Bilgi Teknolojilerinde Gelişmeler, Bilgi Güvenliği ve Bilişim Hukuku (Aracı Kurumlar Açısından)

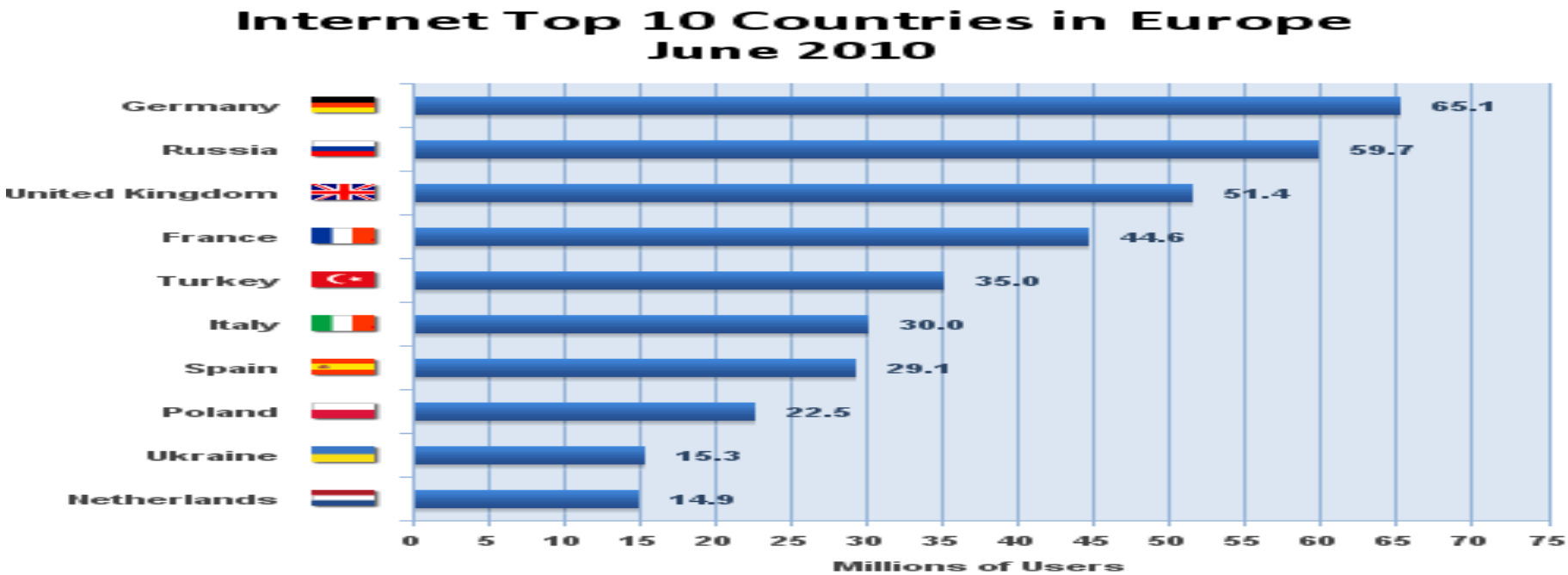
İzzet Gökhan ÖZBİLGİN
MSc, MBA, PhD

TSPAKB
İstanbul, 20 Ocak 2011

Sunum Planı

- Bilgi Teknolojilerinde Gelişmeler
- Bilgi Güvenliği ve Bilişim Hukuku
- Sermaye Piyasaları ve Bilgi Sistemleri
- Aracı Kurumların Bilgi Sistemleri
- Operasyonel Risk
- Mevzuat
- Genel Değerlendirme

İnternet…



Source: Internet World Stats - www.internetworldstats.com/stats4.htm
Basis: 475,069,448 estimated Internet Users in Europe on June 30, 2010

İnternet (Türkiye)

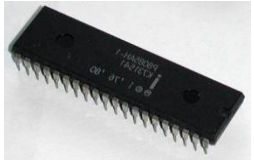
YEAR	Users	Population	% Pop.	User Growth (2000-2010)
2000	2,000,000	70,140,900	2.9 %	
2004	5,500,000	73,556,173	7.5 %	1650 %
2006	10,220,000	74,709,412	13.9 %	
2010	35,000,000	77,804,122	45.0 %	

