönem, dijital dönüşüm ve beraberinde siber güvenlik ve mahremiyet konularında saldırganların da ciddi bir dönüşüm geçirdiğini ve bu dönüşümle beraber neler yapabileceklerini de gösterdi. İnsanlık için bu kadar kritik bir dönemde bile; büyük bir kitlenin iletişimini sağlayan, eğitimin uzaktan yapılmasını kolaylaştıran Zoom gibi platformlara, sağlık hizmetlerine çok yoğun ihtiyaç duyulan bir dönemde hastanelere, hatta Covid-19 aşısının ilk piyasaya sürüldüğü günlerde, aşıların sevkiyatlarında kullanılan soğuk hava depolu araçların ısı kontrol sistemlerine dahi

saldırılar gerçekleştirmeye çalışarak, saldırganların neler yapabileceklerinin bir sınırı olmadığı açıkça ortaya konulmuştur.

2.1 Dijital Teknolojilerdeki Gelişmeler

Dijital teknolojilerdeki gelişmeler, dijital dönüşüm projelerinde kullanılan araçların kapasitesi ve kabiliyetlerinin artmasına ve şirketlerin çok büyük veri kümelerini, çok boyutlu ve çok hızlı işlemelerine imkanlar sağladı. Gelişen bu teknolojilerin başında bulut bilişim, yapay zeka, makine öğrenmesi, veri madenciliği ile detaylı veri analizi, mobil teknolojiler ve nesnelerin interneti sayılabilir. Sekil 2'de bu teknolojiler gösterilmektedir.

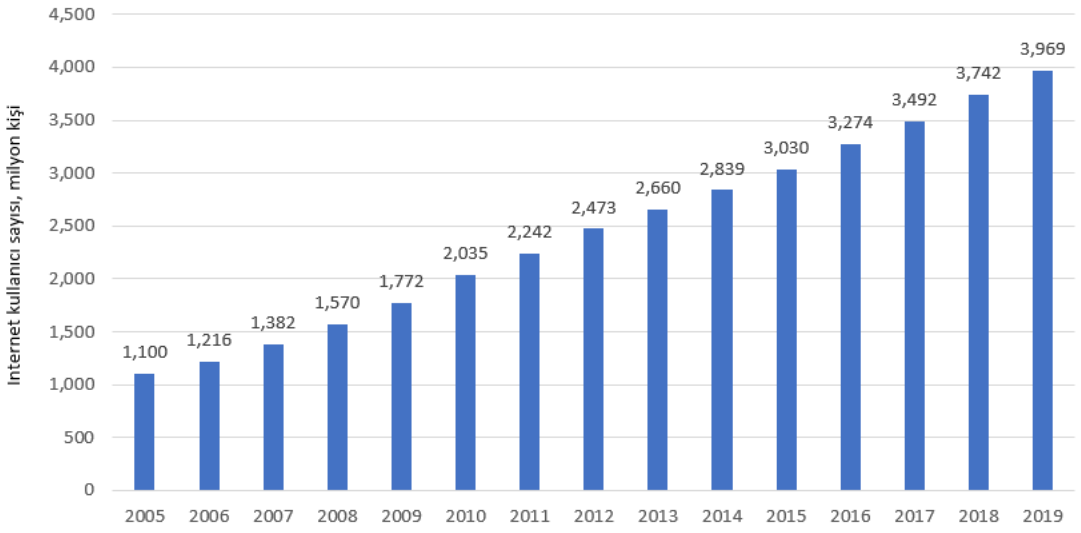


Şekil 2. Dijital teknolojilerdeki gelişmeler

Bulut bilişim teknolojisi, çok büyük şirketlerin sahip olduğu işlem gücünün, girişim şirketleri (startup) tarafından kullanılabilmesini sağladı. Bulut bilişimin gücünü, daha hızlı ürün geliştirme (agile development), Minimum Uygulanabilir Ürün (Minimum Viable Product – MVP), hızlı prototipleme gibi metotlarla birleştiren bu şirketler, müşteri ihtiyaçlarını ve beklentilerini çok iyi anlayarak ürün ve servislerini hızlı bir şekilde uyarlayarak yeni teknoloji devleri haline gelmeye başladılar.

İnternet ilk yıllarda devlet kurumları ve üniversitelerin haberleşmesi için kullanılırken, iletişim ve bilgisayar teknolojilerindeki gelişmelerle beraber önce

şirketlerin, sonrasında da bireylerin kullanımına açıldı. İlk yıllarında tamamen statik olarak üretilen web içerikleri zamanla dinamik hale gelerek kullanıcı ile etkileşimi mümkün kıldı. Bu noktada kullanıcının kendisinin içerik üreticisi olmaya başlaması ve arkasından gelen sosyal medya platformları, kullanıcıların resim, video ve hatta düşüncelerini ve hislerini herkesle paylaşmasına olanak sağlayacak ortamlar sundu.

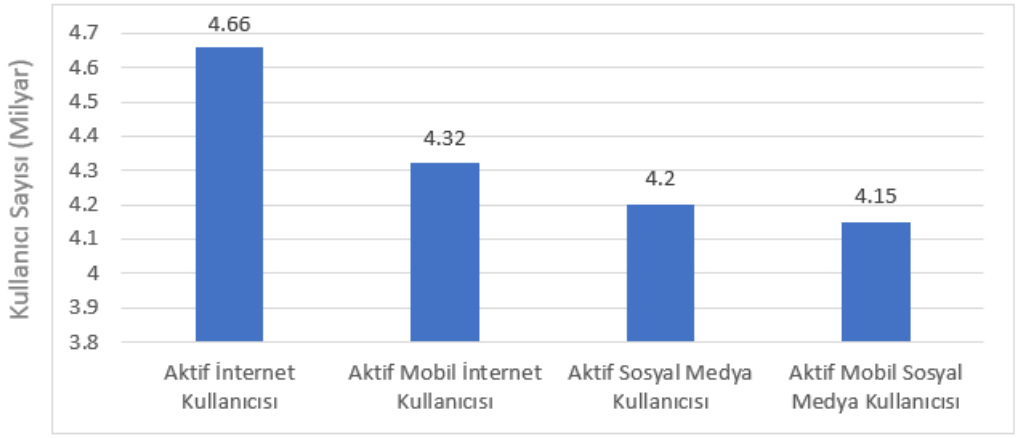


Şekil 3. İnternet kullanıcı sayısı 2005 – 2019 yılları arası değişim. (Statista, 2020)

İnternet kullanımı 15 yıl gibi bir sürede dört kat artarak dünya nüfusunun büyük bir kesimine ulaşmayı başardı. Şekil 3'de İnternet kullanıcı sayısında artan değişim 2005-2019 yılları arası için gösterilmektedir. Bugün internet erişimi öyle boyutlara ulaşmış durumda ki, elektrik, su gibi kamu hizmeti olarak değerlendirilmekte ve insanların ifade ve düşünce özgürlüğünü sağlayabilmesi açısından önemli olduğu vurgulanarak temel insan hakları arasında olması gerektiği ifade edilmektedir (Kurt, 2015).

İnternet son 30 yıldır ve mobil teknolojiler ise son 20 yıldır hayatımızda olsa da, her iki teknolojinin de kullanımı, asıl sıçramasını Apple firmasının iPhone isimli ürünü ile yaşadı. iPhone'un pazar yeri (App Store) adını verebileceğimiz uygulaması ile geliştiricilerin geniş kitlelere ulaşma imkanını kolaylaştırması, hatta sadece yazılım şirketlerinin değil, bireysel geliştiricilerin bile tüm dünyada milyonlarca telefonda kullanılabilmesinin yolunu açtı. Bu durum da beraberinde kullanıcıların mahremiyet konularını telefon üreticisi ile yazılım geliştiricisinin kontrolüne bırakmış oldu (Fuentes, Hunt, Lopez-Ruiz ve Manzano, 2019).

Şekil 4'de Ocak 2021 itibariyle dünya çapındaki dijital nüfus gösterilmektedir. Şekilde görüldüğü üzere, aktif İnternet kullanıcı sayısı ve aktif sosyal medya kullanıcı sayıları milyar kullanıcı düzeyine ulaşmış durumdadır.



Şekil 4. Ocak 2021 itibariyle dünya çapındaki dijital nüfus (Statista, 2021)

2.2. Şirketlerin Topladığı Verinin Miktarının ve Çeşitliliğinin Artması

İletişimden alışverişe, seyahatten sağlığa yaşam tarzını derinden etkileyen dijital dönüşüm, beraberinde ciddi bir mahremiyet riskini de getirmiştir. İlk dönem dijital projelerde, sadece müşterinin sağladığı verilerle analizler yaparak öngörüler oluşturmaya çalışan şirketler, daha etkili ve isabetli öngörüler oluşturabilmek için aslında kişilerin sistemlerinde düşündüklerinden daha fazla izler bıraktıklarının farkına vardılar. Zaman içinde mobil cihazların yayılması, kişilerin sosyal platformlarda daha fazla zaman geçirmesi, şirketlerin bulut, yapay zeka, makine öğrenmesi gibi teknolojileri daha etkin kullanmaya başlaması, kişilerin daha fazla iz bırakmasına ve şirketlerin de daha fazla veri işleme kapasitesine sahip olmasına neden oldu. Durum öyle bir hal aldı ki şirketler artık sadece kendi web siteleri veya kendi uygulamaları üzerinde değil, müşterilerinin başka web siteleri veya mobil uygulamalarda bıraktıkları izleri bile takip etmek ve işleyerek analiz etmelerine kadar ulaştı. Bu süreçte kullanıcıların bir çoğu, çoğu zaman tam olarak neye izin verdiklerini bilmedikleri, karmaşık gizlilik sözleşmeleriyle, şirketlere mahrem verilerini bilinçsiz ve gönüllü olarak vermeye devam ettiler.

Kullanıcıların mahrem verilerinin, onların farkında olmadan şirketler tarafından toplandığı, uzmanlar tarafından gündeme getirilse de çok fazla bu konu dikkate alınmadı ya da komplo teorisi olarak görüldü. Ancak Cambridge Analytica adlı

firmanın 87 milyon kişinin, Facebook üzerindeki tüm verilerine erişerek kişileri profillediği ve bu veriler üzerinde yapılan analizler ile seçim sonuçlarına etki edecek faaliyetlerde bulunduğu ortaya çıkınca konunun ciddiyeti anlaşıldı (Isaak ve Hanna, 2018).

2.3. Dijital Dönüşüm Hızı ve Güvensiz Geliştirilen Projeler

Yazılım geliştirme süreci üzerindeki zaman baskısının, yazılım kalitesi üzerine etkileriyle ilgili araştırmalar bilinmektedir ve son dönemde yapılan yeni araştırmalar, zaman baskısının sadece kalite problemlerine değil aynı zamanda güvenlik risklerine de neden olduğunu ortaya koymaktadır.

Bu konuda ESG Group tarafından 2020 yılında yapılan bir araştırmada konu ile ilgili aşağıdaki değerlendirme yapılmıştır:

"Zaman baskısı, ekipleri zafiyetli kaynak kodu, üretim ortamında canlıya almak zorunda bırakıyor. Geliştirme süreci çevikleştikçe, ekipler güvenli yazılım geliştirme ile hızlı yazılım geliştirme arasındaki dengeyi sağlamak için yoğun mücadele veriyor" (EGS Group, 2020).

2.3.1 Covid-19'un dijital dönüşüm hızına etkisi. Covid-19 tüm dünyada insanların hiç beklemediği bir anda evlerine kapanmasına ve yaşamlarının hiç planlamadıkları şekilde değişmesine sebep oldu. Covid-19 yaşamları kökünden sarstı, etkilediği en önemli alanlardan biri de alışveriş oldu. Kullanıcılar bu dönemde mobil uygulama ve internet üzerinden bugüne kadar hiç olmadığı kadar çok alışveriş yaptı. Uzmanlara göre bu kullanıcıların birçoğu, belki de pandemi sonrasında normal alışveriş alışkanlıklarına geri dönmeyecekler (Kim, 2020). İnternet ve mobil cihazların her yıl artan kullanımıyla beraber müşterilerine ulaşmanın en etkin ve etkili yolunun dijitalleşme ile mümkün olduğunun farkına varan şirketler, pandemi ile bunun tek yolları olduğunu anladılar. Bu dönemde şirketlerin hayatta kalması rekabetten de daha önemli hale geldi ve bu dönemde zaten dijitalleşme süreci içinde olan veya bu sürece hızlı uyum sağlayan şirketler, sadece hayatta kalmayı başarmadı, bazıları bu zor dönemde bile büyümelerini devam ettirdiler.

2.4. Saldırganların Dijital Dönüşümü

Dijital dönüşüm, şirketlerin işlerini ve insanların hayatlarını değiştirirken, aynı zamanda siber suçluların saldırı yöntemlerini de dönüştürüyor. Siber suçlular,

şirketlerin dijital dönüşüm projelerinde kullandıkları teknolojilerin ortaya çıkarttığı zafiyetlerden faydalanırken, kendi kullandıkları yöntem ve araçları da dijitalleştirerek, buluttan yapay zekaya, makine öğrenmesinden veri madenciliğine birçok yeni teknolojiyi, saldırılarında yoğun bir şekilde kullanıyorlar. Sekil 5'de bir saldırı ortamından kullanılabilecek olan farklı enstrümanlar resmedilmektedir.

Şekil 5. ENISA saldırı ortamı (ENISA, 2021)

Yeni ve gelişen teknolojiler, beraberinde yeni saldırı vektörleri oluşturmaya devam edecek ve bu da beraberinde mevcut saldırıları genişletecektir. Suçlular, yeni ve mevcut teknolojileri, suç faaliyetlerini çeşitlendirmek ve geliştirmek için kötüye kullanmaya ve bunlardan yararlanmaya devam edecektir (Europol, 2017).

2.5. Saldırıların Paraya Kolay Dönüşüm İmkanı

Saldırganlar yıllardır farklı saldırı yöntemleri kullanarak şirketleri değişik boyutlarda zararlara uğrattılar, ancak saldırganlar verdikleri zararın ötesinde, bir

kazanç sağlama konusunda aynı oranda başarılı olamadılar. Yıllardır aradıkları yöntemi ise Ransomware saldırı türü ile buldular ve şirketlere zarar vermek yerine para kazanma yolunu seçtiler (Zakaria, 2017). Fidye yazılımı saldırısı olarak ifade edilebilecek olan bu durumlar nedeniyle, birçok firma halen büyük paralar kaybetmektedir.

