KPMG

Bir Suistimalcinin Profili 2016

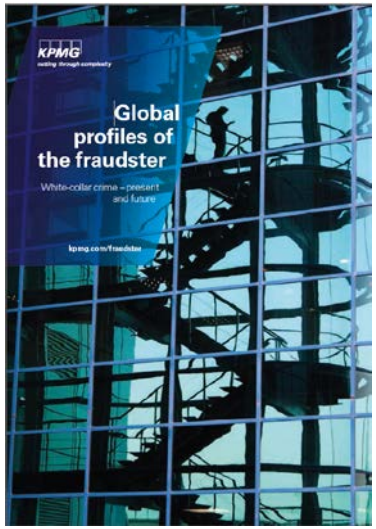
Teknoloji suistimali kolaylaştırıyor, zayıf kontroller ise körüklüyor

Ekim 2016

Suistimalci Profilleri Hakkında

Suistimal Önleme ve İzleme Kitaplığı

2010
69 ülkede 348 vaka



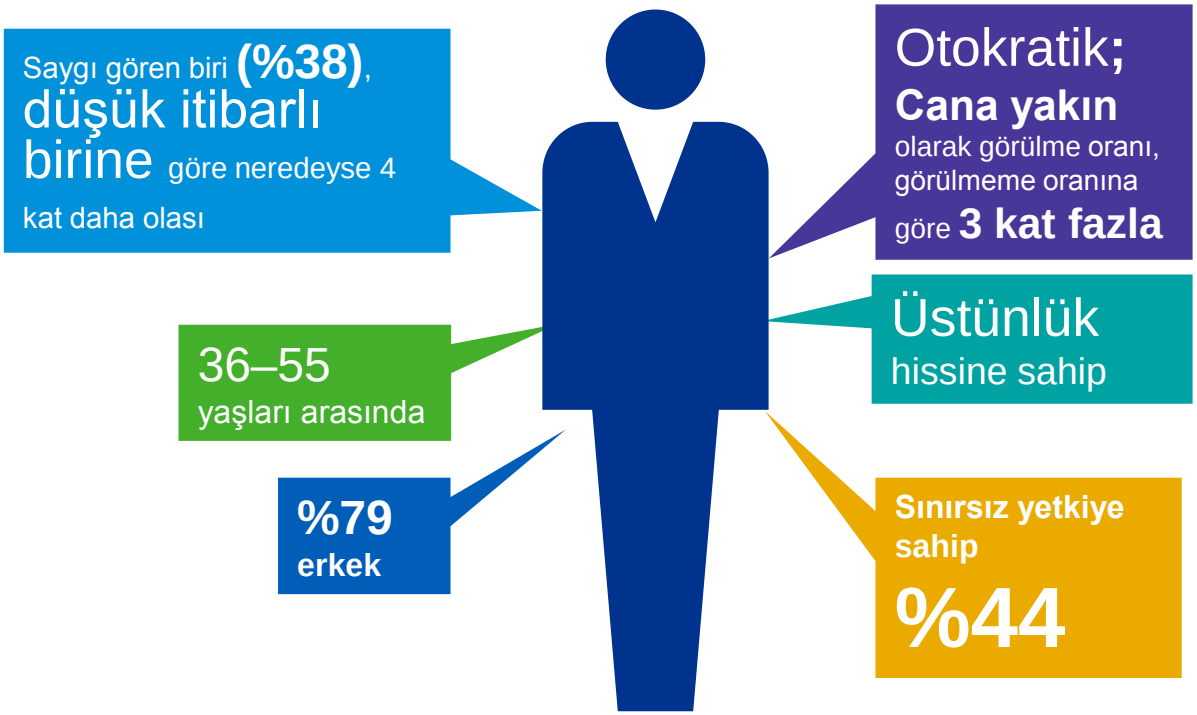
2013
78 ülkede 596 vaka

2015
81 ülkede 750 vaka

2015

- 81 ülkede 750 suistimalci. Bir önceki araştırmaya göre 154 vaka artışı oldu.
- Suistimal soruşturmaları Mart 2013 ve Ağustos 2015 aralığında gerçekleşti.
- Araştırma belirli konuların daha derinlemesine incelenmesi için genişletildi.
- 2016'daki yenilikler: teknolojiye odaklanıldı (kolaylaştırıcı unsur ve tespit edici olarak) ve siber suistimalcilerin özellikleriyle ilgili yeni sorular eklendi.

Temel karakteristik özellikler



Suistimallerin **%65'i** 1 ile 5 yıl arasında sürdü

Suistimal Türü: Varlıkların kötüye kullanımı **(%47)**; Finansal raporlama suistimali **(%22)**.

Suistimal Bedeli: Şirketlere olan zararı **1 milyon dolar** üzerinde **(%27)**.