TEKNOLOJİK GELİŞMELER

(Kaynak: A. Pekel, "Bilişim Teknolojilerinde Yönetişim", Bilgi Teknolojileri Yönetim ve Denetim Konferansı 2010, www.btyd.org)

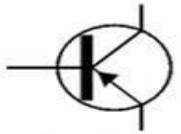
İşlemci Hızı (Mhz) (Intel)

- 500 (1999)
- 3000 (2009)
- 6 katı



Transistör Sayısı (Intel)

- 9,500,000 (1999)
- 820,000,000 (2009)
- 86.3 katı



Mobil İletişim (Kbps)

- 237 (1999)
- 42,000 (2009)
- 177.2 katı

BT GELİŞİMİNDE SON 4 DÖNEM

(Kaynak: A. Pekel, "Bilişim Teknolojilerinde Yönetişim", Bilgi Teknolojileri Yönetim ve Denetim Konferansı 2010, www.btyd.org)

1984 - 1993

- Multimedya Dönemi
  - CD ROM'lar

1994 - 1999

- WEB Başlangıç Dönemi
  - E-posta
  - İnternet
  - İntranet
  - Düşük Kalite Ses ve Görüntü

2000 – 2005

- Yeni Dönem WEB
  - Yüksek kalite ses ve görüntü aktarımı

2006 – Bugün

- Yüksek performanslı mobil iletişim ve uygulamalar

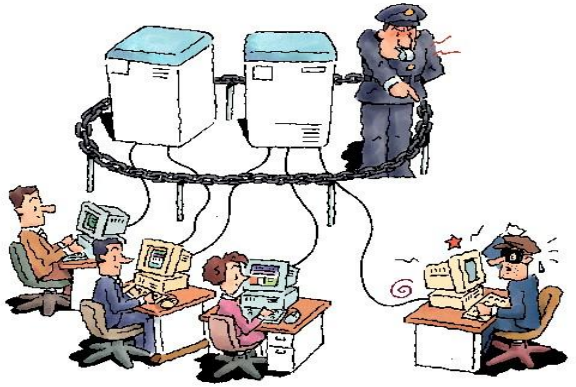
GELİŞEN TEKOLOJİ ve KULLANIM ORANLARI

(Kaynak: A. Pekel, "Bilişim Teknolojilerinde Yönetişim", Bilgi Teknolojileri Yönetim ve Denetim Konferansı 2010, www.btyd.org)

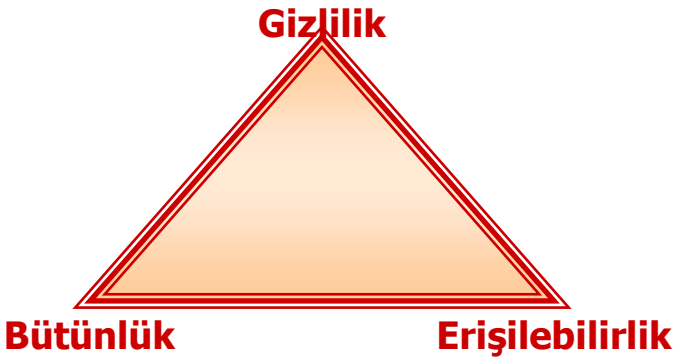
İnternet Kullanıcı Sayısı (kaynak:Internet WorldStats)	• 360,985,492 (2000) • 1,966,514,816 (2010) • 5.4 katı (Dünya Nüfusunun %28.7'i)
E-ticaret (kaynak:PCWorld)	• 27,467,000,000 $ (2000) • 127,395,000,000 $ (2007) • 4.6 katı
İnternet Tehdit Sayısı (kaynak:Symantec)	• 20,547 (2002) • 1,656,227 (2008) • 80.6 katı