2.5.1 Dijital para etkisi. Saldırganların ve saldırıların dönüşümüne sebep olan teknolojilerden biri de blok zincir (Blockchain) ve buna bağlı gelişen kripto para teknolojisi oldu. Şirketler, bu teknolojileri kendi faaliyet alanlarında nasıl kullanacaklarını bulmak için çalışmalar yürütürken, saldırganlar bu teknolojileri şirketlerden daha erken davranarak, mevcut saldırı yöntemlerine uyarladılar ve bugüne kadar kullandıkları saldırı tekniklerini kullanarak, para kazanmanın kolay ve risksiz bir yolunu buldular (Stroukal, 2016).

Kullanım kolaylığı ve dünya çapında kullanılabilirliği, özellikle Bitcoin'in saldırganlar tarafından fark edilmesini sağladı. Kripto para birimlerinin anonimliği, uluslararası terörist gruplar, yasa dışı kullanıcılar ve çeşitli suçluların ilgisini üst seviyede çekti. Kripto para birimiyle ilgili suçlar ve blok zinciri teknolojilerinin suistimali, günümüzde en hızlı büyüyen siber suç türü olarak kabul edilmektedir (Lewis, 2013).

2.6 Dijital Dönüşüm ile Artan Dış Kaynak Kullanımı

Dış kaynak (outsource) kullanımı, firmaların en iyi bildikleri işe odaklanarak bunun dışında kalan tüm fonksiyonları daha uygun maliyetle ve o alanda uzmanlığı olan farklı firmalardan alarak, rekabette ve müşteri memnuniyetinde fark yaratmalarına olanak sağlıyor. Firmalar, dijitalleşmenin getirdiği imkanları da kullanarak bu faydaları en üst seviyeye çıkarabiliyorlar (Quinn ve Hillmer, 1994).

Dış kaynak kullanımının getirdiği en büyük risklerden biri, firmaların dijitalleşme hızına aynı oranda cevap vermeyen tedarikçiler oldu. Firmalar kendi dijitalleşme projelerinde gerekli güvenlik önlemlerini alsalar ve ortamlarını güvenli hale getirmek için gerekli yatırımları yapsalar da, çalıştıkları tedarikçilerin bir çoğu bu süreçte geri kaldılar.

Özellikle BT hizmetlerinde kullanılan dış kaynakların sebep olduğu bilgi güvenliği ihlal olaylarına birçok örnek verilebilir. BT sağlayıcılarıyla bağlantılı siber güvenlik olayları düzenli olarak yaşanmaktadır. Son örnekler, Salesforce'un,

kullanıcıların tüm verilerine erişim izni veren bir veritabanı hatası nedeniyle (Mayıs 2019) CapitalOne'ın, Amazon'un bulutunda barındırılan 100 milyondan fazla müşterinin verilerini çalan eski bir Amazon Bulut Hizmetleri çalışanı nedeniyle veri ihlali (Temmuz 2019) ve Google'ın ABD'nin bazı bölgelerinde YouTube, Gmail ve Snapchat'i çökerten bulut kesintisi (Haziran 2019) *(*Benaroch, 2020) olarak ifade edilebilir.

Bölüm 3

Üst Yönetim ve Dijital Dönüşüm Kaynaklı Riskler

Bilgi güvenliği konusundaki standartlarda ilk maddelerden biri de, üst yönetim desteğidir, zira bilgi güvenliğinin başarısı ancak kurum kültürüne entegre olması ve gerekli yatırımların yapılmasıyla gerçekleşebilir, bunu sağlayabilecek güç ve yetki de şirketlerde üst yönetimlerde bulunmaktadır. Ancak teknolojide meydana gelen hızlı gelişmeler ve dönüşüm, üst yöneticilerin dijital dönüşüm ve getirdiği riskler konusunda güncel konuları takip etmelerini eskiye göre daha da fazla zorlaştırıyor. Şirketlerin dijital dönüşüm stratejilerini belirleyen üst yöneticilerin, siber güvenliğin, bu stratejilerin ana unsurlarından biri olduğunun farkında olması ve şirket stratejisinin bir parçası olarak kurum kültürüne entegre etmesi oldukça önem arz etmektedir. Aksi taktirde tasarımında güvenlik olmayan projelerin, sonradan güvenli hale getirilmesi ya mümkün olmamakta ya da çok yüksek maliyetler ortaya çıkmasına sebep olmakta, en kötüsü ise para ve itibar kaybettiren bilgi güvenliği ve ihlal olayları yaşanmasına neden olmaktadır (Fernandez, 2004).

3.1 Üst Yönetimin Siber Güvenlik Algısı ve Farkındalığı

Şirketlerin dijital dönüşüm konusundaki iştahı ve hızı, geliştirilen projelerin güvenliğinin ikinci planda kalmasına neden olabilmektedir. Bu her şirkette her zaman bilinçli olarak yapılmıyor. Bu husus, şirketlerin geçmişte yaşadıkları ihlal olayları veya siber güvenlik yatırımlarının seviyesine göre değişiklikler gösterebiliyor. Üst yönetimin siber güvenlik ve mahremiyet konularını hangi seviyede takip ettiğine bağlı olarak şirketlerin bu konudaki riskleri de doğal olarak artabiliyor.

"Bilgi Güvenliğinde 10 Ölümcül Günah" adlı çalışmada bu konu; "Ne yazık ki, çoğu durumda, şirketlerdeki üst yönetim, güvenliği sağlamak için gereken tek şeyin teknoloji olduğunu ve bu konunun teknik departmanların sorumluluğu olduğunu düşünüyor" (Von Solms, 2004) şeklinde açık bir şekilde ortaya konulmaktadır.

3.2 Dijital Dönüşüm Projelerinin Güvenli Yapıldığı ile İlgili Algı

Şirketlerin dijital dönüşümde başarılı olmalarının temel şartlarından birisi dijital dönüşüm stratejileri olmasıysa, bir diğeri de siber güvenlik ve mahremiyetin, bu stratejinin parçası olmasını sağlamaktır. Dijital dönüşüm projeleri sayesinde dağınık

olan ve işlenemeyen verilerin toplu bir şekilde bir araya gelmesi, üst yönetimde bir güvenlik hissiyatı yaratmaktadır. Oysa kolay erişilebilen, iyi iş çıktıları sunan ve toplu halde bulunan bu veriler saldırganlar için açık ve ilgi çekici bir hedef olmaktadır. Üst yöneticiler, güvenlik ve mahremiyet konularını, teknik ekiplerin çözecekleri teknik problemler gibi görmemeli, bu konuları dijital dönüşüm stratejilerinin bir parçası olarak mutlaka tanımlamalı ve takip etmelidirler.

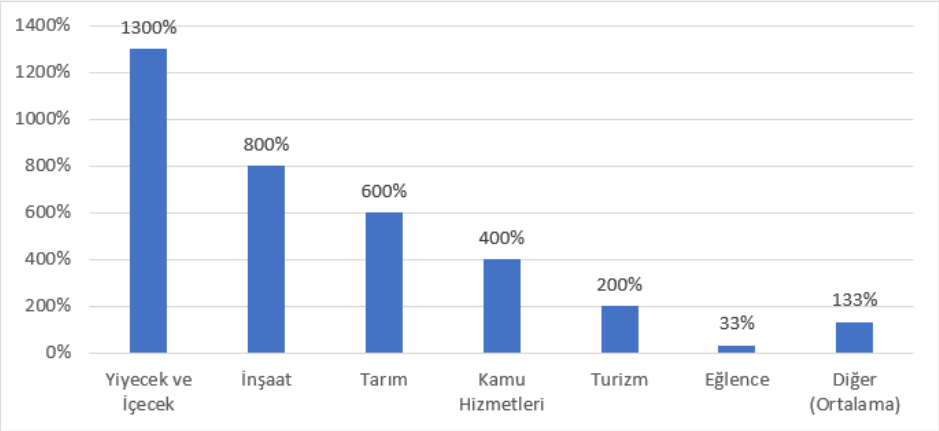
IDC Güvenlik Stratejileri Başkan Yardımcısı Pete Lindstrom, dijital dönüşüm ile güvenliğin paralel gelişmesi gerektiğini belirtmektedir. Bu konuda aşağıdaki değerlendirmede bulunmuştur.

"Şirketler dijital dönüşüm çabalarını hızlandırdıkça, güvenlik programlarının buna göre hızlanması çok önemli. Eski güvenlik yöntemlerine ve manuel uygulamalara güvenmek, güncel kurumsal ihtiyaçlarla ölçeklenemez" (Lindstrom, 2018).

3.3 Dijital Dönüşüm ile Siber Güvenlik ve Mahremiyete Ayrılan Bütçeler

Şirketlerin dijital dönüşüm projelerine ayırdıkları bütçeler, her geçen yıl artarak büyüyor. Pandemi sonrasında şirketler dijital dönüşüm süreçlerini ya çoktan başlattılar ya da planlıyorlar. Firmaları dijitalleşme yarışında birbirinden ayıran artık dijital dönüşüme bütçe ayırıp ayırmadıkları değil dijital dönüşüme ne kadar bütçe ayırdıklarıdır.

Şekil 6'da 2019-2020 yıllarında sektörlere göre saldırılardaki artış oranları gösterilmektedir.



Şekil 6. Sektörlere göre 2019 - 2020 saldırılardaki artış oranları (Kroll, 2021)

Daha önce dış dünyaya ve internete kapalı olarak çalışan, teknolojiyi ya hiç kullanmayan ya da daha az kullanan ve son dönemde yüksek oranda dijital dönüşüm yaşayan bazı sektörlerdeki şirketlerin dijitalleşme süreçlerinde yukarıda anlatılan potansiyel tehditler nedeniyle, daha fazla risk altında oldukları yapılan araştırmalarla ortaya çıkmaktadır. Gerçekleşen saldırılara bakıldığında, her ne kadar hala finans şirketleri ve sağlık kurumları üst sıralarda yer alsa da, geçen yıllara göre ataklarda en fazla artışın yiyecek ve içecek, inşaat ve tarım sektörlerinde olduğu görülmektedir (Kroll, 2021).

3.3.1 Dijital dönüşüme ayrılan bütçe. Günümüzde firmalar dijital dönüşüme yatırım yapan ve yapmayan olarak değil, dijital dönüşüme daha fazla yatırım yapan ve daha az yatırım yapan şeklinde sınıflandırılmaktadır. Pandemi gösterdi ki dijital dönüşüm yatırımı bir seçenek değil, bir zorunluluktur. Önümüzdeki yıllarda bu alanda yatırım yapmayan ve şirketlerinin dijital dönüşümünü gerçekleştiremeyen şirketler yok olup gidecekler (HBR, 2017). Dönüşümün gerçekleşmesi için sadece teknolojik yatırım yapmanın yeterli olduğunu düşünen firmaların projeleri, başarısızla sonuçlanmaktadır. Zira mobil stratejisi olmadan mobil uygulama sahibi olmak, çalışanların birlikte bir ürün ekibi olarak çalışması için gerekli stratejiye ve kurum kültürüne ve yetişmiş insan kaynağına sahip olmadan, eposta yerine Slack veya MS Teams kullanmaya başlamak, şirketlerin dijital dönüşümü başardığı anlamına gelmemektedir. Dijital dönüşüm yatırımları tek boyutlu olarak sadece teknolojik yatırımlar olarak görülür ve beraberinde geliştirilmesi gereken iç süreçler, kurum kültürü, insan kaynağının geliştirilmesi, güvenlik ve mahremiyet koruma bilinci ve farkındalığının arttırılması göz ardı edilirse, şirketlerin başarılı bir dijital dönüşüm sürecini tamamlamaları mümkün olamayacaktır.

Dijital dönüşüm yolculuğuna erken başlayan ve yukarıda saydığımız süreçleri deneyimleyen şirketler yatırımlarını arttırmaları gerektiğinin farkındadırlar. Dijital dönüşüm için yapılan yatırımların nerelere harcandığına bakıldığında, birinci sırada teknoloji yer almaktadır, daha sonra (a) müşteri ve çalışan deneyimi (b) dijital dönüşüm projelerinde çalışan kişilerin yeteneklerinin gelişimi (c) değişimin yönetilmesi (d) yenilik (inovasyon) (e) liderlik (f) kültür bulunmaktadır (Newman, 2018).

Tablo 2'de IDC'nin dijital dönüşüm harcamaları tahminleri yer almaktadır, bu araştırmaya göre önümüzdeki 5 yıl içinde dijital dönüşüm yatırımlarının %85 büyüyeceğini göstermektedir.

Tablo 2

Dijital Dönüşüm Harcamaları Tahminleri (Milyon Dolar) (IDC, 2021)

Bölge/Yıl	**2020**	**2021**	**2022**	**2023**	**2024**
Amerika	$505.782	$588.803	$687.432	$799.134	$923.088
Asya Pasifik	$470.021	$546.223	$645.047	$761.682	$895.372
EMEA	$341.737	$398.932	$464.350	$538.332	$621.636
TOPLAM	**$1.317.540**	**$1.533.959**	**$1.796.831**	**$2.099.149**	**$2.440.097**

3.3.2 Siber güvenliğe ayrılan bütçe. Şirketler zaman içinde deneme yanılma yoluyla, sadece teknolojik yatırım yaparak dijital dönüşümde başarıyı yakalayamayacaklarını gördüler. Zaman içinde dijital dönüşümün faydaları yanında getirdiği risklerden biri olan siber güvenlik ve mahremiyet konularının da yavaş da olsa farkında olmaya başladılar. Özellikle yaşanan ihlal olayları sonrası ya bizzat kendileri deneyimleyerek ya da rakipleri veya başka sektörlerdeki firmaların yaşadıkları deneyimlerden dersler çıkardılar. Ancak aynı dijital dönüşümde olduğu gibi siber güvenlik ve mahremiyet konusunda da şirketler hala sadece teknolojik yatırımlarla bu sorunları çözeceklerini düşünüyorlar. Oysa ki eğer şirketler hem dijital dönüşümlerinde başarılı olmak hem de güvenli bir dijital dönüşüm gerçekleştirmek istiyorlarsa, aynı dijital dönüşümde olduğu gibi siber güvenlik ve mahremiyet konularında da sadece teknolojiye değil diğer konulara da yatırımlar yapmalılar. Bu bağlamda, şirketler Newman'ın (Newman, 2018) dijital dönüşüm için tanımladığı, teknoloji hariç altı alanda yapılması gereken yatırımların benzerlerini siber güvenlik için de gerçekleştirmelidirler; bunlar; (a) siber güvenlik ve mahremiyet çözümlerinin müşteri ve çalışan deneyimine olumsuz etkilerini azaltacak yatırımlar, (b) siber güvenlik ve mahremiyet koruma konularında çalışacak personelin yetkinliklerinin arttırılması, (c) değişim yönetimine entegre güvenlik testleri, (d) yenilikçi fikirlerin güvenlik ve mahremiyet konularında hayata geçirilmesi, (e) güvenlik ve mahremiyet konusunda liderlik etme (f) ve kurum kültürüne siber güvenlik ve mahremiyet koruma konularının dahil edilmesi olarak sayılabilir.

