Mobil Güvenlik ve Denetim

IV. Bilgi Teknolojileri Denetim ve Yönetişim Konferansı

Ümit Şen, Ernst & Young

14 Mart 2013

ERNST & YOUNG
Quality In Everything We Do

Gündem

- Mobil veri üretimi ve kullanımına ilişkin sayısal bilgiler
- Mobil cihazlara güncel tehditler
- Mobil cihazlarda güvenlik
- Mobil cihazlarda denetim

Mobil veri üretimi, ne kadar çok?

Dünyada üretilen verinin

90%'ı

son 2 yılda üretilmiştir...

Mobil, Büyük Veri, Internet of Things?

...ve en iyimser tahminlere göre

2020 yılına kadar...

50 katına çıkacağı öngörülmektedir..

Mobil, Büyük Veri, Internet of Things?

Her dakika:

- 571 yeni web sitesi
- 695.000 Facebook "status update"
- 204.166.667 e-mail
- 2.000.000 arama sorgusu

2012: Internet üzerinde **9 milyar** cihaz

2020: Internet üzerinde (tahmini) **50 milyar** cihaz

Büyük veri: Ne kadar büyük???

6 milyar

mobil kullanıcı

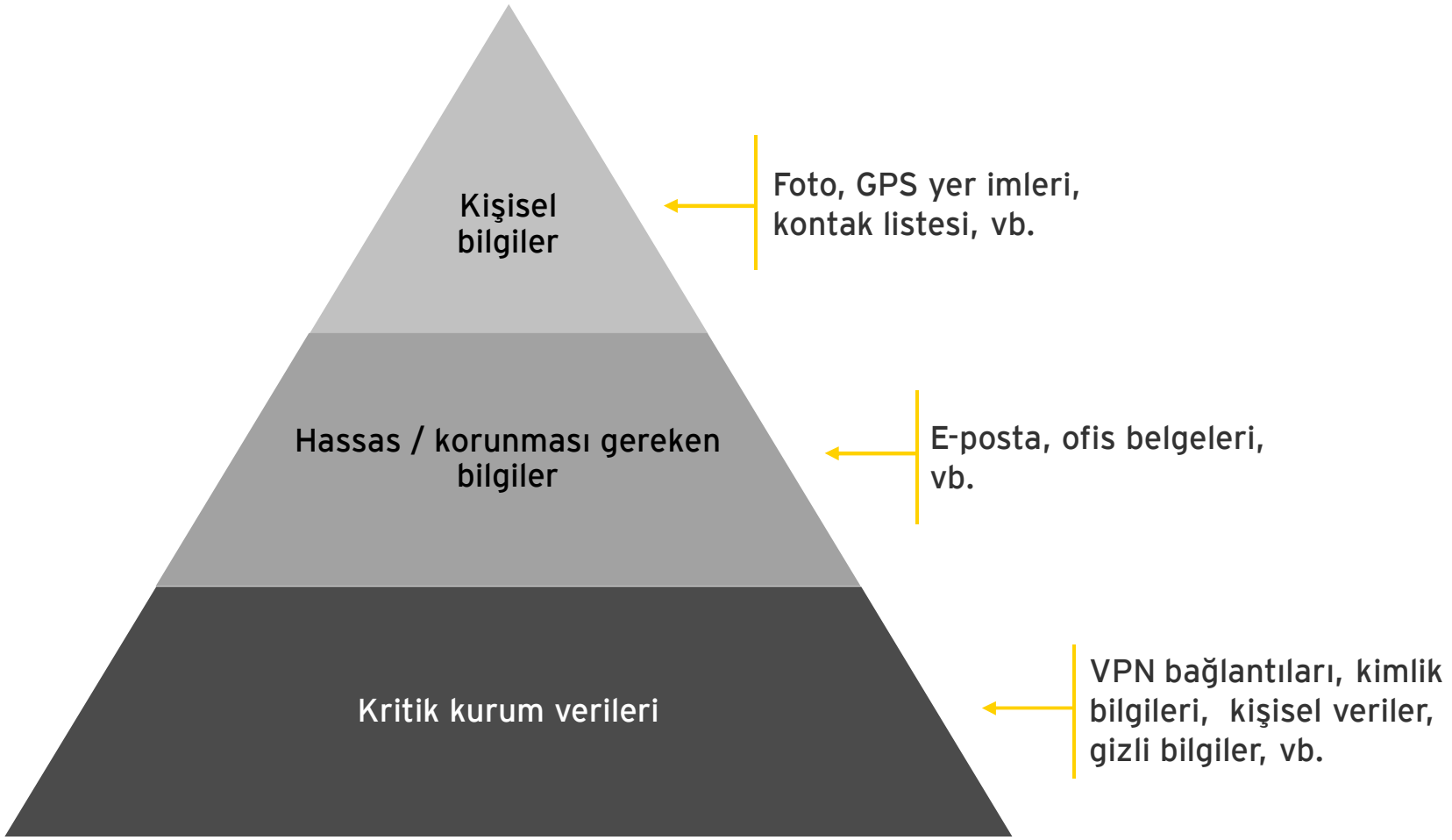
Mobil veri, her yıl 78% büyüme oranı

2016'da her ay...