Bilgi Güvenliği

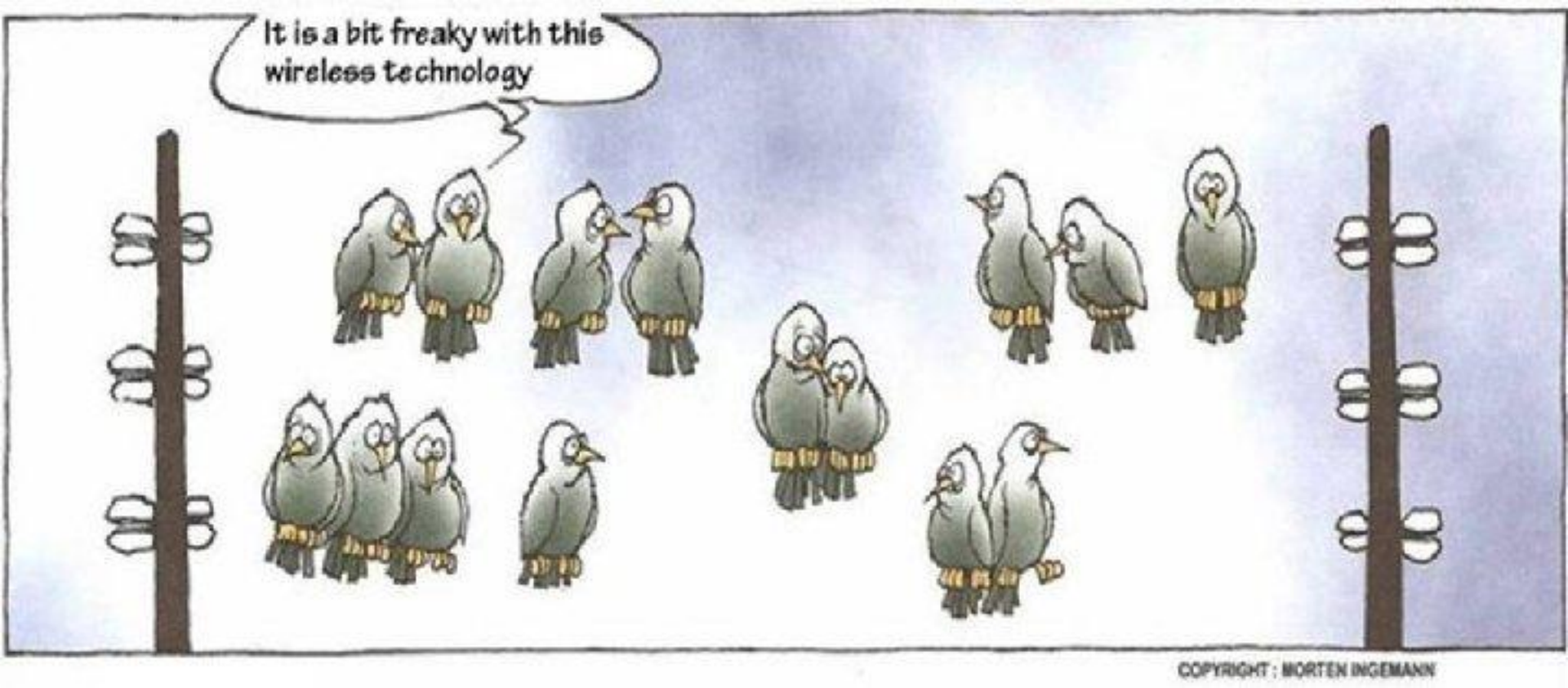
- Yazılı, sözlü, elektronik ortam gibi farklı ortamlardaki bilginin gizlilik, bütünlük ve erişebilirlik bakımından güvence altına alınması ve bu durumun sürekliliğinin sağlanmasıdır.