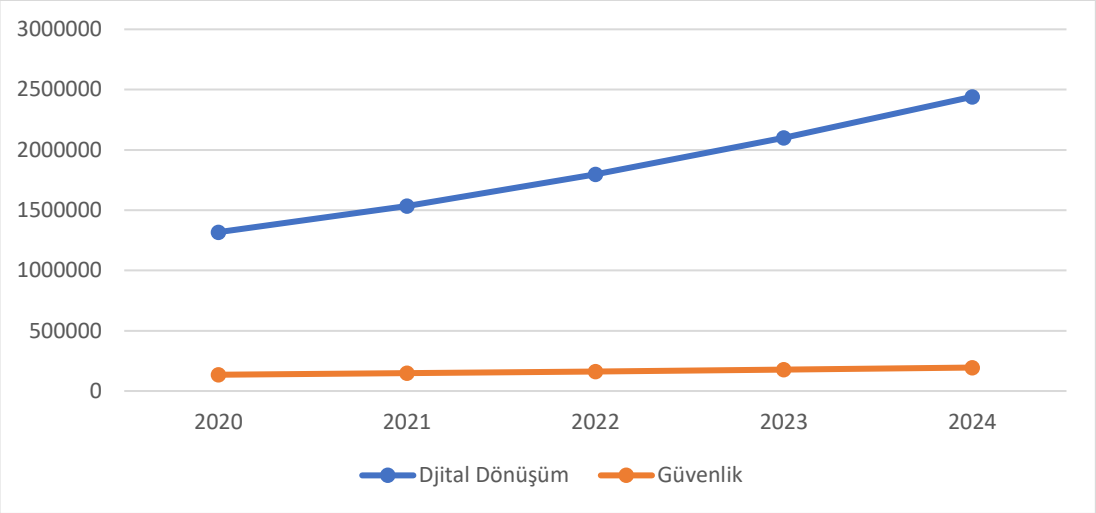
Tablo 3'de IDC'nin siber güvenlik harcamaları tahminleri yer almaktadır, bu araştırmaya göre önümüzdeki 5 yıl içinde dijital dönüşüm yatırımlarının %44 büyüyeceğini göstermektedir.

Tablo 3

Siber Güvenlik Harcamaları Tahminleri (Milyon Dolar) (IDC, 2021)

Bölge/Yıl	**2020**	**2021**	**2022**	**2023**	**2024**
Amerika	$69.927	$77.033	$84.395	$92.047	$99.968
Asya Pasifik	$26.693	$29.992	$33.562	$37.613	$42.201
EMEA	$38.239	$41.305	$44.754	$48.402	$52.293
TOPLAM	**$134.860**	**$148.330**	**$162.712**	**$178.063**	**$194.463**

Dijital dönüşüm harcamaları ile siber güvenlik harcamalarının yıllara göre artışına baktığımızda dijital dönüşüm projelerine olan yatırımların 5 yılda %85 artacağı görülüyor ancak aynı dönemde siber güvenlik harcamalarında sadece %44 bir artış öngörülmektedir. Şekil 7'de aradaki bu fark grafik olarak daha net bir şekilde görülmektedir.



Şekil 7. Dijital dönüşüm ve güvenlik harcamaları 2020 – 2024 tahmini (IDC, 2021)

Her ne kadar her iki alanda da yatırımlar artıyor gibi görünse de Tablo 4'e detaylı bir şekilde bakıldığında yıllar içinde siber güvenliğe yapılan yatırımın dijital dönüşüme yapılan yatırıma oranının artması gerekirken her yıl daha fazla oranda azalacağı tahmin edilmekte.

Tablo 4

Dijital Dönüşüm ile Siber Güvenlik Harcamalarının Yüzdesel Oranları

Yatırım/Yıl	2020	2021	2022	2023	2024
Dijital Dönüşüm	$1,317,540	$1,533,959	$1,796,831	$2,099,149	$2,440,097
Güvenlik	$134,860	$148,330	$162,712	$178,063	$194,463
DD/G % Oranı	10.24	9.67	9.06	8.48	7.97

Günümüzün hızla değişen dijital ekonomisinde, çoğu işletme şu anda ya sundukları hizmetleri iyileştirmek ya da operasyonlarını düzene sokmak için dijital dönüşümden geçiyor ve birçoğu yapılan bu finansal yatırımların faydalarını görüyor. Teknolojinin artan kullanımı ve kişisel verilerin toplanması ile güvenlik ihtiyacı artıyor. Ancak tüm işletmeler kendilerini aktif olarak siber suçlara karşı koruyamıyor.

Dijital dönüşüm, siber güvenlik ve mahremiyet konularında şirketlerin yapması gereken yatırımların mutlaka arttırılmasını gerektiriyor. Bu durum da, bu alanda daha fazla ve yetkin personel çalıştırılması, projelerde siber güvenlik ve mahremiyet konularının tasarım aşamasından itibaren proje ile entegre bir şekilde uygulanması ve test edilmesini gerektiriyor. Tüm bunları yapabilmek için hem güvenlik süreçlerine hem de güvenlik ürün ve servislerine bütçeler ayırmayı gerektiriyor (RSM, 2019).

Yapılan araştırmalar; Avrupa'nın önde gelen kuruluşlarının %80'inin, dijital dönüşümün şirketlerinin stratejik önceliği olduğunu söylüyor ancak bu şirketlerin %21'i yoğun bir şekilde dijital dönüşüm yatırımları yaptıklarını belirttikleri halde bir siber güvenlik stratejileri olmadığını ifade ediyor (Kroll, 2021).

3.4 Kişisel Verilerin Korunması Kanunları

Son yıllarda özellikle kişisel verilerin korunması konusunda gerek ülkemizde gerekse tüm dünyada, özellikle devletler nezdinde ciddi bir farkındalık oluştu ve gerekli korumaları sağlamak maksatlı yasalar çıkartıldı. Türkiye'de 7 Nisan 2016 tarihinde 6689 sayılı "Kişisel Verilerin Korunması Kanunu" (KVKK), Avrupa'da 14 Nisan 2016 tarihinde "Genel Veri Koruma Tüzüğü" (GDPR) yürürlüğe girdi. GDPR 1995 yılında Avrupa Birliği tarafından kabul edilen "Veri Koruma Direktifi"nin (DPA) yerini aldı. Her iki yasa da şirketlere ve kurumlara kişisel verilerin toplanması, işlenmesi ve saklanması süreçlerinde ciddi yükümlülükler getiriyor ve uyumsuzluk durumlarında çok yüksek parasal ceza ve yaptırımlar uyguluyor.

Her iki yasa temel olarak; (a) şirketlerin ve kurumların bir veri sorumlusu atamasını ve bu kişiyi ilgili veri koruma otoritesine bildirmesini istiyor, (b) kullanıcıların talep etmesi durumunda şirketlerin ve kurumların kullanıcıya belirli bir süre içerisinde hangi verilerini tuttuğunu bildirmesi ve kullanıcı talep ederse bu verileri silmesi veya anonim hale getirmesini zorunlu kılıyor, (c) şirketler ve kurumlar, topladıkları, sakladıkları ve işledikleri kişisel verilerin başkalarının eline geçmesine sebep olan bir siber saldırı ya da ihlal olayı yaşaması durumunda, konu hakkında 72 saat içinde ilgili veri koruma otoritesini bilgilendirmek zorundadır (KVKK, 2016) (GDPR, 2016).

Bölüm 4

Yöntem

Bu bölümde çalışma kapsamında gerçekleştirilen anket ile araştırmanın amacı ve yöntemi, evren ve örneklemi, veri toplama analizi ve bulgulara yer verilmiştir. Devam eden bölümde araştırmadan elde edilen bulgular yorumlanmıştır.

4.1 Araştırmanın Amacı

Araştırmanın amacı; dijital dönüşüm ile siber güvenlik ve mahremiyet konularındaki risklerin, kullanılan teknolojilerin, firmaların bu alanlara yaptığı yatırımların ve onları en çok endişelendiren konuların ve teknolojilerin neler olduğunun araştırılmasıdır.

4.2 Evren ve Katılımcılar

Araştırma evrenini Türkiye'de faaliyet gösteren özel ve kamu kurumlarında görev yapan CEO/GM, CIO / BT Direktörü / BT Müdürü yöneticiler oluşturmaktadır. Örneklem, bu yöneticiler arasından tesadüfi olarak seçilen 44 kişiden oluşmaktadır.

4.3 Verilerin Toplanması

Çalışma kapsamında Google formlar kullanılarak hazırlanan ankette yer alan sorular çevrimiçi olarak yöneticilere yöneltilmiştir. Bu sorular şu başlıklar altında toplanmaktadır:

a. Görev ve sektöre ilişkin sorular. Anketin bu bölümü, katılımcıların çalıştıkları şirketlerdeki görevleri ve şirketlerinin bulunduğu sektör ile ilgili bilgi sorularından oluşmaktadır.

b. Dijital dönüşüm ve siber güvenlik konularına ilişkin sorular. Anketin bu bölümünde örneklem grubunda yer alan yöneticilere, şirketlerinin dijital dönüşüm ve siber güvenlik ve mahremiyet için son iki yılda bütçelerinin nasıl değiştiği ve dijitalleşme projelerinde, siber güvenlik ve mahremiyet konularını nasıl ele aldıklarıyla ilgili sorular soruldu. Ayrıca, ankette yöneticilere kendilerini siber güvenlik ve mahremiyet açısından en çok endişelendiren teknolojiler ve risklerle ilgili sorular yöneltildi. Ankette diğer firmaların karşılaştığı siber güvenlik ve mahremiyet olaylarının şirketlerin dijital dönüşüm projelerini nasıl etkilediği de soruldu.

4.4 Verilerin Çözümlenmesi

Ankete 10 adet CEO / GM ve 34 adet CIO / BT Direktörü / BT Müdürü seviyesinde görev yapan toplam 44 üst düzey yönetici katıldı. Katılımcılar ağırlıklı olarak Bilişim, Finans ve Ulaştırma sektöründe çalıştıklarını belirttiler.

Bölüm 5

Bulgular

Çalışmada yer alan kişilerin kurumlarındaki görevleri ve kurumlarının faaliyet gösterdiği sektörlerinin dağılımları analiz edilmiştir.

5.1 Görev ve Sektöre İlişkin Bulgular

Örneklem grubunda yer alan kişilerin görevlerine ilişkin dağılım tablosu Tablo 5'te yer almaktadır. Yapılan analizde katılımcıların kurumlarındaki görevlerinin Şekil 8'deki dağılımları incelendiğinde; yüzde 22,7'sinin CEO / GM, yüzde 77,3'sinin de CIO / BT Direktörü / BT Müdürü olduğu belirlenmiştir.

Tablo 5

Katılımcıların Görev Dağılımı

Çalışılan Kurumdaki Görev	Frekans	Yüzde	Kümülatif Yüzde
CEO/GM	10	22.7	22.7
CIO/BT Direktörü/BT Müdürü	34	77.3	100.0
Toplam	44	100.0	

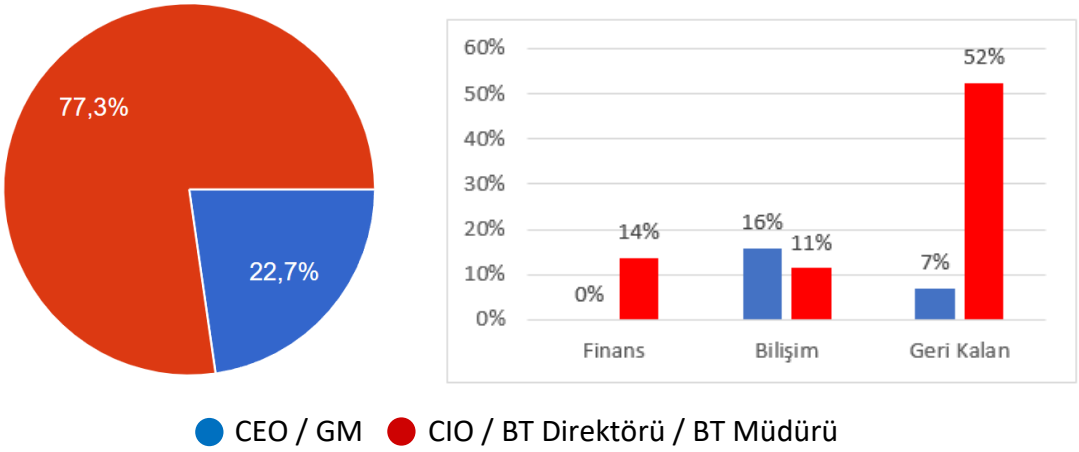
Tablo 6'da katılımcıların finans, bilişim ve geri kalan sektörlere göre dağılımları verilmiştir. Finans sektöründen 6 kişi CIO seviyesinde görev yapmaktadır, bu sektörden katılımcılar arasında CEO seviyesinde katılım olmamıştır. Bilişim sektöründen katılımcıların 7'si CEO seviyesinde 5'i CIO seviyesindedir.

Tablo 6

Katılımcıların Görev Dağılımı (Sektöre Göre)

Çalışılan Kurumdaki Görev	Finans	Bilişim	Geri Kalan
CEO/GM	0	7	3
CIO/BT Direktörü/BT Müdürü	6	5	23

Finans sektörünün, özellikle bu sektördeki kanun uygulayıcı kurum olan BDDK tarafından koyulmuş olan kurallarla yönetildiği ve kurumun bu kuralların uygulanmasını sıkı bir şekilde denetlediği biliniyor. Bilişim sektörü kuruluşları da bu konularda diğer sektörlere göre daha bilinçli ve bilgililer. Bu nedenle yapılan analizde finans ve bilişim sektörü katılımcılarının cevaplarına ayrıca yer verilerek çalışmanın geneline nasıl bir etkisi olduğu gösterildi.