Kaynak: Bir Suistimalcinin Profili, KPMG International, 2016

Temel özellikler: Cinsiyet

Ana Fonksiyon

Finans

Kıdem Seviyesi

Personel

Tek Başına mı İşbirliğiyle mi

Tek Başına

Borcu var

%20

Ana Fonksiyon

Çeşitli

Kıdem Seviyesi

Üst Düzey Yönetici

Tek Başına mı İşbirliğiyle mi

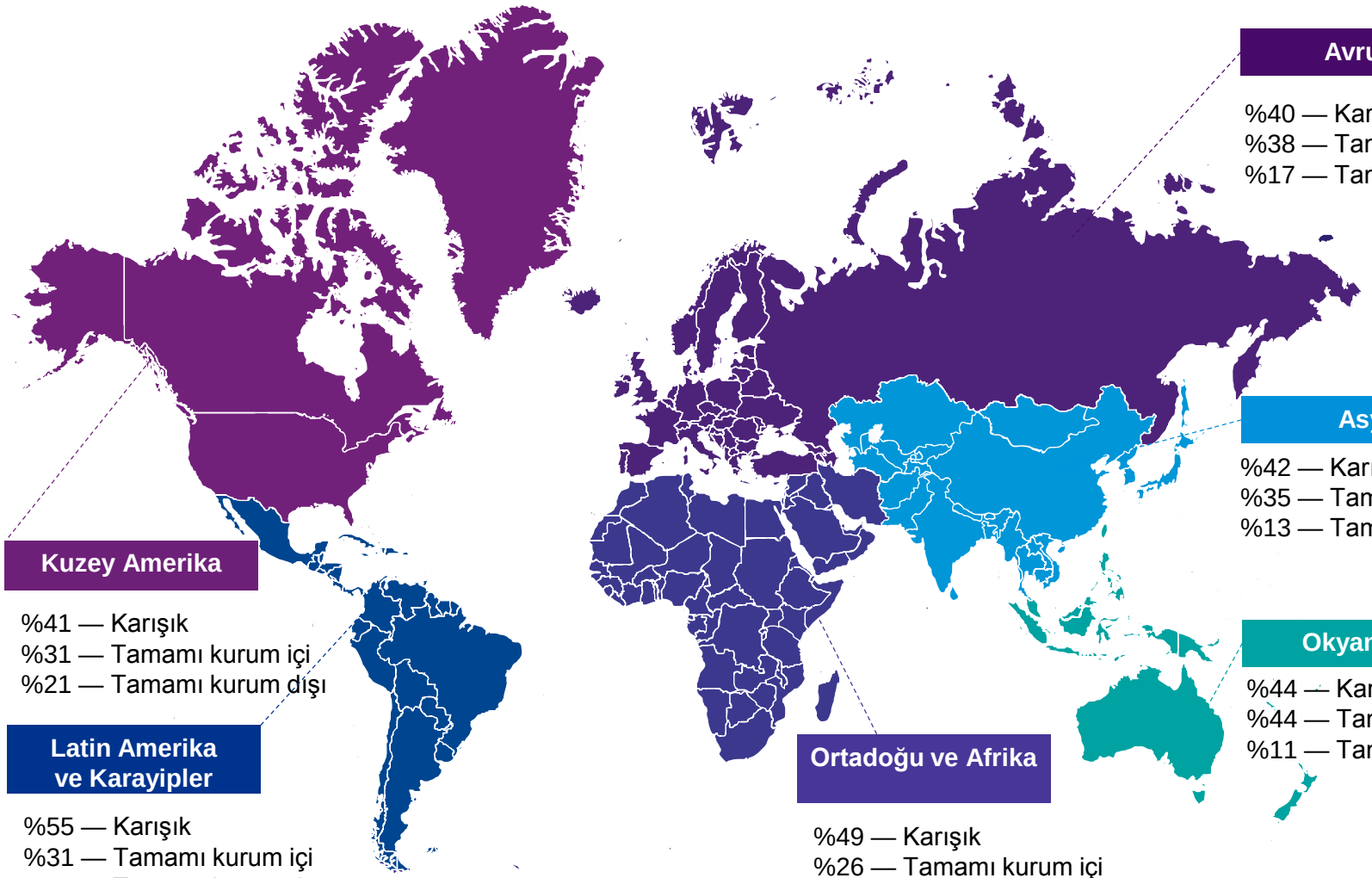
İşbirliğiyle

Borcu var

%8

Kaynak: Bir Suistimalcinin Profili, KPMG International, 2016

Suistimal türleri: İşbirliği



Avrupa

%40 — Karışık
%38 — Tamamı kurum içi
%17 — Tamamı kurum dışı

Asya

%42 — Karışık
%35 — Tamamı kurum içi
%13 — Tamamı kurum dışı

Okyanusya

%44 — Karışık
%44 — Tamamı kurum içi
%11 — Tamamı kurum dışı

Kuzey Amerika

%41 — Karışık
%31 — Tamamı kurum içi
%21 — Tamamı kurum dışı

Latin Amerika ve Karayipler

%55 — Karışık
%31 — Tamamı kurum içi
%13 — Tamamı kurum dışı

Ortadoğu ve Afrika

%49 — Karışık
%26 — Tamamı kurum içi
%24 — Tamamı kurum dışı

Kaynak: Bir Suistimalcinin Profili, KPMG International, 2016

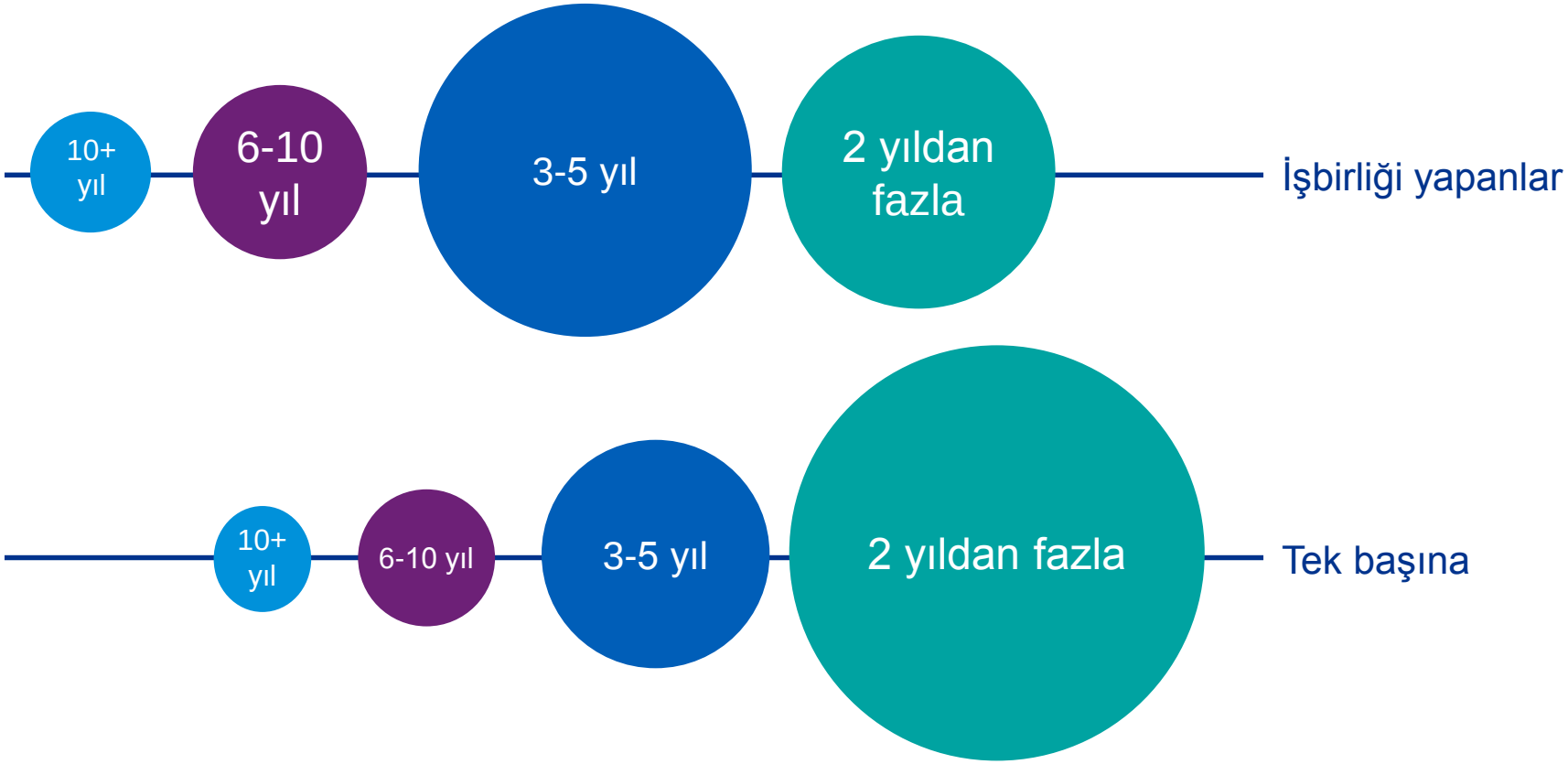
Suistimal türleri: İşbirliği

Suistimal bedeli (USD)

