

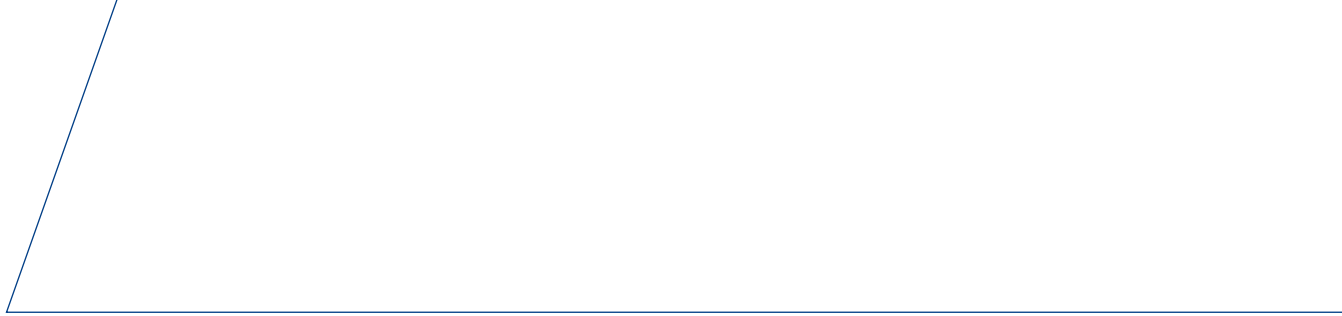
**KPMG**

*cutting through complexity*

# Bir Suistimalcinin Profili

Günümüzden geleceğe  
beyaz yaka suçları

[kpmg.com.tr](http://kpmg.com.tr)



# Önsöz

Suistimal pek çok şirketin yaşadığı bir gerçek. Peki suistimali gerçekleştiren kişilerin ortak özellikleri olduğunu biliyor muydunuz? KPMG tarafından 2007 yılından beri her iki yılda bir hazırlanan “Bir Suistimalcinin Profili” raporu, işte bu özellikleri ortaya koyuyor.

Bu yılki rapor, 78 ülkedeki KPMG üye firmalarının 2011–2013 yılları arasında soruşturmasını gerçekleştirdiği 596 suistimal vakasının analizini içeriyor ve suistimalcilerin genel özellikleri ve motivasyon kaynaklarıyla yetiştikleri çevre arasındaki nasıl bir ilişki olduğunu araştırıyor. 2011 yılında yayımlanan raporda ağırlıklı olarak suistimal örnekleri ve suistimalcilerin çeşitli özellikleriyle bunların önümüzdeki 5 yıl içinde ne yönde gelişeceği yer alıyordu. 2013 araştırmasında yer verilen 596 suistimalcinin profili de 2011’de ortaya konan tipik suistimalci profiliyle oldukça benzer özellikler taşıyor.

Son dönemde, Türkiye’deki ulusal veya uluslararası şirketlerin iç denetim departmanlarının şirkete katma değer sağlama çabalarını memnuniyetle yakından izliyorum. Pek çok iç denetim departmanı kalite güvence değerlendirmesi yaptırıyor, bilgi teknolojileri denetimlerini gerçekleştiriyor, suistimal risk yönetimi ve değerlendirmesi konusunda destek alıyor ve suistimal incelemelerini daha profesyonelce yapmanın yollarını arıyor. Dolayısıyla bu raporun iç denetim profesyonellerine yol göstereceğini umuyorum.

Ülkemizde de, gün geçtikçe şirketlerin üst düzey yöneticilerinin, denetim ve icra komitelerinin, uyum yöneticilerinin ve çalışanların suistimal farkındalığı artıyor. “Bizim şirkette suistimal vakası olmaz” anlayışından “Suistimal risk değerlendirmemizi yapalım”, “Etik hat kuralım ki çalışanlarımız şüpheli durum bildirimlerini yapabilsin”, “Şirkette suistimal farkındalığını artıralım” anlayışına geçtiğimizi söyleyebilirim. “Bir Suistimalcinin Profili” raporunun suistimal farkındalığı konusunda da şirket yöneticilerine ışık tutacağını düşünüyorum.

Bu yılki raporda KPMG firmalarının Suistimal Önleme ve İnceleme Bölümü liderlerinin öngördükleri trendleri dört maddede toplayabiliriz:

- Hem operasyonları kesintiye uğratma hem de maddi kazanç elde etme peşinde olan, üstün teknolojileri kullanabilen, çeşitli suç örgütleriyle işbirliği içerisinde hareket eden “bilişim korsanları” gibi tehditlere karşı savunmasızlığın artmakta olduğu görülüyor.
- Şirket içi ve şirket dışı suç ortaklarının birbirleriyle veya kendi aralarında yaptıkları gizli ittifak ve işbirliklerinde sürekli artan bir trend görülmesi, şirketlerin suistimalcilere karşı olan savunma mekanizmalarını, bağımsız denetim ve iç denetim önlemlerinin ötesine taşımaları gerektiğini vurguluyor.
- Artık tek başına gerçekleştirilen vakalar olmaktan çıkıp diğer beyaz yaka suçlarında da yaygınlaşan rüşvet ve yolsuzluk, günümüz suistimalci profilinin sabit bir parçası haline gelmiş durumda ve suistimalcilerin kendi başlarına hareket etmelerine oranla, mağdur şirkete çok daha büyük maddi zarar veren danişıklı bir ilişki yaratma becerisini geliştiriyor.
- Ekonomik istikrarsızlık, değişken sermaye piyasaları, yeni teknolojiler ve inovasyon, yeni muhasebe sistemleri, bilişim alanında dünyanın her yerinden erişim imkânının giderek artması ve sanal işlemlerin yapıldığı ortam, bu değişimlerden yasadışı biçimde faydalanarak kazanç temin etmek amacıyla gerekli yetkinlikleri gösterebilecek, suç dürtüsüne ve gerekçelere sahip insanlara birçok fırsat sunuyor.

Sürekli değişen suistimal trendlerini ve suistimalci profilini analiz etmek, şirketlerin suistimallere karşı direncini artırmalarını sağlayacaktır. Şirket yönetimlerinin suistimal riskini risk haritasındaki bir nokta olarak görmekten vazgeçip bu riske gereken önemi verme zamanı geldi de geçiyor bile. İyi ve şirketinize uygun bir suistimal risk yönetimi, riskinizi sıfırlamayacak ama önleme yöntemlerinin etkinliğini artıracak ve suistimali ortaya çıkarma sürenizi azaltıp daha az kayıp yaşamanızı sağlayacaktır.

2013 yılı “Bir Suistimalcinin Profili” raporunu ilgilie okuyacağınızı düşünüyorum. Raporla ilgili görüşmek istediğiniz bir konu olursa bana her zaman ulaşabilirsiniz.

Saygılarımla,

**İdil Gürdil**

**KPMG Türkiye Risk Yönetimi Danışmanlığı Bölüm Başkanı**

**Şirket Ortağı**



# Giriş

**S**uistimal inceleme uzmanları kuruluşların, suistimalcileri eylem sırasında ve hatta daha öncesinde yakalayabilmelerini sağlayacak kadar doğru bir suistimalci profili geliştirmenin mümkün olup olmadığı konusunda yıllardır tartışmaktadır. Bir suçta henüz işlenmeden tahmin edebilmek, en azından şimdilik sadece bilim kurgu filmlerinin konusu olabilir. Ancak suistimal ve suistimalcilerin sürekli değişen doğasını iyi bir şekilde analiz etmek, kuruluşların suç faaliyetlerine karşı savunma mekanizmalarını güçlendirmelerine yardımcı olacaktır. Tetikte olan erken davranır!

Bu rapor, KPMG üye firmalarının 2011 – 2013 yılları arasında soruşturmasını gerçekleştirdiği 596 suistimalcinin analizini içermektedir. Okuyucuya suistimalcilerin genel özellikleri ve motivasyon kaynakları ile yaşadıkları çevre arasındaki ilişki konusunda çeşitli bilgiler ve uzman görüşleri sunmayı amaçlamaktadır. Uzman görüşlerini genişletmek amacıyla KPMG üye firmalarının suistimal önleme ve inceleme uzmanlarıyla da görüşmeler gerçekleştirilmiştir. Bu rapor, 2011 yılında yayımladığımız ve 348 vakanın araştırıldığı *Who is the typical fraudster? [Bir Suistimalcinin Profili 2011]*<sup>1</sup> başlıklı rapor ile 2007 yılında yayımladığımız *Profile of a fraudster [Bir suistimalcinin profili 2007]*<sup>2</sup> başlıklı rapor temel alınarak hazırlanmıştır. 2011 yılında yayınlanan raporda ağırlıklı olarak küresel alanda görülen suistimal örnekleri ve suistimalcilerin çeşitli özellikleri ile bunların önümüzdeki 5 yıl içinde ne yönde gelişeceği arasındaki ilişki yer almaktaydı.

2013 araştırmasında yer verdiğimiz 596 suistimalci arasındaki tipik suistimalci profilleri ile KPMG üye firmalarının iki yıl önce sonuçlarını bildirdiği araştırmalarda ortaya konan tipik suistimalci profili oldukça benzerdir. 2013 yılında gerçekleştirdiğimiz araştırmada ortaya çıkan tipik suistimalci profilinin 36 - 55 yaşları arasında, genellikle çalıştığı kuruluşun aleyhine hareket eden ve çoğunlukla yönetim<sup>3</sup>, muhasebe, operasyon veya satış/pazarlama bölümlerinde görev yapan bir kişi olduğu görülmüştür. Üst yönetimde görev almakta, şirkette 6 yıldan uzun bir süredir çalışmakta ve suçlu işlerken çoğunlukla başkalarıyla işbirliği yapmaktadır.

Bununla birlikte, diğer bulgular ise daha farklıdır. Bu defa; suistimalcinin çevresi ve işlediği suistimal suçları arasındaki değişen ilişkiyi anlayabilmek için bir dizi tema geliştirdik. Tüm dünyadaki suistimal önleme ve inceleme uzmanlarımızın görüşlerini de dikkate alarak, hem suistimal türünün hem de suistimalci profilinin sürekli olarak değiştiği sonucuna vardık. KPMG Küresel Suistimal Önleme ve İnceleme Hizmetleri Bölümü Koordinatörü Phil Ostwalt, "Suistimalin en ilginç yanı grip

virüsü gibi sürekli şekil değiştirmesi; bu yılki virüsü etkisiz hale getirebiliyorsunuz ama ertesi yıl daha kötü, daha etkili olarak farklı bir şekilde karşınıza çıkıyor" diyor.

Büyük değişimlerin en önemlilerinden biri de; sadece ABD gibi teknolojik açıdan gelişmiş ülkelerde değil, tüm dünyada, suistimalcilerin gelişen teknolojiyi giderek daha fazla kullanmaya başlamış olmasıdır. KPMG Kolombiya Suistimal Önleme ve İnceleme Hizmetleri Direktörü Arturo del Castillo, "Tüm işletmeler için geçerli olan ortak endişelerden biri de, önceki nesillere göre teknolojiyi çok daha iyi kullanabilen ve bu sayede daha fazla bilgiye ulaşabilen yeni bir nesille karşı karşıya olmamız. Bütün bunlar, suistimal ve yasa dışı faaliyetler konusunda bizleri yeni bir dönemin beklediğini işaret ediyor" diyor. Bu değişkenliğin farkına varabilen şirketlerin, kendilerini suistimale karşı daha iyi koruyabileceklerine ve suç faaliyetlerini uzun dönemlere yayan suistimalcileri tespit

2013 araştırmasında yer verdiğimiz 596 suistimalci arasındaki tipik suistimalci profilleri ile KPMG üye firmalarının iki yıl önce sonuçlarını bildirdiği araştırmalarda ortaya konan tipik suistimalci profili oldukça benzerdir.

edebileceklerine inanmaktayız. Pek çok suistimalci aslında suistimali göz göre göre gerçekleştirmektedir. Söz konusu suistimalciler, bazen arka planda, bazen kurum içinde önemli mevkilerde

<sup>1</sup> Who is the typical fraudster? - Bir Suistimalcinin Profili - KPMG Global Suistimal Modelleri Analizi, 2011

<sup>2</sup> Bir Suistimalcinin Profili Araştırması, 2007

<sup>3</sup> Görev tanımı üst düzey yönetim olarak da bilinir ve CEO'yu da kapsar.

yer almaktadırlar. İşledikleri suistimal suçunun türü ise, her zaman canlı ve hareket halindeki iş ortamı içinde sürekli değişim göstermektedir.

Sürekli olarak yeni suistimal teknikleri geliştirilmekte ve kurumlar bu duruma karşı savunma mekanizmalarını devamlı güncelleyerek karşılık vermek zorunda kalmaktadırlar. Ostwalt, "Şirketler öylece durup bugünün veya geleceğin suistimalcileriyle mücadele etmek için geçmiş dönemde kullandıkları kontrol mekanizmalarıyla yetinemezler," diyor. Elbette teknoloji, suistimalcilerin işini kolaylaştırdığı gibi kuruluşların kendilerini savunmasını da kolaylaştırmaktadır. KPMG Hong Kong Suistimal Önleme ve İnceleme Hizmetleri Bölüm Ortağı Grant Jamieson, "Şirketler geçmiş dönemde kullanılan suistimalle mücadele yöntemlerinin günümüzde işe yarayıp yaramadığını bir kez daha düşünmek zorundalar. Veri analizi ve veri madenciliği gibi yeni yaklaşımlar şirketin suistimalciyi yakalayabilme şansını oldukça artırıyor" diyor.

Üye firmaların 2011 raporundan bu yana küresel alanda soruşturmasını gerçekleştirdiği suistimal vakaları; değişen suistimalci profiline ilişkin analizimiz; değişen suistimalci profilinin, suistimalcinin yaşadığı ortam ve işlediği suçlar ile olan ilişkisi; suistimalcileri nasıl tanıyabileceğiniz ve bunların gelecekte sergileyebileceği davranışlar ile ilgili görüşlerimiz hakkında daha fazla bilgi edinmek için lütfen raporumuzu okumaya devam edin.