10,8 Exabytes

1 Exabyte = 1.000.000 Terabyte

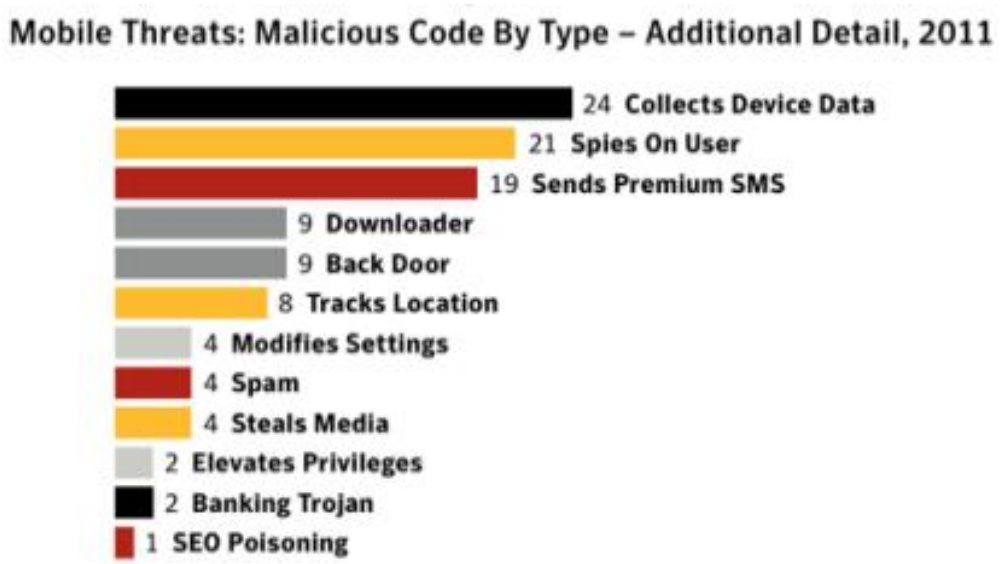
Mobil cihazlar kuruma özgü ve/veya kişisel hassas bilgiler ihtiva etmektedir...



...ve bir çok tehdide maruz durumdalar!

Web ve ağ üzerinden saldırılar	Web siteleri üzerinden cihazlar üzerine yüklenen zararlı yazılımlar ya da kişisel bilgilerin çalınması
Zararlı yazılım	Virüsler, solucanlar ya da Truva Atları...PC'den bir farkı yok...
Sosyal mühendislik saldırıları	Kritik/hassas bilgi çalmak ya da cihaza zararlı yazılım yüklemek amacı ile Phishing başta olmak üzere sosyal mühendislik saldırıları
Hizmet kesintileri	Spam ve hizmet dışı bırakma saldırıları...
Veri/bilgi hırsızlığı	Çalışanların ya da saldırganların kritik bilgileri cihaz dışına çıkarması...bilerek ya da bilmeyerek!
Veri bütünlüğüne saldırılar	Cihaz üzerinde tutulan verilerin, operasyonu duraklatmak ya da kazanç (ör: finansal) sağlamak üzere bütünlüğünün bozulması amacıyla saldırılar...