Kaynak: Bir Suistimalcinin Profili, KPMG International, 2016

Suistimal türleri: İşbirliği

Şirkette çalışma süresi



Kaynak: Bir Suistimalcinin Profili, KPMG International, 2016

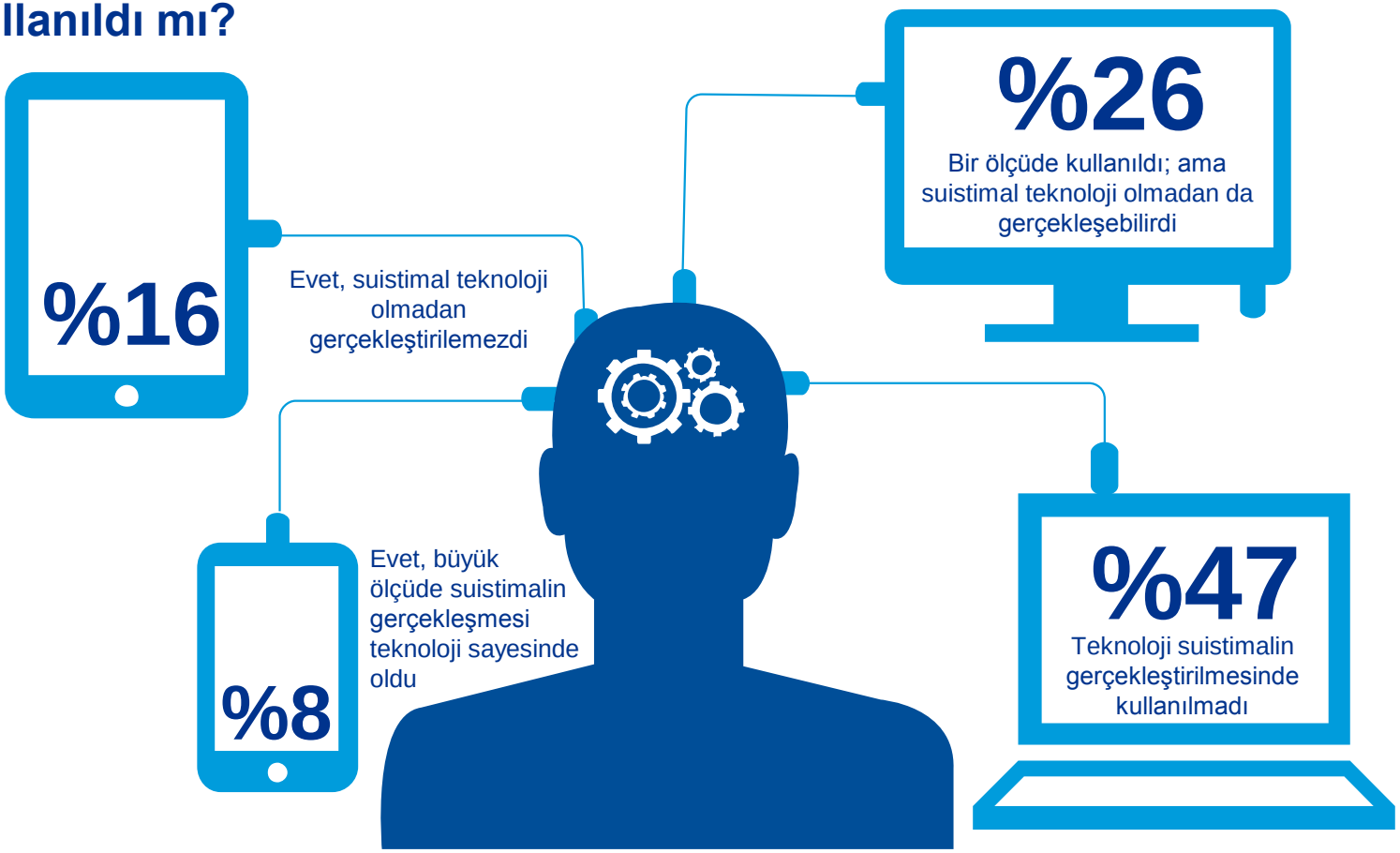
Suistimal türleri: İşbirliği

Kimliğini gizlemeden ve anonim bildirimde bulunanlar, beş kişilik ya da daha kalabalık grupları açığa çıkarma konusunda en yüksek orana sahip. Diğer tespit türleri, büyük işbirliği planlarını saptamada yetersiz olabiliyor.

Zayıf iç kontroller, işbirliği yapanlardan çok tek başına hareket edenler için önemli bir faktör (yüzde 66; işbirliği yapanlarda bu oran yüzde 58). Tek başına hareket edenlerin tesadüfen yakalanma oranı daha fazla (yüzde 19; işbirliği yapanlarda bu oran yüzde 10).

