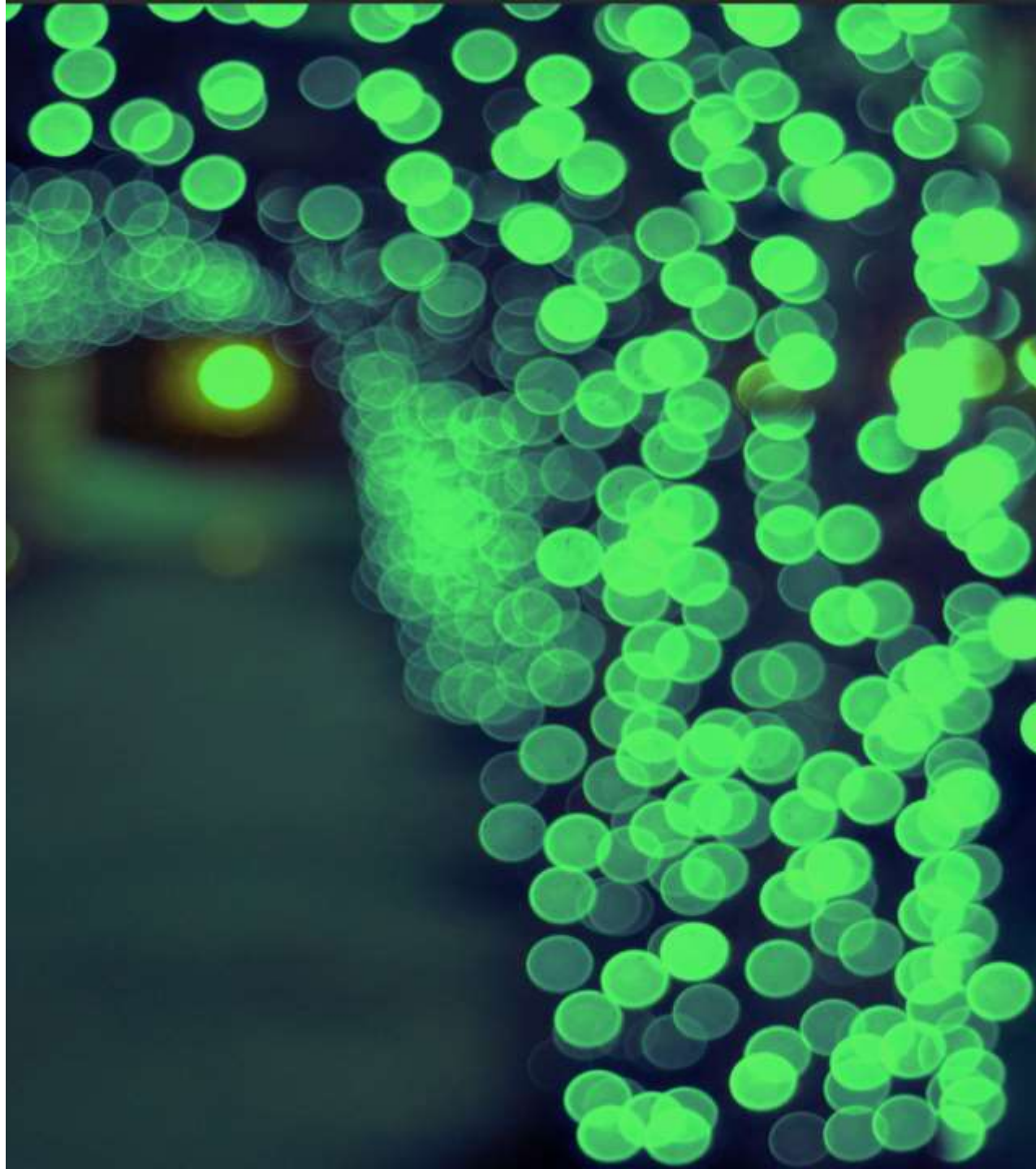


Deloitte.