#### **KPMG üye firmalarının araştırdığı 596 suistimalci profil analizinden yola çıkarak suistimalcilerin bazı temel özelliklerinin aşağıdaki gibi olduğunu söyleyebiliriz:**

- Yaş: Suistimalcilerin %70'i 36 - 55 yaş aralığındadır.
- İstihdam: Suistimalcilerin %61'i bizzat suistimali gerçekleştirdikleri mağdur şirket tarafından işe alınmıştır. Bunların %41'i ise söz konusu şirkette 6 yıldan uzun süredir çalışmaktadır.
- İş birliği: Suistimal faaliyetlerinin %70'inde suistimalci başkalarıyla işbirliği yapmaktadır.
- Tür: En sık görülen suistimal türü, varlıkların kötüye kullanılmasıdır (%56). Bunun %40'ını zimmetine para geçirme, %27'sini ise satın alma/tedarik suistimalleri oluşturmaktadır.
- En sık görülen ikinci suistimal türü ise hileli veya yasadışı faaliyetlerle kazanılan varlıklar veya gelirlerdir (%24).
- Suistimalcinin suistimali tek başına gerçekleştirdiği vakaların %69'u 1 ila 5 yıl arasında sürmüştür. Bu suçların %21'i, mağdur şirkete toplam 50.000 \$ ila 200.000 \$ arasında bir tutarda zarar verirken, %16'sı 200.000 \$ ila 500.000 \$ arasında zarar vermiştir. Bu vakaların %32'sinde mağdur şirketin zararı 500.000 \$'ı, %9'unda ise 5.000.000 \$'ı aşmıştır.
- Suistimal başkalarıyla işbirliği halinde gerçekleştirilmişse, suçun %74'ü 1 - 5 yıl boyunca işlenmiş görünmektedir. İşlenen suistimal suçlarının toplam tutarlarına baktığımızda ise, %18'inin toplam 50.000 \$ - 200.000 \$ arasında olduğunu, %16'sının ise 5.000.000 \$'ı aştığını görmekteyiz. Bu vakaların %43'ünde mağdur şirketin zararı 500.000 \$'ı, %16'sında ise 5.000.000 \$'ı aşmıştır.
- Suistimal suçlarının %93'ü birden fazla işlemle gerçekleştirilmiştir. Bunların %42'sinde, her bir işlemin ortalama tutarı 1.000 \$ ile 50.000 \$ arasında değişmiştir.
- Tüm suistimal suçlarının %72'si 1 ila 5 yıllık bir dönem boyunca işlenmiştir (%33'ü 1-2 yıl, %39'u ise 3-5 yıl boyunca).

## Metodoloji

KPMG, Ağustos 2011 - Şubat 2013 arasında Avrupa, Ortadoğu ve Afrika (EMEA), Amerika Kıtası Ülkeleri ve Asya Pasifik bölgesinde KPMG üye firmaları Suistimal Önleme ve İnceleme uzmanlarının gerçekleştirdikleri suistimal soruşturmasına ait verileri söz konusu uzmanlar ile anket yapma yolu ile elde etmiştir. 78 ülkede suça karışmış toplam 596 suistimalci incelenmiştir. Anket çalışmasında, KPMG Suistimal Önleme ve İnceleme uzmanlarından 42'siyle gerçekleştirilen görüşmelerden elde edilen bu üç bölgede gerçekleştirilmiş, hem suçluyu tespit edebildiğimiz hem de suistimal ile ilgili bağlamsal bilgi edinebildiğimiz "beyaz yaka" suçlarına ilişkin soruşturmalar incelenmiştir.

Gerçekleştirilen incelemede ortaya çıkanlar:

- Suistimalci profilleri ve en yaygın görülen suistimal türleriyle ilgili detaylar,

- Kişiyi suistimale iten çevresel koşullar,
- Suistimalcinin kabiliyetinin suistimale etkisi,
- KPMG'nin faaliyet gösterdiği ülkelerde suistimalcinin eğilim gösterdiği alanlardır.

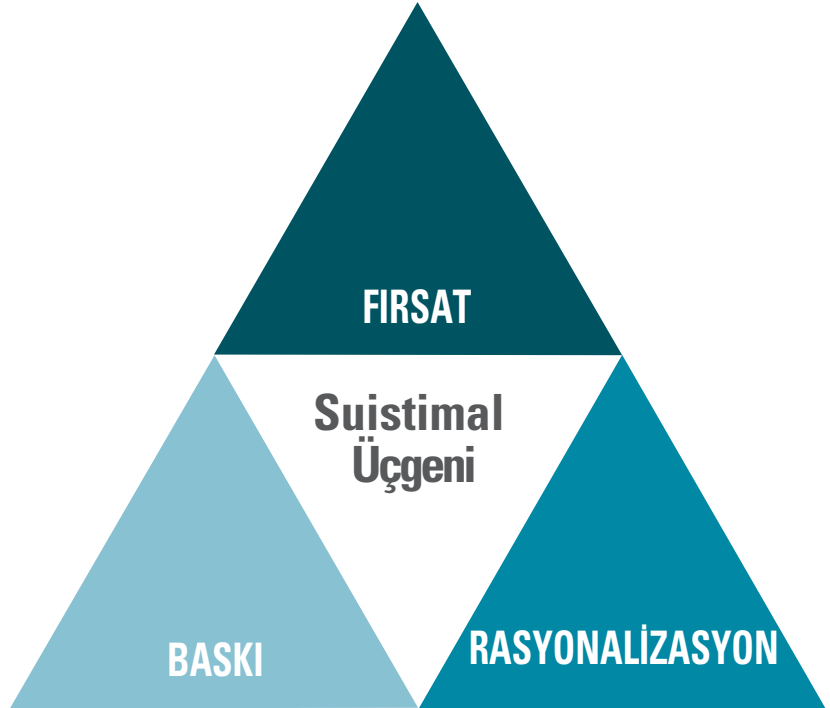
Genel olarak suistimal yapılarındaki değişimleri ortaya koyabilmek ve gelişen trendler hakkında fikir verebilmenin mümkün olduğu durumlarda bu raporda yer alan bulgular ile 2007 ve 2011 raporlarımızda yer alan bulgularımız arasında karşılaştırmalar yapılmıştır.

Gizliliğin korunması amacıyla, suistimal vakalarıyla ilgili hiçbir tarafın ismi bu raporda ifşa edilmemiştir. Burada bahsi geçen vakaların pek çoğu kamuoyuna yansımamış olup, yansımış olan vakalarda ise genellikle ayrıntılara yer verilmemiştir. Raporda geçen tüm tutarlar ABD Doları cinsinden yer almaktadır.



# Suistimal üçgeni

Bir suistimalcinin profilini anlayabilmek için öncelikle kişiyi suistimale yöneltebilecek unsurları ele almak gerekir; fırsat, baskı ve rasyonalizasyon. KPMG Çin Suistimal Önleme ve İnceleme Bölümü uzmanları, "İnsanlar, en uygun koşullar bir araya geldiğinde, yani gerekli motivasyona ve fırsata sahip olduklarında ve gerçekleştirecekleri suistimali rasyonelleştirebildikleri zaman suç işlemektedirler. Hemen her vakada, suistimalin gerçekleşme nedeni ve bazı insanların neden bir suistimalciye dönüştüğünü bu şekilde açıklayabiliyoruz." diyorlar. Bu üç unsur, suistimal soruşturma uzmanları için 1950'lerde geliştirilmiş olan standart metodolojinin bir parçasıdır. Suistimalci hakkında daha ayrıntılı bir resme sahip olabilmek için fırsat unsurunun bir bileşeni olarak "kapasite" 'yi de bunlara ekleyebiliriz. Resmi anlayabilmenin bir yolu olarak: Potansiyel suistimalci, "fırsat" yönünde açılmış bir kapı olduğunu fark eder. "Baskı" ve "rasyonalizasyon" unsurları potansiyel suistimalciyi kapının eşiğine getirir, "kapasite" ise onu kapıdan içeri sokar. <sup>4</sup>



<sup>4</sup> Bkz. "Beyond the fraud triangle - Suistimal üçgeninin ötesinde", Fraud Magazine, Eylül/Ekim 2011.



## Güçlü iç kontrollerin varlığı önemlidir, ancak unutulmamalıdır ki, tüm kontroller insan faktörü üzerine kuruludur.



**Niamh Lambe**

**KPMG İrlanda Suistimal Önleme ve İnceleme Bölüm Başkanı**

Şimdi bir insanı suç işlemeye teşvik eden bu üç unsuru sırasıyla inceleyelim:

### Fırsat

İnsanlar bir fırsatını bulmadıkları sürece suistimal gerçekleştirmezler. Araştırılan vakalardaki suistimalcilerin çoğunluğu, mağdur kurumda 6 yıldan uzun süredir çalışmakta olan kişilerdir ve suistimallerin yaklaşık 3/4'ü 1 - 5 yıl arasında bir dönem içerisinde gerçekleştirilmiştir. Bu durum, suistimalcilerin bir şirkette işe başlarken suistimal gerçekleştirme maksadı taşımadıklarını ancak değişen kişisel koşullar veya agresif iş hedefleri yüzünden suistimale yönelindiklerini göstermektedir. Ancak özel yaşamdaki değişiklikler veya agresif iş hedeflerine ulaşabilme baskısı kişileri suistimal yapmaya yönelten durumları da beraberinde getirmektedir. Bu kişiler suistimali, genellikle işlerinde rahat bir alana sahip olduklarında ve çalışma arkadaşlarının güven ve saygısını kazandıklarında gerçekleştirilmektedir.

Fırsat kendisini nasıl gösterir?

Araştırmaya göre, suistimallerin %54'ü zayıf iç kontrol mekanizmaları mevcut olduğunda gerçekleşmiştir. Bu durum, pek çok kurumun, çalışanlarını daha iyi

denetleyip kontrol edebildiği takdirde suistimal fırsatını önemli ölçüde ortadan kaldırdığını göstermektedir. Ancak şirketler genellikle şirkete özgü, güçlü kontrol mekanizmalarını kurarak suistimal önlemeye odaklanmamakta ve dersini çok geç almaktadır.

KPMG Kanada Suistimal Önleme ve İnceleme Bölümü Şirket Ortağı James McAuley, "Pek çok şirket suistimalle

mücadelede sigorta gibi proaktif yöntemleri tercih etmekte ve böyle bir olay hiç yaşanmayabilir de, neden bunun için para harcansın ki? şeklinde yaklaşmaktadır" yorumunda bulunmuştur. Çok basit kontrol mekanizmalarından bile yoksun olan kurumların

mevcut olduğu görülmektedir. KPMG İsveç Suistimal Önleme ve İnceleme Hizmetleri Bölümü ortaklarından Martin Krüger konuyla ilgili olarak, "Suistimal genellikle temel kontrol mekanizmalarının bulunmamasından kaynaklanır. Örneğin bazı araştırmalarımız, yöneticilerin bir işlemleri onaylamadan önce destekleyici belgelerin kontrolünü her zaman yapmadığını göstermiştir. Bunda İsveç'te yerleşik olan güven kültürünün de payı var," diyor. Ortadoğu'nun bazı bölgelerindeki kurumların pek çoğu

Şirket yönetimleri suistimali genellikle risk haritasındaki tek bir nokta olarak görmekte ve kendine has özelliklerini ve kapsamını her zaman kavrayamayabilmektedir.

### Fırsatçı

- Karakter özellikleri: ilk kez suçla karışmış, orta yaşlı, erkek, evli ve çocuklu, güvenilir personel, sorumluluk yüklenen bir konumda çalışan, iyi bir vatandaş
- Genellikle parayla çözülebilecek ve hiç kimseyle paylaşmadıkları, üzerlerinde baskı oluşturan sorunları vardır
- Vaka ortaya çıktığında, diğer insanlar, kişinin böyle bir suistimal gerçekleştirmesinden büyük şaşkınlık duyarlar

### Avcı

- Genellikle fırsatçı olarak başlar
- İş ararken işe başlar başlamaz ilk fırsatta entrika çevirebilecekleri özellikte olan şirketleri arayıp bulur,
- Kurumları kasten ve vicdan azabı duymadan dolandırır
- Fırsatçı suistimalciye göre daha organize ve daha iyi gizlenme planlarına sahiptir
- Denetçilerle ve diğer denetim mekanizmalarıyla başa çıkmaya daha hazırlıklıdır



suistimalin önlenmesinde kontrol mekanizmalarının önemini daha yeni yeni anlamaya başlamışlardır. KPMG Bahreyn ve Katar'da Sorumlu Direktör ve Suistimal Önleme ve İnceleme Hizmetleri Bölüm Başkanı olarak görev yapan Arindam Ghosh, "Pek çok özel kurum ve kamu kurumunun zayıf savunma mekanizmaları nedeniyle suistimale maruz kaldığını görmekteyiz. İç kontrol mekanizmaları ve suistimal risk yönetimi henüz iş hayatında kabul edilen kültüre yerleşmediyse de, bununla ilgili girişimler başladı," diyor.

Ancak güçlü iç kontrol mekanizmaları da bütün suistimalleri önlemeyecektir. Suistimalcilerin %20'si, kontrol mekanizmalarının varlığını bildikleri halde bunu hiç umursamadan suistimal gerçekleştirmiştir. %11'i ise, iç kontrolleri

atlatılmak için başkalarıyla işbirliği yapmışlardır. Bu tür vakalarda suistimalciler iç kontrolleri tanıyan ve bunları nasıl alt edeceğini bilen ya da iç kontrol noktalarındaki bazı açıkları şans eseri tespit ederek kötüye kullanan kişiler olabilmektedir. Hiçbir sistem tam anlamıyla suistimali önleyecek kadar güvenli değildir. İnsanların her zaman tetikte olması gerekmektedir. KPMG soruşturma uzmanları, kurumların iç ve dış ortamı sürekli izlemeleri gerektiğini, ancak çoğu kuruluşun bunu yapmadığını

gördüklerini belirtmektedirler. KPMG Avustralya Suistimal Önleme ve İnceleme Bölüm Şirket Ortağı Mark Leishman, "Şirket Yönetimi suistimali genellikle risk haritasındaki noktalardan biri olarak görmekte ve kendine has özelliklerini ve kapsamını her zaman kavrayamayabilmektedir. Bu da çoğu zaman riskin etkin bir şekilde yönetilmesi için gereken dikkat ve özenin gösterilmediği anlamına geliyor", diyor.

