Kaynak: Harvard Business Review
Tarih: 17.05.2017

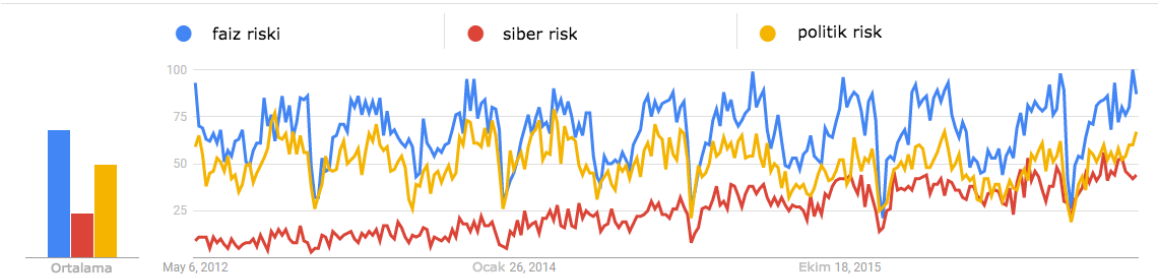
Dijital Şirket, Sanayi 4.0 ve İç İçe Geçmiş Riskler

Yazan: **Ahmet Eryaman**

"Bir gemi sahilde iken her zaman güvendedir. Ama gemiler bunun için yapılmamıştır." Albert Einstein

Teknolojinin her geçen gün hayatımıza daha çok girmesiyle, siber riskler de hayatımıza girdi. Müşterilerine rakiplerinden daha farklı bir deneyim yaratma peşinde olan firmalar, "dijital" kanallara yatırım yapıyor. Bankacılık başta olmak üzere teknoloji odaklı hizmet sektörleri iç süreçlerini iyileştirmek için "dijital şirket" kavramını hayatlarına geçirirken, bu süreçleri olabildiğince yazılım ortamına taşıyorlar. Üretim hatlarına eklenen yeni donamımlar sayesinde yazılım endüstriye de girdi. Sanayi 4.0 çağı açıldı. Bütün yöneticiler yazılım ve donanım teknolojilerindeki göz kamaştırıcı yeniliklerin heyecanını duyuyor, daha rekabetçi organizasyonlar yaratmanın yollarını keşfediyorlar.

Bu iki değişimin (Dijital ve Sanayi 4.0) doğal sonucu olarak, iş hayatında ve medyasında yıllardır yakından takip edilen "faiz riskleri", "politik riskler" gibi konulara ek olarak "siber risklere" ilginin artığını görüyoruz. İnternet arama motorlarında yapılan aramalar incelendiğinde, son beş yıllık istatistiksel veriler artık siber risklerin en az politik riskler kadar arandığı, araştırıldığını işaret ediliyor. (Nisan 2017. Google Trends veri analizi.) Aşağıdaki grafik, son beş yılda dünyada yapılan tüm internet aramaları içerisinde, "faiz riski", "politik risk" ve "siber risk" aramalarının oranını temsil ediyor. Küresel para piyasalarının yılsonu tatili ve Noel tatili nedeniyle yavaşladığı Aralık sonlarında faiz riski ve politik riske olan ilginin azaldığı görülüyor. (Aynı mevsimsellik yaz aylarında da ortaya çıkıyor). Arama motorlarında siber riske olan ilgi, geleneksel olarak para piyasalarının ve ilgili sektörlerin yakından takip ettiği faiz riskine hızla yaklaşmakta ve tüm riskler içerisinde öteden beri takip edilen politik risk ile aynı seviye ulaşmış durumda.



Aon Global Risk Yönetimi Anketi 2017 sonuçlarına göre ilk 10'a giren riskler içerisinde:

- Marka İmajı ve İtibarının Zedelenmesi (1. sırada)
- Yasal Düzenlemelere Bağlı Riskler (4. sırada)
- İş Kesintisi Riskleri (8. sırada)

ile siber riskleri (5. sırada) karşılaştırırsak siber risklere olan ilginin hızla yükselip diğerlerini geçtiğini görebiliriz.