Yönetim Kurulu Gündeminde Siber Güvenlik

Ali Yılmaz Kumcu
Deloitte Türkiye Siber Risk Lideri

TİDE XVIII. Türkiye İç Denetim
Kongresi – İstanbul 20 Ekim 2014



Video Gösterimi – Cyber Evolved

- http://youtu.be/zl5xu_hLYRU?list=PLwhdouPxnpJRatY3hO--Ohwl9ocg2-91O

Beş Önemli Gerçek

Bilgi ağınız saldırıya uğrayacak



Fiziksel güvenlik ve siber güvenlik ilişkisi artmakta



Siber zarar parayla ölçülememekte



Her varlığı aynı ölçüde koruyamazsınız



Yüksek duvarlar koruma sağlamaz



Siber Suçlular Nasıl Davranıyor?

Sızıntının Kaynağı / Sebebi	Oran
POS sistemlere sızma	14%
Web uygulamalarına yönelik saldırılar	35%
Kötü niyetli çalışan	8%
Fiziksel kayıp/hırsızlık	<1%
Genel hatalar	2%
Suç amaçlı yazılım	4%
Kart kopyalama	9%
Hizmet durdurma	<1%
Endüstriyel casusluk (siber)	22%
Diğer	6%

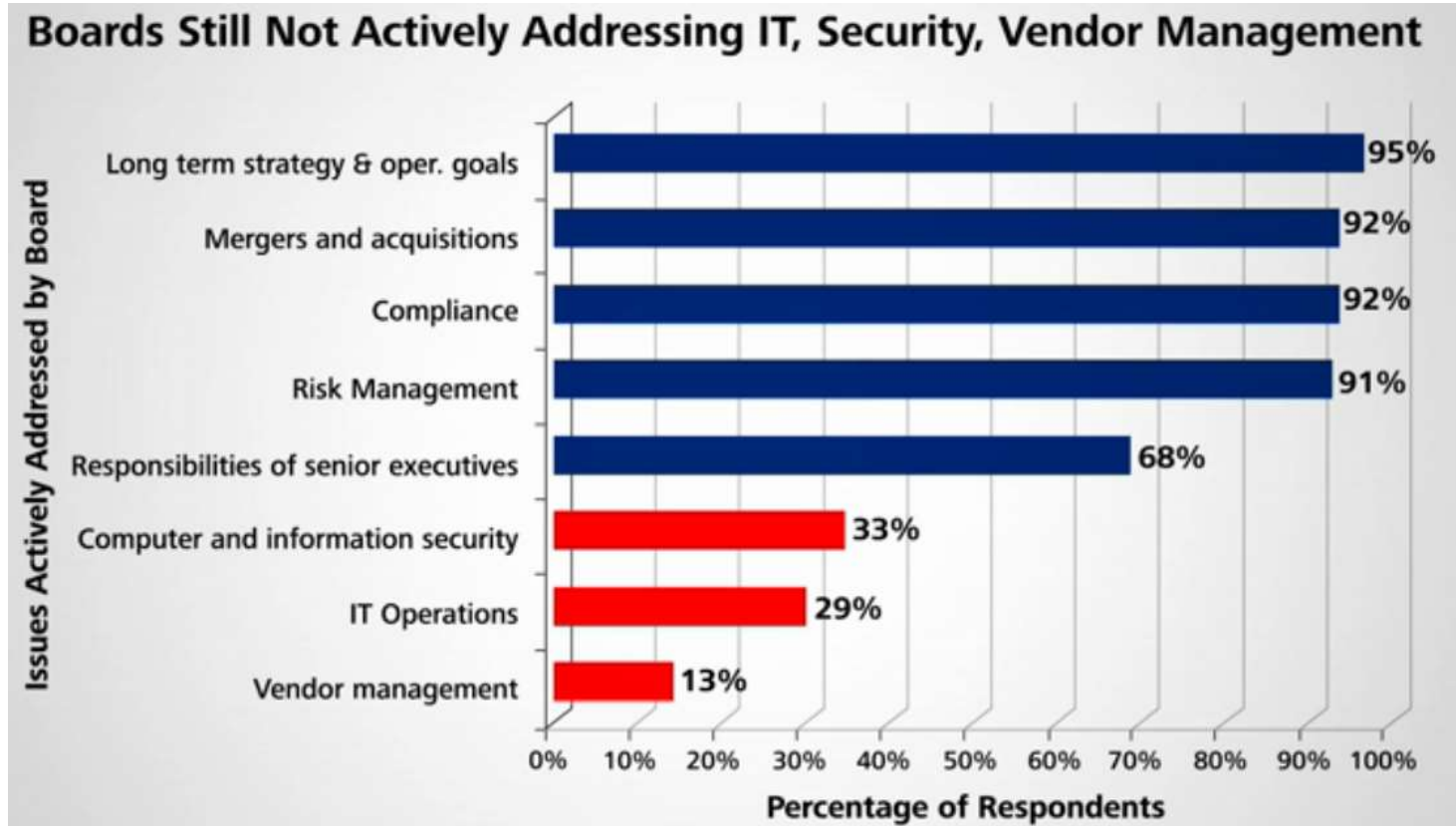
Kaynak: Verizon 2014 Data Breach Investigations Report
1367 veri sızıntısı olayı