- Gizlilik (Confidentiality)
- Bütünlük (Integrity)
- Erişebilirlik (Availability)



Kablosuz ve Mobil Uygulamalar



Bilgi Güvenliği İhlal Olayları

Former network engineer faces jail time for sabotaging patient data

Jon Paul Oson also faces fines of up to $500,000

COMPUTERWORLD Security

Jaikumar Vijayan Today's Top Stories ▸ or Other Cybercrime and Hacking

Comments (7) Recommendations: 133 — Recommend this article

September 5, 2007 (Computerworld) -- A former network engineer and technical services manager at the Council of Community Clinics (CCC) in San Diego could spend 10 years in prison after a federal jury convicted him last week of hacking into his former employer's computers and sabotaging patient data.

In addition, Jon Paul Oson could face fines of up to $250,000 for each of the two charges on which he was found guilty. Oson was arraigned in August 2006 on charges of willfully damaging protected computers belonging to the CCC, a nonprofit organization that provides a variety of services to 17 community health clinics in the area.

Oson worked at the CCC between May 2004 and October 2005, and resigned from the organization following what he perceived to be a negative performance evaluation, according to a statement announcing his conviction from the FBI's San Diego field office.

About two months after he resigned, Oson illegally accessed the the CCC's network and disabled a process for automatically backing up patient data belonging to North County Health Services (NCHS), a clinic that stored its patient management system on the CCC's computers.

A few days later, Oson attacked the CCC's network again and systematically deleted data and software on several servers, including the patient data for the NCHS clinic, the FBI said. The deleted data included billing details, scheduling of patient appointments, case histories, diagnoses and treatment plans. In addition, Oson deleted and attempted to delete data on several other servers used by the CCC and other clinics, according to the FBI.

5 Eylül 2007 tarihli bir haber :

Bir hastanenin eski Ağ Mühendisi eski **işverenin bilgisayarlarını hack ediyor ve hasta bilgilerine hasar veriyor.**

•Öncesinde sisteme girerek veri yedekleme prosesini durduruyor.

•Bundan birkaç gün sonra ise tekrar sisteme girerek, sistematik bir şekilde verileri ve bazı yazılımları siliyor.

• Kaybolan veriler arasında, hasta ödeme bilgileri, hasta randevuları, hasta geçmişleri, hastalık bilgileri ve tedavi planları var.

•Saldırının Sebebi : Düşük performanstan dolayı işten atılma.

•Sonuç : Saldırgan 10 yıl hapis cezası ve 500.000 $ para cezası ile yargılanıyor.

Hastane için ise ağır maddi kayıp, yanlış tedavi riski, prestij ve müşteri kaybı.

Bilgi Güvenliği İhlal Olayları

ZİNCİR E-POSTA

Phishing ve Pharming

- **Phishing;** çevrimiçi dolandırıcılık.İnternet kullanıcısını kandırarak, kullanıcıya ilişkin kredi kartı bilgileri, banka hesap numaraları, İnternet şifresi gibi birçok özel bilgiyi ele geçirmektir.

- **Pharming** kişiyi güvendiği bir web sitesi yerine başka bir siteye yönlendirmektir. Bu sayede bir banka sitesine logon olduğunuzu düşünürken bir saldırganın hazırladığı sahte bir siteye logon olabilir ve şifrelerinizi kaptırabilirsiniz. (bir zararlı kod, DNS ele geçirme vb.)

SOSYAL MÜHENDİSLİK

İnsanlardan önemli bilgileri öğrenmek için aldatıcı konuşmalar yapılması veya diğer haberleşme ve ikna yöntemlerini kullanan kişidir.

Bu kişiler insanların doğasında bulunan zafiyetleri kullanarak sonuca ulaşırlar:

- *Yardımcı olma* isteği
- İnsanlara *güvenme* eğilimi
- *Sorundan uzak durmaya çalışma* çabası
- …

BİR SOSYAL MÜHENDİSTEN ÖĞÜTLER...