Şekil 8. Katılımcıların görev dağılımı

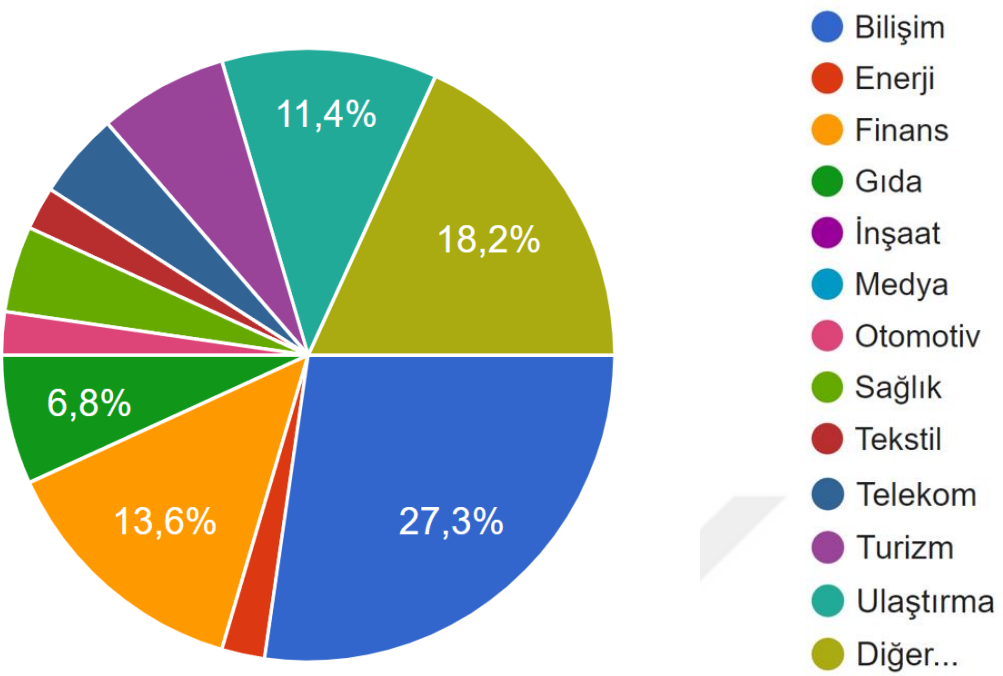
Tablo 7'de katılımcıların kurumlarının bulunduğu sektöre ilişkin dağılımları yer almaktadır. Tablo incelendiğinde; katılımın %27,3 ile en çok bilişim sektöründen olduğu, bunu %18.2 ile diğer sektörler ve %13.6 ile finans sektörünün izlediği görülmektedir. Türkiye'de dijital dönüşümün en yoğun gerçekleştiği, özellikle siber güvenlik ve mahremiyet konularında en fazla farkındalığın ve yatırımların olduğu sektör, finans sektörüdür, ayrıca tüm şirketlere bu konularda projeler üreten sektör de bilişim sektörüdür. Bu bağlamda katılımcıların ankete katkıları konuya ışık tutması açısından oldukça önemlidir.

Tablo 7

Katılımcıların Çalıştığı Sektör Dağılımı

Sektör	Frekans	Yüzde	Kümülatif Yüzde
Bilişim	12	27.3	27.3
Enerji	1	2.3	29.6
Finans	6	13.6	43.2
Gıda	3	6.8	50.0
İnşaat	0	0	50.0
Medya	0	0	50.0
Otomotiv	1	2.3	52.3
Sağlık	2	4.5	56.8
Tekstil	1	2.3	59.1
Telekom	2	4.5	63.6
Turizm	3	6.8	70.4
Ulaştırma	5	11.4	81.8
Diğer	8	18.2	100
Toplam	44	100	

Katılımcıların çalıştığı sektöre göre yüzde dağılımı Şekil 9'da gösterilmektedir.



Şekil 9. Katılımcıların çalıştığı sektör dağılımı

5.2 Dijital Dönüşüm ile Siber Güvenlik ve Mahremiyete İlişkin Bulgular

Türkiye'deki farklı sektörlerde görev yapan üst düzey yöneticiler, şirketlerinde dijital dönüşüm ve siber güvenlik yatırımlarının son iki yılda arttığını ifade etmiştir. Yapılan global araştırmalar ve tahminler de bu tespiti desteklemektedir.

Tablo 8'de tüm katılımcıların kurumlarının dijital dönüşüm yatırımlarının son 2 yılda nasıl değiştiği hususunda ilgili veriler yer almaktadır.

Tablo 8

Dijital Dönüşüm Yatırımlarının Son 2 Yıldaki Değişimi

	Frekans	Yüzde	Kümülatif Yüzde
Değişmedi	7	15.9	15.9
Arttı	33	75	90.9
Azaldı	4	9.1	100
Toplam	44	100.0	

Tablo 9'da finans, bilişim ve diğer sektör katılımcıların kurumlarının dijital dönüşüm yatırımlarının son 2 yılda nasıl değiştiği hususunda ilgili detay veriler yer almaktadır.

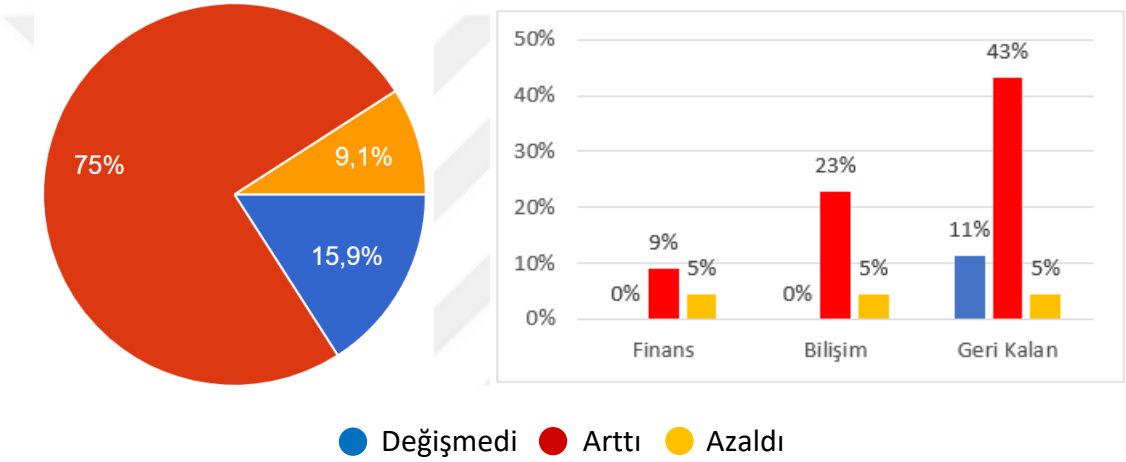
Tablo 9

Dijital Dönüşüm Yatırımlarının Son 2 Yıldaki Değişimi (Sektöre Göre)

	Finans	Bilişim	Geri Kalan
Değişmedi	0	0	5
Arttı	4	10	19
Azaldı	2	2	2

Yatırımların değişimlerinde sektöre göre bir farklılık gözlemlenmemektedir. Tüm sektörlerde Covid-19 etkisine de bağlı olarak artış olduğu görülmektedir.

Katılımcıların kurumlarının dijital dönüşüm yatırımlarının son 2 yıldaki değişim dağılımı grafiği ve sektörlere göre dağılım grafiği Şekil 10'da gösterilmektedir.



Şekil 10. Dijital dönüşüm yatırımlarının son 2 yıldaki değişimi

Tablo 10'da katılımcıların kurumlarının siber güvenlik ve mahremiyet yatırımlarının son 2 yılda nasıl değiştiği yer almaktadır.

Tablo 10

Siber Güvenlik ve Mahremiyet Yatırımlarının Son 2 Yıldaki Değişimi

	Frekans	Yüzde	Kümülatif Yüzde
Değişmedi	11	%25	25
Arttı	31	%70.5	95.5
Azaldı	2	%4.5	100
Toplam	44	%100.0	

Tablo 11'de finans, bilişim ve geri kalan sektörlerden katılımcıların kurumlarının siber güvenlik ve mahremiyet yatırımlarının son 2 yılda nasıl değiştiği yer almaktadır.

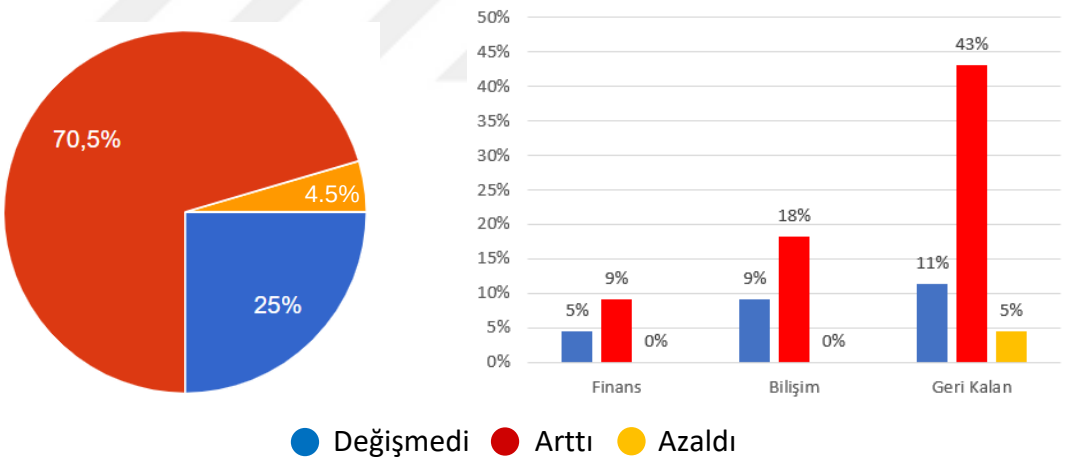
Tablo 11

Siber Güvenlik ve Mahremiyet Yatırımları Son 2 Yıldaki Değişimi (Sektöre Göre)

	Finans	Bilişim	Geri Kalan
Değişmedi	2	4	5
Arttı	4	8	19
Azaldı	0	0	2

Burada da siber güvenlik ve mahremiyet yatırımlarının, dijital dönüşüm yatırımlarıyla paralel bir şekilde artış yönünde olduğu görülmekte ve yatırımların değişimlerinde sektöre göre bir farklılık gözlemlenmemektedir.

Katılımcıların kurumlarının siber güvenlik ve mahremiyet yatırımlarının son 2 yıldaki değişim dağılım grafiği ve sektörlere göre dağılım grafiği Şekil 11'de gösterilmektedir.



Şekil 11. Siber güvenlik ve mahremiyet yatırımlarının son 2 yıldaki değişimi

Tablo 12'de dijital dönüşüm projelerinin kurumlarda siber güvenlik ve mahremiyet risklerine etkisi ile ilgili veriler yer almaktadır. Tablo 13'te bu risklerin finans, bilişim ve geri kalan sektörlere göre dağılımları verilmektedir.

Tabloları incelediğimizde sektörden bağımsız olarak çalışmaya katılan yöneticilerin büyük bir oranda dijital dönüşüm projelerinin siber güvenlik ve mahremiyet risklerini arttırdığını düşündükleri görülüyor.

Tablo 12

Dijital Dönüşüm Projelerinin Siber Güvenlik Risklerine Etkisi

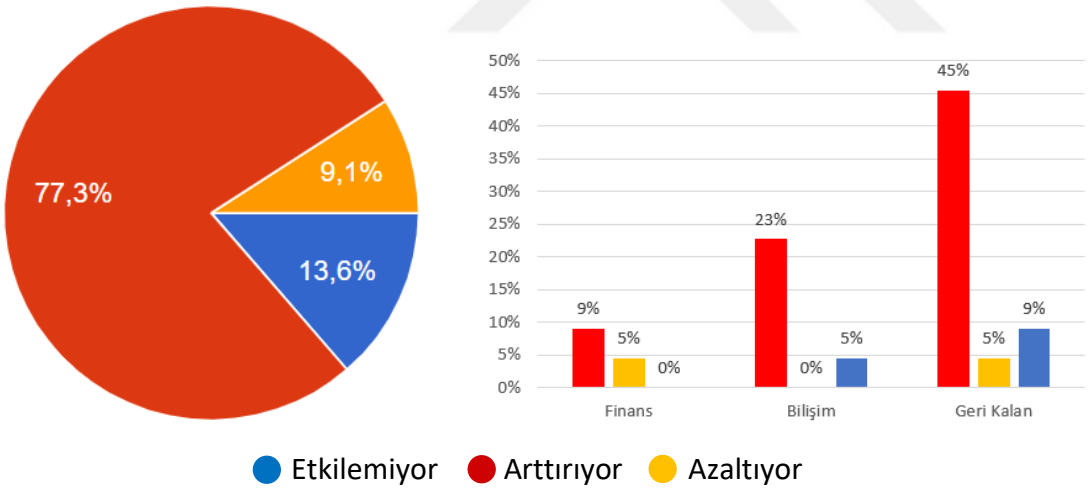
	Frekans	Yüzde	Kümülatif Yüzde
Etkilemiyor	6	13.6	13.6
Arttırıyor	34	77.3	90.9
Azaltıyor	4	9.1	100
Toplam	44	100.0	

Tablo 13

Dijital Dönüşüm Projelerinin Siber Güvenlik Risklerine Etkisi (Sektöre Göre)

	Finans	Bilişim	Geri Kalan
Etkilemiyor	0	2	4
Arttırıyor	4	10	20
Azaltıyor	2	0	2

Dijital dönüşüm projelerinin kurumlarda siber güvenlik ve mahremiyet risklerine etkisinin dağılım grafiği Şekil 12'de gösterilmektedir.



Şekil 12. Dijital dönüşüm projelerinin siber güvenlik risklerine etkisi

"Dijital dönüşüm projelerinizin kurumunuzun siber güvenlik ve mahremiyet risklerine etkisinin nasıl olduğunu düşünüyorsunuz?" sorumuza yöneticilerin % 77.3 oranında "Arttırıyor" cevabını vermiştir. Yöneticilerin % 13.6'sı ise "Etkilemiyor" cevabını vermiştir ki bu durum da toplam katılımcıların sadece % 9.1'nin dijitalleşme projelerinin siber güvenlik ve mahremiyet risklerini azalttığını düşündüğünü göstermektedir.

Gerekli insan kaynağı ile desteklenmeyen ve gerekli bütçenin ayrılmadığı bir projede, güvenli bir tasarımın yapılması, uygulamaya geçirilmesi ve gerekli testlerden geçirilmesi çok mümkün olmamaktadır. Kaldı ki kullanılan teknolojilerin doğası gereği, aşırı veri paylaşımına imkan vermesi ve bunu kolaylaştırması nedeniyle ne yazık ki bir çok proje, kurumların siber ihlal olayları ve veri kayıpları ile ciddi yasal yaptırım ve para cezaları ile karşı karşıya kalmalarına neden olmaktadır.

Tablo 14'de şirketlerin dijital dönüşüm projelerinde siber güvenlik ve mahremiyet konularını nasıl ele aldıkları gösterilmektedir. Tablo 15'te bu verilerin finans, bilişim ve geri kalan sektörlere göre dağılımları gösterilmektedir.

Tablo 14

Dijital Dönüşüm Projelerinde Siber Güvenlik Konuları Ele Alınması

	Frekans	Yüzde
Projelerle birlikte yeni güvenlik ihtiyaçları çıkıyor ve bu yatırımları da yapıyoruz	33	75
Mevcut yatırımlarımız yeterli o yüzden ayrıca ele almıyoruz	4	9.1
Projeler güvenli geliştiriliyor, ek güvenlik ihtiyacı olmuyor	7	15.9
Toplam	44	100.0

"Dijital dönüşüm projelerinizde siber güvenlik ve mahremiyet ile ilgili konuları nasıl ele alıyorsunuz?" sorusuna yöneticilerin % 15.9'u "Projeler güvenli geliştiriliyor, ek güvenlik ihtiyacı olmuyor" şeklinde yanıt vermiştir.