Özel hukuk veya kamu davası gibi yaptırımlar suistimalcilere karşı caydırıcı bir unsur olabilir, ancak pek çok şirket

olayın duyulmasını ve şirket itibarının zedelenmesini istemez. Suistimalcilerin sadece %7'si hapisle cezalandırılırken, açılan hukuk veya kamu davalarının oranı %35 olarak gerçekleşmiştir.

Suistimalcilerin %55'inin işlerinden atılması, bu kişilerin yeni girecekleri şirketlerde de suç işleyebilecek olması riskini doğuruyor. Bu nedenle yapılması gereken en önemli şey, iş yerindeki davranışları kontrol edecek düzenlemeler getirip bunları yürürlüğe sokmaktır. KPMG Singapur Suistimal Önleme ve İnceleme Bölümü Ortaklarından Lem Chin Kok, "Singapur'da diğer ülkelere göre yolsuzluk çok az görülen bir olgu, çünkü bu konuda yaptırımlar oldukça katı," diyor.

Singapur'da diğer ülkelere göre yolsuzluk çok az görülen bir olgu, çünkü bu konuda yaptırımlar oldukça katı ve iş hayatı şeffaf.

### Kapasite

Daha önce de bahsettiğimiz gibi, "kapasite" fırsat dürtüsünün bir altkümüsi olarak ortaya çıkmaktadır. Kapasite, suistimalcinin eline bir fırsat geçtiğinde bunu kötüye kullanmasını sağlayan özelliklerinden oluşur. Suistimalcilerin kişisel özellikleri ve suç işleyebilme becerisi bunların başında gelir.

Bu nedenle de, kapasite sıklıkla suistimalcinin kademine bağlıdır. Suistimalcilerin büyük bölümü, yönetim veya yetki sahibi pozisyonlarda görev yapmaktadır<sup>5</sup> (mağdur şirkette görev yapanların sırasıyla %25'i ve %29'u). KPMG Doğu Afrika Soruşturma Bölümü Başkanı Marion Barriskell şöyle diyor: "Önümüzdeki 3-5 yıl içinde, şirketlerin denetim mekanizmaları geliştikçe ve daha fazla sayıda suistimalci yargılanıp cezaya çarptırıldıkça Doğu Afrika bölgesindeki suistimalcilerin giderek daha tecrübeli ve şirket içinde daha kıdemli kişilerden oluşmaya başladığı görülebilecektir." Suistimalcinin şirket içindeki pozisyonu yükseldikçe, denetim mekanizmalarını aşma imkânı da o kadar fazla olacaktır. KPMG İsviçre Danışmanlık ve Suistimal Önleme ve İnceleme Hizmetleri Bölümü şirket ortağı Anne van Heerden, "Suistimalcilerin genellikle denetim mekanizmalarını etkisiz hale getirme çabasında olduğunu görüyoruz. Her ne kadar İsviçre'deki pek çok şirket standart iç kontrol mekanizmalarına sahipse de, suistimal yapma amacında olan bir kişi, şirkete girdikten 4 veya 5 yıl sonra bir suistimal fırsatı bulabiliyor" diyor.

<sup>5</sup> Daha önce de bahsettiğimiz gibi, KPMG ağırlıklı olarak yüksek kıdemdeki çalışanların gerçekleştirdikleri suistimalleri araştırmaktadır. Dolayısıyla bu bulgular tüm suistimalci profillerini kapsamayabilir ve suçların büyük kısmının alt düzey çalışanlar tarafından işlenmiş olma olasılığı vardır.

### Sektör bazında suistimal

Tüm sektörlerde suistimal, genellikle görevi kötüye kullanma fırsatının ortaya çıkmasıyla şekillenme eğilimindedir. Finansal hizmetler, ilaç, tüketici ve sanayi sektörlerinde yaygın görülen suistimal türünün, zimmet olduğu görülmüştür. Enerji ve doğal kaynaklar, kamu sektörü ve bilişim, iletişim ve eğlence sektörlerinde en yaygın görülen suistimal ise satın alma bölümlerinde gerçekleştirilir. En yüksek bedelli suistimallerin, suistimalci başına 5 milyon doların üzerinde bir tutarla finansal hizmetler sektöründe gerçekleştiği görülmüştür. Diğer sektörlerdeki tutarlar ise 200.000\$ - 500.000\$ aralığındadır. İlaç, finansal hizmetler, enerji ve doğal kaynaklar sektörlerinde görülen suistimaller, diğer sektörlere göre daha yaygındır. Diğer sektörlerle karşılaştırıldığında daha sıkı düzenlemelerin mevcut olduğu ilaç ve finansal hizmetler sektörlerinde suistimalin daha yaygın olması oldukça şaşırtıcıdır.

Diğer çalışanlarla işbirliği yapanlarda bu oran sırasıyla %24 ve %38'dir. Tüm suistimalcilerin %46'sı iyi bilgisayar kullanabilen kişilerdir. Bilgisayarlar, depoladıkları verilerin çokluğu nedeniyle suistimalciler için giderek artan önemli bir saldırı noktası haline gelmekte ve siber dolandırıcılık daha da yaygınlaşmaktadır. Kişisel özelliklere baktığımızda, toplumdan soyutlanmış, yalnız kişi profilinden çok, baskın özelliklerin hakim olduğunu görmekteyiz. Suistimalciler genellikle çevrelerinden büyük saygı gören (araştırılan tüm vakaların %39'u), cana yakın (%35) ve/veya dışa dönük (%33) kişilerdir.

### Baskı

Her suçta olduğu gibi suistimal için de bir motivasyon kaynağı gerekir ve 596 suistimalcinin hepsinde ağır basan baskı unsuru maddiyata yöneliktir. Araştırmada yer alan katılımcılara 14 baskı unsuru sunulmuş ve uygun olduğunu düşündükleri tüm seçenekleri belirtmeleri istenmiştir. 1082 baskı unsurunun 614'ü açgözlülük, maddi kazanç ve maddi zorlukla ilgili olup, 114'ü iş yaşamındaki hedeflerle ilgilidir. Maddi nedenlere dayanmayan tek baskı unsuru ise 106 vaka ile "sırf heves" veya bir başka ifadeyle "çünkü ben yapabilirim" düşüncesidir.

Yukarıda bahsedilen 614 baskı unsuru çok çeşitli maddi unsurları kapsamaktadır. Bunlardan biri, kişinin yaşam kalitesini artırma isteğidir. KPMG İsviçre Suistimal Önleme ve İnceleme Hizmetleri Başkanı Anne van Heerden, "İki yakasını bir araya getirmek amacıyla suistimal gerçekleştiren kişilerden çok, daha lüks veya en azından daha konforlu bir hayat sürebilmek için suistimal gerçekleştiren kişilerle karşılaşmaktayız." diyor. Diğer maddi nedenler arasında ise finansal

bir hedefi yakalayamama korkusu veya daha yüksek bir ikramiye kazanabilme hırsı yer alıyor. KPMG Orta ve Doğu Avrupa Suistimal Önleme ve İnceleme Hizmetleri Bölüm Başkanı Jimmy Helm, "Giderek artan sayıda yabancı şirket, yerel yöneticilere yüksek maaşlar vermek yerine performansa dayalı prim sistemine yöneliyor. Bu durum hedefleri tutturmak isteyen bazı yöneticilerin gelirleri olduğundan yüksek gösterme ve hatalı finansal raporlama gibi suistimal çeşitlerine başvurmalarına yol açıyor." diyor.

Soruşturma yapan pek çok yönetici, gelirlerin manipüle edilmesi şeklinde işlenen suçlarda artış olduğunu ve ekonomik durgunluğun bu durum üzerinde etkisi olduğunu belirtmektedir. KPMG Hollanda Suistimal Önleme ve İnceleme Hizmetleri Bölümü şirket ortağı Yvonne Vlasman, "Ekonomik baskılar nedeniyle pek çok şirket iflasla karşı karşıya kalıyor, finans kuruluşlarınca belirlenen katı hedeflere ulaşamıyor ve kendilerini büyüyen bir şirket gibi göstermek için bilançolarında veya gelirlerinde manipülasyon yapma yoluna gidiyor" diyor.

Açgözlülük, sanılanın aksine pek de etkin ve yaygın bir baskı unsuru değil. Suistimalcilerin sadece %18'i pahalı hobilere sahip ve sadece %17'si lüks otomobiller kullanıyor. Bu durum, suistimalci üst düzey bir yönetici olduğunda, ayırt edilmesi zor bir husus olarak karşımıza çıkmaktadır.

### Rasyonalizasyon

Suistimalciler de, diğer suçlular gibi genellikle işledikleri suç karşısında bir gerekçe uydurma eğilimindedirler. Korku ve öfke gibi duygusal dürtüler suistimalciler tarafından nadiren dile getirilmiştir. Korku ve öfke, 596 suistimalciden sadece %10'u için önemli birer dürtüdür. Suistimalin en

önemli nedenlerinden birinin maddi kazanç sağlamak olduğu düşünüldüğünde; "hak ettiği ücreti alamama"nın suistimalcilerin ileri sürdüğü nedenlerden sadece %16'sını oluşturuyor olması şaşırtıcı bir sonuç olarak karşımıza çıkmaktadır.

Tek önemli duygusal etken olan "üstünlük duygusu" ise, suistimalcilerin %36'sı için önemli bir neden olarak belirtilmektedir. Suistimal faaliyetlerinin %29'unun üst düzey yöneticiler (en yüksek oran) tarafından gerçekleştirilmiş olması, "üstünlük duygusu" ile ilişkilendirilebilir. Üst düzey yöneticilerin %44'ü güçlü bir "üstünlük duygusu" hissetmiş ve görünen o ki, oyunu diğer çalışanların davranışlarını düzenleyen şirket kurallarına uyarak oynamamışlardır.





KPMG üye firmaları soruşturma uzmanlarının gözlemlerine göre, suistimalin nedeni genel anlamda etik ve kültürel unsurlara göre şekillenmekte ve bunlar ülkeden ülkeye farklılık göstermektedir. Devletin getirdiği düzenlemeler ve kuralları uygulanması genellikle etik standartları güçlendirebilir. Bu durumda mahkemeye çıkarılan bir suistimalci, "benim ülkemde bu, kabul edilen bir davranış" diyerek, gerçekleştirdiği suistimali haklı gösteremeyecektir. KPMG Avusturya Suistimal Önleme ve İnceleme Hizmetleri Bölümü şirket ortağı Gert Weidinger, "10 yıl kadar önce Avrupa'nın bazı bölgelerindeki şirketler, yabancı ülkelerde verdikleri rüşveti, harcanması gereken bir gider olarak gösterip, indirimle konu yapabiliyorlardı. Ancak daha önceleri izin verilen ve

işin gerçekleştirilmesi için katlanılması gereken bir maliyet olarak görülen bu durum, artık yasadışı olarak kabul edilmeli; insanlar, alışkanlıklarını yasaları kendilerine uyduracak şekilde değil, kendileri yasalara uyacak şekilde değiştirmek zorunda olmalı" diyor.

Bazı Doğu Afrika ülkelerinde iş hayatı kuralları sıkılaştırılmakta, suistimal soruşturmasına daha fazla para harcanmakta ve görevi kötüye kullanmak giderek daha da kabul edilemez bir hal almaktadır. Barriskell, "Son zamanlarda, göreve gelen yeni hükümetler konuşma özgürlüğünü teşvik edip yasal düzenlemelere daha fazla yatırım yapmaya başladıkça, suistimal gibi suçlara gösterilen toleransın giderek azaldığını

görmekteyiz. Suistimale karşı olan bakış açısı, toplumun tabanından iş dünyasına ve hükümetlere kadar değişim göstermekte ve suistimal kabul edilemez bir davranış haline gelmektedir. Özetle, belli bölgelere özgü yolsuzluk penceresi yavaş yavaş kapanıyor." diyor. Vietnam'da da daha güçlü yaptırımların yürürlüğe girmeye başladığı görülmektedir. KPMG Vietnam ve Kamboçya Başkanı John Ditty, "Satın alma bölümlerinde rüşvet ve komisyon oldukça yaygın ve bu durum, adeta Vietnam'da iş yapmanın doğal bir parçası olarak görülüyor ve genellikle suistimal veya hırsızlıkla karşılaştırıldığında daha zararsız olduğu düşünülüyor. Ancak, suistimalin önlenmesine yönelik çabaların artmasıyla birlikte önümüzdeki 3-5 yıl içinde bu konuda somut sonuçlar alınacağını umuyoruz" diyor.

# Yaradılış ile yetiştirilme karşılaştırması

## Kişisel ve çevresel etkenlerin suistimale olan eğilim üzerindeki etkileri

Suistimale yönelik davranışların gerçekleştirilmesinde, kişisel etkenlerin mi yoksa çevresel etkenlerin mi daha güçlü bir belirleyici olduğunu anlamak çok önemlidir. Bu noktadan yola çıkılarak suistimal suçlarının nasıl daha etkili soruşturulabileceği ve bununla ilgili risklerin nasıl daha etkin yönetilebileceği belirlenebilir. Kişisel etkenler baskınsa, suistimal soruşturularında (ve suistimal risk yönetiminde) suistimalcinin kişiliğine odaklanılmaktadır. Çevresel etkenler baskınsa, bir suistimalin nasıl gerçekleştirildiğini tespit etmede kişinin yetiştirildiği çevresel koşullar dikkate alınır.

KPMG üye firmaları tarafından yürütülen araştırmalardaki suistimal vakalarından rüşvet suçu içerenler ayrı tutulmuştur. Suistimal gerçekleştirilirken gösterilen davranış değişiklikleri suistimalcinin profilinin anlaşılmasında, suistimalcinin davranış biçimlerini göstermek suretiyle yardımcı olan işaretler sunmaktadır. Rüşvet suçunun analiz edilmesinde ise gözlemler üç temel unsur altında gruplandırılmış ve fırsatın bir alt kümesi olarak kapasite de dikkate alınmıştır (fırsat, baskı, rasyonalizasyon ve kapasite; bunlardan ilk ikisi çevresel etkenler, diğer ikisi ise kişisel özelliklerdir).