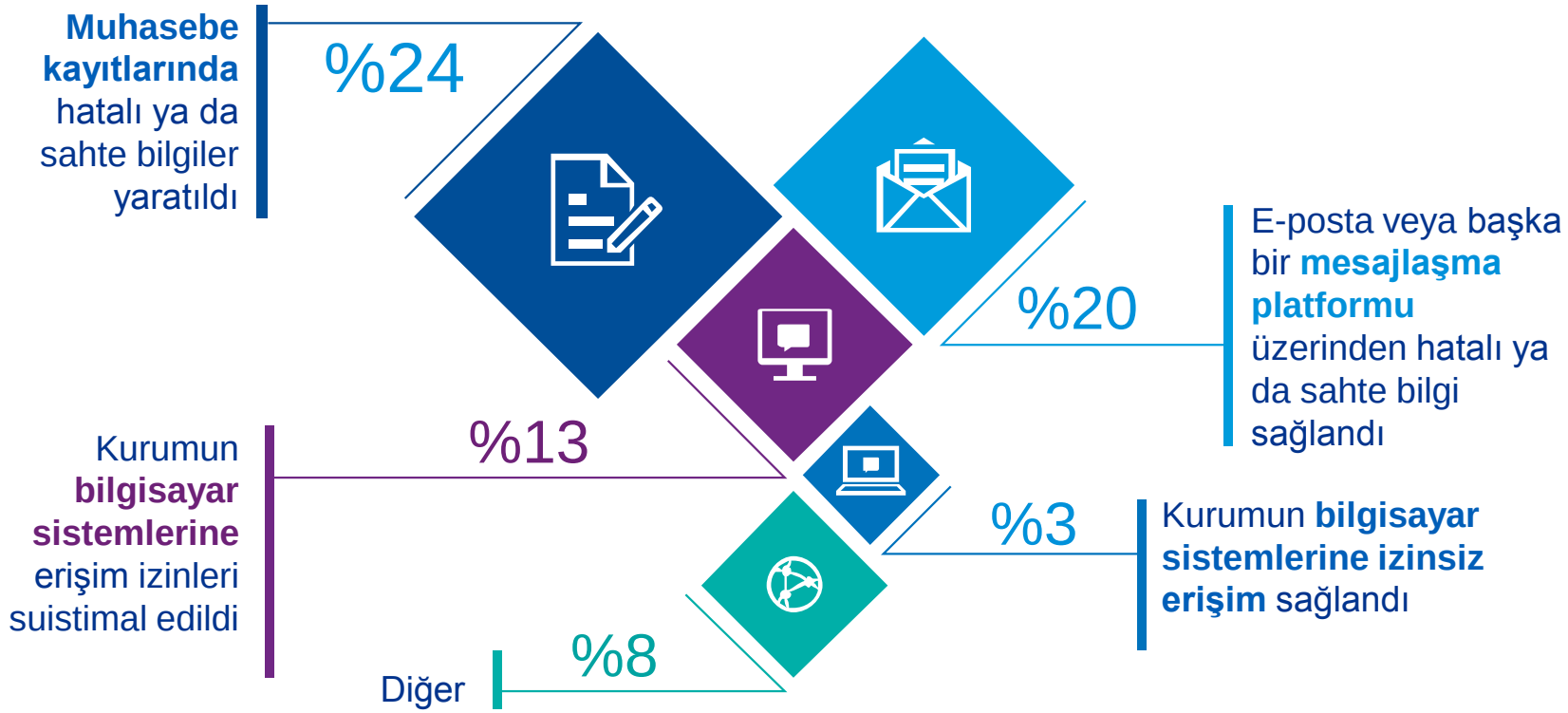
Kolaylaştırıcı unsurlar: Teknoloji

Suistimali gerçekleştirirken teknoloji kolaylaştırıcı bir unsur olarak kullanıldı mı?



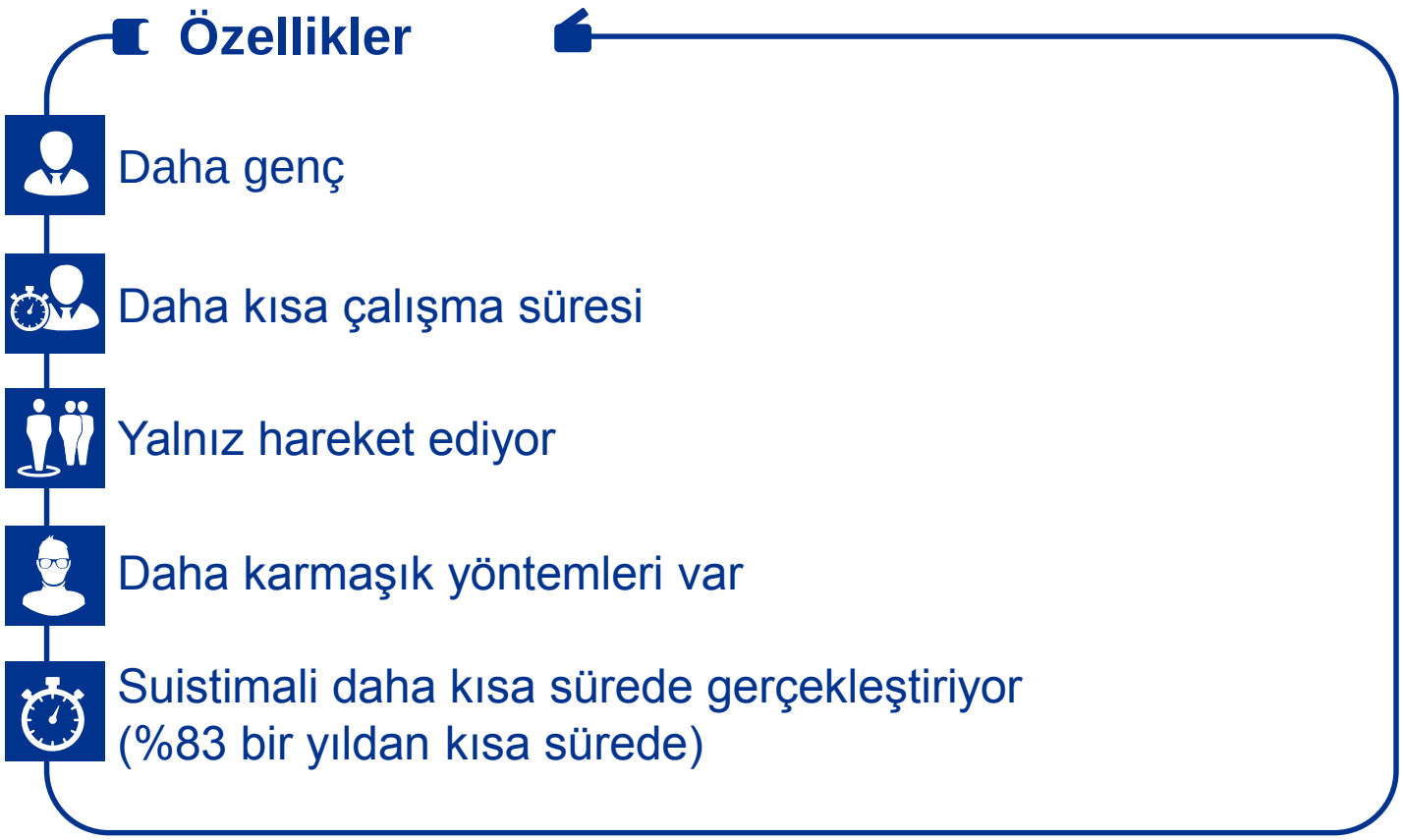
Kaynak: Bir Suistimalcinin Profili, KPMG International, 2016