Tecrübe ve araştırmalarımız, siber risklerin bazı sektörlerde marka imajı ve iş kesintisi ile doğrudan bağıntılı, hatta bunların tetikçisi olduğunu gösteriyor. Firmaların siber evrendeki zafiyetleri doğrultusunda yaşanan olaylar sonucu, birçok ülkede kanun koyucular sıkı önlemler almış durumda. Bunun sonucu olarak siber risk algısı yükselmekte ve hatta yukarıdaki grafikte Eylül 2014'den beri "siber evrenin en önemli rehberi" Google istatistiklerine göre diğer üç riskten daha fazla araştırılan başlık konumuna gelmiş bulunmaktadır. Bu gelişme Aon çatısı altında 2007 yılından beri yapılan Global Risk Yönetimi Anketi sonuçları ile paralellik gösteriyor.

Yıllara Göre	2007	2009	2011	2013	2015	2017
Siber Riskler	19	25	18	18	9	5*

**2017'de küresel ölçekte beşinci sıradayken, Havacılık, Eğitim, Kamu alt sektör kırılımları için birinci en önemli risk olarak saptanmıştır. Ayrıca bölgesel olarak bakıldığında Kuzey Amerika'da yine birinci, Avrupa'da altıncı en önemli risk olarak karşımıza çıkıyor.*

İşin ilginç tarafı, aynı katılımcılar siber risklerin 2020 yılında da ilk 5'te olmaya devam edeceğini tahmin ediyorlar.

Teknoloji, Türkiye ve Kurumsal Risk Yönetimi

Türkiye'de risk yönetimine verilen önemin gittikçe arttığını birçok kanaldan görebiliyoruz. Mesela risk yönetimini odağına ya da kapsamına almış derneklerimiz var:

- Kurumsal Risk Yönetimi Derneği (KRYD).
- Risk Yöneticileri Derneği.
- Türkiye Kurumsal Yönetim Derneği (TKYD)
- Türkiye İç Denetim Enstitüsü (TİDE), bunlardan bazıları.

Türkiye'de "risk" kelimesini iş unvanına yansıtmış olan yaklaşık 2900'dan fazla çalışan olduğu tahmin ediliyor. (Nisan 2017, Linkedin veri analizi. Aynı tarihte Otomotiv, Telekomünikasyon, Perakende, Petrol ve Enerji sektörüne kayıtlı, yerleşkesi Türkiye olan yaklaşık 358 bin çalışan kaydı içinden derlenmiştir)

Ülkelere göre…	… unvanında "Risk" olan çalışanlar
Fransa	± 8000
İtalya	± 7200
İspanya	± 4200
Türkiye	± 2900

Bankacılık ve Sigortacılık sektörleri geleneksel olarak parasal risklere odaklı çalıştıklarından dolayı Kurumsal Risk Yönetimi geleneksel olarak uyguladıkları ve hatta yıllardır mevzuat ve yönetmelikler ile kontrol altında tutulan bir fonksiyon konumunda. Elde ettiğimiz verilere göre Türkiye'deki kurumlarda risk organizasyonu içinde çalışanların yaklaşık olarak yüzde 53'ü bu iki sektörlerde istihdam ediliyor. Bunların takipçisi olan sektörler ise sırası ile Bilişim Teknolojileri ve Servisleri ile Telekomünikasyon sektörü olarak karşımıza çıkıyor. (Elde edilen verinin yaklaşık yüzde 9'u) Yönetim danışmanlığı çatısı altında çalışanları ve daha az sayıda çalışanların olduğu sektörleri (864 kayıt) da bir kenara ayırırsak,

geriye yaklaşık 450 kişilik bir gurubun risk yönetimine odaklı çalıştıklarını görüyoruz. Bu grup büyüklük sırasında göre:

- Bilişim Teknolojileri ve Servisleri,
- Telekomünikasyon,
- Petrol ve Enerji,
- Otomotiv,
- Perakende,
- Bilgisayar ve Şebeke Servisleri sektörlerine mensuplar.