Tablo 15

Dijital Dönüşüm Projelerinde Siber Güvenlik Konuları Ele Alınması (Sektöre Göre)

	Finans	Bilişim	Geri Kalan
Projelerle birlikte yeni güvenlik ihtiyaçları çıkıyor ve bu yatırımları da yapıyoruz	5	9	19
Mevcut yatırımlarımız yeterli o yüzden ayrıca ele almıyoruz	1	1	2
Projeler güvenli geliştiriliyor, ek güvenlik ihtiyacı olmuyor	0	2	5

Katılımcıların sadece % 9.1'i "Mevcut yatırımlarımız yeterli o yüzden ayrıca ele almıyoruz" şeklinde yanıt vermiştir.

Oysa ki yapılan her proje, şirket dijital portföyüne eklenen her ürün ve servis, doğası gereği şirketlerin risk yüklerine yenilerini ekliyor ve mutlaka bu konularda yapılması gereken risk analizi çalışmalarından, risk azaltma çalışmalarına, güvenli tasarım, uygulama ve test pratiklerine kadar bir çok yatırım ihtiyacı bulunmaktadır.

Dijital dönüşüm projelerinde siber güvenlik ve mahremiyet ile ilgili konuların ele alındığı dağılım grafiği Şekil 13'de gösterilmektedir.

Şekil 13. Dijital dönüşüm projelerinde siber güvenlik konularının ele alınması

Yöneticilerin %75 gibi büyük bir oranı da "Projelerle birlikte yeni güvenlik ihtiyaçları çıkıyor ve bu yatırımları da yapıyoruz" cevabını vermiştir. Şirketlerin ve üst düzey yöneticilerin, siber güvenlik ve mahremiyet konularında en çok yanıldıkları konuları saymak gerekirse, bunlar; güvenliğin tüm şirketin bilemeyeceği kadar kompleks ve uzmanlık gerektiren bir konu olduğu ve bu nedenle bu konuda BT ekiplerinin çalışmalar yapması gerektiği, çoğu zaman bir ekibe ihtiyaç olmadığı, güvenlikten sorumlu bir kişinin yeterli olacağı, önce projenin bitirilmesi gerektiği ve güvenliğe sonra bakılacağı, güvenliğin sonradan bazı ürün ve servislerle sağlanabilen bir husus olduğunun düşünülmesidir. Oysaki güvensiz geliştirilen bir projenin sonradan güvenli hale getirilmesi için gereken kaynak ve caba, bazı projelerde projenin kendisinden daha büyük olabiliyor, hatta bazı durumlarda projenin tamamen rafa kaldırılması ya da tamamen baştan geliştirilmesine sebep olabiliyor. Diğer bir olası

seçenek ise şirketler yaptıkları yatırımın boşa gitmesini göze alamadıkları için projedeki zafiyetlere rağmen canlıya geçerek, büyük riskler almalarıdır.

Tablo 16'da kurumların dijital dönüşüme ayrılan bütçenin ne kadarının siber güvenlik ve mahremiyet konularına ayrıldığı gösterilmektedir. Tablo 17'de finans, bilişim ve geri kalan sektörlerde bu bütçelerin nasıl dağıldığı gösterilmiştir.

Tablo 16

Dijital Dönüşüme Ayrılan Bütçenin Siber Güvenlik Bütçesine Oranı

	Frekans	Yüzde	Kümülatif Yüzde
%1-10	22	50	50
%11-25	17	38.6	88.6
%26-50	3	6.8	95.4
%50'den fazla	2	4.6	100
Toplam	44	100.0	

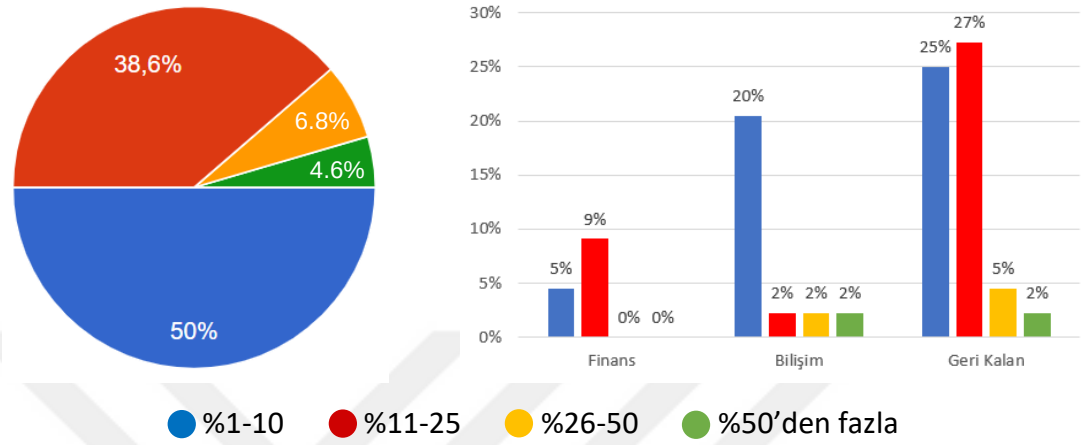
"Dijital dönüşüme ayrılan bütçenin ne kadarı siber güvenlik ve mahremiyet koruma çalışmalarınıza gidiyor?" diye sorulan yöneticilerin %50'si %1-10 arası şeklinde ifade etmiştir ki bu mevcut araştırma ve tahminlerin gösterdiği mevcut rakamların altında kalıyor, zira mevcut göstergeler bu rakamın %10 civarında olduğunu ancak önümüzdeki yıllarda daha da düşeceğini gösteriyor, oysa ki çalışmamızda bu oranın artması gerektiğini, zira dijitalleşme ile her geçen gün siber güvenlik ve mahremiyet risklerinin arttığını farklı araştırma ve kaynaklardan derlediğimiz verilerle ortaya koymaya çalıştık. Anketimize yanıt veren yöneticilerin % 38.6 gibi büyük bir kısmı, şirketlerinin dijital dönüşüm bütçesinin % 11-25 arasında bir bütçeyi siber güvenlik ve mahremiyet koruma konularına ayırdığını ifade etmiştir ki bu iyi bir oran ve küresel rakamların üzerinde olduğu değerlendirilmektedir

Tablo 17

Dijital Dönüşüme Ayrılan Bütçenin Siber Güvenlik Bütçesine Oranı (Sektöre Göre)

	Finans	Bilişim	Geri Kalan
%1-10	2	9	11
%11-25	4	1	12
%26-50	0	1	2
%50'den fazla	0	1	1

Şekil 14'te görüleceği gibi katılımcılarımızın geri kalan %11,4'ü şirketlerinin %26 ve üstü bir bütçeyi siber güvenlik ve mahremiyet konularına ayırdığını ifade etmiştir ki bu da dijital dönüşümde daha ileri seviyede olan veya başından bu süreçte, en az bir siber ihlal olayı geçmiş olan şirketlerin, bu konuda farkındalıklarının arttığını ve gerekli adımları attıkları söylenebilir.



Şekil 14. Dijital dönüşüme ayrılan bütçenin siber güvenlik çalışmalarına etkisi

Tablo 18'de kurumların dijital dönüşüme yaptıkları yatırımlar ile siber güvenlik ve mahremiyete yaptıkları yatırımların artış oranlarını karşılaştırmalarını istediğimizde verdikleri yanıtlar gösterilmektedir. Tablo 19'da finans, bilişim ve geri kalan sektörlerde kurumların dijital dönüşüme yaptıkları yatırımlar ile siber güvenlik ve mahremiyete yaptıkları yatırımların artış oranlarının dağılımı gösterilmekte.

Tablo 18

Dijital Dönüşüm ile Siber Güvenlik Yatırımlarının Karşılaştırılması

	Frekans	Yüzde	Kümülatif Yüzde
Daha az artıyor	16	36.4	36.4
Daha fazla artıyor	14	31.8	68.2
Aynı seviyede artıyor	14	31.8	100
Toplam	44	100.0	

"Dijital dönüşüm ile siber güvenlik ve mahremiyet yatırımlarınızı oransal olarak karşılaştırmanızı istesek" diye sorduğumuz yöneticilerden yaklaşık üçte biri siber güvenlik ve mahremiyet yatırımlarının dijital dönüşüm yatırımları ile "aynı oranda arttığını" ifade derken yaklaşık üçte biri "daha fazla artıyor", kalan yaklaşık üçte biri de "daha az artıyor" cevabını vermiştir.

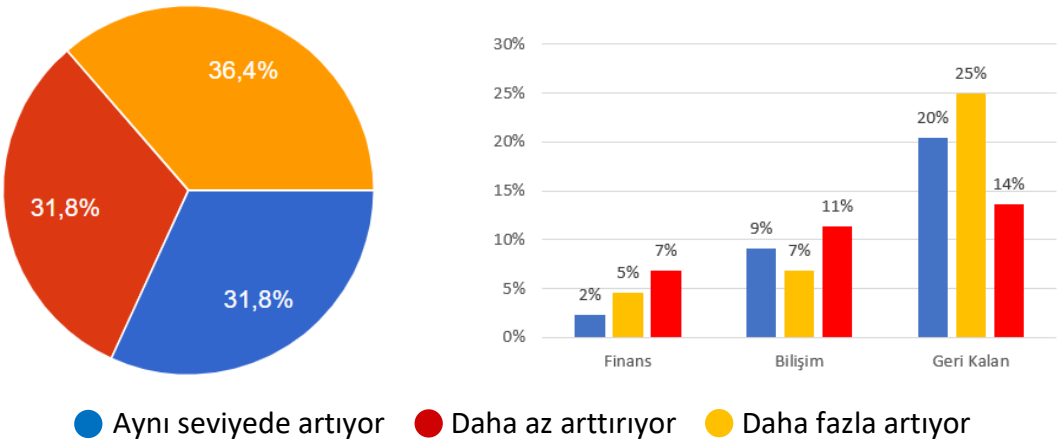
Tablo 19

Dijital Dönüşüm ile Siber Güvenlik Yatırımlarının Karşılaştırılması (Sektöre Göre)

	Finans	Bilişim	Geri Kalan
Daha az artıyor	2	3	11
Daha fazla artıyor	3	5	6
Aynı seviyede artıyor	1	4	9

Burada cevapların oransal olarak bu kadar yakın olmasının sebebi, ankete katılan farklı sektörlerdeki şirketlerin, dijital dönüşümün değişik evrelerinde olmalarının verdikleri cevapları belirlediği değerlendirilmekte. Dijital dönüşüme yeni başlamış şirketler, ana odakları bir an önce dijitalleşme sürecini tamamlamak olduğu için nispeten daha az siber güvenlik ve mahremiyet yatırımı yaparken, dijital dönüşümün ileri evrelerindeki şirketler, dijital dönüşüm ile beraber siber güvenlik ve mahremiyet risklerinin farkına vardıkça, bu yatırımlarını arttırma eğilimi göstermekteler. Eğer şirket bir de siber ihlal olayı yaşamış veya yasal bir ceza veya yaptırım ile karşı karşıya kalmışsa, bu farkındalık daha da artmakta ve yatırımlarını daha da arttırma eğiliminde olmaktadır.

Dijital dönüşüm ile siber güvenlik ve mahremiyet yatırımlarının oransal karşılaştırılması dağılım grafiği Şekil 15'de gösterilmektedir.



Şekil 15. Dijital dönüşüm ile siber güvenlik yatırımlarının karşılaştırılması

Tablo 20'de kurumların diğer firmaların karşılaştığı siber güvenlik ve mahremiyet olaylarının dijital dönüşüm projelerini nasıl etkilediğini gösteriyor. Tablo 21'de finans, bilişim ve geri kalan sektörlerin bu durumdan nasıl etkilendiklerinin dağılımı gösterilmekte.

Tablo 20

Diğer Firmaların Karşılaştığı İhlal Olaylarının Projelere Etkisi

	Frekans	Yüzde	Kümülatif Yüzde
Olumlu Etkiliyor	27	61.4	61.4
Olumsuz Etkiliyor	4	9.1	70.5
Etkilemiyor	13	29.5	100
Toplam	44	100.0	

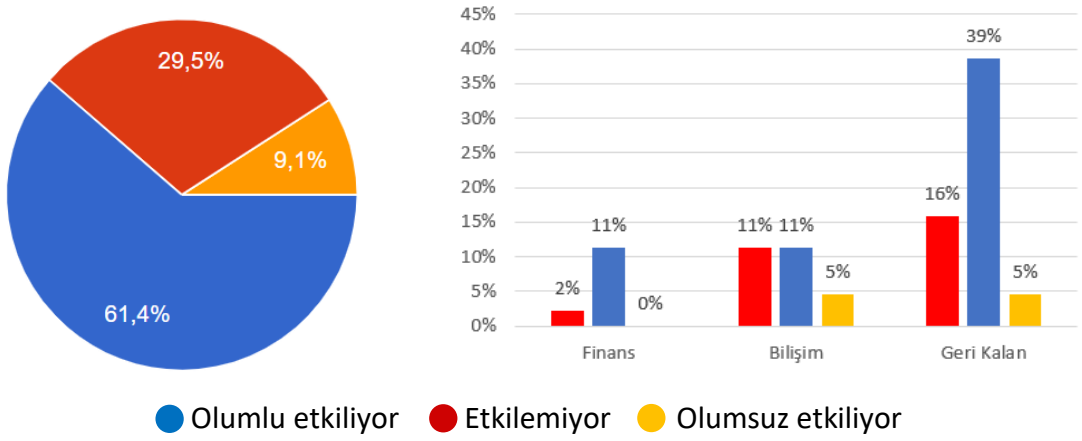
"Diğer firmaların karşılaştığı siber güvenlik ve mahremiyet olayları dijital dönüşüm projelerinizi nasıl etkiliyor?" sorumuza yöneticilerin %61.4'ü "olumlu etkiliyor" cevabını vermiş. Buradan çıkartılan sonuç, yöneticilerin dijital dönüşüm projelerini daha güvenli yapmaları konusunda bu olayları bir kaldıraç olarak kullanarak gerekli zaman ve kaynakları alma konusunda avantaj sağladıkları yönündedir. Bu soruya yöneticilerin %29.5'u "etkilemiyor" cevabını verirken %9.1'i ise olumsuz etkiliyor cevabını vermiştir.