Kolaylaştırıcı unsurlar: Teknoloji



Kaynak: Bir Suistimalcinin Profili, KPMG International, 2016

Suistimal türleri: Siber



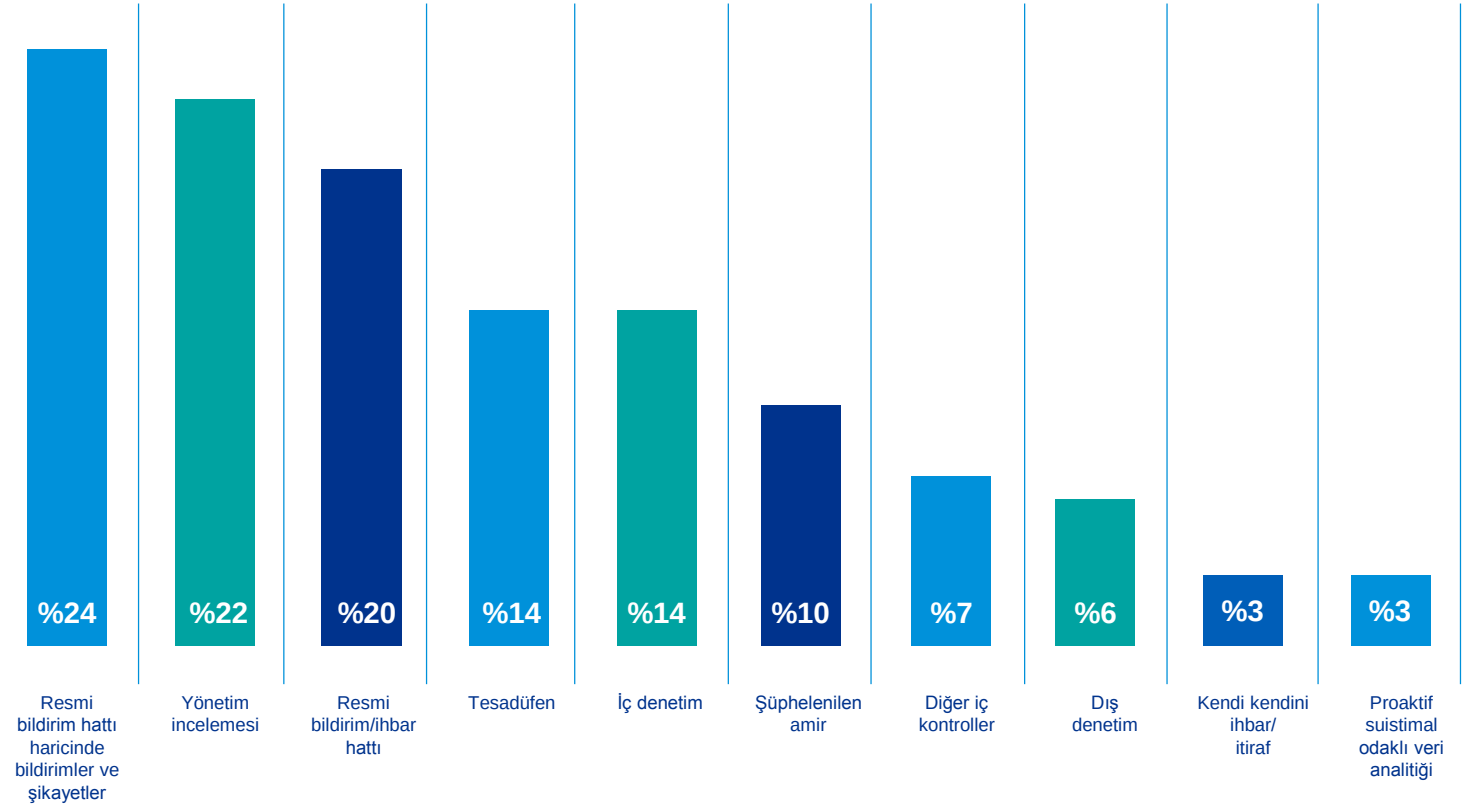
Kaynak: Bir Suistimalcinin Profili, KPMG International, 2016

Kolaylaştırıcı unsurlar – zayıf kontroller

Kaynak: Bir Suistimalcinin Profili, KPMG International, 2016

Tespit etme yolları

Suistimaller nasıl tespit edildi?



Kaynak: Bir Suistimalcinin Profili, KPMG International, 2016

Tavsiyeler

Risk değerlendirmesi gerçekleştirin

- Suistimal Risk Yönetimi

Teknolojiyle karşılık verin

- Adli bilişim teknolojisi
- Siber güvenlik
- Veri analitiği

İş ortaklarını ve üçüncü tarafları tanıyın

- Üçüncü Taraf Risk Yönetimi
- Kurumsal istihbarat/Astrus

İç tehditlere karşı dikkatli olun

- Etik hat / Bildirim hattı
- Soruşturmalar
- Adli veri analitiği
- Bildirim programları/dış kaynak kullanımı

Kaynak: Bir Suistimalcinin Profili, KPMG International, 2016

Risk değerlendirmesi gerçekleştirin

Suistimal Risk Yönetimi

Yönetim Kurulu/Denetim Komitesi gözetimi
İdari ve yatay yönetimin fonksiyonları
İç denetim, uyum ve izleme fonksiyonları

- Yolsuzluk ve suistimal risk belirleme
- Şirket içi davranış kuralları ve oluşturulan ilgili standartlar
- Çalışanlara ve üçüncü şahıslara yönelik durum değerlendirmeleri
- Şirket içi iletişim ve eğitimler
- Süreçlere özgü yolsuzluk önleyici kontroller
- Önleyici veri analizi araçları/çalışmaları

- Yardım ve etik hat mekanizmalarının kurulması ve etkin çalışmasının sağlanması
- Denetleme ve izleme
- Ortaya çıkarıcı veri analizi araçları/çalışmaları

- İç soruşturma politika ve prosedürleri
- Uygulama ve güvenilirlik politika ve prosedürleri
- Bilgilendirme politika ve prosedürleri
- İyileştirme aksiyonlarına yönelik politika ve prosedürler

Teknolojiyle karşılık verin

En yaygın 5 Siber Güvenlik Yanılgısı

	Yanılgı	Doğru
1	%100 güvenliği sağlamak zorundayız.	%100 güvenlik doğru bir hedef olmadığı gibi bunu başarmak da imkansızdır.
2	Sınıfının en iyisi teknik araçlara yatırım yaparsak güvende oluruz.	Etkin bir siber güvenlik, teknolojiye sandığınızdan daha az bağımlıdır.
3	Elimizdeki silahlar bilgisayar korsanlarının silahlarından daha güçlü olmalı.	Güvenlik politikalarınızı, saldırganların hedeflerine göre değil kendi hedeflerinize göre belirlemeniz gerekir.