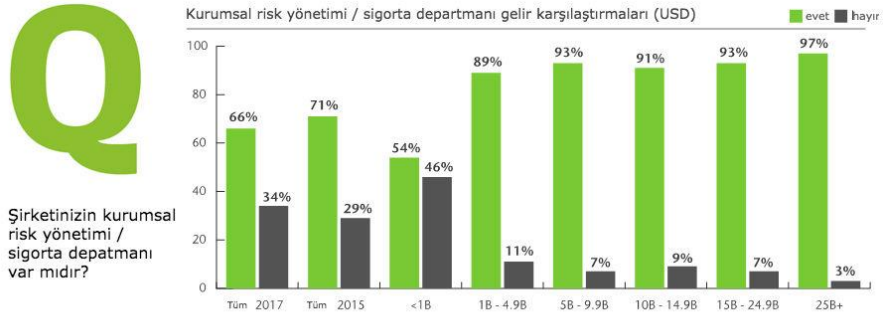
Yukarıdaki sektörlere bakınca, bunların yoğun olarak teknoloji yatırımı yapan sektörler olduğu göze çarpıyor. Forbes Dergisi'ne (Forbes, 5 Aralık 2016. Trends In Tech Investing 2017 by Murray Newlands) göre 2017 yılında firmalar şu teknolojilere daha fazla yatırım yapacaklar:

- Sosyal medya
- Kurumsal kaynak planlaması ve benzeri şirket yazılımları
- Eğitim Teknolojisi (EdTech)
- Mobil Teknolojiler
- Teknoloji Destekli Tıp
- Sanal Gerçeklik/Zenginleştirilmiş gerçeklik
- Otomasyon

Yukarıda adı geçen sektörler bu teknolojileri yakından takip ediyorlar. Bu teknolojik yatırımlar arttıkça, bankacılık ve sigorta dışındaki firmalarda da risk yönetiminin organizasyon yapısında yer buluyor. Yönetim kurulları, CEO'lar Dijital Değişim ve Sanayi 4.0'ın beraberinde getirdiği ciddi risklerle mücadele edebilmek için ekipler yaratıyor.

ABD çalışan verileri de (yaklaşık 15100 çalışan) aynı yönde. Burada önemli bir fark, ABD'de hastane ve sağlık sektöründe ciddi miktarda "risk" odaklı çalışan göze çarpıyor. Forbes Dergisi'nde değinilen "Teknoloji Destekli Tıp" yatırımları arttıkça, sağlık sektörünün siber risklere karşı daha ciddi organizasyonlar kurması gerekecek. Hem iş devamlılığı hem de hacker'lar ile mücadele öncelik sıralamasında yukarılara çıkmaya devam ediyor.

Öte yandan Bankacılık, Sigortacılık ve Finansal Hizmetler sektörlerine bakıldığında, unvanında "risk" olan (Yaklaşık 1500 kayıt) ama fonksiyonu Bilişim Teknolojileri, Program/Proje İdaresi, Operasyon olan 271 kayıt göze çarpıyor (yüzde 18).Teknolojinin getirdiği dijital değişim ve Sanayi 4.0'ın en yaygın olduğu kurumların yapısında risk odaklı yönetim ve yapılaşma parasal risklerin idare edildiği bölümlerin dışındaki bölümlerde de ön plana çıkıyor. Firmalar organizasyon yapısında birçok bölüme yayılmış risk odaklı sorumlulukları olan işgücünü bir elden idare etmek için Kurumsal Risk Yönetimi disiplinine yöneliyor. Aon Global Risk Yönetimi Anketi, cirosu 1 milyar doları aşan firmaların risk/sigorta yönetimini kurumsallaştırdığını ortaya koyuyor.



Dijital Şirket ve Sanayi 4.0

Birçok üst düzey yönetici, Dijital Şirket veya Sanayi 4.0 olarak adlandırılan gelişmelerin kendi şirketlerini nasıl etkileyeceklerini, nasıl bir pozisyon almaları gerektiğini değerlendiriyor. HBR makalesinde (Harvard Business Review. The Most Digital Companies Are Leaving All the Rest Behind. James Manyika, Gary Pinkus, Sree Ramaswamy. JANUARY 21, 2016) geçen bilgiye göre dijital olanakları en yoğun kullanan sektör liderleri, diğer sektör üyelerine göre müşterileri ve tedarikçileri ile beş kat daha fazla iletişim ve etkileşim sağlıyorlar. Çok daha fazla verimlilik ve bunun sonucunda daha yüksek net kâr marjı elde ediyorlar. Bu iki gelişme karşısında aynı sektördeki rakip yöneticiler, karşı karşıya kaldıkları risk ve fırsatları değerlendirmek için yatırımlar yapıyorlar ancak. Dijital Şirket ve Sanayi 4.0 rekabet avantajı sağlarken, siber risklere de kapı açıyor.

