DOI: iibfdkastamonu.395004
Geliş Tarihi/Submitted: 14.02.2018
Kabul Tarihi/Accepted: 23.10.2018

Kastamonu Üniversitesi
İktisadi ve İdari Bilimler Fakültesi Dergisi
2018, 20 (4)

Araştırma Makalesi/Research Article

Teknolojik Risk Yönetiminde İnternet Bankacılığının Fırsat ve Tehditleri

Bülent GÜNCELER[1]
Murat KESEBİR[2]

Öz: Modern çağ teknolojik dönüşüm ile birlikte kendisini iyiden iyiye hissettirmeye başlamıştır. Böyle bir gelişim ve dönüşümün oluştuğu ortamda her sektör gibi bankacılık sektörü de etkilenmektedir. Sektörde gerçekleşen çoğu işlemin gelişen teknoloji ile birlikte yapılması birtakım tehditleri de oluşturmaktadır. Ancak bunların yanında işlem kolaylığı, hızlılık ve verimlilik açısından da birçok fırsatları içinde barındıran teknolojik dünya, her anlamda dikkatle incelenmesi gereken bir konu olmuştur. Çalışmamızda risk kavramları içerisinde yer alan operasyonel risklerden birini oluşturan teknolojik riski inceleyecek olup, bu riskin nasıl yönetilmesi gerektiği ile ilgili düşüncelere yer verilecektir. Çeşitli örnek olaylarla da detaylandırılacak bu risk türü, internet bankacılığı açısından da ele alınarak bu riskin önemine değinilecektir.
***Anahtar sözcükler*:** Bankacılık, İnternet, Teknolojik Risk, Tehditler, Fırsatlar
Jel Kodu: G21, G32, O30

Opportunities and Threats of Internet Banking in Technological Risk Management

Abstract: The modern era has begun to feel itself well with the technological transformation. In such a development and transformation environment, the banking sector as well as every sector is affected. Most of the processes in the sector are accompanied by developing technology, which also creates some threats. However, the technological world, which has many opportunities in terms of ease of operation, speed and efficiency, has been a subject that has to be carefully examined in every sense. We will examine the technological risk that is one of the operational risks included in the risk concepts in our work and will give some thought about how this risk should be managed. This risk type, which will be detailed with various case studies, will be discussed in terms of internet banking, and the importance of this risk will be mentioned.
Keywords: Banking, Internet, Technological Risk, Threats, Opportunities
Jel Kodu: G21, G32, O30

[1] *Dr. Öğretim Üyesi, İstanbul Okan Üniversitesi, İşletme Bölümü, bulent.gunceler@okan.edu.tr*
[2] *Dr. Öğretim Üyesi, Yozgat Bozok Üniversitesi, Bankacılık ve Finans Bölümü, murat.kesebir@bozok.edu.tr*

Atıf Künyesi: *Günceler, B. ve Kesebir M. (2018). Teknolojik Risk Yönetiminde İnternet Bankacılığının Fırsat ve Tehditleri, Kastamonu Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 20/4, 158-171.*
Cititaion: *Günceler, B. ve Kesebir M. (2018). Teknolojik Risk Yönetiminde İnternet Bankacılığının Fırsat ve Tehditleri, Journal of Kastamonu University Faculty of Economics and Administrative Sciences, 20/4, 158-171.*

Extended Abstract

Introduction

Many work done with the development of technology is much easier. These works, which are made faster and easier than before, can cause some problems even if they have contributed to our lives. For this reason, the technology considered as an opportunity can be threatened by people at times. Because, as well as using technology well, there are people who misuse and deceive people. In our study, the concept of risk was explained based on these threats and the operational and technological risk which is one of the types of risk is emphasized. Operational risk is the risk that occurs due to operational operations and includes the elements that need attention. Technological risk is an important risk which has emerged with the development of the latest technology. It is necessary to act by taking these risks into consideration. In our study, these risks were explained and supported by various examples via internet banking.

Method

The method of our study is planned to be given with detailed information about the subject and supported with experienced examples. The errors described here are how big losses have occurred. It is perhaps necessary to carefully examine every detail even if it is considered as a small detail. six cases have been examined, and the definitions described in literature have been examined in real life. The examination of the cases shows what will happen to people in terms of opportunity and threat. In our study, information was given about the use of mobile banking and these cases were supported with case examples.

Findings (Results)

When the results obtained in our study are examined in cases; in the first case, there are frauds with mobile phones. Due to the problem caused by the GSM operator, there are customers who have emptied the account using internet banking. The bank also establishes a new system when it comes to the transaction question that is made with a copy of the Sim Card. Thus, such errors can be prevented. In the second case, a bank wants to move to a brand new system. But this system must be adapted to the employees at first. Since the employees cannot adapt, there is a big problem and problems. Then the customers have changed their banks. This is a good planning and training of the personnel. In the third case, the customer will receive a credit application for the counterfeit mail. But the purpose here is to capture the customer's personal information. With this information, the internet banking password is changed and the accounts are emptied. The point to note here is that the customer should not share his personal information in this way. In the fourth case, the precautions against the pirates that leaked to the system through the virus were emphasized. Care must be taken when installing the system. In the fifth case, it is necessary to take adequate measures in internet transactions. In the sixth case, they have stolen the information of the customers by copying the website. Here the bank will take adequate measures and be careful against such cases.

Conculusion and Discussion

In our study, technological risk, one of the operational risks, was emphasized. Technological risk is explained and the risks encountered are detailed. It is important that the institutions take adequate measures for the safety of the customers. Not only the bank, but also the customer should be careful, do not share his / her personal information and be more careful when trading on the Internet. Both customers and banks need to take measures against their threats while using technology. Banks should be more careful about internet banking and should be sensitive to loss of customers. New defense mechanisms should be created against new technology and threats. Special protection against viruses should also be created and warn customers about messages, verbal and mail fraud. While technology has opportunities, threats will always be. Therefore, it is always necessary to perform operations carefully and cautiously.