Rüşvet veren 198 suistimalcinin %53'ü suistimal sırasında zayıf iç kontrol mekanizmalarından yararlanmış. Ancak iç kontrolün, bir kişinin rüşvet suçuna karışıp karışmayacağına etki eden çok güçlü bir etken olmadığı görülmüştür. Zira rüşvet, en az iki kişiyi kapsar ve bunlardan en az biri büyük olasılıkla iç kontrol mekanizmalarının uygulanmadığı kurumlarda görev yapmaktadır. Kurumların küreselleşmesi sonucunda, farklı bölgelerde yer alan ofislerde gerçekleştirilen faaliyetlerin izlenmesi gittikçe zorlaşmıştır. KPMG Birleşik Krallık Suistimal Önleme ve İnceleme Hizmetleri Bölüm Başkanı Alex Plavsic şöyle diyor: "Birleşik Krallık'taki rüşvet ve yolsuzluk soruşturularının %60'ından fazlası başka ülkelerin yetki alanlarına giren sorunlarla ilgili. Buradan diğer ülkelerde yolsuzluğun daha yaygın veya seyrek olduğu sonucu çıkarılmamalı. Gerçek şu ki; özellikle çalışanlar üzerindeki hedeflere ulaşma baskısı dikkate alındığında, genel merkezden uzaklaştıkça verilen mesajların etkisi azalacaktır."

Suçla ilişkin bir başka etken de, suistimalcinin çalışmakta olduğu otoritenin yapısı. Suistimalcinin sahip olduğu yetki derecesini belirleyebildiğimiz 130 suistimal vakasının %62'sinde, suistimalcinin (sözleşme imzalama yetkisi, ödeme yapma yetkisi vb.) sınırsız bir yetkiye sahip

olduğu gözlemlenmiştir. Helm, "Orta ve Doğu Avrupa'daki pek çok suistimal soruşturmasında karşılaştığımız suistimalci profilinin, şirkette 4 yıldan uzun bir süredir çalışmakta olan ve hem sistemi hem de sistemin zayıf yönlerini bilen üst düzey yönetici veya idari yetkiye sahip yönetici profili olduğunu görmekteyiz. Değişen tek şey ise başkalarıyla yapılan işbirliğinin ve umursamazlığın giderek artması," diyor.

Bu bağlamda, sınırsız yetki, (sadece suçun işlendiği etki alanının yönetimi konusunda olsa bile) iç kontrol mekanizmalarının eksikliğini ortaya koymaktadır. KPMG firmalarının araştırdığı sınırsız yetkinin söz konusu olduğu 214 suistimal vakasının %61'inde, suistimalin daha zayıf düzenlemelere tabi ortamlarda gerçekleştiği görülmüştür. Dolayısıyla denetim ve kontrol mekanizmalarının çevresel içerikleri, yukarıda bahsettiğimiz dört kategoriden üçünün (fırsat, baskı, rasyonalizasyon) merkezini oluşturmaktadır. KPMG Yunanistan Suistimal Önleme ve İnceleme Hizmetleri Bölüm Başkanı Christian Thomas, "Suistimalin en yaygın olarak görüldüğü şirketler, küçük aile işletmeleridir, çünkü bu şirketler kendilerini suistimale karşı koruyacak denetim mekanizmalarından yoksundur. Oysa bu şirketler Yunanistan ekonomisinin temelini oluşturmaktadır," diyor.



Sonuç olarak, diğer ülkelerde gerçekleşen suistimallerin tespit ve incelemesini yapmak oldukça zorlu bir süreçtir. Birçok şirket için dünyanın öbür ucuna gidip yerel çevrede oluşan riskleri belirlemek zordur.



**Phil Ostwalt**

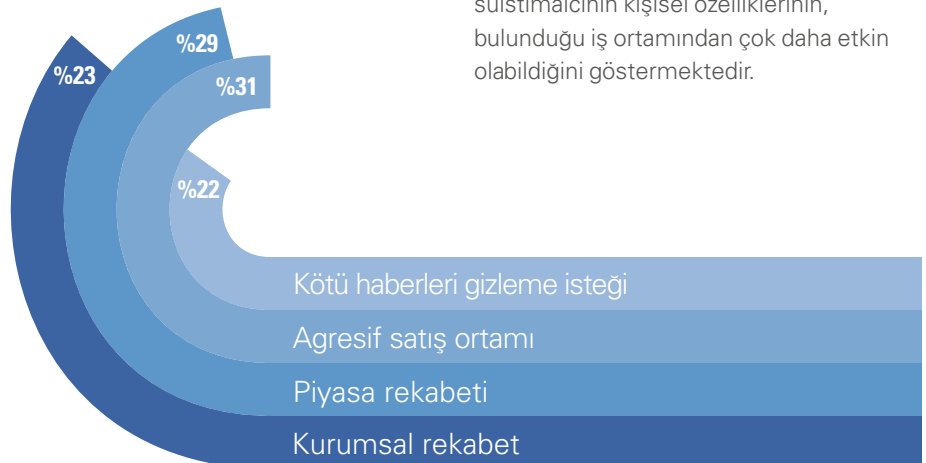
**KPMG Küresel Suistimal Önleme ve İnceleme Bölümü Koordinatörü**

Dört önemli etken; yani kurumsal rekabet (çalışanlar arasındaki rekabet), piyasa rekabeti (şirketler arasındaki rekabet), agresif satış kültürü ve suistimalcinin kötü haberleri gizleme isteği (kısmen çevresel etkenler, ancak suçlunun kişisel özellikleriyle daha ilişkili) olduğuna inanmaktayız. Bir suistimalci bu çevresel etkenlere vereceği karşılığı (en yüksek satış primini kazanmak için rakipleri saf dışı bırakmaya çalışmak gibi) kendisi belirlemektedir. Belirli vakalarda, “herkes yapıyor” düşüncesi de suistimali körükleyebilir. KPMG Arjantin Suistimal Önleme ve İnceleme Hizmetleri Bölümü Kıdemli Müdürü Raul Saccani, “Yapılan bir KPMG araştırması<sup>6</sup>, hemen her şirketin; iş almak amacıyla rakiplerin mutlaka etik ilkeleri ihlâl ettiği düşüncesinde olduklarını gösterdi,” diyor.

Bununla birlikte, sadece bu verilerden yola çıkarak bahsi geçen dört etkenden herhangi birinin kesin olarak suistimale karışan 198 suistimalci için harekete geçirici bir etken veya baskı kaynağı olduğunu söyleyemeyiz. Bu etkenlerin görülme sıklıkları Şekil 1’de verilmiştir:

Araştırmamızın sonuçları, bir suistimal suçunun işlenmesinde baskı ile ilgili etkenlerin, fırsat ile ilgili etkenlere göre daha zayıf bir etkisi olduğunu ortaya koymaktadır. Örneğin bir suistimalci şirketi dolandırmak için işbirliği yapabileceği kişiler arıyorsa, şirket görevlilerine rüşvet vermek zorunda kalabilir. Bir başka ifadeyle, suistimalciler amaçladıkları suçu işleyebilmek için bir fırsat yakaladıklarında bunu değerlendirmişlerdir. Bu durum, ihtiyaç veya baskı unsuru ile ilgili bir husus değildir, suistimalin gerçekleştirilmesinde, suistimalcinin kişisel özelliklerinin, bulunduğu iş ortamından çok daha etkin olabildiğini göstermektedir.

**Şekil 1**



<sup>6</sup> KPMG Latin Amerika Kurumsal Suistimal Raporu 2008-10 (2011’de yayımlandı)

### Kişilik Özellikleri ve Kapasite

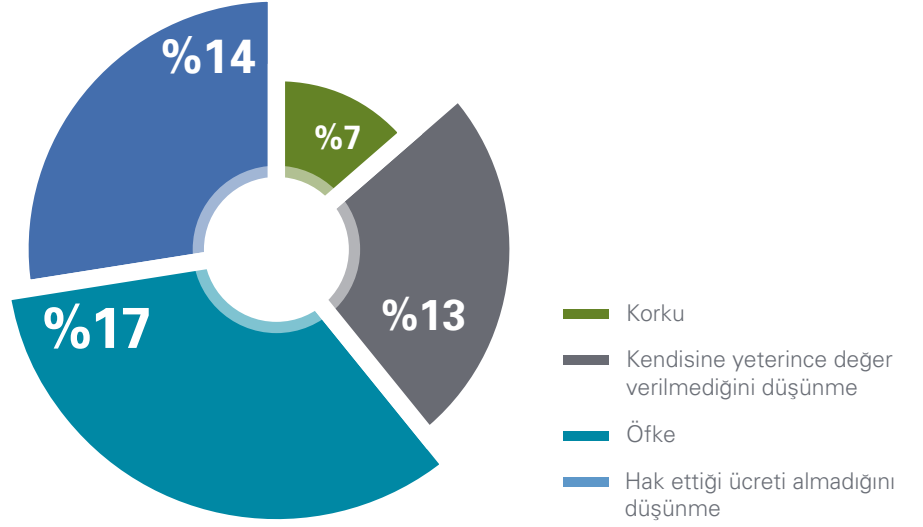
Şimdi de suistimalcinin kişilik özelliklerini ve kapasitesini inceleyelim. Öncelikle, gerçekleştirilen suistimallere yönelik öne sürülen gerekçelere ilişkin etkenleri değerlendirdik ve duygusal etkenlerin (öfke, korku ve intikam alma duygusu gibi) suistimalcinin eyleminin bir gerekçesi olarak nadiren dile getirdiğini gördük. Duygusal etkenlerin bazıları Şekil2’de gösterilmiştir.

Araştırdığımız vakalardaki suistimalcilerin kişisel özellikleri ve kapasiteleri ile ilgili olarak öncelikle kişiliklerine ve durumlarına ilişkin gözlemler gruplandırılmıştır.

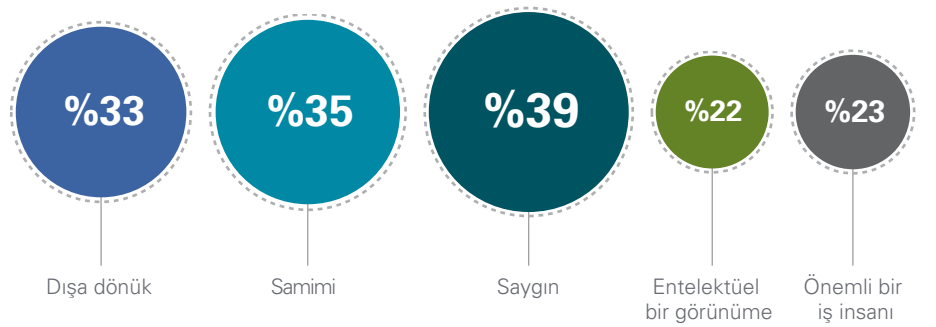
Suistimalcilerin büyük bir kısmının dışa dönük, samimi, saygın gibi kişisel özelliklere sahip kişilerden oluştuğu düşünüldüğünde, sadece bu özelliklerden yola çıkarak yolsuzluk yapmaya eğilimi olan bir suistimalciyi tespit etmek güçleşmektedir. Üstelik 596 suistimalcinin büyük kısmı (%39) mesai arkadaşları tarafından büyük saygı gören kişilerden oluşmaktadır. Van Heerden, “Karşılaştığımız suistimalci profili genellikle finans bölümünde çalışan güvenilir bir yönetici veya personel. Bu tip suistimalciler, ifşa edildiğinde diğer insanlar büyük şaşkınlık yaşıyor ve bu davranışı, suistimali gerçekleştirmiş olan kişilerle bağdaştıramıyorlar,” diyor.

Ahlaksızlık biçimleri arasında yüksek seviyede yer alan aç gözlülük ve kişisel

Şekil 2



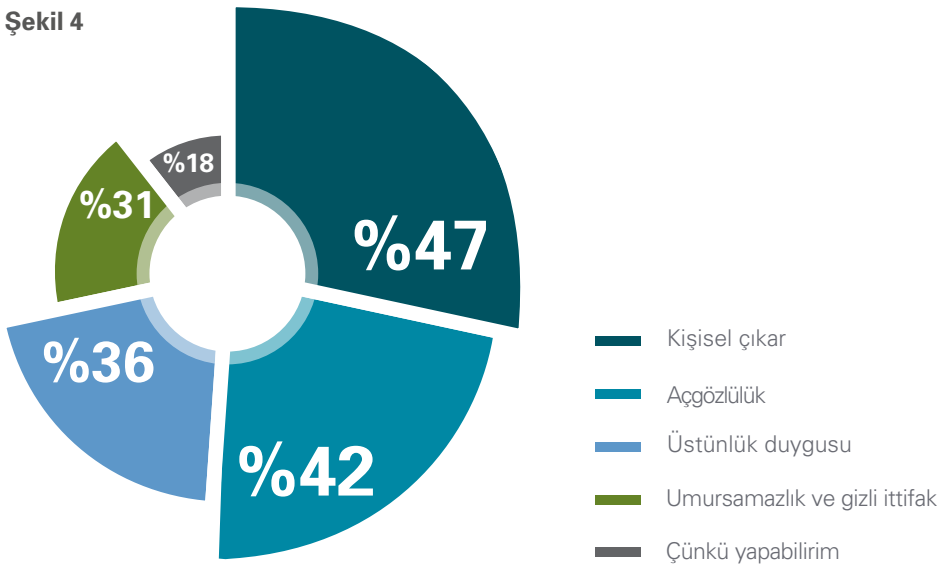
Şekil 3



çıkar, rüşveti de içeren vakalarda suistimalcileri bu suça iten en baskın iki kişisel özellik olarak karşımıza çıkmaktadır. KPMG üye firmaları tarafından araştırılan 596 suistimalcinin %47'sinde kişisel çıkarın, %42'sinde ise aç gözlülüğün baskın etkenler olduğu görülmektedir. Bu nedenle, iç kontrol ve yönetim mekanizmalarında bir zayıflama olduğunda, sıradan insanlar aç gözlülük ve kişisel çıkar gibi etkenlerin tuzağına düşebilmektedir. Böyle bir durumda, kişiler işleyecekleri suistimal suçuna

ahlak dışı davranışları da dâhil etmeye daha eğilimli olabilmektedirler. KPMG Malezya Suistimal Önleme ve İnceleme Hizmetleri Bölüm Başkanı Sukdev Singh, "İş dönüp dolaşıp suistimalin insanlarla, bu insanların istekleriyle ve bu istekler karşısında ne kadar dirençle karşılaştıklarıyla ilgili bir unsur olduğuna geliyor. Bu direnç de, insanların yaşam tarzıyla, kültürel olarak neyin kabul edilebilir olduğuyula ve şirketin savunma mekanizmalarının kalitesiyle alakalı," diyor.