Katılımcılara Soru (1)

- Şirketinizde siber riskler yönetim kuruluna raporlanıyor mu?
 - (1) Düzenli olarak
 - (2) Ancak bir olay olduğunda
 - (3) Hiç

Yönetim Kurulu Gündeminde Siber Güvenlik

Mevcut ama yetersiz!



Kaynak: Carnegie Mellon CyLab 2012 Survey

Yönetim Kurulunuz Oyuna Dahil Mi?

- Yönetim kurulunda bilgi teknolojileri ve siber risklerden anlayan bir üye var mı?
- Siber güvenlik risklerini takip eden bir komite var mı? Bu komite kimlerden oluşuyor?
- Şirketin güvenlik risklerinden sorumlu yöneticisi BT organizasyonu dışında mı?
- Sosyal medyada Şirketin itibarı yönetim kurulunun gündeminde mi?
- Tedarikçiler, iş ortakları ve taşeronlar Şirketin güvenlik politikalarına uyuyor mu?
- Çalışanlara yönelik bir siber güvenlik farkındalık programı var mı?
- Siber güvenliğe ayrılan bütçe yeterli mi?
- Yönetim kurulu bir siber güvenlik krizine hazırlıklı mı?
- Yönetim kurulunun siber riskleri danışabileceği uzmanlar var mı?

Yönetim Kurulunuz Neyi Merak Ediyor?



Odağımız doğru mu?



Doğru yardımı alıyor muyuz?



Proaktif mi reaktif miyiz?

Doğru yetenek ve kaynaklara sahip miyiz?



Değişime ayak uyduruyor muyuz?