Gelişen dünya birçok yenilikleri de hayatımıza katmıştır. Teknoloji ile tanışmamızla birlikte, bilgisayar ve cep telefonu hayatımızın her alanına giren ve günlük yaşantımızı kolaylaştıran cihazlar olmuşlardır. Düşünülmedir ki, her fırsatın doğuşu aynı anda tehditleri de oluşturabilir. Çünkü böyle bir ortamın kötüye kullanımı ile ilgili oluşumlarda maalesef ortaya çıkmıştır. Teknolojinin bu fırsat ve tehditleriyle dolu olduğu düşünülerek, her alanda olduğu gibi bankacılık anlamında da artık birçok insan internet bankacılığını kullanmaktadır. Müşterilerine kolaylık ve hızı sunan gelişmiş uygulamalarla, birçok işlemlerini (para çekme, yatırma, havale, elektronik fon transferi, kredi kullanmak, pos cihazı talep vb.) bu mecradan gerçekleştirmektedir.

Bankacılık işlemlerinde en önemli unsur tabi ki güvenlik olmaktadır. Güvenlik açığı olduğu zaman müşterinin kaybedilmesi ve memnuniyetsizliği gibi kötü sonuçlar ortaya çıkar. Burada değinilmesi gereken konu ise risk kavramıdır. Risk kavramının alt başlıklarından birisi olan operasyonel risk de işlemlerin gerçekleştirilmesi esnasında meydana gelen bir risk olup önemle dikkat edilmesi gereken ve bankanın itibarı açısından önemli bir risk olmaktadır. Ayrıca risk verileri belirlenip bu risklerin neler olacağının saptanması gerekmektedir. Bankanın bunu iyi analiz ederek karşı karşıya olduğu riskin ne olduğuna dair önlemlerini almalıdır. Bunu sağlamak için, bankanın risklere karşı iyi bir veri tabanı oluşturması ve bu veri tabanının amaca uygun olarak yönetimini gerçekleştirmesidir.

Çalışmamızın temel amacı, teknolojinin gelişmesi ile ortaya çıkan yenidünya içerisinde bulunan internet bankacılığının karşı karşıya kaldığı tehditler ve fırsatlardır. Hayatımıza kattıkları açısından fırsatları ile ilgili akıllarda birçok olumlu düşünceler bulunmakla birlikte, esas üzerinde durulması gereken tehditler yani oluşturmuş olduğu risklerdir. Bunu inceleyebilmek için operasyonel risk kavramının içerisinde bulunan teknolojik risk detaylandırılacak olup, ayrıca çeşitli örnek vakalar ile karşılaşılan riskler ortaya konulmaktadır. Maruz kalınan bu durumun sebepleri ve bankanın bu duruma karşı almış olduğu önlemler açıklanarak, karşılaşılan risklerin ve tehditlerin nasıl yönetilmesi gerektiği incelenmektedir.

1. RİSK KAVRAMI

Risk kavramı denildiği zaman, bankacılık sektörü açısından değişime konu olan şey para olduğu için üzerinde durulması gereken önemli bir konu olmaktadır. Bu sebeple öncelikle risk kavramını açıklamamız gerekmektedir. Risk, Türk Dil Kurumu'na göre; Fransızca "risque" olarak dilimize girmiş ve "zarara uğrama tehlikesi, riziko" olarak ifade edilmektedir. Portekizce "cesaret" anlamına gelen risk, İngilizceye on yedinci yüzyıl içinde girdiği düşünülmektedir ve "kayalıklara doğru gitmek veya tehlikeye girmek" anlamındaki denizcilik teriminden meydana gelmektedir. Geleneksel kültürleri olanlar risk kavramını kullanmaz iken, sonradan ortaya çıkan ve modern toplumun ürünü bir kavram olmuştur (Sayım ve Er, 2009:7).

Risk yukarıdaki tanıma istinaden zarara uğramayı ifade etmektedir. Fakat risk kavramı ile olasılık da oluşmaktadır. Çünkü ilerideki beklentilere yönelik olarak gerçekleşip gerçekleşmeme ihtimaline karşı oluşabilecek durumlar için de risk kavramı kullanılmaktadır. Dolayısıyla risk kavramına birde finansal açıdan bakıldığında, "kurumun stratejik, mali ve operasyonel hedeflerini gerçekleştirmesini engelleyecek, her türlü olayın gerçekleşme olasılığı"

olarak ifade edilmektedir (Günceler, 2015). Bu tanımdan da anlaşılacağı üzere, hedeflere ulaşma esnasında beklenmeyen zararların meydana gelme olasılığı risk kavramının temelini oluşturmaktadır.

Bir riskin tanımlanabilmesi için öncelikle kurumun, amaçlarını ve hedeflerini belirlemiş olmalıdır. Amaç ve hedefleri belli olduğu zaman, ona ulaşılmasını engelleyecek riskler tanımlanır, değerlendirilir ve bu risklere karşı hangi önlemlerin alınması gerektiği tespit edilir. Ayrıca riskler sistematik ve sistematik olmayan riskler olarak ikiye ayrılmaktadır. Sistematik risk, ekonomide bulunan bütün kurumları etkileyen ekonomik, politik olaylardan kaynaklı olarak ortaya çıkan riskler olurken; sistematik olmayan risk ise, belirli bir kuruma ya da şirkete özgü olan ve sadece bu kuruluşu etkileyen risk olmaktadır (Karadeniz, Kandır, İskenderoğlu, 2013:1057). Bankalarda gerek sistematik olarak (ekonomik krizlerden kaynaklı), gerekse sistematik olmayan (içsel anlamda oluşan) risklerin meydana gelebildiği yapılar olmaktadır. Dolayısıyla, bütün oluşan bu risklere karşı etkin bir risk yönetimi de gerçekleştirilmesi gerekmektedir.

2. BANKACILIKTA RİSK YÖNETİMİ VE RİSK ÇEŞİTLERİ

Bankalar finansal sistem içerisinde yer alan en önemli yapılardan birisidir. Bu yapıda fon talep edenler ile fon arz edenler arasında bir anlamda aracı olarak finansal aracılık yapmaktadırlar. Bu sebeple, böyle bir sistem içerisinde yer alan bankalar açısından, risk kavramı denildiğinde ilk başta sektörel anlamında oluşan risk ve ardından banka bazlı olarak karşılaşılması muhtemel riskler bulunmaktadır. Dolayısıyla, bu şekilde oluşan risklere karşı önlemlerin geliştirilmesi ile risk yönetimi kavramı ortaya çıkmaktadır.