Şekil 4



# Suistimalin değişen yüzü

## Şirketler kendilerini sürekli değişen suistimalci profiline uydurmak zorunda

Suistimal için tek bir kalıp olmadığı gibi suistimalcinin de sabit, hiç değişmeyen özellikler taşıdığı söylenemez. Suç ve suçun tanımı, suistimalin üç unsurunun önemine ve suistimalcinin kapasitesine bağlı olarak değişecektir ve suistimalin tespit edilmesini güçleştiren neden de genellikle bu değişimdir. KPMG Rusya ve BDT ("Bağımsız Devletler Topluluğu") Suistimal Önleme ve İnceleme Hizmetleri Bölüm Başkanı Nigel Layton, "Suistimali gerçekleştiren yalnızca tek tip bir suistimalci profili ile karşılaşmıyoruz; fırsat doğduğunda her tipte insanın suistimal gerçekleştirebileceğini görüyoruz" diyor. Lem de bir başka ifadeyle, "Tecrübelerimiz, suistimal için uygun tetikleyiciyle karşılaşınca insanların çoğunun suistimal gerçekleştirebileceğini gösteriyor" diyor.

İnsanların çoğunun suistimal gerçekleştirebileceği yönündeki tüyler ürperten bulgu göz önünde bulundurulduğunda; kurumların, suistimal suçlarını önlemeye yönelik oldukça güçlü çözümler üretmesi gerekmektedir. Ghosh, "Suistimalci profilinin yakın gelecekte radikal bir şekilde değişeceğine yönelik hiçbir gösterge yok. Suistimalci, o gün kimin fırsatı yakaladığına bağlı olarak herhangi biri olabilir. Bir şirketin suistimal riskini en aza indirebilmesinin yolu ise davranışları değiştirmeye yönelik çözümler üretmekten geçiyor" diyor. Suistimal profilindeki önemli değişimlerden biri de, sonraki bölümde de inceleyeceğimiz "gizli ittifak"tır.

### İşbirlikçiler, şirket içindekiler ve şirket dışındakiler

Bir işi tek başına yapmak genellikle güçtür. Pek çok suistimalci yalnız çalışmayı tercih eder, çünkü böylece diğerlerinin ağızını sıkı tutması konusunda endişelenmek zorunda kalmaz, ama suistimallerin büyük bölümünün gerçekleştirilebilmesi için işbirliğine ihtiyaç vardır. Suistimal genellikle insanın tek başına uygulamaya koyamayacağı kadar karmaşık bir suçtur; başkalarının da göz yumması, bazı şifreleri sunması veya belgeler üzerinde sahtecilik yapmasını gerektirir. KPMG profesyonellerinin bu rapor kapsamında araştırdığı 596 suistimalcinin %70'i başkalarıyla işbirliği içinde hareket etmiş, bunların %56'sında 2-5 kişi suça karışmıştır. Araştırılan suistimalcilerin 3/4'ünün ise bu suçta başrol oynadığı görülmüştür.

İşbirliği yapmanın kurum içi ve kurum dışı olmak üzere pek çok çeşidi vardır. Özellikle üçüncü şahısların işlediği suistimalleri ortaya çıkarmak çok zor olabilir. Layton, "Bir şirket adına rüşvet veren ve sonra

bunun karşılığında hizmetler için yasal faturalar kesen gümrük müşavirleri gibi acentalar veya üçüncü şahıslarla sıklıkla karşılaşmaktayız. Fatura yasal bir hizmetin bedeliymiş gibi düzenlendiği için suistimali tespit etmek zorlaşmaktadır." diyor.

Suistimalcinin başkalarıyla işbirliği yaptığı suçların %21'inde zimmet suçu görülmekte, suistimalcinin tek başına

hareket ettiği suçlarda ise bu oran %27 olmaktadır. Satın alma/ tedarik üzerine gerçekleştirilen suistimaler ise işbirliğinin yapıldığı en yaygın ikinci suistimal türüdür. İşbirliği içeren suistimalerin neden olduğu maddi zarar da daha fazladır. İşbirliği yapılan vakaların %33'ünün mağdur şirkete maliyeti 1 milyon \$'ı aşmıştır. Tek

**KPMG**  
profesyonellerinin  
bu rapor kapsamında  
araştırdığı 596  
suistimalcinin %70'i  
başkalarıyla işbirliği  
içinde hareket etmiş,  
bunların %56'sında  
2-5 kişi suça  
karışmıştır. Araştırılan  
suistimalcilerin  
3/4'ünün ise bu  
suçta başrol oynadığı  
görülmüştür.

başına işlenen suçların ise %24'ünde mağdur şirketin zararı 1 milyon \$'ın üzerinde olmuştur.

İşbirliği, yükselen bir trend olarak karşımıza çıkmaktadır. 2007 araştırmasında %32 olan



işbirliği içeren vaka oranı 2011’de %61’e, 2013’te ise %70’e yükselmiştir. Bölgesel bazda bakıldığında ise, resim bu kadar net olmamaktadır. İşbirliği içeren suçların oranı 2011 - 2013 yılları arasında EMA ve Asya Pasifik bölgelerinde artarken, Amerika Kıtası ülkelerinde bir artış görülmemiştir. İş ilişkilerinin genellikle sosyal ilişkilere dayalı olarak yürütüldüğü Afrika ve Asya’nın bazı bölgelerinde yer alan ülkelerde işbirliğinin daha yaygın olduğu görülmektedir. Ancak daha ataerkil bölgelerde, suistimal suçunun genellikle astlarına yasadışı işlem yapma talimatı veren kıdemli personel tarafından gerçekleştirilmekte olduğu görülmektedir. Jamieson, “İnsanlar bazen kişisel fayda için değil, kendilerine verilen talimat gereği suistimal gerçekleştirmektedirler” diyor.

#### **Şirket içi ve şirket dışı işbirlikçiler**

Önemli bir işbirliği biçimi de şirket içi ve şirket dışı tarafların arasındaki ittifaklardır ve bunlar özellikle faturaların şişirilmesi gibi satın alma/tedarik üzerine gerçekleştirilen suistimaller şeklinde ortaya çıkmaktadır. Pek çok şirket, tedarikçilerine ve kurumsal müşterilerine yönelik gerekli olan durum değerlendirmelerini gerçekleştirmemektedir<sup>7</sup>. Plavsic, “Günümüzde kullanılan tek savunma mekanizması, birlikte iş yapılan veya kendisi aracılığıyla iş ilişkisinde bulunan insanların güvenilir olup olmadığını sormak” diyor. Suistimallerin %43’ünde hem şirket içi hem de şirket dışı kişilerle işbirliği yapılmış, bir başka %19’luk kısımda ise şirket içinden sadece bir kişiyle ve

şirket dışından bir ya da birkaç kişiyle işbirliği yapıldığı görülmüştür. KPMG üye firmalarının soruşturma uzmanları, şirket içindekiler ile şirket dışındakilerin işbirliği yaptığı vakaların çoğunda liderliği savunma mekanizmalarını iyi bilmesi nedeniyle ve fırsatları daha kolay tespit edebilmesinden ötürü şirket içindeki kişinin üstlendiğini söylemektedir. Gerçekten de suistimalcilerin %42’sinden fazlasının mağdur şirkette 6 yıldan uzun bir süredir çalışmakta olduğu görülmüştür.

İşbirliği vakalarının ortak unsuru yolsuzluktur; vakaların %29’unun rüşvet içerdiği tespit edilmiştir (kişi yalnız hareket ettiğinde gerçekleşmemektedir). Ortaya çıkarma şekillerinde de birtakım farklılıklar görülmektedir. Tek başına işlenen suçlar ağırlıklı olarak yönetimin yaptığı incelemelerde (%27) veya tesadüfen (%25) ortaya çıkarılmıştır. İşbirliği içeren suçlarda en yaygın tespit yöntemi gayriresmi yollardan anonim bildirimler (%22) ile resmi bildirimlerdir (%19).

Bilişim sektöründe gerçekleştirilen suistimaller daha da önemli hale gelmeye başladığında şirket dışındakilerin hakimiyetinin gelişim gösterdiği de görülmeye başlanacaktır. Teoride,

kurumların savunma mekanizmalarındaki zayıf noktaları arayan bilişim korsanlarının sayısı artacaktır, ancak bu kişiler şirketin içinden olduğu kadar şirket dışından kişiler de olabilecektir. KPMG Danimarka Risk Danışmanlığı ve Suistimal Önleme ve İnceleme Hizmetleri Bölüm Başkanı Torben Lange, “Suistimal fırsatlarından yararlanan çalışan ve yöneticilerin, gelecekte de şirketleri tehdit

**İşbirliği içeren suistimallerin neden olduğu maddi zarar, diğer suistimal türlerinin neden olduğu zarardan daha fazladır. İşbirliği yapılan vakaların %33’ünün mağdur şirkete maliyeti 1 milyon doları aşmıştır. Tek başına işlenen suçların ise %24’ünde mağdur şirketin zararı 1 milyon doların üzerinde olmuştur.**

etmeye devam edeceğini düşünüyoruz. Ancak kurumlar, ister tek başına hareket eden şirket dışı bilişim korsanları ister üçüncü şahıslarla işbirliği yapan şirket çalışanları olsun, dış unsurların daha yoğun tehdidi altında olacaktır” diyor. Şimdi de teknolojinin suistimal üzerinde gelişen rolünü inceleyeceğiz.

<sup>7</sup> Üçüncü Şahıs Risk Yönetimi: İş ortaklarınızın size verebileceği zararlar hakkında bilmedikleriniz, KPMG, 2013.

# Siber alanda yaşananlar

## Yeni teknoloji, yepyeni suistimal davranışlarını da beraberinde getirdi

Son zamanlarda "siber güvenlik" terimi iş dünyasında, insanı korkutacak bir hızla yaygınlaştı. Terimin bu kadar popülerite kazanmasındaki önemli bir neden de; hükümetlerin başka hükümetler tarafından geliştirilecek nükleer silahları engellemesi ve buna benzer stratejik faaliyetleri geliştirilmesi yönünde çıkan haberler olmuştur. Oysa şirketlerin, çoğu haber konusu yapılmayan siber saldırılar karşısındaki savunmasızlığı giderek artmaktadır. Vlasman, "Siber saldırılar ve yüksek teknoloji suistimalleri konusunda en fazla endişe veren nokta, suçluların sistemlere çok kolay erişim sağlayabilmeleridir. Ancak pek çok şirket bu durumu fark edemiyor bile" diyor.

Kuruluşlar (şirketler veya başka kurumlar), bilişim korsanlarının kullandıkları, her geçen gün daha fazla gelişmekte olan bu teknolojilere ayak uydurmakta zorlanıyorlar. Ostwalt, "Bazı sektörler bilişim suçlarına karşı diğerlerine göre daha hazırlıklı olsa da bazı şirketler, kamuoyuna da yansımış siber saldırılara maruz kalmış olmalarına rağmen, gelecekte uğrayabilecekleri saldırılara karşı daha iyi tedbirler geliştirmemektedir. Söz konusu şirketler, bu riskle proaktif olarak nasıl baş edilmesi gerektiği konusunda sıkıntılar yaşamaktadır" diyor.

Birkaç yıl önce, bilişim korsanları siyasi amaçla harekete geçerek ideolojik bir konuya parmak basmak maksadıyla bilgisayar ağlarını çöktürdüler. Kuruluşlar kendilerini savunmak için gereken

adımları atmazlarsa, suistimalciler hem kendilerinin hem de suç örgütlerinin kabiliyetlerini geliştirmek için teknolojinin tüm imkânlarıyla donanmaları kaçınılmaz olacaktır. KPMG Türkiye Risk Yönetimi Danışmanlığı Başkanı İdil Gürdil, "Bilgisayarlar ve ağ teknolojileri, beyaz yakalı suçluların daha etkin bir şekilde ve daha az riskle çalışmalarına olanak tanıyor; bu sayede erişim kolaylaşıyor ve yeni nesil suistimalcinin önündeki engeller azalıyor" diyor.

### Mevcut büyüme

Bu noktada, tespit edilen bilişim suçlarının ölçeği<sup>8</sup> küçük görünmektedir. Analiz ettiğimiz bilişim saldırılarının büyük bölümü bilgisayar sistemlerine kötü amaçlı yazılım gönderilmesi, bilgisayar ağlarına saldırı vb. yöntemlerle gerçekleştirilmiştir. Zayıf iç kontrol mekanizmaları genellikle hileli finansal raporlama ve varlıkların kötüye kullanımını da içeren suistimal faaliyetlerini kolaylaştırmıştır. Suistimalcilerin çoğunun mağdur şirketin başta bilgi teknolojileri ("BT"), finans ve operasyon bölümlerinde çalışan kişilerden oluştuğu söylenebilir. Bu kişiler, personel kademesinden kıdemli üst düzey yöneticilere kadar değişen pozisyonlarda görev yapan, 18 - 55 yaş arasında ve şirkette 1-6 yıldan beri çalışmakta olan kişilerdir. Pek çok vakada başkalarıyla işbirliği yapılmış ve işbirliği yapılan kişilerin büyük bölümünün de mağdur şirkette çalışan diğer kişilerden oluştuğu görülmüştür.

Üye firma soruşturma uzmanlarıyla yapılan görüşmeler, bilişim suçlarının kurumlar için hızla büyüyen bir sorun haline geleceğini ve eskiye göre çok daha geniş bir coğrafi ölçeğe sahip olacağını ortaya koymaktadır. Lem, "Bilişim suçlarında artış var ve hem siber saldırıların hem de yüksek teknoloji kullanılarak gerçekleştirilen suistimal faaliyetlerinin katlanarak artmasını bekliyoruz" diyor.

