

› THE HUMAN
DIMENSION

bilgi guvenliginde insana dair

eminim hepiniz
benimle bu konuda
hembiz
olacaksınız....



bilgi güvenliđi açığı

şirket güvenliđi açığı

kredibilite kaybı

**bilgilerimizi, ticari sırlarımızı,
varlıklarımızı ve işimizin akışını
koruduğumuzdan emin
olmalıyız**

bu konuda en uzak bir
ihmale yer
vermiyorsunuz

ama...



ÇALIŞANLARIMIZ ŞİRKET DATASINI VE ŞİRKET SİSTEMLERİNİ KULLANIYOR. MÜŞTERİLERİMİZE, HİZMETLERİMİZE VE ÜRÜNLERİMİZE DİREKT OLARAK ETKİ EDİYORLAR.

ÇALIŞANLARIMIZ BİLGİ GÜVENLİĞİNİN TEMEL PRENSİPLERİNİ TAM OLARAK ANLAMAK ZORUNDALAR.

Bir gerek:

bilgi gvenligi
sorunlarının %42'si
insan kaynaklı
sorunlar

Bilgi güvenliđi bugün, iş dünyasının karşıındaki en karmaşık durumlardan biri

55%

**network
güvenliklerini
sağlamak için 7 ayrı
hizmet şirketiyle
çalışan şirketlerin
yüzdesi.**

50%

**çalışanların yarısının data
güvenliđi ve şirket
güvenlik prosedürü
hakkında çok az veya hiç
fikri olmadığını düşünen
şirketlerin yüzdesi.**



Willing
for the
risk
his new

“bir çalışan” ne zaman
risk haline gelir?

bunların ne olduğunu
biliyor musunuz?

123456

Password

iloveu

yani...

sizlerle

ortalama bir çalışan
arasındaki fark

ÇOK BÜYÜK

Bir gerek:

biz bu konudan sizin
kadar anlamıyoruz

kâğıt, kalem, mektup

daktilo

bilgisayar

internet, e-mail

web 2.0, sosyal medya

sanal topluluklar

insanlar hareket halinde...

hem sanal, hem de gerçek
dünyada...

ve bilerek veya bilmeyerek

risk yaratıyorlar!

bir fotoğraf...

Büyük işletmelerin %87,5'unda bir güvenlik prosedürü bulunuyor.

Güvenliğe önem verdiğini belirten şirketlerin %67'sinde ayrıca bir bilgi güvenliği prosedürü de var.

Şirketlerin büyük çoğunluğu çalışanlarda bu konuda bilinçlendirme yapıyorlar.

Şirketlerin %50'sinden fazlası çalışanların uzaktan erişimine izin veriyor.

Internet erişimini kısıtlayan şirketlerin sayısı 2006'ya göre %50 azaldı.

Şirketlerin %10'dan azı çalışanların Internet erişimini yasaklıyor.

Çalışanlar artık daha çok sosyal mühendislik saldırılarının hedefi oluyorlar.

Şirketler, kendileri hakkında sosyal medyada yapılan yorumlara artık daha çok önem veriyorlar.

Büyük şirketlerin %80'i uygunsuz sitelere erişimi yasaklıyor.

Şirketlerin %86'sı çalışanlarının girdikleri siteleri logluyor ve izliyor.

daha çok iletişim,
daha çok hareket,
daha çok bilgi paylaşımı,
daha çok etkileşim

kazanc büyük ama
getirdiği risk de büyük

çalışanlarınız

hızla bilgi güvenliğinizdeki

en Zayıf halka haline

gelebilirler

**alıřan davranıřını deęiřtirmek,
bilgi gvenlięini saęlamamanın en
nemli yolu.**



nash ?

çalışanlara net bir resim çizin

EMAIL GÜVENLİĞİ

INTERNET GÜVENLİĞİ

DATA GÜVENLİĞİ

VARLIK GÜVENLİĞİ

prosedürleriniz var mı?

neden?

erişimi çalışanlarınızın bilgi seviyesi ve ihtiyaçlarına göre düzenleyin

riskinizi kişiye özel hale getirin

ama prosedürleriniz daima standart olsun

bir prosedürü aktarmanın
en kötü yolu, onu
yayınlamaktan geçes

eğitin, eğitin, eğitin:

çalışanlarınızın

“bilinçlenme” kasını

çalıştırmalarını sağlayın

iyi alışkanlıklar kazandırın

en iyi uygulamalarınızı
paylaşın

bir bilinç kültürü

oluşturun:

diyalogu elden bırakmayın

**Resmiyet
kazandırın:
çünkü bu ciddi bir
konu**

basitleştirin,

eglençeli hale getirin,

katılımcı hale getirin

bilgi güvenliğini
yönetimin
sahiplenmesini
sağlayın

tamamen proaktif
olun

notatların:

kıssısel $\neq$ profesyonel

yasaklamak

sınırlamak

kısıtlamak

başarıya giden yol değil

güven ortamı oluşturun

cevapsiz bırakmayın

WIIIFM?*

BBYNNV?

ik & it ortaklığı

ik bunlardan söz ediyor mu?

korkarım hayır...

konunun hukuki tarafı çok net değil...

sizler, bilgi güvenliği ve süreçlerinin **mentor'u** olmalısınız

çalışanlarınız bilgi güvenliği ve süreçler konusunda **okur-yazar** olmalı

şirketiniz bilgi güvenliği ve süreçleri dilini **en akıcı şekilde konuşmalı**

bana ulaşmak isterseniz



E-mail:

pinar.akkaya.pa@gmail.com

LinkedIn:

<http://tr.linkedin.com/in/pinarakkaya>

Twitter: <http://twitter.com/PINARAKKAYA>

<http://twitter.com/lifesocialmedia>



HR Leaders
Turkey

<http://tr.linkedin.com/groups/hrleadersturkey>