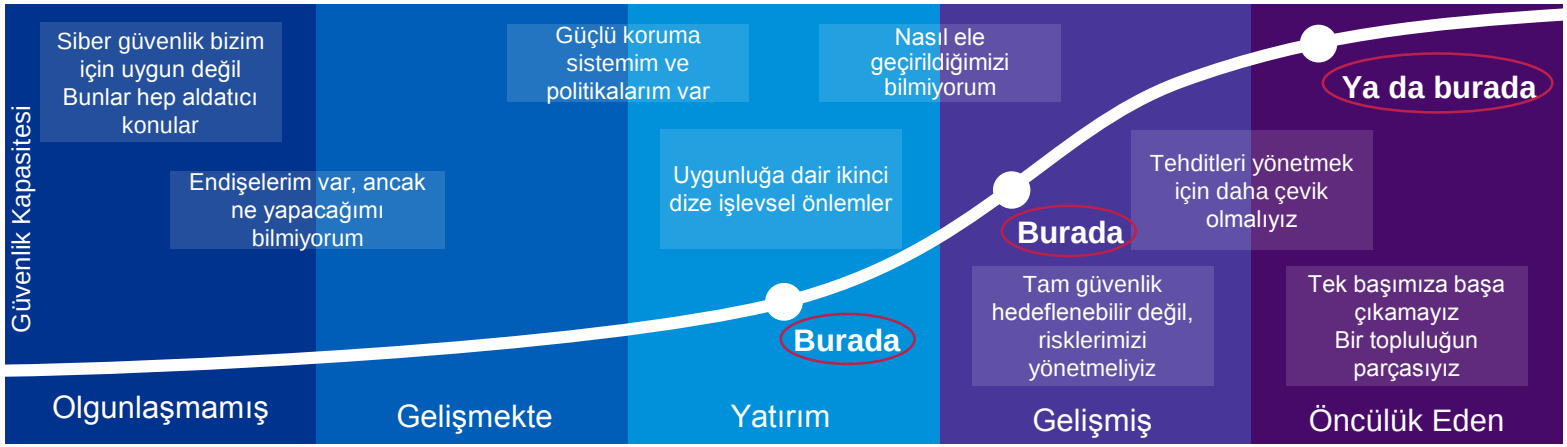
Teknolojiyle karşılık verin

En yaygın 5 Siber Güvenlik Yanılgısı

Yanılgı	Doğru
4 Siber güvenlik konusunda mevzuata uyum tamamen etkin gözetimle ilgili bir durum.	Öğrenme kabiliyeti en az izleme kabiliyeti kadar önemlidir.
5 Kendimizi siber suçtan korumak için en iyi profesyonelleri işe almamız gerekiyor.	Siber güvenlik sadece bir departmanın işi değil, kurumsal bir anlayıştır.

Teknolojiyle karşılık verin

Siber Güvenlik Olgunluk Değerlendirme Skalası



Önceliklerinizin değişmesi…

Olgunlaşmamış	Gelişmekte	Yatırım	Gelişmiş	Öncülük Eden
Kısıtlı farkındalık	Şirket için ne anlama geldiğinin tartışılması	Geliştirme için yatırım	Kurulların risk tartışmalarını detaylandırması	Topluluğun parçası olarak öncülük
Basit güvenlik teknolojilerine güven	Destek ve tavsiye için iletişime geçme	Hedef odaklı teknik çözümlerin benimsenmesi	Yapılandırılmış güvenlik programlarına geçiş	Siber ekosistemin tedarikçi ve müşterilerle kurulması
Mevcut olmayan kontrol ya da uygunluk süreçleri	Temel güvenlik süreçleri ve politikalar	Uyumluluk ve politikaların güçlendirilmesi	Güvenlik işlemlerinin gerçekleştirilmesi	Zeka ile yönetilen yaklaşımın kuruluşa yansıtılmasıı
Sorunu teknoloji problemi olarak görme	Genellikle düzenlemelerden kaynaklı endişeler	Güvenlik mimarisinin başlangıcı	Güvenlik arttırma testleri	Siber direnç
		Farkındalık eğitimlerinin başlangıcı	Erken dönem tedarik zinciri güvenlik önlemleri	Risk ölçümlendirmesi ve azaltma stratejisi
				Teknolojinin geçerli hale gelmesi

Siber Olgunluk Değerlendirmesi

HUKUK VE UYGUNLUK
- 3 Fazlı Korunma
- Finansal Risk Devri
- Kanuni Uygunluk

İŞLEMLER & TEKNOLOJİ
- Personel Güvenliği
- Fiziksel Güvenlik
- Kimlik & Erişim Yönetimi
- Tehdit & Zafiyet
- Ağ Güvenliği
- Siber Hijyen
- Hizmet Sunumu
- Denetim İzi & Gözetleme
- Mobil & Kablosuz Güvenlik

İŞ SÜREKLİLİĞİ
- Siber Güvenlikte İş Sürekliliği
- Paydaş Yönetimi
- İş Etki Analizi & Felaket Kurtarma
- Kriz Yönetimi

ÖNDERLİK & YÖNETİŞİM
- Siber Anlayış ve Vizyon
- Önderlik/Kurul Sorumlulukları
- Politikalar

İNSAN FAKTÖRLERİ
- Kültür
- Eğitim & Farkındalık
- Yetenek Yönetimi
- Uzmanlık Yetenekleri

BİLGİ RİSK YÖNETİMİ
- Bilgi Paylaşımı
- Mimari
- Risk İştahı
- Varlık Yönetimi
- Bilgi Risk Yönetimi Süreçleri
- Tedarikçiler

Ve daha fazlası....

Organizasyonlarda insanların davranışlarını etkileyen 7 faktör

1. Netlik: Direktörler, müdürler ve çalışanlara istenen ve istenmeyen davranışlar konusunda açıklık getirmek gerekiyor.

2. Şirketteki rol modellerin, yani müdürlerin, üst düzey yönetimin ve direktörlerin davranışları: etik lider

3. Hedeflerin, sorumlulukların ve görevlerin ulaşılabilir olması

4. Direktör, müdür ve çalışanların şirkete olan bağlılığı

5. Şeffaflık

6. Çalışanların görüşleri, çıkmazları ve duyguları hakkında açıkça konuşabilmeleri