Bilişim suçlarına karşı savunmanın en etkin yöntemlerinden biri, bilişim korsanlarını tespit ederek şirketin altyapısına zarar vermelerini veya şirket bilgilerini çalmalarını önleyecek güçlü BT sistemleri geliştirmektir. KPMG İtalya Suistimal Önleme ve İnceleme Bölümü Şirket Ortağı Pasquale Soccio, "Diğer ülkelerde olduğu gibi İtalya'da da siber saldırılarda çok büyük bir artış görülmekte," diyor. "Teknolojiye bel bağlamış günümüz iş dünyasında, şirketlerin kendilerini şirket içi saldırılar dâhil, her türlü saldırıya karşı koruyacak sağlam bir BT güvenliği sistemine sahip olmaması çok ciddi sorunlara sahip olduğu anlamına geliyor. Güçlü bir BT güvenliği sistemi, şirket faaliyetlerinin gerçekleştirilmesinin ön şartlarından biridir. "Oysa pek çok şirket, savunma mekanizmaları oluşturma konusunda oldukça yavaş ilerliyor. KPMG Tayvan Suistimal Önleme ve İnceleme Hizmetleri Direktörü Rex Chu, "Pek çok şirket, sistemdeki olağandışı işlemler için

<sup>8</sup> Siber dolandırıcılığın genel kabul görmüş bir tanımı yoktur. Suistimalciler işledikleri suçu kolaylaştırmak için yıllardır bilgisayarlardan faydalanmaktadır. Yani bu "bilgisayar destekli" bir suistimal türüdür. Siber suçlar suistimalcinin son derece ileri seviye teknolojik konuları suistimalci profiline eklemesi açısından yeni bir dönemi başlatmıştır.



Birçok şirketin mevcut çeşitli sistemleri vardır, ancak bu sistemlere sızma için bir iki küçük hata yeterli olmakta ve böylece yıllarca emek verilen inovasyon çalışmaları bir rakibin eline geçebilmektedir. Bu şekilde kaçırılan fırsatları engellemenin paha biçilmez olduğu söylenebilir.



**Alex Plavsic**

**KPMG Birleşik Krallık Suistimal Önleme İnceleme Hizmetleri Bölümü Başkanı**

önceden haber verebilecek yeterlilikte uyarı mekanizmaları oluşturamamakta, bu durum olağandışı faaliyetlerin tespit edilip izlenmesini güçleştirmektedir” diyor.

Suistimalin tespit edilebilmesinin 3 ila 5 yıl sürdüğü ve bilişim suçlarının yeni yeni gündeme geldiği göz önünde bulundurulduğunda, siber suçların istatistiklerimizde önemli bir yer bulması biraz zaman alabilecektir. KPMG Bermuda Başkanı Charles Thresh, “Yapılan araştırmalarda off-shore piyasalarda henüz yüksek düzeyde teknoloji içerikli suç veya organize siber suçlar görülme de, küresel trend bu durumun yakın zamanda gündeme geleceğine işaret ediyor” diyor. “Mobil teknolojilerin kara para aklama yöntemlerinin değişmesinde de etkili olacağını tahmin ediyoruz.” Tüm bunlar, bir siber dolandırıcı profili oluşturulmasını zorlaştırmaktadır. Tipik bir bilişim korsanı 20’li yaşlarında olabilir, ancak bilgisayar ağlarına sızmada uzman, şirket içi suistimalcilerin bu yaşta olması bir anlam ifade etmeyebilir. Siber dolandırıcıların yaş ortalamasının diğer suistimalci türlerine göre daha düşük olması mümkündür. Ayrıca üst düzey yöneticilerin şirket dışından genç yaştaki bilişim korsanlarıyla işbirliği yaptıkları da görülebilmektedir.

Oswalt “Sonuç olarak yarının suistimalcisi o günün fırsatlarına bağımlı olacaktır” diyor. Bundan yirmi yıl kadar önce, örneğin bir bankadan yasa dışı yolla para almak için küçük de olsa bir çete kurmak ve bazen şiddet ya da zorla senet

imzalatma gibi yollara başvurmak tercih edilirdi. Günümüzdeki banka soyma fırsatları ise artık internet, akıllı aygıtlar ve çok büyük miktarda veriyi analiz edebilme yeteneği sayesinde şekil değiştirmiştir.

Gelecekte de suistimal gerçekleştirmek için bazı durumlarda insanların işbirliği yapması gerekecek, ancak kullandıkları teknolojik araçlar değişim gösterebilecektir. Üstelik böyle bir grupta bir kalpazana değil, e-posta şifrelerini ele geçirebilen birine ihtiyaç duyulacaktır. Ya da çalıntı bir çeki bozdurmak için veznedarı kandırabilecek ikna yeteneği güçlü birine değil, korumalı bir bilgisayar ağına sızabilen bir bilişim korsanına ihtiyaç duyulacaktır. Belki kişisel özellikler ve duygular artık suistimalci profilinin bir parçası olmayacak, mağdur kuruluşun siber dolandırıcı hakkında bildiği tek şey; elektronik donanım, imzalar ve bu yöndeki izler olacaktır. KPMG Avrupa, Ortadoğu ve Afrika Soruşturma Ağı Lideri Dean Friedman, “Gelecekteki suistimal vakalarının çözülmesinde başarı elde edecek olan soruşturma uzmanları, yığınla veriyi doğru teknolojik çözümler kullanarak yorumlayabilen, verilerin sorunsuz halde çalışmasını sağlayan ve bu verilere, tarihsel ve coğrafi erişime olanağı sunan gelişmiş kurumsal zekaya sahip kişiler olacaktır” diyor.

Bilişim suçu işleyenler, kurumların kullandığı koruma sistemlerinin tam kalbine saldırarak suçu işlemek için birbirlerinin aynısı olan şifre ve teknikleri kullanabilirler. KPMG İrlanda Suistimal Önleme ve İnceleme Hizmetleri

Bölüm Başkanı Direktör Niamh Lambe, “Teknolojinin neden olduğu en önemli değişim; şirketler tarafından fikri mülkiyetin korunamamasıdır. Şirketler bilgi işlem sistemlerinin gizli ve önemli bilgilerinin kaybedilmesine ne kadar açık olduğunun farkında değil gibiler” diyor. Bilgisayar ortamı, web tabanlı bilişim sistemleri ve internet, bilişim suçlarının her zamankinden daha kolay gizlenebilmesine olanak sağlamaktadır. Bu davranış biçimleri soruşturma uzmanlarının genelde karşılaştıkları davranış türlerinden oldukça farklıdır ve soruşturma uzmanlarının kendi yöntemlerini bu davranış türlerine uygun hale getirmeleri gerekir. Ancak bilişim suçları bile daha önce bahsettiğimiz suistimalci profili özellikleri tarafından tetiklenebilmekte, bu durumda ise sadece davranış biçimleri değişmektedir. McAuley, “Önümüzdeki 3-5 yıl içinde, BT’ye ve yapılan işin her alanında mobil ödeme yöntemleri gibi sıklıkla kullanılan yeni teknolojilere olan bağımlılığa paralel olarak, suistimal riski de artacaktır. Eski suistimal yöntemleri de halen varlığını sürdürüyor olacak; yani tüm yaptığımız daha fazla risk alanıyla uğraşmak olacak” diyor.

### **Modern suç örgütleri**

Oswalt, “Bilişim suçları, teknolojik açıdan oldukça gelişmiş durumda olduğu için suç örgütlerinin ilgisini giderek daha fazla çekecektir” diyor. Fikri mülkiyet haklarının çalınması yönünde bir karaborsa oluştuğuna ve suç örgütlerinin bu durumun içinde olduğuna dikkat çekiyor. “Organize suç örgütleri, şirketlerden para

koparma konusunda gitgide ustalaşmaya başladılar. Son aylarda üye firmalarımız, suistimalcilerin genellikle şirketteki yeni veya toy çalışanları kullanmak suretiyle tedarikçi bilgilerini değiştirip, ödemeleri off-shore adreslere yönlendirdiklerini ve bu şekilde gerçekleştirilen ödeme yönlendirme suçunda bir artış olduğunu tespit etmişlerdir” diyor Plavsic.

Bilişim alanında suistimal gerçekleştirmek, suçlular tarafından diğer suistimal yöntemlerine göre daha mantıklı bir

adım olarak görülmektedir. Del Castillo, “Organize suç örgütleri, beyaz yakalıların gerçekleştirdiği suistimali farklı bir şekilde gerçekleştiriyorlar. Bilgi edinmek ve suistimali gerçekleştirmek için gelişmiş teknolojileri kullanıyor ve kurumların içine kendi adamlarını yerleştiriyorlar. Kısacası, şirket içi suistimalcinin arkasında artık organize bir suç örgütü mevcut” diyor. Ne yazık ki, suç örgütlerinin her türden suistimale ne ölçüde dahil olduğunu hesaplamak oldukça zor. Araştırmamız konu 596 suistimalcinin sadece 15

tanesi suç örgütleriyle işbirliği yapmış ve bunlardan 13’ü hem şirket içinden hem şirket dışından olan suç örgütlerini kullanmıştır. Ayrıca bahsi geçen 13 vaka varlıkları kötüye kullanma suçunu da içermekte. Organize suç örgütleri, özellikle Latin Amerika ve Afrika’da şirket yöneticilerini kaçırmaya gibi suçları işlemeye devam etseler de, dünyanın pek çok bölgesinde suistimal eylemlerinin kapsamının bilişim suçlarını da içine alarak gittikçe genişleyeceğine inanılmaktadır.

## Bilişim Suçlarının iç yüzü: teknolojik hizmetlerin kullanılması modeli

Teknolojik gelişmelere bağlı olarak şirketlerin ve tüketicilerin elektronik hizmetleri giderek daha yaygın bir şekilde kullanmaları, organize ve bireysel suçlardan önemli kazançlar elde edilmesini sağlamaktadır. Son zamanlarda küresel alanda görülen suistimal türleri, geleneksel banka soygunculuğunun, daha az riskli, daha anonim ve çok daha büyük kazançlar getiren bütünüyle bilişim suçları yaklaşımına dönüştüğünü göstermektedir. Pek çok vakada, organize hareket eden suçlular, dikkatlerini bilişim dünyasının sunduğu çok sayıda farklı hizmete yöneltmiştir. Bilişim hizmetleri; kullanıcıların gerçek kimliklerini gizleyerek dünyanın hemen her yerinden erişim sağlayan bilgisayar ağları (virüs bulaşmış yüz binlerce bilgisayardan oluşan suçlu ISP’leri), suçlular tarafından, virüs koruma programları ya da güvenlik duvarlarına takılmadan mağdurun bilgisayarında çalışmak için yazılmış olan ve kimlik bilgilerini (kullanıcı adı, parolası ve kredi kartı bilgileri gibi) çalan kötü amaçlı yazılımlar (malware), hedeflenen kurumlara veya aygıtlara saldırı yapmak üzere kiralanmış bilişim korsanları, çalınan kimliklerin veya fikri hakların depolanmasında kullanılan web tabanlı bilişim hizmetleri (tespit edilemeyen depolama hizmetleri), sahte web sitelerinin kimlik avı amaçlı kampanyaları ve kara para aklama/aktarma hizmetleri konularını içermektedir.

Finans kuruluşlarındaki ana saldırı hedefleri banka hesapları ve kredi kartlarıdır. Yakın zaman önce dünyanın pek çok farklı noktasından neredeyse eş zamanlı olarak gerçekleştirilen bir siber saldırıda suçlular yukarıda bahsedilen bilişim dünyasının teknolojik hünelerlerini, benzersiz bir ATM sistemi bilgisiyle birleştirmişlerdi.

Bilişim korsanları bankanın veri tabanlarına erişerek yüzlerce kredi kartını görünürde yasal olan banka hesaplarına bağladılar. Banka içindeki işbirlikçilerden de yardım alan bilişim korsanları bir terminale uzaktan erişim sağlayarak bu kartların her birinin günlük nakit çekim limitlerini 100.000 doların üzerine çıkardılar. Bankanın BT güvenlik sistemindeki bu açığı kötüye kullanan bilişim korsanları “sahte para” yarattılar ve kartların manyetik şeritlerini uygun şekilde kodlayarak dünyanın her yerindeki ATM’lerden çekilebilecek hale getirdiler. Son adımda ise bu suç örgütünün, dünyanın her yerindeki 100’den fazla ATM’den nakit çekiminde yardımcı olacak “para kuryeleri”ni kullanması gerekti. Sadece birkaç saat içinde 45.000.000 dolardan fazla para kolayca çekildi. Bu raporun yazıldığı tarih itibari ile gerçek zarar ise 100.000.000 doları aştı. Teknoloji bilgisi ve işbirliği ile bilişim dünyasının sunduğu kaynaklar böylesine kapsamlı küresel bir suçun işlenmesini mümkün kılmış oldu.

Peki bu, gelecekte bizi bekleyen tehlikelerin bir habercisi olabilir mi? Evet, hatta bundan daha fazlasının olabileceği söylenebilir. Suistimalciler, siber suç ağlarının sunduğu hizmetleri satın alarak veya kiralarak hem tek başlarına hem toplu olarak hareket edebiliyor ve bu sayede suç zincirinde daha az yer alıp “aynı anda farklı yerlerde olma” imkânlarını artırıyorlar. Oldukça yetenekli kiralık bilişim korsanları genellikle neredeyse sınırsız işlem yapma kapasitesine sahip üst düzey sunucularla çalışmaktalar. Çok yakın bir gelecekte, organizasyonel siber alt yapının sürekli olarak bir açık bulmak üzere test edilmesi için kendi kendine öğrenen ve kendini kopyalayabilen yapay zekâya sahip “tarayıcılar” oluşturulacak. Bir boşluk bulunca tarayıcılar bir “ajana” dönüşerek bu giriş yapılan site yapısının suistimal için bir fırsat sunmadığını araştırabileceklerdir. Ardından, mağdur şirketin türüne, büyüklüğüne, altyapısına, veri hacmine ve diğer parametrelere göre özelleştirilmiş “saldırı” tarayıcıları oluşturulabilecek. Son olarak da tarayıcılar gizli veya şifrelenmiş taşıyıcılar içindeki varlıkları alarak, organize suç şebekesinin doğrudan hasılat elde edeceği sanal konumlara taşıyabilecekler. Suçlular böylelikle görünmez hale gelmiş olacaklar.