Hal böyleyken, mobil dünyada son zamanlarda yaşanan olaylar….



Kaynak: Symantec

Olay: X cihazı kullanıcılarına malware/spyware tehdidi, 2011

Olay: X markası telefon modellerinde yer (location) izleme, 2011

Olay: X firmasının mobil yazılımlarının cihaz üzerindeki bilgileri kaydetmesi, 2011-2012

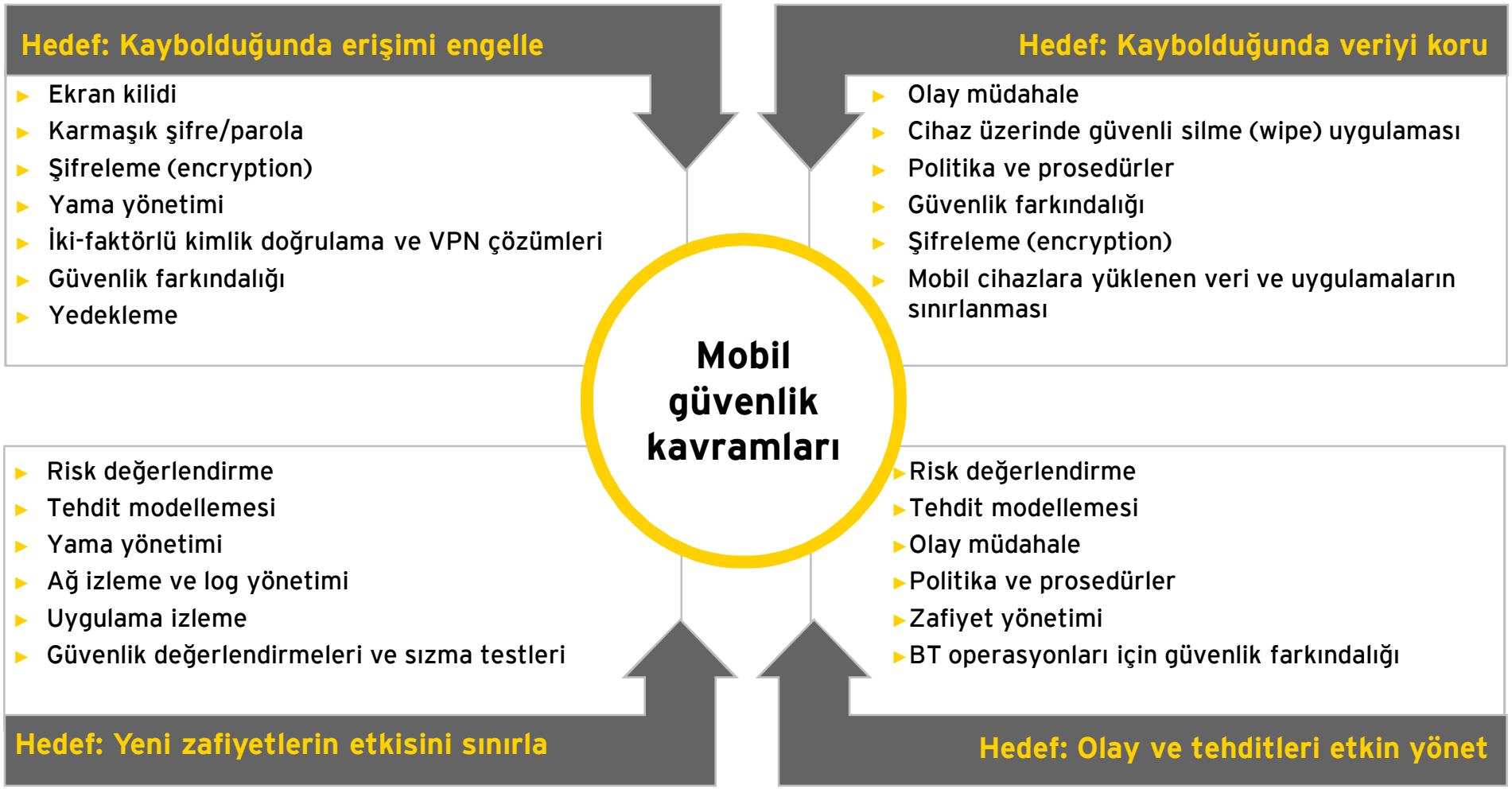
Olay: X sitesinin mobil uygulamasında güvenlik açığı – kişisel bilgilere erişim imkanı, 2012