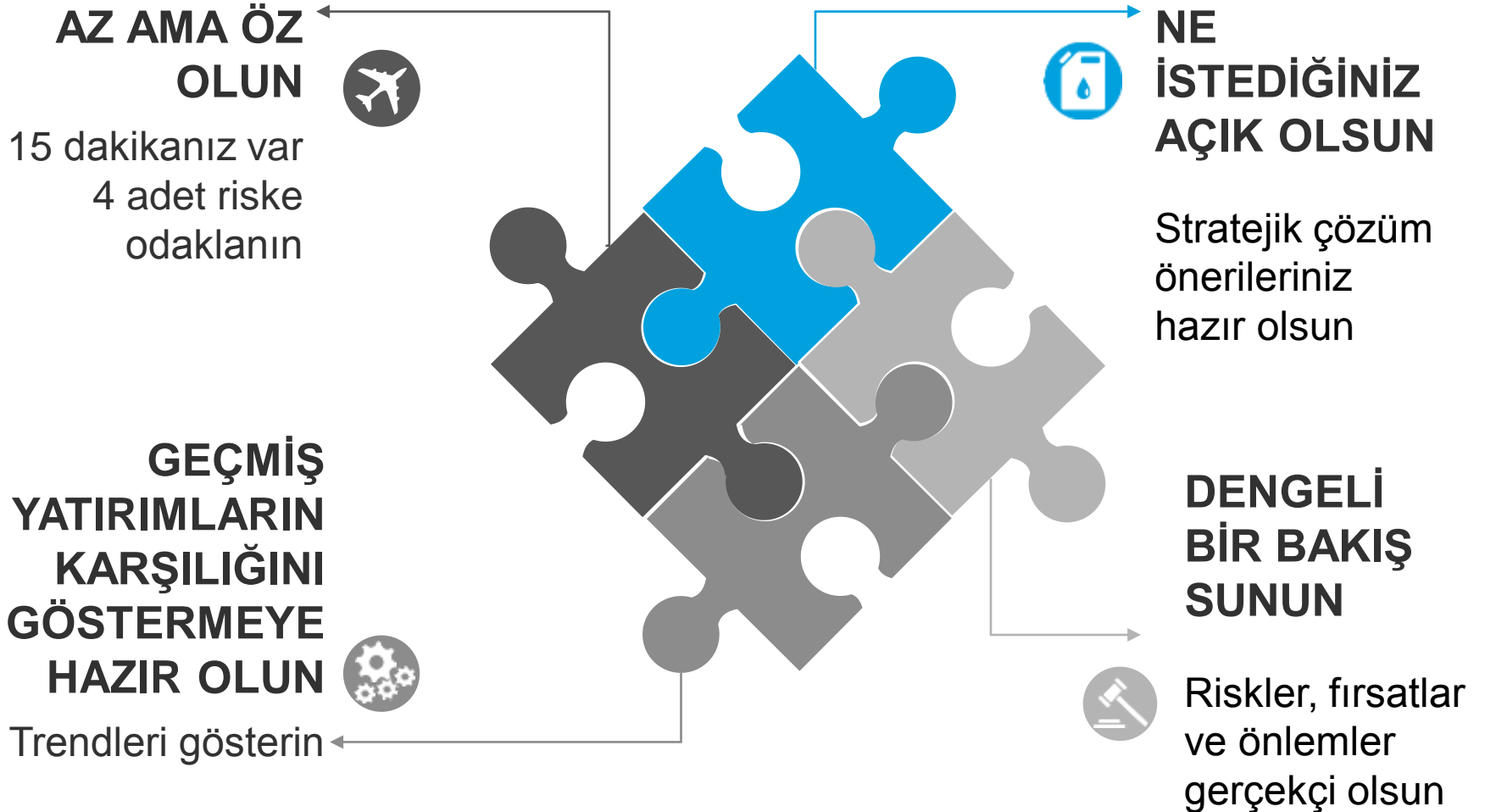


Katılımcılara Soru (2)

- Siber riskleri yönetim kuruluna ağırlıklı olarak kim raporluyor?
 - (1) Denetim veya Risk Komitesi