# Yolsuzluk kültürü

## Kültürel özelliklerin suistimal ve suistimalin tespiti üzerindeki etkisi

Bazı ülkelerde iş yapılan kişilere hediye vermek ticari hayatın olağan bir parçası olarak görülürken, bazı ülkelerde bu durum rüşvet olarak algılanmaktadır. Kültür, büyük ölçüde davranışlarımızı etkilemekte ve neleri etik veya toplumsal değerlere uygun bir davranış olarak gördüğümüzü belirlemektedir. Farklı ulusların kültürlerindeki farklı kriterler nedeniyle, (örneğin Çin'deki bir kişinin suistimal anlayışı, Kuzey Amerika'daki birininkinden farklı olabilir) suistimal anlayışları da değişkenlik gösterecektir. KPMG Çin Suistimal Önleme ve İnceleme Hizmetleri Bölüm uzmanları, "Yerli çalışanlar ile yabancı iş ortakları etik değerler konusunda farklı bir bakış açısına sahip olabilmektedir. Hediyeler ve ilişkili taraflarla gerçekleştirilen işlemler başka ülkelerde riskli bir durum olarak görülürken, Asya Pasifik bölgesinde yer alan birçok kesimde, hediye vermek, ilişki kurmanın önemli bir parçası olarak görülmektedir" diyorlar. Bu nedenle bir suistimalcinin profiline kültürel bir perspektiften bakmak ilgi çekicidir. Suistimal örneklerinde bölgesel farklılıkları incelemek üzere, 20 ve üzeri suistimalcinin rapor edildiği ülkelerde (Almanya, Birleşik Krallık, Çek Cumhuriyeti, Güney Afrika, Hindistan ve Kanada) gerçekleşen vakaların sonuçları analiz edilmiştir.

Genel olarak, araştırma yapılan suistimalcilerin profillerine ait değişkenler farklı ülkelerde büyük ölçüde benzerlik göstermiştir. Suistimalcilerin büyük çoğunluğunun Hindistan, Kanada, Güney Afrika ve Almanya'da 36 ila 45 yaşları arasındayken, Çek Cumhuriyeti

ve Birleşik Krallık'ta 46-55 yaşları arasında olduğu görülmüştür. Tüm ülkelerdeki suistimalcilerin büyük bir çoğunluğunun yüksek öğrenim gördüğü ve mağdur kuruluşta 6 yıldan uzun bir süredir çalışmakta olduğu anlaşılmıştır. Bir istisna olarak Çek Cumhuriyeti'nde, mağdur şirkette 1 ila 4 yıl, 4 ila 6 yıl ve 6 yıldan uzun bir süredir çalışan suistimalcilerin oranlarının eşit olduğu görülmüştür. Buna karşılık, Hindistan'da suistimalcilerin büyük çoğunluğu 1 ila 4 yıllık çalışanlardır. Birleşik Krallık, Kanada, Çek Cumhuriyeti ve Hindistan'da, şirkette çalışmaya başladıktan sadece 1 ila 4 yıl sonra suistimal eylemi gerçekleştirenlerin sayısının Güney Afrika ve Almanya'dakinden daha yüksek olduğu görülmüştür. Bu durumun nedeninin bahsedilen ilk 4 ülkede bireye duyulan güvenin daha fazla olması olduğu söylenebilir.

Elde edilen sonuçlara göre, Güney Afrika, Hindistan ve Kanada'da en fazla suistimal gerçekleşen şirket departmanları, başta Finans ve Satın Alma birimleri olmak üzere, Operasyon Departmanı; Birleşik Krallık, Almanya ve Çek Cumhuriyeti'nde ise üst düzey yöneticilerin yer aldığı departmanlardır. Benzer şekilde, Finans ve Operasyon departmanları ile yönetici mevki bu 6 ülkede de suistimalcilerin en fazla çalıştıkları departmanlar ve birimler olmuştur. Kıdem seviyesinin ise suistimal üzerinde karışık bir etkisi olduğu görülmektedir. Birleşik Krallık, Kanada, Almanya ve Çek Cumhuriyeti'nde suistimalcilerin büyük çoğunluğu üst

düzey yöneticilerden oluşmaktadır. Kendilerine daha fazla güven duyulduğu için yöneticiler iç denetimlere daha az tabi tutulmaktadır. Kanada'daki suistimal suçlarında ise suistimalcilerin şirketteki pozisyonlar arasındaki dağılımı eşittir, bu da kıdem seviyesinin bu bölgede suistimal suçu işleme becerisinde önemli bir rol oynamadığını göstermektedir. Güney Afrika ve Hindistan'da suistimal suçlarının büyük çoğunluğunun yöneticiler tarafından işlenmekte olduğu görülmüştür.

### Suistimal türü

Bütün ülkeler genelinde bakıldığında, birden fazla işlemler gerçekleştirilen suistimal türünün sayısının tek bir işlemler gerçekleştirilen suistimal türünden daha fazla olduğu görülmüştür. Tek bir işlemler gerçekleştirilen suistimal vakalarının sayısının ülke başına en fazla "2" olduğu görülmüştür. 6 ülke içinde, tüm suistimal suçlarının birden fazla işlem şeklinde işlendiği tek ülke "Kanada" olmuştur. Söz konusu suç birden fazla işlemler gerçekleştiriliyorsa suistimalcinin yakalanma olasılığı daha yüksek olacaktır ve bu da tek işlemler suistimalin tespit edilememesine ihtimalinden dolayı, sonuçlarda bir sapma olabileceğine işaret etmektedir. Birkaç suistimal eyleminin gerçekleştirilmesi için geçen süre tüm ülkelerde yaklaşık 1 ila 5 yıl arasında olmuştur. Bu süre zarfı içinde mağdur şirketin uğradığı toplam zarar 50.000 \$ ila 200.000 \$ arasındadır. Güney Afrika, Kanada ve Birleşik Krallık'ta ise bu rakamın daha da yüksek olduğu görülmüştür.



İspanyol şirketleri farklı bir ülkede yeni bir pazara giriş yaparken potansiyel kanun ihlali ve diğer suistimal risklerini göz önünde bulundurmalıdırlar. Farklı kültürlerin ve farklı faaliyet uygulamalarının şirket faaliyetleri üzerinde yaratabileceği etki hakkında bilince sahip olmamak, bir şirket için öldürücü olabilir.



### Angel Requena

Ortak, KPMG Suistimal Önleme ve İnceleme Bölümü,  
İspanya

Tüm ülkelerde en yaygın karşılaşılan suistimal türü, açık ara farkla varlıkların kötüye kullanılması olup, bunun içinde zimmete para geçirme, satın alma yolsuzlukları ve maaş bordroları vasıtasıyla gerçekleştirilen suistimaller ilk sıraları almaktadır. Haksız kazanç sağlama veya varlık temin etme ya da hileli finansal raporlama ve masraf veya borç kalemlerinde usulsüzlük yapma, tüm ülkelerde orta ve büyük ölçekte görülen diğer vakalar olmuştur. Suistimalcilerin bu suçu işlerken başkalarıyla işbirliği yapma yüzdeleri ile suçu tek başlarına işleme oranları Çek Cumhuriyeti'nde 91-9, Kanada'da ise 48-52 olarak gerçekleşmiştir. Bu bulgu, Kanada'daki suistimalcilerin, diğer ülkelerde görünen aksine bir suç ortağı ile işbirliği yapma riskini almaktan kaçındıklarını ortaya koymaktadır.

Birleşik Krallık ve Kanada hariç olmak üzere 6 ülkenin büyük bölümünde, işbirlikçilerin hem şirket içinden hem de şirket dışından kişiler olduğu görülmüştür. Birleşik Krallık'ta suç ortakları çoğunlukla şirket personeliyken, Kanada'da suistimalciler çoğunlukla şirket dışındaki kişilerle işbirliği yapmıştır. İşbirliğinin en çok görüldüğü ikinci bölgede işbirlikçilerin; Almanya, Birleşik Krallık ve Güney Afrika'da şirket dışından kişiler, Çek Cumhuriyeti ve Kanada'da ise şirket içinden kişiler olduğu görülmüştür. Sonuçlar, Kanada'da şirket içi ve şirket dışı işbirlikçileri oranının aynı olduğunu göstermektedir. Suç ortaklarının tümünün erkek, kadın-erkek karışık ve tümünün kadın olma oranları

Almanya dışındaki tüm ülkelerde hemen hemen aynı olurken, Almanya'da ise suç ortaklarının tümünün kadın olduğu bir vaka bile bildirilmemiştir. 6 ülkede insanları suça teşvik eden temel motivasyon kaynağının ağırlıklı ve kişisel maddi kazanç olduğu görülmüştür. Sonuçlar, kişisel maddi sıkıntılarının da Kanada, Çek Cumhuriyeti ve Almanya'da ortak bir suça teşvik kaynağı olduğunu, Hindistan, Çek Cumhuriyeti ve Güney Afrika'da ise suçluların önceden planlamaksızın buldukları suistimal fırsatını değerlendirdiklerini göstermiştir.

### Ortaya çıkarma ve sonuçları

Suistimalin gerçekleşmesine neden olan etkenler arasında en çok dile getirilen, zayıf iç kontrollerdir. Zayıf iç kontroller, bütün ülkelerde ortak bir sorun olarak karşımıza çıkmaktadır. Bunun yanı sıra, denetim mekanizmalarının varlığının bilinmesine rağmen umursanmaması, Almanya dışındaki tüm ülkelerde sıklıkla belirtilen bir durumdur. Güçlü denetim mekanizmalarını atlatmak için işbirliği/gizli ittifak yapmak da Almanya dışındaki 6 ülkede suistimale olanak tanıyan bir unsur olarak gözlemlenmiştir. Almanya ve Kanada dışındaki tüm ülkelerde suçların önemli bir bölümü bildirimler aracılığıyla tespit edilmiştir. Almanya, Çek Cumhuriyeti, Hindistan ve Kanada'da ise, resmi olmayan anonim bildirimlerin sayısının da dikkate değer olduğu görülmüştür. Suistimalin ortaya çıkarılması aşamasında faydalanılan diğer yöntemlerin ise, daha proaktif yöntemler olarak bilinen, yönetim tarafından yapılan incelemeler ile iç denetim ve şirket dışı denetimler olduğu gözlenmiştir.

Suistimalin sonuçları genel olarak 6 ülkede de benzer olmakla birlikte işten çıkarma, suistimalcinin en çok karşılaştığı sonuç olmuştur. Her ne kadar suçluların polise bildirilmesi çok güçlü caydırıcı bir etken olabilse de, olayın kamuoyuna yansımalarından endişe etmeleri nedeniyle şirketler hukuki yollara başvurmadan kaçınmaktadır. Almanya'da ise şirket itibarının zedelenme riskinin diğer ülkelere göre daha düşük görüldüğü gözlenmiştir.

### İnce ayrıntı gereksinimleri

Çek Cumhuriyeti, Almanya, Birleşik Krallık, Güney Afrika, Hindistan ve Kanada'da suistimalin çeşitli özelliklerini karşılaştığımızda ulusal niteliklerin birbirine benzemesine rağmen kültürel değişiklikler nedeniyle aralarında bazı önemli farklar olduğu tespit edilmiştir. Bu durum, uluslararası şirketlerin risk yönetimi programlarını, farklı ülkelerdeki kültürel özelliklere uyarlamalarının oldukça faydalı olabileceğini göstermektedir. Örneğin, başka kişiler hakkındaki bilgileri açığa çıkarmanın yanlış bir davranış biçimi olarak değerlendirildiği ülkelerde, şirket içi ihbar mekanizmaları işe yaramayabilir. Benzer şekilde, Hindistan'da suistimali caydırma tedbirlerinin yönetim kademesi ile personel arasında eşit dağıtılması daha faydalı olabileceği gibi, Almanya'da üst düzey yöneticilere odaklanmak daha isabetli olacaktır. Birleşik Krallık'ta ise bu tedbirlerin Yöneticiler ile Finans departmanı arasında eşit ağırlıklı uygulanması faydalı olabilir. Kurumlar suistimalle mücadele çabalarını farklı kültürlerle uyularak geliştirilebilirler.

# İzafiyet teorisi

## Bir suistimalcinin profili ahlaki koşullardan nasıl etkilenir?

Bu bölümde, suistimalcinin suçu işlediği ya da hatalı davranışlar sergilediği ahlaki koşulların suistimalcinin profili üzerindeki etkisini inceleyeceğiz. Finansal ve ticari suç işleyen kişilerin ahlak dışı davranışları, işin içine bir şekilde rüşvet ve yolsuzluk da eklendiğinde daha da fazlaşmaktadır. Bu nedenle rüşvet ve yolsuzluğun suistimalcinin profili üzerinde etkisi olduğu söylenebilir. Bu raporda analiz edilen suistimalcinin yolsuzluk unsurlarını da içerip içermediği sorulmuş ve önemli oranda yolsuzluk olduğu belirtilen suistimalcinin %14'ünde rüşvet ve yolsuzluğun bir arada gerçekleştirildiği belirlenmiştir.

Küresel alanda rüşvet ve yolsuzluğun varlığını açıklayan çevresel unsurlara bakıldığında kesin bir trend tespit edilememiştir. Ancak, KPMG üye firmalarının ABD, Çin, BDT ülkeleri ve Batı Afrika'da soruşturmasını gerçekleştirdikleri vakalar karşılaştırıldığında bazı belirgin trendlerin daha ön planda olduğu görülmüştür. 4 ülke/bölgede de, soruşturması gerçekleştirilen suistimal vakalarında

rüşvet ve yolsuzluk unsurlarının küresel ortalaması %33'lük bir orana denk gelmiştir: ABD (%24), Çin (%48), BDT (%64) ve Batı Afrika (%67).

### Düzenlemeler

Araştırmamız, mevcut ahlaki standartları ölçmek üzere tasarlanmamıştır. Bunun yerine, yolsuzluğun da yer aldığı suistimal vakalarının söz konusu 4 ülkede, sıkı düzenlemelere tabi ortamlarda işlenip işlenmediği incelenmiştir. ABD ve Çin'de araştırılan vakaların %50'sinin, BDT ülkelerinde ise %33'ünün sıkı düzenlemelere tabi ortamlarda gerçekleştiğini, Batı Afrika'da ise bu oranın 0 olduğu görülmüştür.