Tablo 21

Diğer Firmaların Karşılaştığı İhlal Olaylarının Projelere Etkisi (Sektöre Göre)

	Finans	Bilişim	Geri Kalan
Olumlu Etkiliyor	5	5	17
Olumsuz Etkiliyor	0	2	2
Etkilemiyor	1	5	7

Diğer firmaların karşılaştığı siber güvenlik ve mahremiyet olaylarının dijital dönüşüm projelerine etkisine ilişkin dağılım grafiği Şekil 16'da gösterilmektedir.



Şekil16. Diğer firmaların karşılaştığı ihlal olaylarının projelere etkisi

Geçmiş dönemlerde yapılan bazı araştırmaların şirketlerin siber güvenlik ve mahremiyet riskleri nedeniyle, dijital dönüşüm projelerine hatta bulut bilişim, mobil uygulama gibi bazı teknolojilere bile mesafeli olduklarına dair araştırmalar vardır. Ancak artık günümüzde pandemi baskısı ile beraber dijital dönüşüm hiçbir şirketin geride kalmayı göze alabileceği bir konu değildir. Günümüzde şirketlerin dijital dönüşüm projesi yapıp yapmadığı değil, ne kadar dijital dönüşüm projesi yaptıkları daha önemli hale gelmiş durumdadır. Ancak bu sürecin bir sonraki adımı şirketleri birbirinden ayıracak yeni kriter, şirketlerin ne kadar güvenli dijital dönüşüm projeleri yaptıkları olacaktır.

Tablo 22'de yöneticileri en çok endişelendiren teknolojiler gösterilmektedir. Tablo 23'te finans, bilişim ve geri kalan sektör yöneticilerinin bu soruya verdiklerin yanıtların dağılımı verilmektedir.

Tablo 22

Yöneticileri En Çok Endişelendiren Teknolojiler

Teknolojiler	Frekans	Yüzde
Web	29	65.9
Mobil	24	54.5
Bulut	23	52.3
Nesnelerin Interneti (IoT)	19	43.2
3.Parti entegrasyonlar	37	84.1
Yapay Zeka/Makine Öğrenmesi	11	25
Kullanıcı hataları	1	2.3

"Dijital dönüşüm projelerinizde sizi siber güvenlik ve mahremiyet açısından en çok endişelendiren teknolojiler hangileri?" diye sorduğumuz yöneticilerimizin %84.1'i "3. Parti entegrasyonlar" cevabını vermiştir. Günümüz en popüler iş modellerinden biri olan dış kaynak kullanımı, şirketlerin masrafları azaltma, ana işlerine odaklanma ve karlılığı arttırmadaki rolü yadsınamaz bir gerçektir. Ancak bu iş modeli ile ya mevcut şirketlerin içindeki bazı departmanların ayrılarak şirketleşmesi ya da bazı iş alanlarında niş bir konu gören kişilerin girişimleriyle, organizasyonel yapısı henüz oluşmamış birçok yeni şirket, iş hayatına hızlı bir giriş yapmıştır. Bu şirketler, kendilerine oranla devasa şirketlerin işlerini alt yükleniciler olarak almaya başladılar. Ancak çalıştıkları büyük organizasyonlar, yoğun bir şekilde

dijitalleşme sürecinde oldukları için çalıştıkları bu alt yüklenicilerin de kendileriyle entegre olarak dijital süreçlerine dahil olmalarını ve yeni iş yapış şekillerinde kendileriyle aynı hızda ilerlemelerini istediler. Gerek gelir yapısı gerekse organizasyonel yapılanması buna uygun olmayan bu alt yüklenici firmalar da, dijitalleşme süreçlerini ve büyük firmalarla olan entegrasyon çalışmalarını, kendilerine benzeyen küçük bilişim firmaları, hatta tek kişilim yazılımcılara alt yüklenici olarak verdiler. Bu sürecin sonucunda hiçbir güvenlik önlemi olmayan bu alt yükleniciler, fonksiyon olarak destekledikleri büyük firmaların büyük verilerini kendi güvensiz ortamlarında saklamaya ve işlemeye başladılar. Bazı büyük firmalar bu risklerin farkına vararak küçük alt yüklenicilere entegrasyon desteği sağlayarak, verilerinin riskini azaltmaya çalışsa da, onlar da kendi sistemlerine bu entegrasyonlar üzerinden gelen saldırılardan kaçınmayı başaramadılar.

Tablo 23

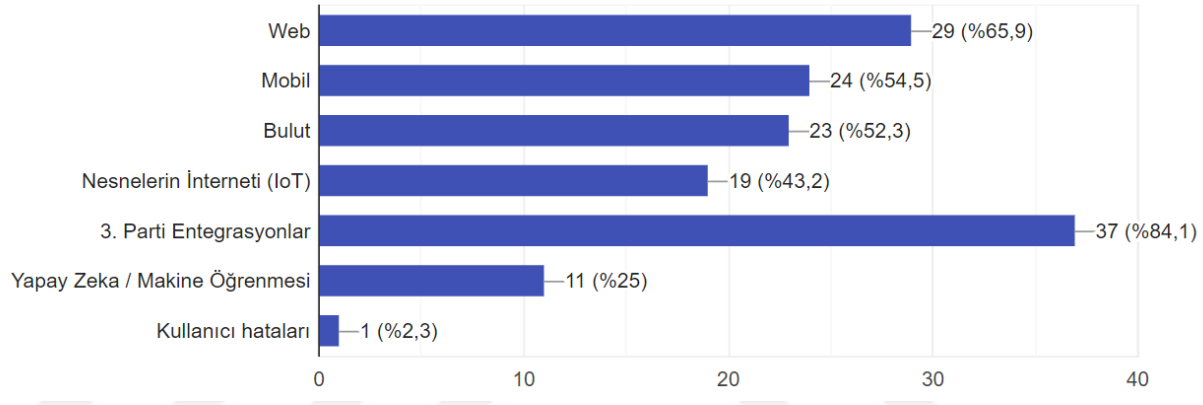
Yöneticileri En Çok Endişelendiren Teknolojiler (Sektöre Göre)

Teknolojiler	Finans	Bilişim	Geri Kalan
Web	5	5	19
Mobil	3	6	15
Bulut	2	8	13
Nesnelerin Interneti (IoT)	3	4	12
3.Parti entegrasyonlar	6	8	23
Yapay Zeka/Makine Öğrenmesi	1	2	8
Kullanıcı hataları	0	1	0

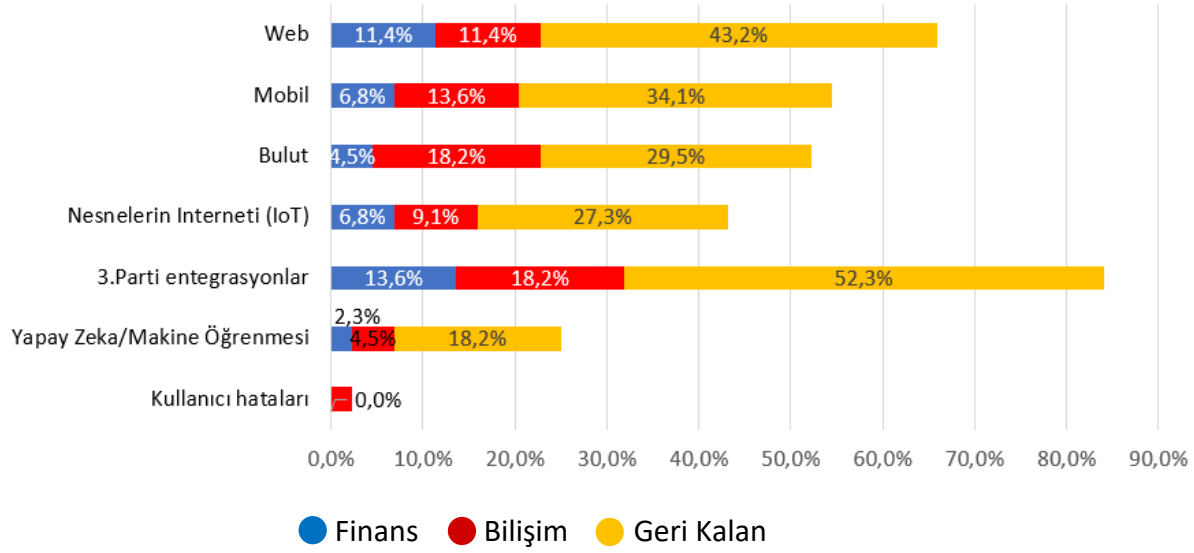
Yöneticileri endişelendiren ikinci önemli teknolojinin %65.9 ile web olması hem doğal hem de bir hayli şaşırtıcıdır. Bugün kullandığımız anlamıyla herkese açık web'in 1991'de hayatına başladığı düşünüldüğünde, üzerinden 30 yıl geçmesine rağmen hala yöneticileri endişelendiren konular arasında ikinci sırada yer alması oldukça düşündürücüdür, zira eğer 30 yıldır hayatımızda olan web'i güvenli hale getiremediysek, sadece 5-10 yıldır hayatımızda olan bulut bilişim, mobil teknolojiler, yapay zeka, blok zincir, nesnelerin interneti ve makine öğrenmesi gibi teknolojileri kullandıkları için şirketleri, siber dünyada daha ne tür tehlikeler bekliyor olabilir. Web bu 30 yıl içinde oldukça büyük değişimler geçirdi. İlk yıllarında tamamen statik HTML sayfalarıyla yapılan sitelerin en büyük riski, sunucuların saldırıya uğraması

veya servis kesintisine uğraması ya da içeriklerin değiştirilmesiydi. Web 2.0 denilen yeni nesil web ile dinamik içerikler ve etkileşimli web kavramları hayatlarımıza girdi. Bu yeni gelişmeyle beraber web tabanlı saldırılarda içeriği değiştirmek yerine, başka bilgisayarlara bulaşan içerik ekleme, servisi kesintiye uğratmak yerine, içeriği çalmaya yönelik saldırılar gerçekleşmeye başladı. Günümüzde hala saldırıların çoğu web'i hedef almakta ve veri sızıntılarının büyük kısmı web servisleri üzerinden gerçekleşmektedir.

Dijital dönüşüm projelerinde siber güvenlik ve mahremiyet açısından en çok endişelendiren teknolojilerin dağılım grafiği Şekil 17'de gösterilmektedir. Şekil 18'de finans, bilişim ve geri kalan sektörlere göre dağılım detayları verilmektedir.



Şekil 17. Yöneticileri en çok endişelendiren teknolojiler



Şekil 18. Yöneticileri en çok endişelendiren teknolojiler (sektöre göre)

Yöneticileri endişelendiren üçüncü sıradaki %54.5 yüzdeyle mobil teknolojiler aslında büyük oranda web'in en büyük rakibi, zira günümüzde mobil teknolojiler o

kadar ilerlemiş durumda ki, çok başarılı bazı yeni projeler sadece mobil olarak hayata geçiyor ve hayatına bu şekilde devam ediyor ya da sonrasında çok daha basit fonksiyonlarla bir web surumu de çıkabiliyor. Buna en iyi öreklerden biri tüm dünyada kullanılan Instagram, Türkiye'deki en iyi örneği de Getir sayılabilir. Mobil uygulamalardaki risklere baktığımızda genel olarak birinci ve ikinci sıradaki 3. Parti riskler ve web risklerinin bir karışımı olarak karşımıza çıkmakta, zira ya mobil uygulama geliştirmede kullanılan 3. Parti yazılım veya servisler kaynaklı olaylar yaşandığını ya da hala mobil servislere yazılan, web arka planlardaki zafiyetlerden kaynaklı sorunlar görüyoruz. Mobil teknolojilerin hedef alındığı siber güvenlik ve mahremiyet risklerine baktığımızda, özellikle hesap çalınması, kredi kartı bilgisi çalınması ve kişisel bilgilere yetkisiz erişilmesi konularının öne çıkmaktadır.

Yöneticileri en çok endişelendiren dördüncü sıradaki teknoloji %52.3 ile bulut bilişim teknolojisidir. Bu teknolojinin oluşturduğu risklerden bir tanesi; verinin sınırlarını ortadan kaldırmasıdır, bu konu şirketler ve kişiler kadar ülkelerin de en çok gündeminde olan bir konudur. Ülkemiz de dahil bir çok ülke özellikle finansal ve kişisel verilerin ülke sınırları içerisinde tutulması konusunda yasalar ve genelgeler hazırlamış durumdalar. Şirketleri endişelendiren en önemli unsurlardan biri, bulut tabanlı sistemleri yönetebilecek yetişmiş insan kaynağı eksikliğidir, bu eksiklik kendini buluta taşınan sistemlerin güvenliği sağlayacak personel konusunda da gösteriyor. Bulut teknolojilerin şirketlerin projelerini nasıl bir adım öne çıkardığını daha önceden görmüş, çok güçlü bilgisayarlar ve gelişmiş algoritmaları şirketlerin servisine sunduğunu gözlemlemiştik. Bulut bilişimi bu kadar tehlikeli kılan bir diğer yanı da, bulut servislerini saldırganların da kullanabiliyor olması ve aynı yetenek ve kapasitelere onların da erişimlerinin olmasında yatıyor. Saldırganların kendilerine ait bulut yapıları ve kendilerine ait Servis Olarak Yazılım (SaaS), Servis Olarak Platform (PaaS), Servis Olarak Altyapı (IaaS) modelinde saldırı araçlarını çok uygun maliyetlerle isteyen herkesin hizmetine sundukları düşünülürse, riskin boyutu daha iyi anlaşılacaktır.

Yöneticileri en çok endişelendiren beşinci sıradaki teknoloji %43.2 ile Nesnelerin İnterneti (IoT) olarak tespit edilmiştir. IoT, mobil teknolojileri bir adım öteye götürerek hayatımıza ve fiziksel dünyamıza entegre olup, kullanıcıdan ve ortamdan daha fazla veri toplayarak mobil teknolojinin yarattığı riskleri katlayarak attıracaktır. Akıllı saat veya yüzük, gözlük veya evde bulunan ve ortamdaki komutları dinleyen bir hoparlör formatında karşımıza çıkan bu cihazlar, kalp atışımızdan,

kanımızdaki oksijen miktarına kadar birçok hassas kritik veriyi dahi işleyebilmektedir. Evimizin içinde yapılan tüm konuşmaları dinlemekte ve işlemektedir. Bu verilerin saldırganların yeni hedefi olması kaçınılmazdır. Bu cihazların kendisi oldukça küçük olduğu için hemen hemen hepsi çalışırken, bulut bilişim ile yapay zeka ve makine öğrenmesi gibi teknolojileri yoğun bir biçimde kullanmaktadır. IoT teknolojileri de diğer tüm teknolojiler gibi önce fonksiyon ve değer yaratmaya odaklanmış durumda, bu nedenle, çok büyük firmaların projeleri bile güvenlik zafiyetleriyle beraber gelmektedir. Hatta, bazen bu ürünlerin fiyatını erişilebilir kılmak adına, geçmişte eski teknolojilerde yapılan hatalar IoT'de tekrarlanıyor ve şifreleme, güçlü kimlik doğrulama gibi çok temel özelliklerden bile yoksun olarak piyasaya sürülmektedir. Benzer risk şirketlerin Operasyonel Teknoloji (OT) ortamları için de geçerlidir. Eski teknoloji ve güvensiz SCADA sistemleri, analiz edilmek üzere veri toplamak maksatlı BT sistemlerine bağlanmakta, hatta verimliliği arttırmak ve maliyetleri düşürmek amacıyla, bu analizler sonunda gerçek zamanlı olarak bu cihazlara geri besleme yapacak projeler üzerinde çalışılmaktadır. Geçtiğimiz bir veya iki yıl içinde üretim sektöründe, özellikle yiyecek ve içecek sektöründe meydana gelen saldırıların %1300 arttığını düşündüğümüzde, bu projelerin sistemleri ne kadar savunmasız bıraktığı ve saldırganların ne kadar dikkatini çekmeye başladığı açık şekilde görünüyor.