Olay: X operatörünün müşterilerine ait bilgileri paylaşması, 2012

…ve yanlış sosyal medya kullanımı!!!

Twit'i yazan CFO, işten çıkarıldı!!!

Mobil cihazlarda güvenlik kavramı



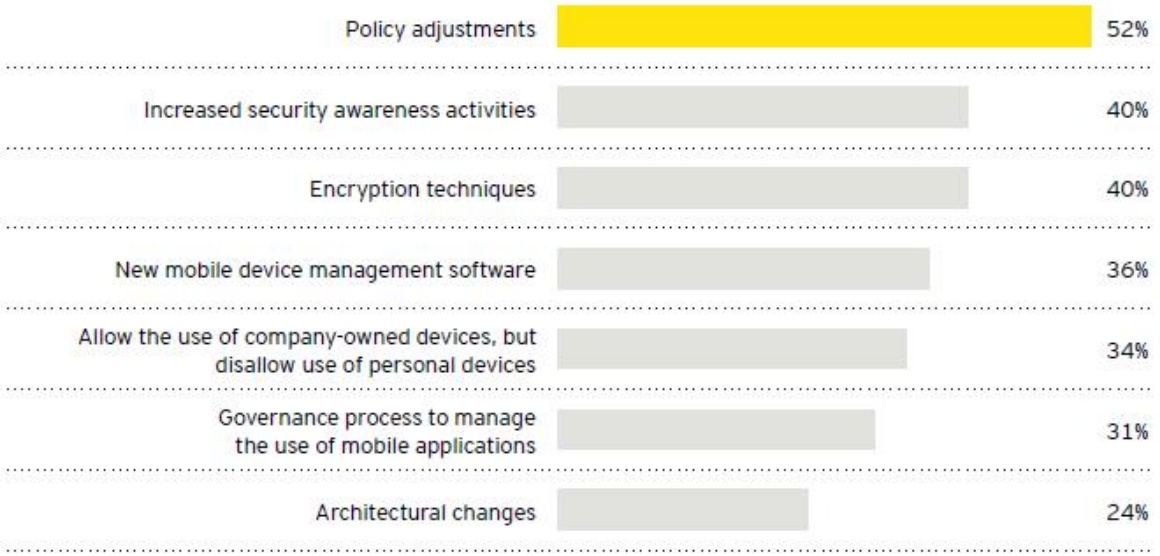
Dünyada önlemler?

Tablet bilgisayar kullanımı 2011'den 2012'ye **iki (2) misli** artmış durumda!

Organizasyonların %44'ü kurumsal ya da kişisel tablet kullanımına izin vermektedir.