Risk yönetimi, risklerin tanımlanması, değerlendirilmesi ve muhtemel etkilerinin makul bir seviyede tutulabilmesi için gerekli kontrollerin yapılması, gözden geçirilmesi ve raporlanmasını sağlayan yönetim olmaktadır (İç Denetçilerin Çalışma Usul ve Esasları Hakkında Yönetmelik, Madde:4). Buradaki tanımda ifade edilen durum, kurumun hedefine ulaşabilmesi için, her seviyede sistematik olarak risklerin tespit edilmesi, değerlendirilmesi, risklerin etkilerini azaltıcı önlemlerin alınması ve bu sürecin etkin bir şekilde yürümesini sağlayacak şekilde izlenmesidir (Maliye Bakanlığı, İç Kontrol Broşürleri). Bankaların risk yönetimi güçlü olduğu zaman, etkin bir risk yönetimini oturtmuş yapı olarak sermayesini verimli olarak yönetmeyi amaçlar. Zayıf bir risk yönetimi olduğunda ise, muhtemel durumlara karşı önlemlerini alamadıkları için zararları da yüksek olacaktır. Ülkemizde yaşanan mali krizlerden dolayı birçok banka döviz kuru, likidite darlığı ve aktif-pasif vadesi uyuşmazlığı risklerinden dolayı büyük kayıplara uğramışlardır. Bu durumdan ortaya çıkan, zayıf risk yönetimi olan bankalar bu tür krizlerin olasılığını dikkate almamış ve olası kayıpların büyüklüğünü değerlendirememişledir (Şahin, 2008:7).

Yukarıda ifade edildiği üzere, bankaların etkin bir risk yönetimi sağlamaları ile birlikte muhtemel zararlara karşı kendi önlemlerini almaları hem müşterileri açısından hem de iç müşteri açısından sağlam bir duruş sergilemek odaklı olarak önem arz etmektedir. Bu açıdan risk yönetimi gibi riskin çeşitleri de bir diğer önemli konu olmaktadır. Risk çeşitlerine baktığımızda; kredi riski, kur riski, likidite riski, piyasa riski, stratejik risk, ülke riski, yasal risk,

hazine riski, itibar riski vb. gibi birçok risk çeşidi karşımıza çıkmaktadır. Bankacılık açısından burada en dikkat çeken üç risk çeşidi vardır. Bunlar: kredi riski, piyasa riski ve operasyonel risktir. Kredi riski ve piyasa riskine kısaca değinilecek olup; operasyonel risk ayrı bir başlıkta ele alınacaktır.

Kredi riski en yalın ifade ile "bir bankanın kredi müşterisinin ya da kendisiyle anlaşmaya taraf olanın anlaşma koşullarına uygun biçimde yükümlülüklerini karşılayamama olasılığıdır". Kredi riski yönetiminin amacı, bankanın kalabileceği riskleri yöneterek, risk ayarlı getirisini maksimize etmektir. Bankalar bütün kredi risklerini yönetmek durumundadır. Çünkü kredi riski diğer birçok riski de içerdiğinden dolayı dikkate alınmalıdır (Türkiye Bankalar Birliği).

Piyasa riski ise; içerisinde faiz oranı riski, döviz kuru riski ve likidite riskinden meydana gelmektedir. Piyasanın şartları gereği, ekonomik yapıda meydana gelen dalgalanma her üç risk türünü de etkilediği için birbirleriyle ilişki halinde olmaktadırlar. Faiz oranlarında olan yukarı ve aşağı yönlü hareket, aynı anda döviz kurlarından oluşan bozulma ve likidite sıkıntısı gibi birçok faktör toplandığı zaman, piyasa riskini oluşturmaktadır. Her üç tanımı da detaylandırdığımızda; faiz oranı riski, "bankanın, faiz oranlarındaki değişimlerden etkilenen alım satım hesaplarında yer alan finansal araçlara ilişkin pozisyon durumuna bağlı olarak genel piyasa riski ile spesifik riskten kaynaklı maruz kalabileceği zarar olasılığını" ifade etmektedir (BDDK). Kur riski, döviz kurlarında oluşan aşağı veya yukarı yönlü hareketlerin bankaların mali durumu üzerinde meydana getirebileceği olumsuz etki döviz kuru riski olarak tanımlanmaktadır (Aksu, 2016:151). Likidite riski ise, bir bankanın bugün ve gelecekte yükümlülüklerini yerine getirememekten dolayı gelirinde ve sermaye yapısında oluşabilecek muhtemel kayıpları ifade etmektedir (Aloğlu, 2005:22).

3. OPERASYONEL RİSK VE TEKNOLOJİK RİSK

Her iki kavram da birbiri ile iç içe geçmiş olsalar da, ayrı ayrı tanımlanmalı ve üzerinde durulmalıdır. Operasyonel riskin içerisinde yer alan teknolojik risk bir bankanın en çok dikkat etmesi gereken unsurdur. Günümüzde çoğu işlemlerin internet üzerinden gerçekleştirildiği düşünüldüğünde, hatalar, yanlışlar, suiistimaller, ihmaller gibi pek çok şeyler meydana gelebilmektedir. Dolayısıyla, bankacılığın en çok değer vermesi gereken bu risk unsuru, hem müşterilerin güveni açısından hem de kurum kalitesi ve imajı açısından en fazla önem gösterilmesi gereken başlık olmaktadır.

Operasyonel risk, yetersiz ve başarısız iç süreçler, insanlar ve sistemlerden ya da harici olaylardan kaynaklanan ve içerisinden yasal riski de kapsayan zarar etme olasılığıdır (Günceler, 2015). Bir başka ifade ile bankanın bilgi ve raporlama sistemlerinin, içsel risk izleme kurallarının bozulması nedeniyle maruz kalınan risktir (Anderson, 2001). Basel 2'de ise operasyonel riskin tanımı; yetersiz ve başarısız içsel süreçlerden, personel ve sistemlerden ya da dışsal olaylardan kaynaklanan, doğrudan veya dolaylı zarar riskidir (Basel Committee on Banking Supervision, 2001:2). Operasyonel risk, BDDK'nın ilgili yönetmeliğinde ise şu şekilde tanımlanmıştır: "banka içi kontrollerdeki aksamalar sonucu hata ve usulsüzlüklerin gözden kaçmasından, banka yönetimi ve personeli tarafından zaman ve koşullara uygun hareket edilmemesinden, banka yönetimindeki hatalardan, bilgi teknolojisi sistemlerindeki hata ve

aksamalar ile deprem, yangın, sel gibi felaketlerden kaynaklanabilecek kayıplara ya da zarar uğrama ihtimalidir"(Varlı, 2006:14).