%25 ile Yapay Zeka ve Makine Öğrenmesi altıncı sırada yer almaktadır. Henüz bu teknolojilerin gelişim aşamasında olması nedeniyle, yoğun bir kullanımının ülkemizde olmaması ve bu teknolojilerden kaynaklı yaşanan olaylara henüz rastlanmıyor olması, bu riskin aşağı sıralarda yer almasına sebep olmuş olabilir. Ancak saldırganların bu teknolojileri yoğun bir şekilde kullanmak için çaba içinde oldukları düşünülürse, bu riskin önümüzdeki günlerde daha üst sıralara çıkması kaçınılmaz görünüyor.

%2.3 gibi çok düşük bir oran ile insan hatasının en son sırayı aldığını görüyoruz. Oysa ki çok yakın zamana kadar tüm şirketler, insanın bilişim teknolojilerindeki en zayıf halka olduğunu ve gerçekleşen kesinti olayları ya da siber ihlal olaylarında ilk sıraya insan hatasını koyarlardı. Bu sonucun listedeki diğer teknolojilerde yaşanan baş döndürücü gelişme hızına, yöneticilerin uyum sağlamakta zorlanmaları nedeniyle, yaşadıkları endişeden kaynaklı olduğu değerlendirilmektedir. Zira günümüzde insan hatası ya da insan kastı sonucu oluşan, veri sızıntıları ve siber güvenlik ihlal olayları hala hafife alınmayacak kadar yüksek orandadır.

Tablo 24'te yöneticileri en çok endişelendiren siber güvenlik ve mahremiyet riskleri gösterilmektedir. Tablo 25'te bu verilerin finans, bilişim ve geri kalan sektörlere göre dağılımı verilmektedir.

Yöneticilere "Dijital dönüşüm projelerinizde sizi en çok endişelendiren siber güvenlik ve mahremiyet riskleri hangileri?" diye sorduğumuzda aldığımız en fazla cevap %88.6 ile "Şirket verisinin çalınması" olmuştur

Tablo 24

Yöneticileri En Çok Endişelendiren Siber Güvenlik Riskleri

	Frekans	Yüzde
Müşteri verisinin çalınması	38	86.4
Şirket verisinin çalınması	39	88.6
Üretimin/Hizmetin aksaması ya da durması	31	70.5
Para Kaybı	20	45.5
Yasal yaptırımlar ve cezalar	27	61.4
İtibar ve müşteri kaybı	1	2.3

Tablo 25

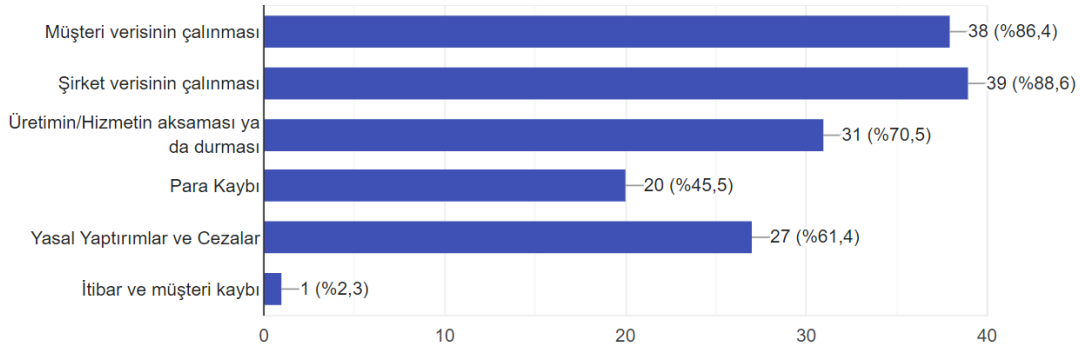
Yöneticileri En Çok Endişelendiren Siber Güvenlik Riskleri (Sektöre Göre)

	Finans	Frekans	Yüzde
Müşteri verisinin çalınması	6	11	21
Şirket verisinin çalınması	6	11	22
Üretimin/Hizmetin aksaması ya da durması	4	7	20
Para Kaybı	1	7	12
Yasal yaptırımlar ve cezalar	4	8	15
İtibar ve müşteri kaybı	0	1	0

%86.4 gibi çok yakın bir oranla "Müşteri verisinin çalınması" ikinci sırada yer almıştır. Üst düzey yöneticileri uzun süredir endişelendiren en önemli konuların başında veri çalınması gelmektedir. Ancak saldırganların çalınan verileri paraya dönüştürmesi her zaman çok kolay olmuyor. Bu nedenle son yıllarda veriyi çalmak yerine, olduğu yerde şifreleyerek fidye isteme yönteminde ciddi artış yaşanmaktadır. Fidye saldırıları saldırganlara ikinci bir fırsat daha verdi, o da ankette %70.5 ile üçüncü sırada yer alan "Üretimin/Servisin aksaması ya da durmasıdır". Son dönemde yürürlüğe giren veri koruma kanunları nedeniyle verilen cezalar sonrası üst düzey

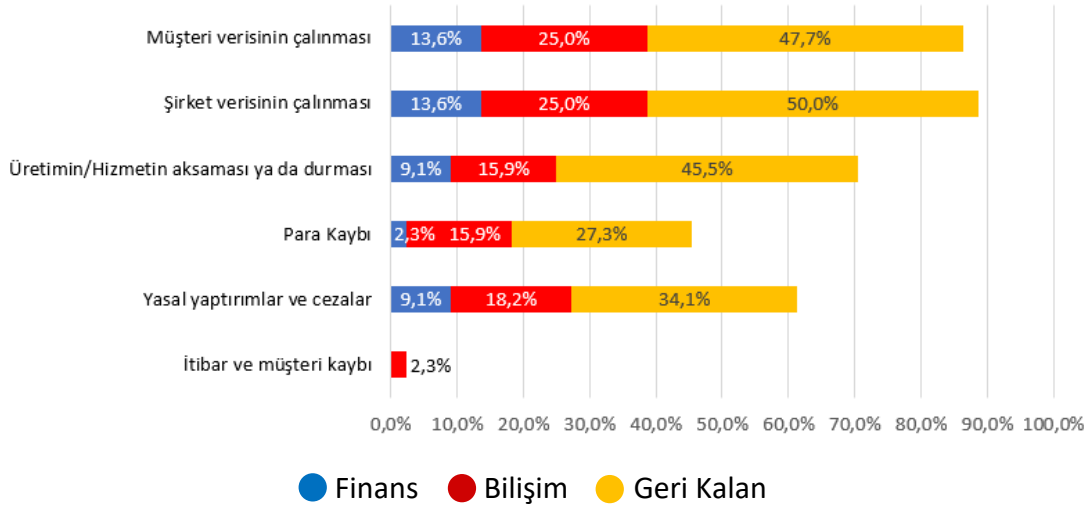
yöneticilerde yeni oluşmaya başlayan diğer bir endişe de ankette %61.4 oranında tercih alan "Yasal yaptırımlar ve cezalar"dır.

Dijital dönüşüm projelerinden en çok endişelendiren siber güvenlik ve mahremiyet riskleri dağılım grafiği Şekil 18'de gösterilmektedir.



Şekil 19. Yöneticileri en çok endişelendiren siber güvenlik riskleri

Bu soruya verilen yanıtlarda ilgi çeken sonuçlardan biri, yukarıda belirtilen ilk 4 sıradaki tüm konular, şirketlere "Para Kaybı" ve "İtibar ve müşteri kaybı" ile sonuçlanabilecekken, yöneticilerin bu konularda daha az endişeli olduklarını ifade etmiş olmalarıdır. Son dönemde dünya devi şirketler başta olmak üzere, birçok şirketin başından siber ihlal olayları geçmesi ve bunların basında yoğun bir şekilde yer alması, bu konuların artık biraz daha normal karşılanmasına sebep oluyor olabilir.



Şekil 20. Yöneticileri en çok endişelendiren siber güvenlik riskleri (sektöre göre)

Son yıllarda şirketlerin yaşadığı siber ihlal olayları, yürürlüğe giren veri koruma kanunları ve yayınlanan genelgeler ile birlikte, siber güvenlik ve mahremiyet konularının ele alındığı seviye gün geçtikçe daha yukarılara doğru çıkmaktadır.

Ülkemizde de BDDK, SPK gibi düzenleyici kurumlar, yayınladıkları genelgeler ile siber güvenlik konularının yönetim kurulu seviyesinde ele alınmasını beklemektedir.

Tablo 26'da kurumlarda siber güvenlik ve mahremiyet konularının kurumun hangi seviyesinde ele alındığı gösterilmektedir. Tablo 27'de finans, bilişim ve geri kalan sektörlerde bu dağılımın nasıl olduğu verilmektedir.

"Şirketinizde siber güvenlik ve mahremiyet konuları hangi seviyede ele alınıyor?" sorumuza yöneticilerin %27.3'ü "Yönetim Kurulu" cevabını vermiştir ki katılımcılarımızın yaklaşık %13.6'sının finans sektöründen olduğu düşünülürse, bunun bir tercihten çok, zorunluluk olarak yapıldığını ifade edebiliriz.

Tablo 26

Siber Güvenlik ve Mahremiyet Konularının Ele Alınma Seviyesi

	Frekans	Yüzde	Kümülatif Yüzde
Bilgi Güvenliği Müdürü (CISO)	4	9.1	9.1
BT Müdürü (CIO)	12	27.3	36.4
Genel Müdür (CEO)	12	27.3	63.7
İcra Kurulu	4	9.1	72.8
Yönetim Kurulu	12	27.3	100
Toplam	44	100.0	

Verilen cevapların %27.3'ü "Genel Müdür (CEO)" ve %9.1'i "İcra Kurulu" seviyesinde alınıyor şeklindedir ki bu sonuçlara %27.3 ile "Yönetim Kurulu" cevabını da eklediğimizde, toplamda %63,7 gibi büyük bir oranda siber güvenlik ve mahremiyet konularının, stratejik karar alabilecek ve kurumda liderlik gücü olan kurum kültürünü değiştirebilecek seviyede temsil edildiğini gösterir.

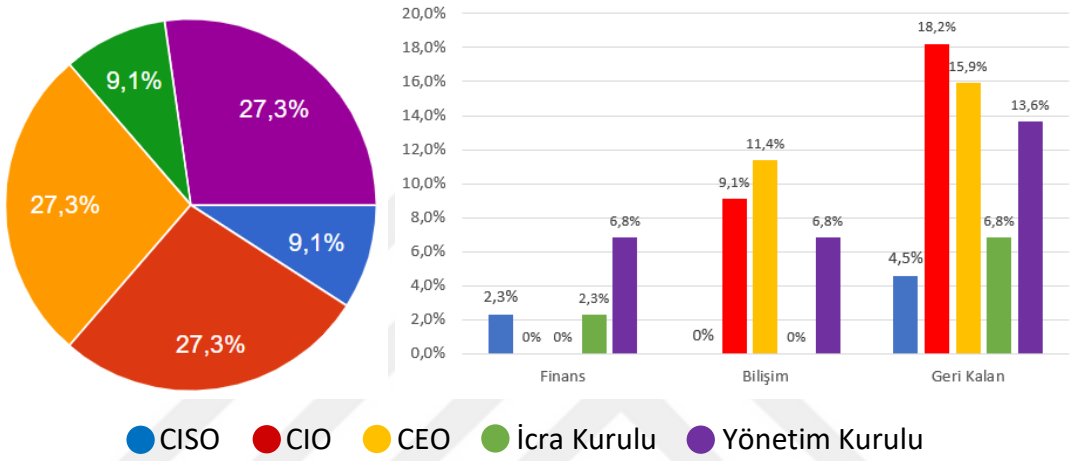
Tablo 27

Siber Güvenlik ve Mahremiyet Konularının Ele Alınma Seviyesi (Sektöre Göre)

	Finans	Bilişim	Geri Kalan
Bilgi Güvenliği Müdürü (CISO)	1	0	2
BT Müdürü (CIO)	0	4	8
Genel Müdür (CEO)	0	5	7
İcra Kurulu	1	0	3
Yönetim Kurulu	3	3	6

Finans sektöründe regülasyonların da etkisiyle konuların icra kurulu ve yönetim kurulu seviyesinde ele alındığı görülmektedir. Bilişim sektörünün kurumlara ürün veya hizmet sunduğu düşünüldüğünde bu temsiliyetin finas kuruluşlarında olduğu gibi daha yüksek olması beklenirdi ancak CIO ve CEO seviyesinde kaldığı gözlemlenmektedir.

Kurumlardaki siber güvenlik ve mahremiyet konularının ele alınma seviyesine ilişkin dağılım grafiği Şekil 19'da gösterilmektedir.



Şekil 21. Siber güvenlik ve mahremiyet konularının ele alınma seviyesi

%27.3 ile "BT Müdürü (CIO)" ve %9.1 ile "Bilgi Güvenliği Müdürü (CISO)" cevaplarıyla hala %36,3 gibi büyük bir oranda, konuların teknik ve taktik seviyeden daha yukarıya çıkamadığını söylemek mümkündür.