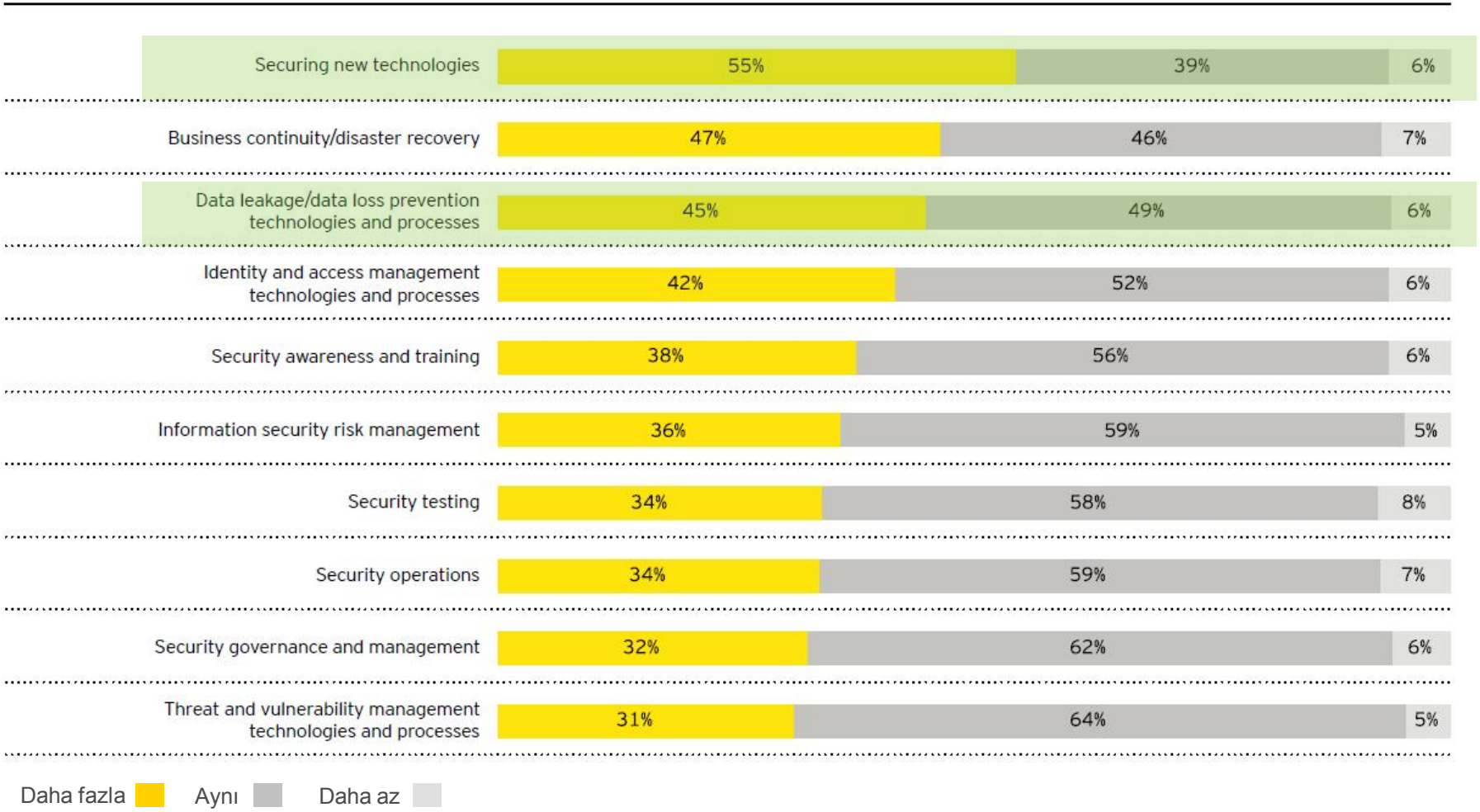
Önlemler nedir?

BYOD?



Kaynak: Ernst & Young, 2012 Küresel Bilgi Güvenliği Anketi

Peki ya harcamalar?