Yukarıda da değinildiği gibi, operasyonel risk kavramı içerisinde teknolojik risk de bulunmaktadır. Teknolojik risk ise bilgi sistemleri riski olarak ifade edilmektedir. Bilgi sistemleri riski, "iş süreçlerini olumsuz yönde etkileyecek şekilde otomasyon sisteminin, ağ veya diğer kritik bilgi teknolojileri kaynaklarının kaybedilmesi potansiyelidir"(Bağcı, 2010). Bu tanımda da görüldüğü gibi günümüzde bankacılık ve finans sektöründe teknolojik risk kavramının önlenebilmesi için bilgi teknolojilerine çok önem verilmiştir. Ayrıca, iş hedeflerine ulaşıp ulaşmama konusunda bilgi teknolojileri olmadan işlemleri devam ettirebilmeleri imkansız hale gelmiştir (Özbilgin, 2011:79).

3.1. İnternet Bankacılığı ve Fırsatlar

Teknolojinin gelişmesi ile birlikte uzun yıllardır uygulamada olan birçok işlemin internet ortamına taşındığı bilinmektedir. Son dönemde devletin ve özel sektörün bütün kurumlarının internet ortamında olduğu görünmektedir. Teknolojiye en fazla yatırım yapan sektörlerden birisi olan bankacılık sektörü de bu kurumların arasında en önemli yeri oluşturmaktadır. Bankacılık sektöründe gerçekleştirilen işlemler açısından ve müşterilerine hizmet bağlamında, elektronik bankacılık üzerine yoğun uğraş ve çaba ile yatırımlar yapılmıştır.

Dünyadaki internet bankacılığı fikri Amerika ve Avrupa'da 1970'li yılların sonları ile 1980'li yılların başlarında ortaya çıkmıştır. Özellikle "ev/ofis bankacılığı" kavramı ile internet bankacılığı hizmeti sunmak isteyen bankalar, pazardan büyük bir payı kapmayı hedeflemişlerdir. Ülkemizde ise internet bankacılığının geçmişi Amerika ve Avrupa'dan sonra, 1997 yılındadır. İlk olarak Türkiye İş Bankası ve Garanti Bankası müşterilerine sunulmaya başlanan bu hizmet, günümüzde Türkiye Bankalar Birliği üyesi toplam 45 yerli ve yabancı banka ile 26 finansal kurum sunmaktadır (Eroğlu ve Yücel, 2012:5). Artık sadece belirli bir işlem yapılması için değil ev ya da ofis ortamından bankacılığa dair bütün işlemlerin tek bir tık ile hızlıca gerçekleştirilmektedir. Dolayısıyla, kolaylığı açısından ve hızlılığı açısından tercih edilebilir bir hizmet olmaktadır. Aşağıdaki tabloda 2008 yılından sonra elektronik bankacılık alanında yaşanan önemli gelişmeler bulunmaktadır.

Tablo 1. Elektronik Bankacılıkta Yaşanan Önemli Gelişmeler: 2009-2015

	Gelişmeler
2009	"Türkiye'nin bütün ATM'leri birleşti" sloganı ile Türkiye genelinde ulusal ATM ortaklığı başladı. Finansbank, banka kartı ile Taksitli alışveriş uygulamasını başlattı. Halkbank, Avrupa'nın ilk ön ödemeli EMV temassız kartını Visa logosuyla çıkardı.
2010	Türkiye ve Avrupa'nın ilk "temassız banka ve kredi kartını" bünyesinde toplayan Simply One kartı Finansbank tarafından kullanıma sunuldu. Telefon bağımsız ilk NFC uygulaması, Avea ile Garanti işbirliğiyle gerçekleştirildi.
2011	Garanti Bankası, NFC teknolojisine sahip ilk ön ödemeli kartını kullanıma sundu. Akbank Avrupa'nın ilk micro SD tabanlı NFC uygulamasını hayata geçirdi.

2012	Tüm bankaların temassız özelliği taşıyan kartlarının bir araya geldiği ve toplu taşımada devrim niteliği taşıyan Konya ulaşım projesi Kuveyt Türk Katılım Bankası ile Türk Ekonomi Bankası'nın işbirliğinde başlatıldı. Vakıfbank'ın ana banka olduğu projenin ilk işlemi de projeye kısa süre içinde katılan Ziraat Bankası kartı ile gerçekleşti.
2013	Citibank, Türkiye'de ilk satın alma kartı "Purchasing Card"ı pazara sundu. 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları hakkında kanun yayınlandı. Böylece e-para işlemi yasal güvenceye kavuştu. Türkiye ve Avrupa'da bir ilke imza atan Şekerbank, esnaf ve KOBİ'ler için hem şirket hem banka kartı özelliği taşıyan "Üreten Kart"ı kullanıma sundu. Denizbank dünyanın ilk POS bütünleşik yazarkasa uygulamasını kullanıma sundu.
2014	İş Bankası Türkiye'nin ilk QR(Quick Response) kod kullanılan ödeme sistemi Parakod'u hizmete sundu.
2015	Çok sayıda şirket elektronik para ya da ödeme kuruluşu lisansı almak üzere BDDK'ya başvurularını ileterek faaliyet izinlerini almaya başladı.

Kaynak: Gündoğdu, Aysel (2016). Küresel Kriz Sonrası Gelişmeler Işığında Bankacılığın Temelleri s.329.

Yukarıda görüldüğü gibi birçok alanda yeniliğe imza atan bankacılık sektörü, elektronik bankacılıkta sürekli kendisini gelişme ve teknolojik yenilikleri yakalama anlamında çalışmalar yapmıştır. Gerek ATM olarak, gerek de kartlar anlamında teknoloji ile birlikte müşterilere yepyeni kolaylıklar gelmiştir. Konuya elektronik bankacılık olarak incelendikten sonra, birde 2007 tarihinden sonraki süreçte internet bankacılığı açısından incelenmek istendiği zaman, aşağıdaki tabloda bulunan verilerin yıllar geçtikçe nasıl değiştiğini ve internet bankacılığına olan talebin artışını göstermektedir.