 - (2) CIO veya BT Müdürü
 - (3) Güvenlik Yöneticisi
 - (4) Risk Yöneticisi
 - (5) Dış Uzmanlar

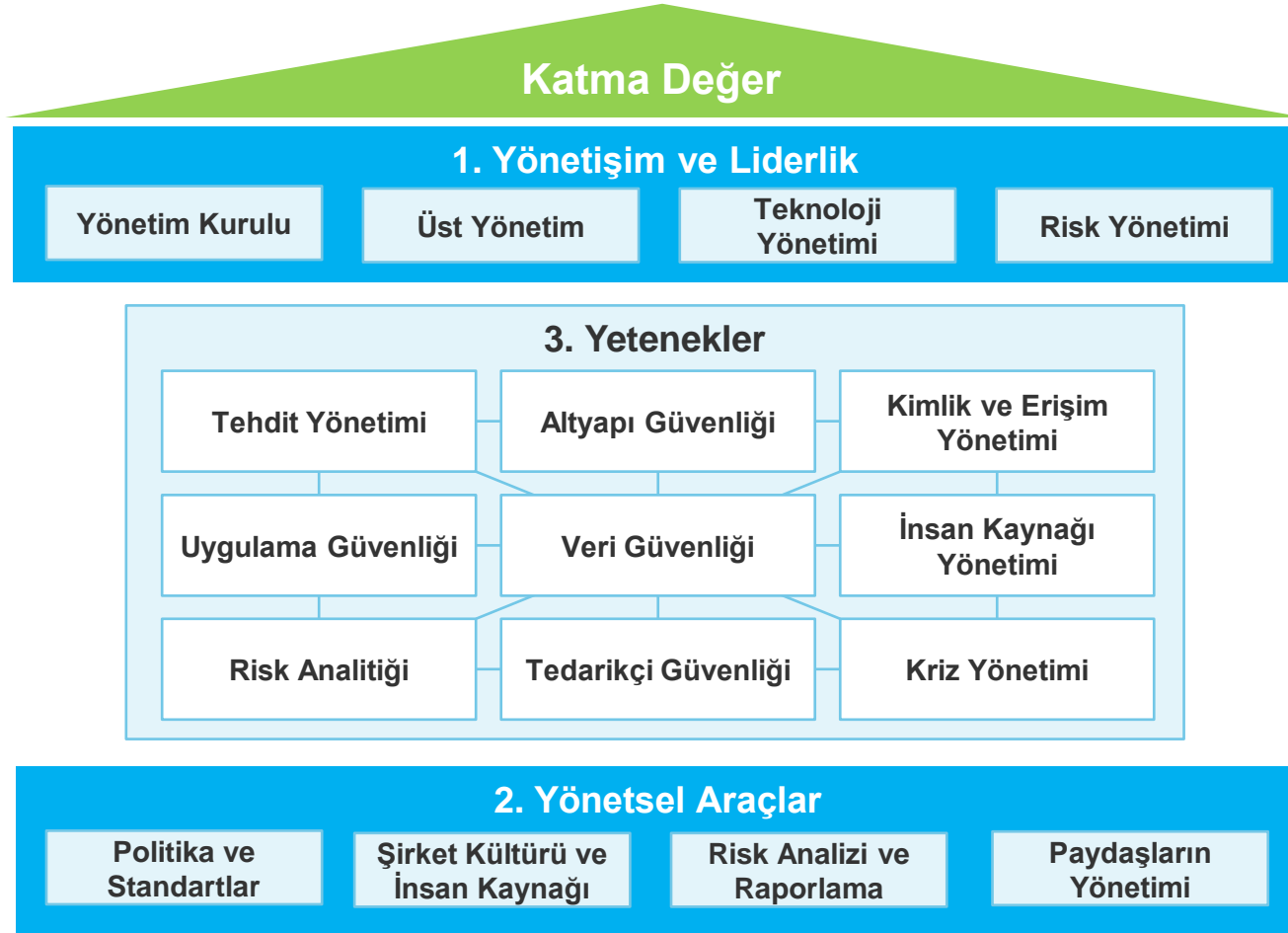
Yönetim Kurulu'na Siberi Sunarken Öneriler