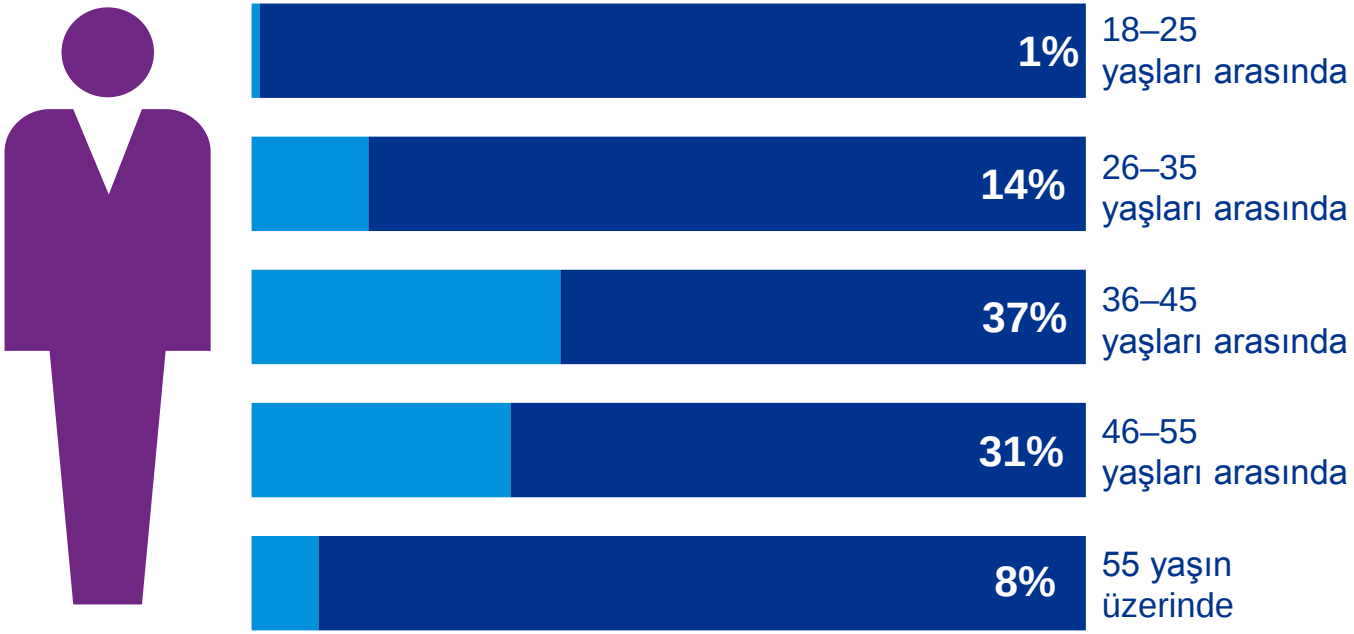
7. Uygulama

KPMG

EK

EK

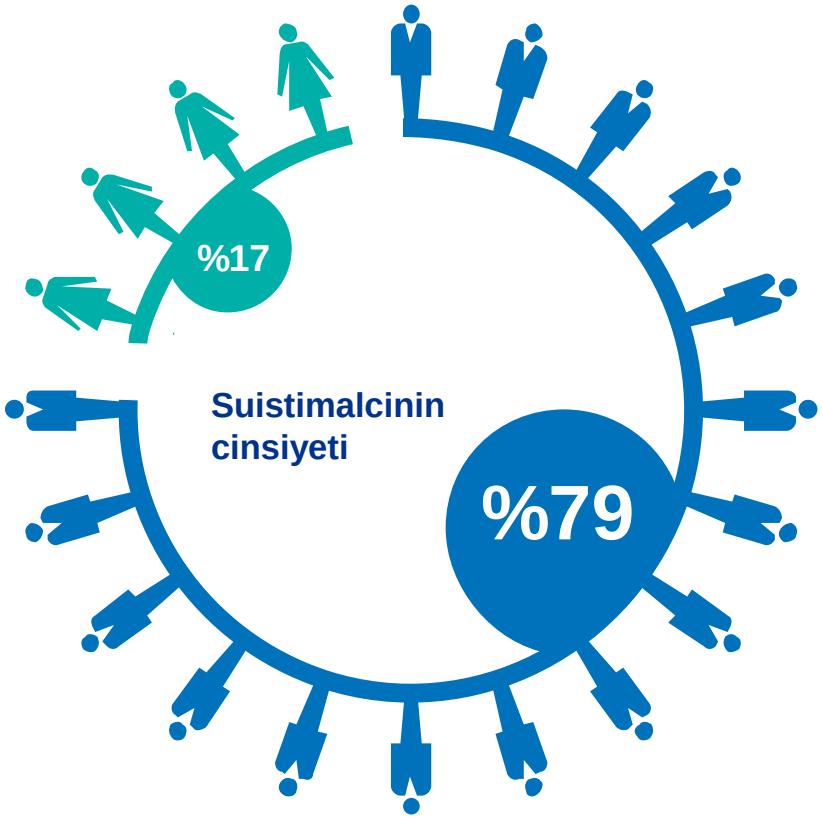
Suistimalcinin yaşı



*Diğerlerinin yaşı bilinmiyor

Kaynak: Bir Suistimalcinin Profili, KPMG International, 2016

EK



Diğerlerinin cinsiyeti bilinmiyor

Kaynak: Bir Suistimalcinin Profili, KPMG International, 2016

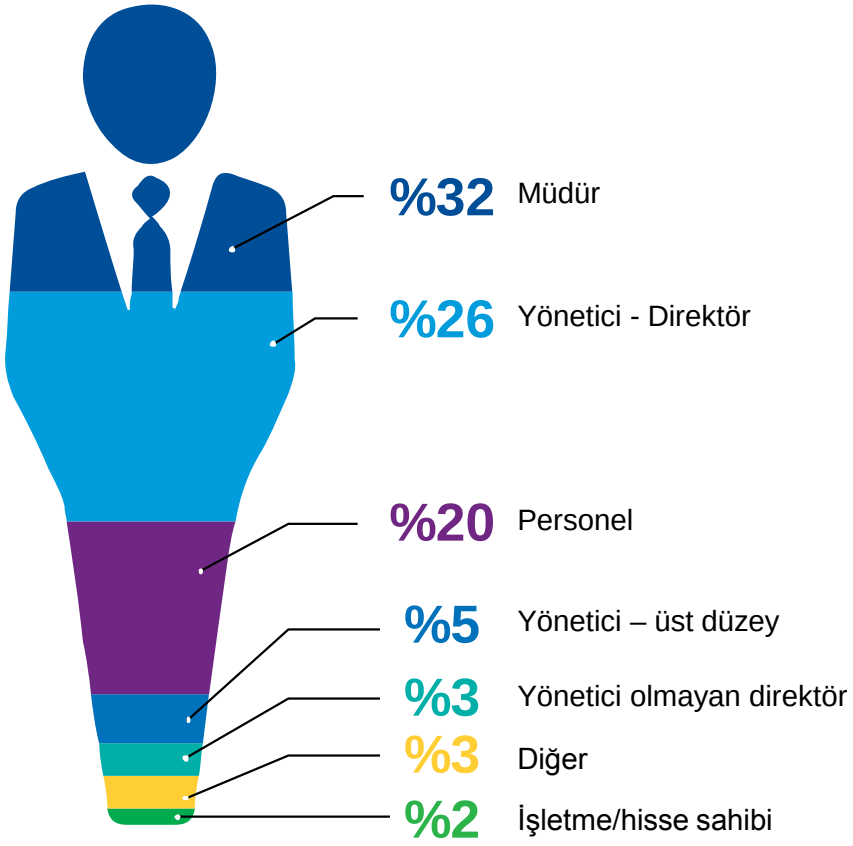
EK

Çalışma süresi

Kaynak: Bir Suistimalcinin Profili, KPMG International, 2016

EK

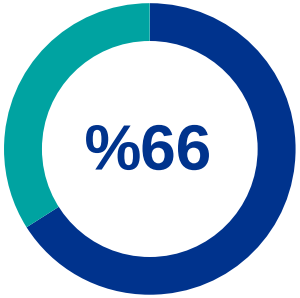
Kıdem seviyesi



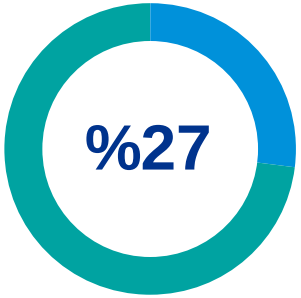
Kaynak: Bir Suistimalcinin Profili, KPMG International, 2016

EK

Suistimalcinin öne çıkan motivasyon kaynağı neydi?