2017 yılında birçok sektörün risk haritalarında ekonomik yavaşlama ön sıraları alırken dijitalleşme ile verimlilik artırma bir fırsat olarak görülüyor. Bu yönelim siber suçların artması için elverişli bir ortam sunuyor. Aon Global Risk Yönetimi Anketi'ne göre, 2015 yılında 9. sırada olan siber riskler (siber suçlar, hack'lenme, virüs saldırıları), 2017 yılında 5. sıraya yükselmiş durumda. Ankette siber riskler şöyle tanımlanmış; "bilişim sistemlerine izinsiz erişim veya hack'leme sonucu verilerin, yazılım kodlarının bozulması/kaybolması, gelir kaybı, ek maliyetler, itibar/şerefiye değer kaybı" Bu tanımı okuyarak ankete katılan 1800'ü aşkın firmanın yüzde 35'i siber riskleri 2. sıraya koymuş. Ankete katılan firmaların paylaşımlarına göre aynı dönemde siber risklerle mücadele için hazır olduklarını düşünenlerin oranı yüzde 82'den yüzde 79'a gerilemiş.

Yapılan çalışmada üst düzey yöneticilerin siber riskler konusundaki endişelerinin başka tehlikeler ile beraber ön plana çıktığı görülüyor. En bariz haliyle, liderler "İş İhtiyaçlarını Destekleyecek Teknolojik Altyapı Eksikliğinin" ve "Teknolojik Aksaklıklar / Sistem Aksaklıklarının" siber risklere davet çıkardığının farkında. Bu etkileşimler aşikâr. Ancak daha üstü kapalı etkileşimler de var. Mesela çalışanların "Etik Dışı Davranışlara" yönelmesi, siber saldırılara kapı açan en önemli etmen. Dijitalleşmeyi stratejik hedefleri arasına koyan firmaların, çalışan bağlılığına yatırım yapması, çalışan eğitimlerini kuvvetlendirmeyi kurumsal hedefler içine koyması gerekiyor.

Bir başka etmen ise, uluslararası medyada örneklerini sıkça duyduğumuz "Politik Riskler /Belirsizlikler" sonucu ortaya çıkan "Terörizm ve Sabotajların" siber saldırılar olarak kendini göstermesi. Rusya ve Ukrayna arasındaki anlaşmazlık sırasında elektrik dağıtım işi ile uğraşan şirketlere siber ataklar düzenlenmişti. (MIT Technology Review. Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks. Jamie Condliffe. December 22, 2016.) Maalesef talihsiz bir coğrafyada olan ülkemizdeki iş dünyasının liderleri bu faktörü göz önünde bulundurmalı. Sanayi 4.0'a doğru atılan her adım ile, şirketin büyüklüğüne ve sağladığı hizmetlerin kamudaki yaygınlığına göre, siber terörizm ve sabotaj hedefi olunması artık mümkün gözüküyor.

Küresel iş dünyasını temsil eden 1800'ü aşkın yönetici aşağıdaki riskleri de siber risklere etmen olarak kaydetmişler:

- "Marka İmajı ve İtibarının Zedelenmesi"
- "İş Kesintisi" sonucu bilişim sistemlerinde gedik açılması ile fırsat kollayan siber saldırıya olanak çıkması
- "Sosyal Medya" olanaklarının kullanılması ile
- "Kurumsal Sosyal Sorumluluk/Sürdürülebilirlik"

Öte yandan siber riskler gerçekleştiğinde birçok sorunu tetikleyerek firmayı "artçıl" diye sınıflandırabileceğimiz başka risklere maruz bırakıyor. Başta CIO ve CRO'lar olmak üzere C-Takımı siber ataklara karşı her türlü önlemi alıyorlar. Ancak bütün önlemlere rağmen, en sağlam kurumlarda bile güvenlik ihlalleri olduğunu görüyoruz. Kurumun bilişim sistemlerinde bir siber saldırı ile gedik açıldığında, hangi risklere kapı açıldığını bilerek gerekli tedbirleri almak gerekli. Artçıl risklerin bazıları zaten aşikâr. Bunlar siber risklerin sebebi olabildiği gibi, sonucu da olabiliyorlar:

- "Marka İmajı ve İtibarının Zedelenmesi"
- "İş Kesintisi"
- "Terörizm ve Sabotaj"
- "Teknolojik Aksaklıklar / Sistem Aksaklıkları"
- "Sosyal Medya"

Küresel iş dünyası olası bir siber saldırının ardından yukarıdakilerin dışında "Üçüncü Şahıs Mali Mesuliyetler"e maruz kalacağını öngörüyor ve önlemler alıyor. Tarihsel olarak Amerikan iş dünyası daha fazla çekişmeli geleneğe sahip. ABD'de başkalarına veya onların mallarına karşı yapılan haksız fiil ya da zarar davaları için yılda 310 milyar dolar harcandığı tahmin ediliyor. (Aon Global Risk Yönetimi Anketi Raporu. (URL)) Küreselleşmenin de etkisi ile Avustralya, Avrupa ve Latin Amerika'daki tüketiciler de git gide daha fazla hukuk yollarına başvuruyorlar. Tüketici haklarının yaygın kabul görmesi, gelişmekte olan ekonomilerdeki hükümetlerin bu yönde yeni düzenlemeler getirmesi, "hakkını mahkemede arayan" bir toplum yaratıyor. Yöneticiler, siber saldırı ile oluşan ihlaller neticesinde ortaya çıkacak olumsuzluklardan dava edilme endişesi ile "Üçüncü Şahıs Mali Mesuliyetler" konusunda tedbirler hayat geçirtiyorlar. Firmaların yüzde 70'i bu artçıl riske karşı hazırlıklı olduklarını bildiriyorlar. Aynı şekilde "Yöneticilerin şahsi Sorumluluk" riski de siber risklerle beraber algılanıyor.

Aynı ankette inovasyon ve yıkıcı teknolojiler (kendi kendine giden arabalar gibi) yeni bir risk olarak listeye 20. sıradan girmiş. 2020'de 10. sıraya yükselmesi bekleniyor. Özelikle küresel cirosu 10 milyar dolar ve üstünde olan firmalarda bu risk ilk 10 içinde yer alıyor. Ancak bununla tezat oluşturmak istercesine, firmaların atılım projesi başarısızlığı riski 15. sıradan listeye girmiş. Teknoloji ve inovasyon konusunda Kuzey Amerika ile olan farkı kapatmaya çalışan Asya/Pasifik firmalarında bu risk 10. sırada yer alıyor. Firmaya rekabet avantajı sağlayacak inovasyonların ve teknolojilerin peşi sıra gelen projeler ile hayata geçtiği düşünülürse dijitalleşmeye odaklanan firmalar bu riskleri yönetmek zorunda.

Bu değişime ayak uydurmak için en önemli kaynak teknoloji konusunda ilgili, bilgili, eğitimli çalışanlar. Üstelik bu çalışanları sadece bilişim teknolojileri ekibinin işi olarak görülmemeli. Satış ve pazarlamadan, operasyona kadar her fonksiyonda böyle çalışanlara ihtiyaç var. Bu da yüksek performanslı çalışanları bulma ve elinde tutma riskini akıllara getiriyor. 2017 yılında firmalar bu riski 7. sıraya koyuyorlar.

Dijitalleşmeye ve otomasyona bu kadar fazla ilgi olunca, karmaşık hale gelen operasyonlar iş kesintisi risklerini de artırıyor. Teknoloji aksaklıkları, sistem göçmeleri yöneticilerin 18. problemi olarak önümüze çıkıyor. İş kesintilerinden doğan zararların konu alındığı iş kesintisi riski ise ankette 8. sırada yer alıyor.

Mücadelede ilk adım

"Ölçmediğiniz şeyi yönetemezsiniz!" düsturundan yola çıkarak, Yönetim Kurullarının ajandasına giren ilk aksiyon "siber risk değerlendirmesi" olarak öne çıkıyor. Üst Yönetim gitgide daha fazla "3. kişilerden bağımsız değerlendirme" almaya yöneliyorlar. Bu servislere alınmasında şirket içinde karşılaşılan direnç Orta Doğu'da ve Latin Amerika'da dünyanın geri kalanına göre daha fazla.

Kurumsal siber risk değerlendirmenizi yaptırdınız mı?