Kaynak: Ernst & Young, 2012 Küresel Bilgi Güvenliği Anketi

Mobil - Top 10 güvenlik önerileri (1/2)

1. Mobil güvenlik konusunu güvenlik farkındalığı programına eklemek
2. Cihaz kullanımını düzenleyen politikalar yaratmak ve devreye almak
3. Mobil ortama adapte edilen uygulamalardan kaynaklanacak tehditleri modellemek
4. Mobil uygulama geliştiricileri "güvenli uygulama geliştirme" konusunda eğitmek
5. Mobil cihazlara aktarılan verileri kısıtlamak – mümkün mertebe "salt okunur/read only" erişim vermek

Mobil - Top 10 güvenlik önerileri (1/2)

6 Mobil cihaz yönetim sistemleri/araçları kullanarak parola, encryption ve cihaz tarafında uygulanacak teknik önlemleri uygulamak

7 Cihazlar ve bunları destekleyen altyapı üzerinde cihaz üzerindeki verilere odaklanarak teknik güvenlik değerlendirmeleri yapmak

8 Mobil ortamdaki yeni ve güncel tehditlerin sürekli izlenmesini sağlayan bir program oluşturmak

9 Mobil cihaz bağlantı noktalarında izleme kontrolleri tesis etmek

10 Web tabanlı uygulamalara ve altyapıya karşı klasik tehditlerin değerlendirmesini yapmak

Ya denetim? ISACA ne diyor?

Konu başlığı	Denetleme alanları
Politika	▸ Güvenlik politikası ▸ Veri sınıflandırma ▸ Mobil cihaz tipleri (akıllı telefonlar, tablet, notebook, PDA, USB depolama, RFID destekli cihazlar) ▸ Onaylı / güvenilen uygulama listesi ▸ Kimlik doğrulama yöntemi ve şifreli depolama / iletim ▸ Cihaz üzerinde tutulan veri
Risk yönetimi	▸ Cihaz tipleri için risk değerlendirmeleri
Cihaz yönetimi	▸ Cihaz izleme ve yer tespit mekanizmaları ▸ Çalıntı / kayıp cihazlar için uzaktan güvenli veri silme (remote wipe) ▸ BYOD ya da üçüncü kişilerin cihazlarında kurum verisi tutulması, cihazların kurum mobil ağına eklenme koşul ve şartları ▸ Cihaz ekleme/çıkarma süreçleri
Erişim yönetimi	▸ Cihaz tipleri için erişim doğrulama mekanizmaları ▸ Erişim kontrol listeleri ve hakları ▸ Cihazların merkezi yönetimi ya da etkin dışı bırakılması ▸ Yüklenebilecek uygulama ve veri listesi

Ya denetim? ISACA ne diyor?

Konu başlığı	Denetleme alanları
Depolanan veri	▸ Şifreleme ▸ Şifreleme anahtarlarının yönetimi ▸ Veri transferi kuralları ve izleme ▸ Veri saklama koşulları, süresi ve imhası
Zararlı yazılım	▸ Zararlı yazılıma karşı koruma ▸ Zararlı yazılıma karşı kuralların düzenli güncellenmesi
Güvenli iletim	▸ VPN, IPSec, vb.
Farkındalık	▸ Eğitim ve bilinçlendirme ▸ Yeni teknolojiler, tehditler, önlemler

Diğer denetim teknikleri

Mobil cihaz konfigürasyon incelemesi

- Mobil cihaz platformu ve ilgili altyapı için risklerin tespit edilmesi
- Her cihaz tipi için uygulama modelleri ve konfigürasyon gözden geçirmeleri

Uygulama odaklı

Mobil uyumlu web uygulama değerlendirmesi

- Mobil cihazlar için tasarlanmış web sitelerine sızma testleri
- Destekleyici altyapı ve sunucuların değerlendirilmesi

Mobil uygulama değerlendirmesi

- Mobil cihazlarda yüklü uygulamalara sızma testleri
- Ağ bağlantıları ve veri yönetimine ekstra önem

Mobil kod "gray box" değerlendirme

- Mobil cihazlar üzerinde yüklü uygulamalara kaynak kod incelemesi ile birlikte sızma testleri

Teşekkürler...

ERNST & YOUNG

Quality In Everything We Do