Tablo 2. Türkiye'de İnternet ve Mobil Bankacılık Uygulamalarına İlişkin Veriler (2007-2016)

	2007/ Aralık		2008 / Aralık		2010/ Aralık	
	İnt. Bnk.	Mbl. Bnk.	İnt. Bnk.	Mbl. Bnk.	İnt. Bnk.	Mbl. Bnk.
Aktif Müşteri sayısı (Bin Adet)	4.274	-	5.169	-	6.693	-
PARA TRANSFERLERİ						
İşlem Adedi (Bin)	29.335	-	29.718	-	39.868	-
İşlem Hacmi (000 TL)	112.693	-	115.218	-	181.110	-
ÖDEMELER						
İşlem Adedi (Bin)	15.393	-	20.578	-	26.186	-
İşlem Hacmi (000 TL)	3.400	-	4.626	-	8.535	-
	2012/ Aralık		2014/ Aralık		2016 / Mart	
	İnt. Bnk.	Mbl. Bnk.	İnt. Bnk.	Mbl. Bnk.	İnt. Bnk.	Mbl. Bnk.
Aktif Müşteri sayısı (Bin Adet)	10.551	1.375	14.315	6.711	18.511	13.961
PARA TRANSFERLERİ						
İşlem Adedi (Bin)	54.914	3.503	63.281	17.528	68.275	42.364
İşlem Hacmi (000 TL)	332.320	6.464	488.705	42.851	570.812	111.961
ÖDEMELER						
İşlem Adedi (Bin)	36.708	2.783	48.748	15.361	48.699	36.084
İşlem Hacmi (000 TL)	19.970	217	30.390	1.933	38.110	5.548

Kaynak: Gündoğdu, Aysel (2016). Küresel Kriz Sonrası Gelişmeler Işığında Bankacılığın Temelleri s.331.

Yukarıdaki tabloda dikkat çeken en önemli unsur aktif müşteri sayısındaki artış olmaktadır. 2007 yılında 4 milyon civarında iken, 2016 yılına gelindiği zaman 18 milyon seviyelerine ulaşmıştır. Ayrıca 2012 yılından itibaren bunun içerisinde mobil bankacılık da dâhil olarak hızlı bir şekilde 13 milyon seviyelerine ulaşmıştır. Verilere bakıldığı zaman internet ve mobil bankacılığın kullanımındaki artışın son yıllarda ne kadar fazlalaştığı görülmektedir. İşlem adedi ve işlem hacmi bazlı artış da dikkate değer bir unsur olmaktadır.

İnternet bankacılığını bankalar ve müşteriler için sunduğu fırsatlara kısaca değinilecek olursa; bankalar açısından: Potansiyel müşterilere daha düşük bir maliyetle birçok ürünü sunabilmek, yer ve zaman olarak düşünülmeden her daim ulaşılabilir olmak, şubedeki işlem maliyetlerinin azaltılması ve bunun internet bankacılığını kullanan müşteri sayısı ile artış göstermesidir. Müşteriler açısından fırsatları ise; kullanılan sistemin rahat ve hızlı olması ile kolay ulaşılabilir olması, zaman ve maliyet tasarrufu sağlaması böylece bazı durumlar dışında müşterinin bankaya gidip işlem yapmasına ihtiyaç duyulmamasıdır (Uzundağ, 2013:45-46). Her iki taraf açısından ortak nokta ise maliyet anlamında olup, gerek şube içindeki masraflar gerek de müşterinin şubeye gelebilmesi için katlandığı zahmetler onları bu ortak noktada birleştirmektedir.

3.2. Operasyonel Risk Örnekleri ve Tehditler

Bankaların yoğun teknoloji odaklı olmaları onları operasyonel risk ile karşı karşıya bırakmaktadır. Bu sebeple bu riske karşı gereken önlemleri almaları onların itibarlarını korumaları açısından önem arz eder. Bu bölümde, operasyonel anlamda bankaların karşılaştıkları risklerden birkaç tanesine yer verilerek, bu tehditlere karşı nelerin yapıldığı ve nasıl başa çıkıldığı anlamında örnekler verilecektir. İnternetin olduğu her mecrada böyle durumlar olabilirken, içerisinde paranın geçtiği ve parasal işlemlerle dolu olan bankadaki potansiyel risk de incelenmiş olacaktır.

Aşağıda yer alan vakalarda banka isimleri ve çalışan isimleri değiştirilmiş olup teknolojik risk ile ilgili gerçek konulara yer verilmiştir.

Vaka 1. İnternet Bankacılığı (Cep Telefonu Problemi)

Güzel Bank 320 şubesi ile Türkiye'de geniş şube ağına sahip bankalar arasındadır. Güzel Bank yönetimi teknolojiye de yoğun yatırım yapmakta ve şubesiz bankacılık alanında da müşterilerine hizmet vermektedir. Güzel Bank yöneticileri internet bankacılığı güvenliği ile ilgili olarak sistemlerine ve güvenlik alanında yatırımlarına çok güvenmektedir. Yaptığı Basın açıklamalarında Güzel Bank Bireysel Bankacılıktan Sorumlu Genel Müdür Yardımcısı Hamdi Tek 1 Ocak 2010 tarihi itibariyle bireysel internet bankacılığına giriş için SMS'le gelen "tek kullanımlık şifre" kullanımının zorunlu hale geldiğini hatırlatmıştır. Kendilerinin de son teknolojiyi kullandıklarını ve bankacılık sektöründe "tek kullanımlık şifre" uygulaması sayesinde sanal banka dolandırıcılığının yüzde 70 oranında azaldığını, bu uygulamanın internet bankacılığında dolandırıcılık olaylarına büyük ölçüde çare olduğunu belirtmişlerdir. Tek'in bu basın açıklamasının ardından 1 ay geçmemiştir. Banka üst düzey yöneticileri Güven Bank merkez şubesi müdürü Cansu Hanım ve bölge müdürü Hüseyin beyden gelen mail neticesinde alarm durumuna geçmişlerdir. Gelen mail 'de merkez şubenin en iyi müşterilerinden olan Haydar Bahtiyar'ın hesaplarının kendi bilgisi dışında boşaltıldığı bilgisi yer almaktadır. Bahtiyar, internet bankacılığı güvenliği ve bilişim konusunda çok bilgili bir müşteridir. Bankadan gelen e-postaya da bankanın gerçek sitesiymiş görünümü verilen sahte siteler vasıtasıyla, şifre ve parolaları ele geçirme yöntemiyle kullanıcıların dolandırılma gibi yöntemlerini bildiği için, ücretli olmasına rağmen tek kullanımlık şifre ve sonrasında ise SMS şifre uygulamasını ilk kullanan müşteriler arasında olmuştur.