Eski köyde eski adetler!



Yönetmek için ölçebilmek

Siber güvenlik çerçevesi



Yeni teknolojiler, yeni riskler...

Bugün:

- Mobilite
- Bulut Bilişim
- Big Data



Yarın ?

- Kuantum bilgi işlem
- Giyilebilir teknolojiler
- Makinelerin İnterneti
- E-coins



Katılımcılara Soru (3)

- Siber risklerinin tespiti veya yönetiminde dış kaynak kullanıyoruz:
 - (1) Asla
 - (2) Şimdilik hayır
 - (3) Sadece tespit için
 - (4) Operasyon dahil dış uzmanları kullanırız

Pratik Öneriler



Yönetim kuruluna teknoloji riskleri ve kişisel verilerin korunması konusunda tecrübesi olan bir üye kazandırın



Denetim komitesinden bağımsız bir risk komitesi kurun



Şirket çapında farkındalık faaliyetlerine destek olun



Siber risklerin YK'na düzenli olarak raporlanmasını sağlayın



Yönetim kurulu ve üst düzey yöneticiler olarak siber krizlere hazırlıklı olun



Tedarikçi ve taşeronlarınızın yol açtığı riskleri anlayıp, sizin standartlarınıza gelmelerine destek olun

Son Sözlür

İsimlere takılmayın

Riskleri kimin raporladığından çok doğru olarak raporlanıyor olması önemlidir

Vites yükseltin

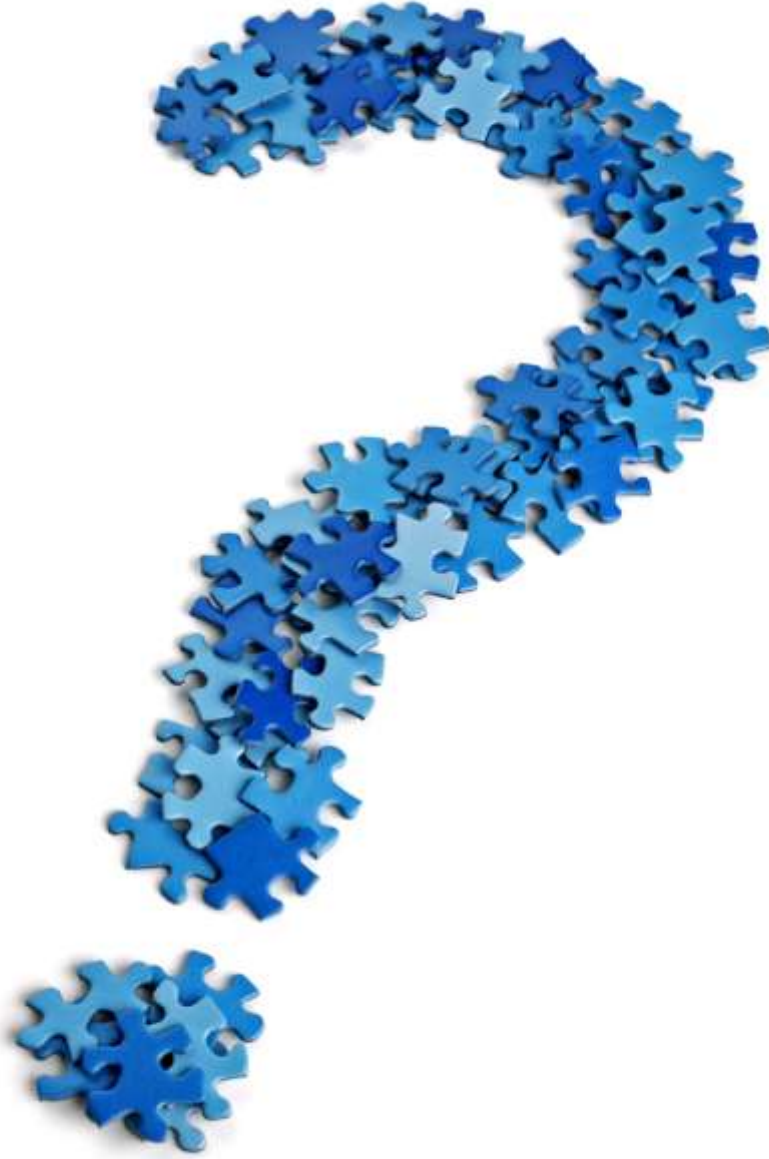
Siber tehditlerin hiç olmadığı kadar arttığı bir döneme girdik

Odaklanın. Hemen

İdeal organizasyonu kuracağınız zamana kadar geçen vakti iyi değerlendirin

Değişim kaçınılmaz

Yaklaşımınızı ve kaynaklarınızı nereye ayırdığınızı en az yılda bir kere gözden geçirin





Deloitte; İngiltere mevzuatına göre kurulmuş olan Deloitte Touche Tohmatsu Limited (“DTTL”) şirketini, üye firma ağındaki şirketlerden ve ilişkili tüzel kişiliklerden bir veya birden fazlasını ifade etmektedir. DTTL ve her bir üye firma ayrı ve bağımsız birer tüzel kişiliktir. DTTL (“Deloitte Global” olarak da anılmaktadır) müşterilere hizmet sunmamaktadır. DTTL ve üye firmalarının yasal yapısının detaylı açıklaması www.deloitte.com/about adresinde yer almaktadır.

Deloitte, denetim, vergi, danışmanlık ve kurumsal finansman alanlarında, birçok farklı endüstride faaliyet gösteren özel ve kamu sektörü müşterilerine hizmet sunmaktadır. Dünya çapında farklı bölgelerde 150’den fazla ülkede yer alan global üye firma ağı ile Deloitte, müşterilerinin iş dünyasında karşılaştıkları zorlukları aşmalarına destek olmak ve başarılarına katkıda bulunmak amacıyla dünya standartlarında yüksek kaliteli hizmetler sunmaktadır. Deloitte, 200.000’i aşan uzman kadrosu ile kendini mükemmelliğin standardı olmaya adanmıştır.

Bu belgede yer alan bilgiler sadece genel bilgilendirme amaçlıdır ve Deloitte Touche Tohmatsu Limited, onun üye firmaları veya ilişkili kuruluşları (bütün olarak Deloitte Network) tarafından profesyonel bağlamda herhangi bir tavsiye veya hizmet sunmayı amaçlamamaktadır. Deloitte Network bünyesinde bulunan hiçbir kuruluş, bu belgede yer alan bilgilerin üçüncü kişiler tarafından kullanılması sonucunda ortaya çıkabilecek zarar veya ziyandan sorumlu değildir.

© 2014. Daha fazla bilgi için Deloitte Türkiye (Deloitte Touche Tohmatsu Limited üye şirketi) ile iletişime geçiniz.