Aşağıdaki tabloda bulunan iki etken arasındaki ters ilişki (suistimal vakaları içerisinde yolsuzluk oranı ve bu oranın düzenleme seviyesiyle karşılaştırması), etik değerlerin kurumsallaştırılmasının suistimalci profilini yakından etkileyebildiğini göstermektedir. Bu durum, en azından kişinin suistimale yönelik davranışlarına yolsuzluğu dahil etme eğilimini gösterebilir. Ditty, "Yatırımlar, finans kuruluşlarının gücüne ve kurumsal yönetimin kalitesine bağlıdır. Kurumlara etik standartlar getiren ve şeffaflığa teşvik eden kurumsal davranış kurallarına sahip olmak, yalnızca suistimalin önlenmesiyle ilişkili değil, uzun vadeli büyüme için bir zorunluluktur" diyor.

	Bölge				
	Küresel	ABD	Çin	BDT	Batı Afrika
<b>Suistimal vakalarında yolsuzluğun varlığı</b>	<b>%33</b>	<b>%24</b>	<b>%48</b>	<b>%64</b>	<b>%67</b>
<b>Düzenleme seviyesi</b>	<b>%38</b>	<b>%50</b>	<b>%50</b>	<b>%33</b>	<b>%0</b>







### Çevresel Etkenler

Araştırmamızın ilerleyen süreçlerinde, 4 ülkede gözlemediğimiz ortak suistimalci özellikleri; mağdur şirketle daha yakından ilişkili olan çevresel etkenlerle karşılaştırılmıştır. Etik ve ahlaki koşullar, kurumsal rekabet, piyasa rekabeti ve suistimalcinin sınırsız yetkiye sahip olması gibi etkenler karşısında hassas olduğu bilinen aşağıda belirtilen unsurlar değerlendirilmiştir. Aşağıdaki sonuçlar, yolsuzluğu da kapsayan suistimal vakalarında bu üç çevresel etkenin etkisini oransal olarak göstermektedir.

BDT ve Batı Afrika ülkelerindeki suistimalci profilinde kurumsal rekabet ortamı ile yolsuzluğun yaygınlığı arasında ters orantı, ABD ve Çin’de ise doğrudan ilişki olduğu görülmüştür. Piyasa rekabeti ortamıyla ilişkili göstergelerin kurumsal rekabet ile aynı olduğu, yalnızca ABD’de bu etkenler arasında ters ilişki olduğu gözlemlenmiştir. Sınırsız yetkiye sahip olunan ortamlar ile suistimalci profillerinde kasıt unsurunun yaygınlaştığının görülmesi arasında da ters ilişki olduğu görülmüştür. Küresel alanda bakıldığında, suistimal suçunu işlerken yolsuzluk da yapan suistimalcilerin %40’ının bunu sınırsız yetkiye sahip oldukları bir ortamda gerçekleştirdikleri tespit edilmiştir.

Bu gözlemler, suistimalci profillerinin davranışsal unsurları ile suistimalcinin etik değerlerini etkileyebilecek bazı çevresel etkenler arasında ilişkiler bulunduğunu

	Bölge				
	Küresel	ABD	Çin	BDT	Batı Afrika
<b>Kurumsal rekabet</b>	<b>%23</b>	<b>%25</b>	<b>%43</b>	<b>%33</b>	<b>%25</b>
<b>Piyasa rekabeti</b>	<b>%29</b>	<b>%0</b>	<b>%50</b>	<b>%39</b>	<b>%33</b>
<b>Agresif satış ortamı</b>	<b>%31</b>	<b>%25</b>	<b>%43</b>	<b>%28</b>	<b>%8</b>
<b>Kötü haberleri gizleme isteği</b>	<b>%22</b>	<b>%25</b>	<b>%7</b>	<b>%11</b>	<b>%8</b>
<b>Sınırsız yetki</b>	<b>%40</b>	<b>%50</b>	<b>%36</b>	<b>%33</b>	<b>%17</b>

ortaya koymaktadır. Bununla birlikte, bu ilişki her alanda görülmeyebilir, hatta bazı ülkelerde hiç görülmemektedir. Vakalar bu kez çevresel olmayan, yani kişisel bir bakış açısına göre değerlendirmeye tabi tutulmuştur. Bu bağlamda da, suistimalcilerin çevresel bir etken olmayan “üstünlük duygusunu” taşıyıp taşımadıkları incelenmiştir.

Bu konuda belirgin bir özellik tespit edilememekle birlikte üstünlük hissini, suistimalci profilini şekillendiren çevresel bir etkenden ziyade soruşturması gerçekleştirilen suistimalcilerin karakteristik bir özelliği olma olasılığı yüksektir.

### Değerler ve normlar

Tek tip ve hiç değişmeyen bir suistimalci profilinin mevcut olmadığı düşünülürse, yukarıda belirtilen trendin (ABD, Çin, BDT ve Batı Afrika’daki düzenlemeler ile suistimal vakalarında yolsuzluğa da başvurulması arasındaki ilişki) her zaman geçerliliğini koruyacağından şüphe duymaktayız.

Görünüşe bakılırsa, bazı ülkelerde suistimal, zaman ve mekân ile farklı etkenlerin yoğunluğuna göre değişmektedir. Kurumsal değerlerin ve normların yarattığı etkilerin suistimalci profilini şekillendirdiği ve zaman ile mekâna bağlı olarak gelişen tutarsızlıkların suistimalcinin profilinin değişkenliğinin altını çizdiği görülmektedir.

	Bölge			
	ABD	Çin	BDT	Batı Afrika
<b>Suistimal vakalarında yolsuzluk unsuru</b>	<b>%24</b>	<b>%48</b>	<b>%64</b>	<b>%67</b>
<b>Üstünlük duygusu</b>	<b>%50</b>	<b>%43</b>	<b>%67</b>	<b>%50</b>

# Sonuç

KPMG üye firmalarının Suistimal Önleme ve İnceleme Bölümü liderlerinin öngördükleri trendler hakkındaki görüşlerinden elde edilen önemli noktaları vurgulayacak olursak:

1

Hem operasyonları kesintiye uğratma hem de maddi kazanç elde etme peşinde olan, üstün teknolojileri kullanabilen, çeşitli suç örgütleri ile işbirliği içerisinde hareket eden "bilgi korsanları" gibi tehditlere karşı zafiyetin artmakta olduğu görülmektedir.

2

Şirket içi ve şirket dışı suç ortaklarının birbirleriyle veya kendi aralarında yaptıkları gizli ittifak ve işbirliklerinde sürekli artan bir trend görülmesi, şirketlerin suistimalcilere karşı olan savunma mekanizmalarını, iç kontrol sistemlerinin ötesine taşınmaları gerektiğini ortaya koymaktadır.

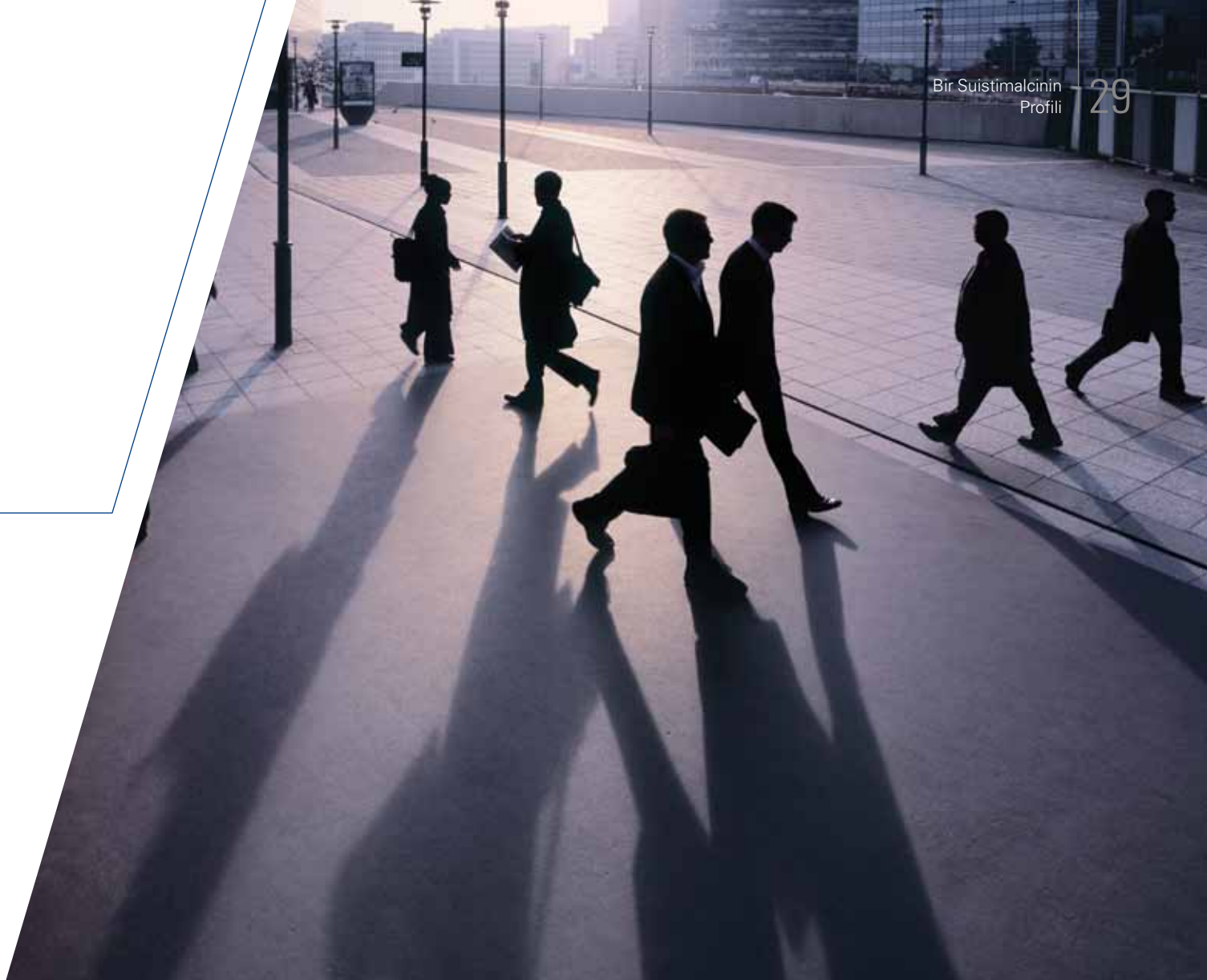
3

Artık tek başına gerçekleştirilen vakalar olmaktan çıkıp diğer beyaz yaka suçlarında da yaygınlaşan rüşvet ve yolsuzluk, günümüz suistimalci profilinin sabit bir parçası haline gelmekte ve suistimalcilerin kendi başlarına hareket etmelerine oranla, mağdur şirkete çok daha büyük maddi zarar veren danişıklı bir ilişki yaratma becerisini ortaya koymaktadır.

4

Ekonomik istikrarsızlık, değişken sermaye piyasaları, yeni teknolojiler ve inovasyon, yeni muhasebe sistemleri, bilişim alanında dünyanın her yerinden erişim imkanının giderek artması ve sanal işlemlerin yapıldığı ortam, bu değişimlerden yasadışı biçimde faydalanarak kazanç temin etmek amacıyla gerekli yetkinlikleri gösterebilecek, suç dürtüsüne ve gerekçelere sahip insanlara birçok fırsat sunmaktadır.

Bazı şeylerin mutlaka değişeceğine inanıp bilişim suçlarının görünmez hale gelmelerinden endişe ederken tipik suistimalcinin ise "kadrolu, güvenilir çalışan" olma ihtimali asla unutulmamalı. Her zaman gözünüzün önünde olan, asla şüphelenmeyeceğiniz, belki farkına bile varmadığınız o kişi...







# İletişim



## İdil Gürdil

**Risk Yönetimi Danışmanlığı  
Bölüm Başkanı, Şirket Ortağı  
İstanbul, Türkiye**

**T:** + 90 216 681 90 14

**F:** + 90 216 681 90 90

**E:** igurdil@kpmg.com



## Çiğdem Gürer

**Suistimal Önleme ve İnceleme  
Hizmetleri, Direktör  
İstanbul, Türkiye**

**T:** + 90 216 681 91 55

**F:** + 90 216 681 90 90

**E:** cgurer@kpmg.com

## KPMG Bölgesel Suistimal Önleme ve İnceleme Liderleri

### Petrus Marais

**KPMG Bölgesel Suistimal Önleme  
ve İnceleme Liderleri**

**T:** +27 795159469

**E:** petrus.marais@kpmg.co.za

### Richard H. Girgenti

**KPMG Bölgesel Suistimal Önleme  
ve İnceleme Liderleri**

**T:** 212 872 6953

**E:** rgirgenti@kpmg.com

### Jack DeRaad

**EMA Bölgesi Suistimal Önleme  
ve İnceleme Lideri**

**T:** +31206 567774

**E:** deraad.jack@kpmg.nl

### Grant Jamieson

**AsPAC Bölgesi Suistimal Önleme  
ve İnceleme Lideri**

**T:** +85 221402804

**E:** grant.jamieson@kpmg.com

## KPMG Küresel Adli İncelemeler Ağı

### Phillip Ostwalt

**Küresel & Amerika Kıtası Adli  
İncelemeler Lideri**

**T:** 404 222 3327

**E:** postwalt@kpmg.com

### Dean Friedman

**EMA Bölgesi Adli İncelemeler Lideri**

**T:** +27 116478033

**E:** dean.friedman@kpmg.co.za

### Mark Leishman

**AsPAC Bölgesi Adli İncelemeler Lideri**

**T:** +61 7 3233 9683

**E:** mleishman@kpmg.com.au

[kpmg.com.tr](http://kpmg.com.tr)



[kpmg.com/app](http://kpmg.com/app)



Bu dökümanda yer alan bilgiler genel içeriklidir ve herhangi bir gerçek veya tüzel kişinin özel durumuna hitap etmemektedir. Sürekli güncel ve doğru bilgi sunumuna özen gösterilmesine karşın bu bilgiler her zaman her durumda doğru olmayabilir. Hiç kimse özel durumuna uygun bir uzman görüşü almaksızın, bu dökümanda yer alan bilgilere dayanarak hareket etmemelidir.

© 2014 Akis Bağımsız Denetim ve Serbest Muhasebeci Mali Müşavirlik A.Ş., KPMG International Cooperative'in üyesi bir Türk şirkettir. KPMG adı ve KPMG logosu KPMG International Cooperative'in tescilli ticari markalarıdır. Türkiye'de basılmıştır. KPMG adı, logosu ve "cutting through complexity" KPMG International'a ait tescilli markalardır.