Yapılan ilk incelemede olağan dışı bir işlem yoktur. Zira işlem SMS şifre ile onaylanmıştır. Ancak Haydar Bahtiyar böyle bir SMS doğrulamanın kendi telefonuna gelmediğini belirtmektedir. GSM operatörleri ile yapılan görüşmeler neticesinde Bahtiyar'ın telefon numarası için yeni bir SIM kart çıkartıldığı bilgisi alınmıştır. Güzel Bank'ın ilgili ekipleri kısa bir araştırma yapar. Daha önce fark edilmemiş bir yöntemin uygulanmakta olduğunu fark etmişlerdir. Mağdurun kimliğinin detayı ya da fotokopisinin daha önce Bahtiyar'ın firmasında çalışan finans elemanı tarafından temin edildiği; dolandırıcının, bu şekilde elde ettiği kimlik bilgileri ya da fotokopisiyle GSM operatörüne başvurarak, kimlik bilgilerini ve çıkartılan SIM karta SMS'le gelecek tek kullanımlık şifreyi kullanıp, internet bankacılığından hesabı boşalttığını tespit etmişlerdir.

Teknolojiye yoğun yatırım yapmasına rağmen bu şekilde yapılabilecek bir saldırıyı göz ardı eden Güzel Bank yönetimi kısa süre içinde Fraud Monitoring (suiistimalin analiz edilebilmesi için işlemlerin kontrolünü sağlayan bir sistem) sistemini kurarlar. Bu sistem sayesinde, GSM operatörleri tarafından kart kopyalanmalar takip edilebilmekte ve kötü niyetli kullanımlar engellenebilmeye başlanmıştır.

Vaka 2. Yeni Sistem Uygulanma Problemi

Sağlam bank yöneticileri yıllardır kullandıkları bankacılık sistemini değiştirmeye karar vermiştir. Alınacak yeni sistem hem şubelerde hızlanmaya neden olacak, hem de yeni alınan CRM sistemi ile entegre çalışabilecek bir bankacılık sistemidir. Yöneticiler, bu işlemin 2 ay gibi kısa bir zaman içerisinde tamamlanmasını istemişledir. Sağlam bankın IT yöneticileri böyle ciddi bir çalışmanın 2 ay gibi bir sürede gerçekleştirmesinin mümkün olmayacağı, iyi bir iş planlaması ve detaylı bir aksiyon planının alınması gerektiğini yönetime gerek e-posta gerekse yapılan toplantılar ile belirtmişlerdir. Zira bu geçiş esnasında müşteri kaybı olması ve entegrasyon esnasında müşterinin hizmet alamama gibi bir durumla karşılaşmaması gerekmektedir. Bu sebeple, CRM programı ile entegrasyon ise ayrı bir faz olarak devreye alınması düşüncesi vardır.

Bankanın IK yöneticileri ise yeni sistemin entegrasyonunun belli bir eğitim programı gerektireceğini aktarmıştır. Yönetim ise sistemi tanıtacak firmanın kendilerine demo yaptıklarını, averaj seviyede bilgisayar bilgisi olan her personelin programı rahatlıkla kullanabileceğini iddia etmişlerdir. IT ekibinin olağan üstü çalışmaları neticesinde 2,5 ay gibi bir süre içinde yeni bankacılık sisteminin aktarılacağı gün olarak 10 Mart Pazar günü gece yarısı olarak belirlenmiştir. Ancak IT ekibi halen tedirgindir. Zira geçiş esnasında olabilecek bir aksaklık işlemin uzamasına sebep olabilir. IT Müdürü Mert Bey bu plansız ve acele çalışmadan memnun değildir.

Pazartesi günü olduğunda işlem halen bitmemiştir. Müşteriler 4 gün boyunca şubelerde uzun kuyruklar oluşturmuş, müşteri şikâyetlerinden çağrı merkezi kilitlenmiştir. Eğitim alan çok az sayıda personel dışında kimse sisteme adapte olamamıştır. 2 ay sürecinde Sağlam bankın birçok müşterisi banka tercihini değiştirmiş ve 12.000 müşteri kartlarını iptal ettirmiştir.

Vaka 3. İnternet Bankacılığı (Gelen Mail Problemi)

Banka tarafından gönderilen maili açan kurban müşteri, mailde yer alan cazip kampanya bilgilerini incelemeye başlamıştır. Mailde çok avantajlı faiz oranı ve müşteriye özel tutarda kredi bilgileri yer almaktadır. Bu krediyi kullanmak isteyen müşteri, maildeki linke tıklayarak başvuru yapmaya başlar. Gelen başvuru linkinde istenen tüm bilgileri tuşlar. (TC kimlik, anne adı, baba adı, cep telefon numarası, anne kızlık soyadı, adres bilgileri vs.) Sonrasında ise "başvurunuz alınmıştır, size en kısa süre içerisinde yanıt verilecektir" bilgisini alır ve güncel yaşamına devam eder. Bu noktadan sonra dolandırıcı şahıslar çalışmaya başlarlar. Müşterinin vermiş olduğu bilgiler üzerinden müşterinin hesabı olduğu bankaları ararlar. Bu bankalardan internet bankacılığı şifrelerini alınan özlük bilgileri ile birlikte değiştirirler. Bu bilgiler ile internet şubelerine girerek hesapları boşaltırlar.

Bu noktada müşterilerin kontrol noktası ise, hiçbir şekilde kendisine gelen maillerde özlük bilgilerini paylaşmamasıdır. Bu tip bilgi paylaşımları bankalar tarafından yapılmamaktadır. Bu tipte gelen maillerin form kısımları ve tıklanan linkler kontrol edildiğinde, banka ile ilişiği olmadığı anlaşılabilmektedir.