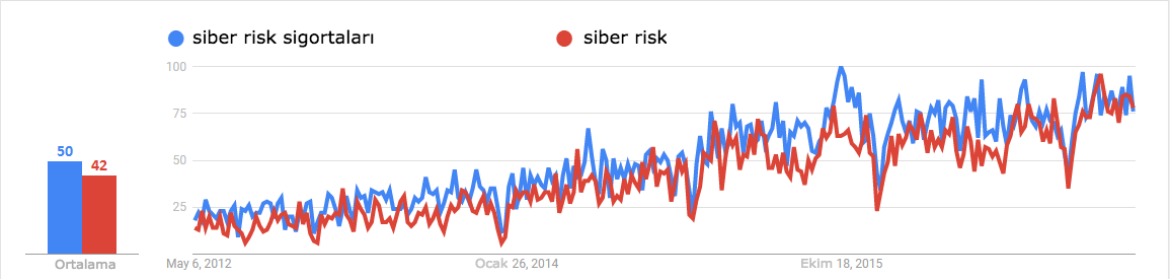
Bölgelere göre siber risk değerlendirmesi yaptırma oranları

Bölge	Değerlendirme yaptıranlar	Evet, Nicelikli	Evet, Nitelikli	Evet, ikisi de, Nicelikli ve Nitelikli	Evet, ama hangisi emin değilim	Emin Değilim	Hayır
Tümü	53%	2%	12%	21%	18%	16%	31%
Kuzey Amerika	76%	2%	13%	35%	25%	8%	16%
Asya Pasifik	51%	2%	15%	21%	13%	13%	36%
Avrupa	45%	3%	11%	16%	15%	18%	37%
Ortadoğu & Afrika	43%	4%	14%	8%	17%	17%	40%
Latin Amerika	38%	2%	9%	13%	15%	26%	36%

Gelire göre siber risk değerlendirmesi yaptırma oranları (usd)

Bölge	Değerlendirme yaptıranlar	Evet, Nicelikli	Evet, Nitelikli	Evet, ikisi de, Nicelikli ve Nitelikli	Evet, ama hangisi emin değilim	Emin Değilim	Hayır
< USD 1B	45%	2%	10%	15%	17%	17%	39%
USD 1B – USD 4.9B	72%	5%	18%	33%	17%	9%	19%
USD 5B – USD 9.9B	74%	5%	16%	29%	24%	9%	17%
USD 10B – USD 14.9B	69%	2%	18%	29%	20%	18%	13%
USD 15B – USD 24.9B	78%	0%	17%	44%	17%	5%	17%
USD 25B+	75%	0%	7%	56%	11%	15%	11%

Bu bölgelerde CIO ve CTO'ların genelde operasyonlarını dışarıya açmak istemediklerini gözlemliyoruz. Dolayısıyla firmayı/markayı korumak için gerekli önlemleri alma sorumluluğu aynı yöneticilerin sırtında kalıyor. Teknolojik ilerlemeler o kadar hızlı ve çeşitli ki! En iyi eğitimleri almış, en kuvvetli donanımlara sahip ekiplerin bile şirketi yüzde 100 koruduklarına inanmak mümkün görünmüyor. Bu sebeple, Google Trend istatistiklerinde "siber risk sigortaları" aramalarının "siber risk" aramaları ile aynı hızda artığını gözlemleyebiliyoruz.



Her türlü savunma yöntemleri hayata geçirilmiş olsa bile, marka değerinin ve markaya olan güvenin tüketici gözünde ne kadar kırılgan olduğunu bilen yönetim kurulları gitgide daha fazla risk transferi opsiyonunu kullanıyorlar.

Ülkemizde, büyük bir siber krizi patlak verdiğinde, ilgili yönetici ve yakın çalışma arkadaşlarının işlerini kaybetmelerine kadar varabilen sonuçlar gözlemlendiği halde, yönetim kurullarının bağımsız değerlendirmelerden yeterince faydalanmaması, sigorta kullanmaması bir tezat oluşturuyor. Bunun kök nedenlerini daha iyi anlamak ve bir yandan teknolojiye yatırım yaparken, diğer yandan teknoloji kaynaklı riskleri kontrol altında tutmak için her türlü yöntem ve yaklaşımı C-Takımının emrine vermek en mantıklı yol gibi görünüyor.

Harvard Business Review Türkiye'nin internet sitesinden alınmıştır. İlgili yazıya ulaşmak için lütfen tıklayınız.