Bölüm 6

Tartışma ve Sonuçlar

6.1 Araştırma Sorunlarının Bulgularının Tartışılması

Dijital dönüşüm, rekabette öne geçme, müşterinin gözünde fark yaratma, şirketin karlılığını arttırırken çalışan memnuniyetine katkı sağlama ve işleri daha verimli yapma gibi birçok konuda şirketlerin vazgeçilmez birincil stratejileri haline geldi. Teknolojik gelişmeler ve bu teknolojilerin her geçen gün daha da ucuzlaması, sadece büyük şirketlerin değil, yeni kurulmuş çok küçük şirketlerin bile bu teknolojileri kullanarak, milyonlarca müşteriye küresel pazarlarda ürün ve servis sunabilmesine olanak sağlıyor. Geçmişte sadece çok büyük şirketlerin AR-GE merkezlerinde kullanabildiği çok büyük bilgisayar gücü artık bulut bilişim sayesinde bir öğrenci projesinde, küçük bir girişim şirketinde ya da çok büyük bir şirketin bir projesinde kullanılabilir hale gelmiş durumdadır. Ayrıca, bulut yapısı üzerinden yapay zeka, makine öğrenmesi, ses tanıma, yüz tanıma, sohbet robotu, görüntü işleme gibi çok gelişmiş teknolojileri de çok uygun ve kullandıkça öde modelleriyle isteyen herkes projelerinde kolaylıkla kullanabiliyor. İnternet ve mobil teknolojilerde yaşanan gelişmeler sayesinde tüm dünya artık yerel bir Pazar haline gelmiş durumda. Bir veya iki yazılımcısı olan küçük bir girişim şirketi Türkiye'de geliştirdiği bir mobil uygulamayı tüm dünyada müşterilerin beğenisine sunabiliyor ve günler, haftalar içinde milyonlarca müşteriye sahip olabiliyor.

Tüm bu imkanlar, irili ufaklı on binlerce şirketin, mobil cihazlar ve internetin de gelişimi ve yaygınlaşması ile tüm dünyada milyonlarca müşteriye ulaşmasını sağladı. Bu etkileşim sonucunda on binlerce şirket, milyonlarca kişinin verisini toplamaya, işlemeye, saklamaya ve zenginleştirmeye başladı. Hatta durum belli bir süre sonra öyle bir hale geldi ki, bu şirketler yaptıkları iş birlikleri ile mobil cihazlara ve geliştirdikleri uygulamalara ekledikleri özelliklerle müşterilerin sadece verilerini değil deneyimlerini ve kullanım alışkanlıklarını da birbirlerine satmaya veya birbirleriyle paylaşmaya başladılar. Bir süre sonra iç yapıları çok düzenli ve belli etik kurallar ile iş yapan şirketler de hiçbir kuralın olmadığı, tek kişinin yazılım geliştirdiği şirket bile olmayan girişimler de, bu yapıda kendilerine bir yer buldu. Bu noktadan sonra kullanıcılar ne tür verilerinin kimler tarafından ne maksatla kullanıldığını kontrol edemez duruma geldi.

Bu duruma gelinirken kullanıcılarda ciddi bir değişim döneminden geçtiler. İnternet ve mobil cihazların yaygınlaşması ve erişilebilirliğinin artması ile geçmişte mobil cihazlarla yapılan işlemlerin çeşitliliği artarken, temel kullanım alanları da ciddi bir değişim geçirdi. Eskiden sesli görüşme ve mesajlaşma için kullanılan mobil cihazlar, bir süre sonra fotoğraf çekme, grup sesli ve görüntülü görüşme gibi ek özelliklere kavuştu. Eskiden cihazın sadece fiziksel olarak bir değeri varken, bu yeni eklenen özelliklerle beraber cihazlarda birikmeye başlayan kişisel veriler, cihazın değerinden kat ve kat daha fazla değerli hale geldi. Kişilerin o güne kadar özel ve mahrem saydıkları ve sadece yakın çevreleri ve sevdikleri ile paylaştıkları bu verileri, tüm dünya ile paylaşmaya teşvik eden sosyal medya şirketleri belki de mahremiyet konusunda dünya tarihindeki en büyük değişimin başlamasına neden oldular. Sosyal medya şirketlerinin ücretsiz sundukları özellikler, her geçen gün kullanıcıların daha da fazla kişisel verisini paylaşmasını farklı yöntemler ve kampanyalarla teşvik etti. Bu kadar çok veriye sahip olan sosyal medya şirketlerinin kapıları, kısa bir süre içinde yıllardır aradıkları fırsatı gören şirketler tarafından tek tek çalınmaya başladı. Şirketler yıllardır gazete, radyo ve televizyon gibi mecralardan hedefleyemedikleri müşterilere, sonuçlarını istedikleri ölçüde ölçemedikleri kampanyalarla sonuçlar almaya çalışıyorlardı. Oysa, sosyal medya şirketlerinin elindeki veriler şirketlerin artık kişileri tekil olarak hedefleyebilecekleri detayda veri içermekteydi. Hatta durum öyle bir hale geldi ki sosyal medya şirketlerinin elindeki veriyi kullanan şirketler, kişinin kendisinin bile farkında olmadığı ihtiyaçlar konusunda hedeflenebilir hale gelmişti. Şirketler için çok büyük bir başarı olan bu durum, maalesef kişiler için alarm sinyalleri veriyordu. Nitekim bu verileri kişilerin oy eğilimlerini ölçerek, bu eğilimlerini değiştirme amacıyla kullanan Cambridge Analytica şirketinin yaptıkları, şirket içinden bir kişinin itirafları ile ortaya çıktığından durumun vahameti de anlaşıldı.

6.2 Sonuçlar

Bu çalışma Türkiye'deki üst düzey yöneticilerde dijital dönüşümün siber güvenlik ve mahremiyet konularına etkisi konusunda belirli bir farkındalıkları olduğunu, güncel tehdit ve ihlal olaylarını takip ettiklerini ve projelerini yaparken bu konuları da ele aldıklarını gösteriyor. Özellikle finans sektöründeki düzenlemeler sayesinde bu konuların yönetim kurulu seviyesine kadar çıktığını gözlemliyoruz. Diğer sektörlerde hala teknik seviyede takip edilen şirketler olsa da, bir çok firmanın

konuyu icra kurullarında veya genel müdür seviyesinde ele aldıkları görülüyor. Yöneticilerin en endişelendikleri teknolojilerin başında 3. Taraflarla yapılan entegrasyonlar geliyor. Ayrıca, yöneticiler şirket ve kişisel verilerinin çalınmasından yoğun endişe duyuyorlar.

6.3 Öneriler

Yaptığımız bu çalışma ile kişilere, verilerini paylaşma konusunda dikkat etmeleri gereken hususları, şirketlere, dijitalleşirken aldıkları siber güvenlik ve mahremiyet risklerini ve bu riskleri nasıl kontrol altına alabileceklerini, araştırmacılara ise bu alanda yapılabilecek tamamlayıcı yeni araştırmalar konusunda öneriler sunuyoruz. Aşağıda bu öneriler farklı kategoriler altında verilmektedir.

6.3.1 Şirketlere ve Üst Yöneticilere Öneriler. Çalışmadan çıkan sonuçlara bakıldığında, özellikle siber güvenlik ve mahremiyet konularının strateji karar verebilme, liderlik etme ve kurum kültürünü değiştirme etkisine ve yetkisine sahip üst yöneticiler tarafından sahiplenilmesi ve takip edilmesi oldukça önemlidir. Bu konuda şirketlerin üst düzey yöneticilerine önerilerimiz aşağıda sıralanmaktadır:

1. Dijital dönüşüm projelerinizin yeni güvenlik ve mahremiyet riskleri yaratacağını ve bu risklerle ilgili gerekli bütçe, insan kaynağı ve zamanın projeye eklendiğinden emin olun.
2. Siber güvenlik ve mahremiyet konusunun dijital dönüşüm stratejinizin ana unsurlarından biri olduğundan emin olun ve bunu kurumsal kültürünüzün bir parçası haline getirmek için liderlik edin.
3. Sadece teknolojik yatırımlarla bu konuların çözülemeyeceğini farkında olarak insan kaynağının geliştirilmesi ve bu konuların tüm birimler tarafından anlaşılması ve sahiplenilmesi için yatırımlar yapın.
4. 3. Taraflarla entegrasyonlar yaparken gerekli altyapı ve güvenlik önlemlerine sahip olup olmadıklarını sorgulayın, gerekiyorsa kendi ekiplerinizle onları destekleyin. Mevcut yasalar veri sahibi olarak tedarikçilerden kaynaklı sorunlarda dahi şirketinizi sorumlu tutacaklardır.
5. Kendinizin de başka şirketlerin müşterisi olarak verilerinizi onlarla paylaştığınızı unutmayın. Onlardan verilerinizi nasıl korumalarını ve nasıl etik olarak kullanmalarını bekliyorsanız, kendi şirketinizde de bu konuların o hassasiyette ele alındığından emin olun.

6.3.2 Bireylere Öneriler. Çalışmadan çıkan sonuçlara bakıldığında şirketlerin siber güvenlik ve mahremiyet konularında belli bir farkındalık seviyesinde olduğu söylenebilir, şirketlerin de bireylerden oluştuğu düşünülerek, hem bir şirketin müşterisi hem de bir şirketin çalışanı olarak bireylerin de bu konularda yapabilecekleri vardır. Bireylere öneriler aşağıda sıralanmaktadır:

1. Paylaşımlarınızda dikkatli olun ve paylaşımlarınızın kimler tarafından görülebildiği ve nasıl, ne şekilde kullanılabileceği konusunda iki kere düşünün.
2. Kendi verilerinizi paylaştığınız şirketlerin onları nasıl korumalarını ve nasıl etik olarak kullanmalarını bekliyorsanız, siz de bir çalışan olarak kendi şirketinizde bu konuların o hassasiyette ele alındığından emin olun.
3. Tüm cihazlarınıza sadece güvenilir kaynaklardan uygulamalar indirin.
4. İndirdiğiniz uygulamaların cihazınızda ne tür verilere eriştiğini ve fonksiyonu itibariyle çalışması için gerçekten bu verilere erişmesi gerekip gerekmediğini sorgulayın.

6.3.3 Araştırmacılara Öneriler. Çalışma esnasında birçok kaynak ve araştırmadan faydalanıldı. Bu araştırmaları yaparken çalışmayı daha da zenginleştirmek maksatlı eklenebilecek bazı konularda yeterince bilimsel araştırmanın henüz yapılmadığı ve bu çalışmadan sonra bu konulara eğilmek isteyen araştırmacılar olabileceği değerlendirildi. Araştırmacılara öneriler aşağıda sunulmaktadır:

1. Dijital dönüşüm ile siber güvenlik ve mahremiyet arasındaki ilişkiyi ölçecek bir yapı kurarak araştırılması.
2. Dijitalleşme olgunluk skoru yüksek olan kurumlarda gerçekleşen siber ihlal olayları ile dijitalleşme skoru düşük olan şirketlerin yaşadığı siber ihlal olayları arasında karşılaştırma araştırması.
3. Hızlı kod geliştirme baskısının, kodda çıkan güvenlik zafiyetleri ile arasındaki ilişkinin araştırılması.
4. Şirketlerin dijital dönüşüme adapte olma hızı ile saldırganların dijital dönüşüme adapte olma hızı arasındaki ilişkinin araştırılması.

KAYNAKÇA

Ardagna, C. & Corbiaux, S. & Sfakianakis, A. & Douligeris, C. (2021). ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Benaroch, M. (2020). Cybersecurity Risk in IT Outsourcing—Challenges and Emerging Realities. In Information Systems Outsourcing (pp. 313-334). Springer, Cham.

Ebert, C. & Duarte, C. H. C. (2018). Digital Transformation. IEEE Softw., 35(4), 16-21.

ESG Grup, 2020. Modern Aplicaiton Develepment Security https://www.synopsys.com/software-integrity/resources/analyst-reports/modern-application-development.html

Europol, S., & Assessment, O. C. T. (2017). Crime in the Age of Technology. https://www.cepol.europa.eu/sites/default/files/924156-v7-Crime_in_the_age_of_technology_.pdf

Fernandez, E. B. (2004, June). A Methodology for Secure Software Design. In Software Engineering Research and Practice (pp. 130-136).

Fuentes, R., Hunt, L. C., Lopez-Ruiz, H. G., & Manzano, B. (2019). From the "iPhone Effect" to the "Amazon" of Energy. Network Industries Quarterly, 21, 8-11.

GDPR, General Data Protection Regulation 2016/679.: European Union; (2016). http://eur-lex.europa.eu/eli/reg/2016/679/oj

HBR, (2017). Digital Transformation Is Racing Ahead and No Industry Is Immune. https://hbr.org/sponsored/2017/07/digital-transformation-is-racing-ahead-and-no-industry-is-immune-2

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. Computer, 51(8), 56-59.

Kim, R. Y. (2020). The impact of COVID-19 on consumers: Preparing for digital sales. IEEE Engineering Management Review, 48(3), 212-218.

Kroll (2021). 2021 Data Breach Outlook - "Under-attacked" Industries Feel the Heat https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2021

Kurt, Z. E. (2015). Ucuz, Sansürsüz ve Hızlı İnternete Erişim Hakkı. Ankara Barosu Dergisi, 2, 287-293.

KVKK, Kişisel Verilerin Korunması Kanunu 2016/6689.: (2016) https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

Lewis, J. A., & Baker, S. (2013). The economic impact of cybercrime and cyber espionage.

Lindstrom, P., Rosen, M., Pike, S.: DX Security: A Security Model for the DX Platform, pp. 2–13 (2018)

Mosquera, R., Odunowo, M., McNamara, T., Guo, X., & Petrie, R. (2020). The economic effects of Facebook. Experimental Economics, 23(2), 575-602.

Möller, D. P. (2020). Cybersecurity in Digital Transformation: Scope and Applications. Springer.

Newman, D. (2018). Understanding the six pillars of digital transformation beyond tech. Retrieved, 11, 2019.

Quinn, J. B., & Hilmer, F. G. (1994). Strategic outsourcing. MIT Sloan Management Review, 35(4), 43.

Rogers, D. (2016). The digital transformation playbook. Columbia University Press.

RSM (2019). Catch-22: Digital Transformation and Its Impact on Cybersecurity https://www.rsm.global/catch-22-digital-transformation-and-its-impact-cybersecurity

Statista, Global Digital Population as of January 2021, (2021). https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

Statista, Number of internet users worldwide from 2005 to 2019, (2019). https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

Statista, Percentage of organizations victimized by ransomware attacks worldwide from 2018 to 2021, (2021). https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

Stroukal, D. (2016, November). Bitcoin and other cryptocurrency as an instrument of crime in cyberspace. In Proceedings of Business and Management Conferences (No. 4407036). International Institute of Social and Economic Sciences.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. Computers & security, 23(5), 371-376.

Vox.com, 2017. How Apple's iPhone changed the world: 10 years in 10 charts https://www.vox.com/2017/6/26/15821652/iphone-apple-10-year-anniversary-launch-mobile-stats-smart-phone-steve-jobs

Yüksel, M. (2003). Mahremiyet Hakkı ve Sosyo-Tarihsl Gelişimi. Ankara Üniversitesi SBF Dergisi, 58(01).

Zakaria, W. Z. A., Abdollah, M. F., Mohd, O., & Ariffin, A. F. M. (2017). The rise of ransomware. In Proceedings of the 2017 International Conference on Software and e-Business (pp. 66-70).

EKLER