Vaka 4. Güvenliğin Önemli Bir Şekilde İhlali (Sistem Virüsü)

Ankara'da bir bankanın sistemine sokulan virüs banka müşterilerinin hesaplarını, müşteri portföylerini, iş yazışmalarını ve veri tabanını ele geçirmiştir. Yetkililer bu yeni virüs türünün bankalardaki muhasebeye kayıtlı uygulamaların da yer aldığı programları tehdit ettiğini belirtmiştir. Bankanın bilgi işlem sistemini çökerten virüs, bulaştığı bilgisayarla ana sunucu arasında şifre korumalı bağlantı kurduğu ve bu şekilde yasadışı olarak bankacılık işlemlerini gerçekleştirdiği öğrenilmiştir. Bu virüsün online bankacılık müşterilerinin bilgilerini çaldığı, bulaştığı tüm sistemleri aynı şekilde etkilediği ve banka hesaplarını dahi boşaltabileceği belirtilmiştir. Şifre ve diğer kullanıcı bilgilerini öğrenmek isteyen hackerlar kullanıcıların klavyesine odaklanan bir virüs oluşturmuşlardır. Bu virüs klavyede basılan her butonu kaydetmiş ve bu şekilde kullanıcıların hesaplarını kolayca ele geçirebilmişlerdir. Hackerler müşteri bilgilerini talep edilen USD 500.000 vermemeleri halinde dokümanları internet ortamında yayınlama tehdidinde bulunmuşlardır. Uzlaşma yoluna gitmeyen banka yönetimi adli mercilere müracaat etmiştir. Birçok şirketi ve bankaları dolandıran hackerların peşine düşen polis, çeteyi ele geçirmiştir.

Vaka 5. Müşteri Güvenlik Uygulamalarında Mevcut Olan Yetersizlikler

Turizm işletmesinde çalışan oya hanım işlerinin yoğunluğundan mesai saatinde kirayı yatırmayı unutmuştur. Akşam eve gittiğinde, ertesi gün de unutabileceği endişesiyle "Şahin Bank" internet şubesine girerek ev sahibinin hesabına EFT talimatını yapar.

Üç gün sonra elektrik faturasını yatırmak için tekrar hesabına baktığında hesabında para olmadığını görerek şaşırır ve hesap hareketlerini kontrol eder. Hesap hareketlerine baktığında, "Nazlı Sakin" isimli şahsın "Ülke Bank" hesabına tüm paranın EFT yolu ile aktarıldığını görür, endişelenir ve hemen bankasını arayarak karışıklık olup olmadığını sorar ve ayrıntılı bilgi ister. "Şahin Bank" müşteri temsilcisi, işlemi inceler fakat anormal bir durumun söz konusu olmadığını, sistemsel bir sıkıntının bulunmadığını ve son zamanlarda benzer türde itiraz gelmediğini fakat kapsamlı araştırma yapabilmeleri için işleme itiraz edilmesi gerektiğini belirtir. Ayrıca internet şubesi şifre güvenliği, müşterilerin sorumluluğunda olduğundan maddi anlamda zararı karşılayamayacaklarını, fakat savcılığa başvuru yapılması durumunda olayın savcılıkta çözümlenebileceğini, banka tarafında da herhangi bir sorun bulunup bulunmadığı ile ilgili gerekli incelemelerin yapılacağını belirtir.

Mağdur oya hanım hemen savcılığa başvurur ve sonrasında hesabına havale yapılan şahıs adına suç duyurusunda bulunarak olay ile ilgili dava açar. Duruşmaya katılan "Nazlı Sakin" isimli bayan, kendisinin öğrenci olduğunu, ailesinin uzakta olması sebebiyle paranın ailesi tarafından yatırılmış olduğunu düşündüğünü, fakat parayı harcadığını ve durumu olmadığından bu parayı geri ödeyemeyeceğini belirtir. Yeterli delil bulunamadığından durum mağdur bayanın maddi

zarara uğramasıyla sonuçlanır.

Mağdur oya hanım başına gelen olay hakkında detaylı araştırma yaparak bilgi edinmiştir. Anlaşılan hesabından en son yaptığı işlem; kirayı yatırmak için akşam kişisel bilgisayarından internet şubesine girerek yaptığı EFT olmuştur. Fakat bu işlemi yaparken kişisel bilgisayarının güvenlik duvarını açmamış ve güvenlik önlemlerini oluşturmamıştır. Bu sebeple, sanal ortamda kişisel bilgisayarına ulaşılarak bilgileri ele geçirilmiştir.

Vaka 6. İnternet Bankacılığı (Web Sitesi Problemi)

Düzen bank web sitesini yeni güncellemiş ve müşterilerine yeni yüzünün tanıtımını yapmaya başlamıştır. Düzen bank yöneticileri yenilenen web siteleri ile gurur duyuyorlardır. Bu esnada İstanbul'da bir apartman dairesinde Bilgisayar mühendisliği öğrencisi 2 arkadaş hummalı bir çalışma içindedir. Ali ile Yunus Romanya'da bazı hacker grupların çeşitli web sitelerini çökerttiklerini ve bu konuda ünlendiklerini duymuşlardır. Ali kararını vermiştir. Kesinlikle Düzen bankın web sitesi çökertilecektir. Ancak Yunus'un planı daha büyüktür. Planı Ali'ye aktarır. "Madem Düzen bank web sitesini çökertebilecek potansiyele sahibiz, o zaman bu sitenin kopyasını da yapabiliriz. Hatta müşterilerin bilgilerini alabilirsek bu bizim için çok değerli bir bilgi olur. Hem de Rus ve Bulgar Hackerlara karşı namımız yürür" der.

İkili çalışmalarını sürdürürler, web sitesinin aynısını kopyalarlar ve bir mail taslağı hazırlayarak birçok kişiye gönderirler. Gönderdikleri linkte Düzen bankın web sitesinin yenilendiği bilgisi yer alıyordur ve giriş için bir link verilmiştir. Plan kısa süre içinde işlemeye başlamıştır. Birçok müşteri ilk etapta Ali ve Yunus'un yarattığı Düzen bank sitesine erişmişler ve burada yer alan forma kendi özlük bilgileri ve hesap bilgilerini girmişlerdir.

Dikkatli bir müşterinin durumu fark etmesi ile Düzen bank yetkilileri hemen önlemlerini almışlardır. Ancak, bu olay gazetelerde haber olmuş ve Düzen bank yetkilileri, müşterilerinin finansal işlemlerine ilişkin çeşitli bilgi ve verileri, söz konusu müşterilerin bilgisi dışında ve yasalarla yetkili kılınanlar haricindeki başka kişilere vermek ile itham edilmişledir.

SONUÇ

Teknoloji, herkes için son yıllarda bir ihtiyaç olarak kullanımı giderek artmış ve yaygınlaşmıştır. Özellikle bütün kurumlar bu kolay sistemi kullanarak satış fırsatları elde ederken, ürün pazarlama anlamında da bankacılık sektörü başta gelmektedir. İnternet bankacılığı ile yepyeni ürünler, fırsatlar, kolaylık, hızlılık, maliyetin düşük olması onun tercih edilebilir olmasını güçlendirmiştir. Fakat bankacılık açısından fırsatlar olduğu kadar tehditleri de bulunmaktadır. Tehditler ise riski içermektedir. Riskin birçok çeşidi bulunmaktadır. Bunlardan biri olan operasyonel risk ise en dikkat edilmesi gereken risk unsurudur.