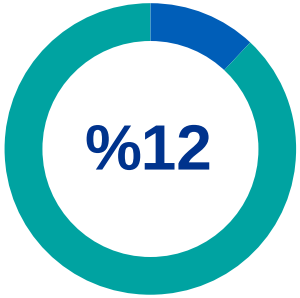


Kişisel maddi kazanç ve hırs

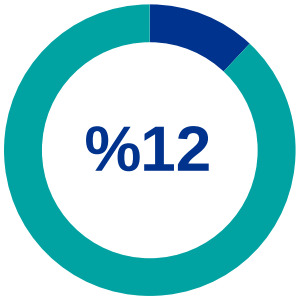


İstek/"Yapabiliyorum Duygusu"

Organizasyonel Kültür odaklı



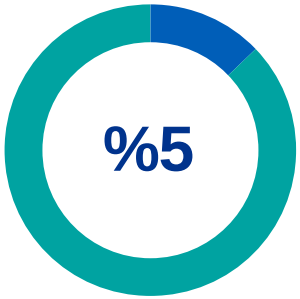
Bonus kazanmak için hedefleri tutturma/kayıpları gizleme isteği



İşini kaybetmemek için bütçeyi tutturma/kayıpları gizleme isteği

Şirketi korumak için hedefleri Tutturma/kayıpları gizleme isteği

Yukarıda sayılmayan diğer bir neden

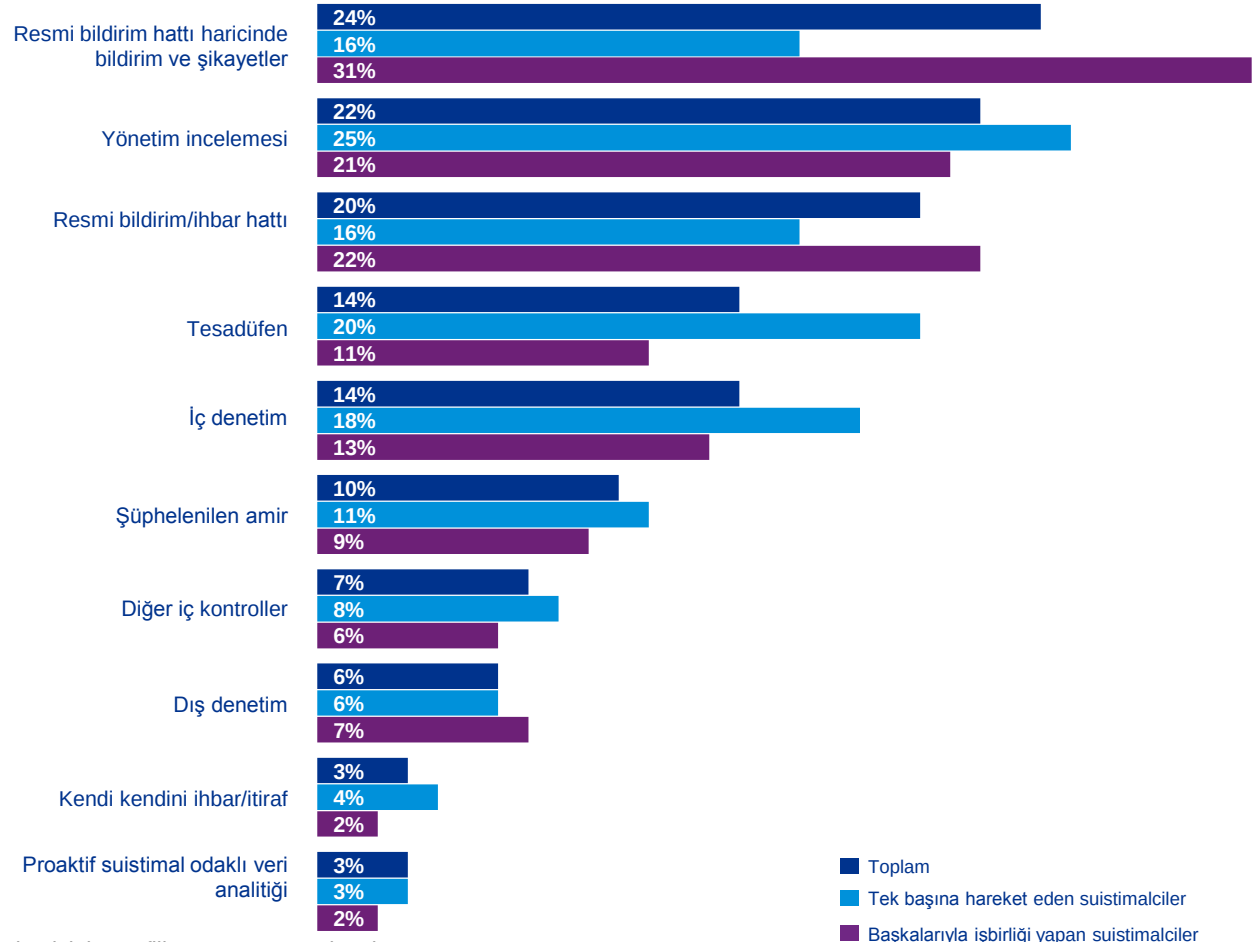


Diğer motivasyonlar arasında (% 5 ve altında oranla) kendine güvenin kaybolması, düzenleyici uyum gerekliliklerinden kaçınma, değerlendirme odaklı, medya görünürlüğü odaklı, operasyonların aksaması vb nedenler yer alıyor

Kaynak: Bir Suistimalcinin Profili, KPMG International, 2016

EK

Suistimaller nasıl tespit edildi?



Kaynak: Bir Suistimalcinin Profili, KPMG International, 2016

Teşekkür ederiz

İdil Gürdil
Suistimal Önleme ve
İnceleme Lideri
Risk Yönetimi Danışmanlığı,
Şirket Ortağı
E: igurdil@kpmg.com

Hakan Aytekin
Risk Yönetimi Danışmanlığı,
Bölüm Başkanı
Şirket Ortağı

E: hakanaytekin@kpmg.com