Operasyonel risk ile karşı karşıya kalındığı zaman, müşterinin gözünde itibarı da etkileyen, sistemsel hataları içeren, bazen de suiistimaller ile müşteriyi zor duruma düşüren bir risk olmaktadır. Bu sebeple, bankalar bu riskin oluşmasını engellemeye yönelik birçok koruyucu program kullanmaktadırlar. Fakat yine de bu kadar önleme rağmen bazı olumsuzlukların yaşandığı görülmektedir.

Çalışmamızda, risk kavramı ile birlikte ortaya konulan operasyonel riske ait gerçek örnekler verilmiş olup; bu vakaların nedenleri ve sonuçları ile alınan önlemler açıklanmıştır. Teknolojik riskin konusu para olan bankacılık alanında ne kadar etkili olduğu da gösterilmektedir. Ayrıca, vakalarda gerek mail ile gerek de cep telefonu hattı, web sitesi, virüsler ile müşterilerin özlük bilgilerine ulaşılarak yapılan işlemlere değinilmiş olup; bu konuda bankacılık sektörünün en çok önem göstermesi gereken yerin risk birimi olduğu düşünülmektedir.

Bankacılık sektörü için her yeni teknoloji yeni fırsatları doğururken, yeni tehditleri de karşımıza çıkarmaktadır. Sonuçta, riskin oluşabilme ihtimaline göre alınan önlemler; hem müşteri memnuniyetinin sağlanması hem de bankanın prestijinin korunması olarak kayda geçecektir. Bu ikisi için de sağlam bir risk yönetimi yapısının kurulması ve internette gerçekleşen bütün işlemler için takibinin sürdürülmesi gerekmektedir.

KAYNAKÇA/REFERENCES

Aksu, D. (2016). İmalat sektöründe kur riskinin birincil ve ikincil etkileri ve kur riskine karşı çözüm önerileri. Muhasebe ve Finansman Dergisi. 71. 149-164.

Aloğlu, Z. T. (2005). Bankacılık sektörünün karşılaştığı riskler ve bankacılık krizler üzerindeki etkileri. Türkiye Cumhuriyet Merkez Bankası Bankacılık ve Finansal Kuruluşlar Genel Müdürlüğü. Uzmanlık Yeterlilik Tezi. Ankara.

Anderson, A. (2001). Riskler ve risk yönetimi. seminer notları. Ankara.

Bağcı, B. (2010). Türkiye BT yönetişimin neresinde? 1.Bilgi Teknolojileri Yönetişim ve Denetim Konferansı.

Basel Committee on Banking Supervision (2001). Operational risk. Consultative Document https://www.bis.org/publ/bcbsca07.pdf ,Erişim Tarihi: 05.10.2017

BDDK, Bankaların sermaye yeterliliğinin ölçülmesine ve değerlendirilmesine ilişkin yönetmelik, Tanımlar, Madde: 3, Faiz Oranı Riski, https://www.bddk.org.tr/WebSitesi/turkce/Mevzuat/Bankacilik_Kanununa_Iliskin_Duzenlemeler/15067syr_09_12_2016_degisiklikisleme.pdf ,Erişim Tarihi: 09.10.2017

Eroğlu, N. & Yücel, İ. S. (2012). Türkiye'deki kurumsal banka müşterilerinin internet bankacılığı kullanım eğilimlerini belirleyen başlıca faktörler üzerine ampirik bir çalışma. Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü E-Dergisi. 2(2). ISSN: 1303-8281.

Günceler, B. (2015). Risk Yönetimi ve değerlemesi ile ilgili temel kavramlar nelerdir. Ders Notları. 11.05.2015.

Gündoğdu, A. (2016). Küresel kriz sonrası gelişmeler ışığında bankacılığın temelleri. Nobel Yayıncılık. İstanbul.

İç Denetçilerin Çalışma Usul ve Esasları Hakkında Yönetmelik, Madde:4, Risk Yönetimi, http://www.idkk.gov.tr/SiteDokumanlari/Mevzuat/Ikincil%20Duzey%20Mevzuat/icdencalusulveesas.pdf ,Erişim Tarihi: 05.01.2018

Karadeniz, E. Kandır, S. Y. & İskenderoğlu Ö. (2013). sistematik riskin belirleyicileri: borsa istanbul turizm şirketleri üzerinde bir araştırma. Erciyes Üniversitesi 14. Ulusal Turizm Kongresi Bildiriler Kitabı. 1056-1073.

Maliye Bakanlığı Strateji Geliştirme Başkanlığı, Risk Yönetimi Nedir?, İç Kontrol Broşürleri, https://www.sgb.gov.tr/Kontrol%20Brorleri/04.%20Risk%20Y%C3%B6netimi%20Nedir.pdf ,Erişim Tarihi: 08.01.2018

Özbilgin, İ. G. (2011). Bilgi Teknolojileri Yönetişimi. Bilişim Dergisi. S.134. 78-81.

Sayım, F. & Er, S. (2009). Risk kavramı ve bankacılıkta risk. Çatı Bilimsel Yayın Organı. 4 (22). 7-17.

Şahin, S. (2008). Bankacılıkta risk yönetimi ve türk bankacılık sisteminin risk yönetimi açısından değerlendirilmesi. Yayımlanmamış Yüksek Lisans Tezi. Marmara Üniversitesi İktisat Anabilim Dalı. İstanbul.

Türkiye Bankalar Birliği, Kredi riskinin yönetimine ilişkin ilkeler, https://www.tbb.org.tr/Dosyalar/Arastirma_ve_Raporlar/risk_yonetim.doc ,Erişim Tarihi: 12.12.2017

Uzundağ, Ş. (2013). Türkiye'de internet bankacılığının gelişimi ve internet bankacılığına ilişkin tüketici davranışları analizi: aydın ili merkezinde görev yapan öğretmenler üzerine bir araştırma. Yayımlanmamış Yüksek Lisans Tezi. Adnan Menderes Üniversitesi. Aydın.

Varlı, A. T. (2006). Bilgi sistemleri denetiminde BDDK yaklaşımı. *Bilgi Teknolojileri Denetimi Sempozyum&Workshops.*(19-22 Nisan).