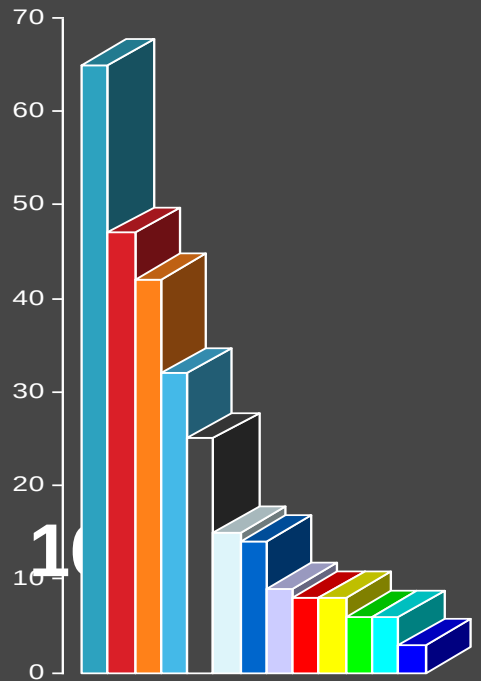
Kevin Mitnick, insanların kurumsal güvenliğin en zayıf halkası olduklarını ve kuruluşların en çok bu konuda dikkatli olması gerektiğini vurguladı.

Güvenlik danışmanı ve ünlü bir saldırgan olan Mitnick'e göre hassas bilgileri hedefleyen sosyal mühendislik saldırılarına karşı alınacak en iyi önlem iyi eğitilmiş personel.

Genellik
teknoloji
çözüm o
görüldüğ
ancak so
mühendi
teknikle
teknoloj
devre d
bıraktı
eden
"Tekn
önem
taşıma
ancak s
mühen
teknikl

"There is no patch for human stupidity…"

İSTATİSTİKLER NE DİYOR?



- Virus
- Taşınabilir bilgisayar hırsızlığı
- Kurum içi kullanıcıların saldırıları
- Bilgiye yetkisiz erişim
- Servis dışı bırakma saldırıları
- Sisteme sızma saldırısı
- Kablosuz ağların kötü niyetli kullanımı
- Gizli bilgi çalınması
- Finansal dolandırıcılık
- Telekom dolandırıcılığı
- Kamuya açık web uygulamalarının kötüye kullanımı
- Web sitesinin tahrifatı
- Sabotaj

KAYNAK: CSI / FBI Computer Crime and Security Survey, Computer Security Institute

Bilişim Hukukundan…

CMK

- Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma
  - Madde 134 – (1) … **Cumhuriyet savcısının istemi** üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine **hâkim tarafından karar verilir.**

CMK

- Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma (Devam)
  - Madde 134 – (2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir.

CMK

- Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma (Devam)
  - Madde 134 – (3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.
  - (4) İstemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

CMK

- Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma (Devam)
  - Madde 134 – (5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir.

    Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır.

TCK Onuncu Bölüm: Bilişim Alanında Suçlar

➢Bilişim Sistemine Girme

Madde 243:

(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

➢ Sistemi engelleme, bozma, verileri yok etme veya değiştirme

Madde 244:

(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

➢ Sistemi engelleme, bozma, verileri yok etme veya değiştirme

Madde 244:

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.

➢ Banka veya kredi kartlarının kötüye kullanılması

Madde 245:

(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adlî para cezası ile cezalandırılır.

(2) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır.

Hürriyete Karşı Suçlar

➢ Haberleşmenin Engellenmesi

Madde 124:

(1) Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi hâlinde, altı aydan iki yıla kadar hapis veya adlî para cezasına hükmolunur.

(2) Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engelleyen kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

….

Şerefe Karşı Suçlar

➢ Hakaret

Madde 125:

(1) Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden ya da yakıştırmalarda bulunmak veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran kişi, üç aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Mağdurun gıyabında hakaretin cezalandırılabilmesi için fiilin en az üç kişiyle ihtilât ederek işlenmesi gerekir.

(2) Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi hâlinde, yukarıdaki fıkrada belirtilen cezaya hükmolunur.

(4) Ceza, hakaretin alenen işlenmesi hâlinde, altıda biri; basın ve yayın yoluyla işlenmesi hâlinde, üçte biri oranında artırılır.

Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar

➢Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması

Madde 133:

(1) Kişiler arasındaki alenî olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki aydan altı aya kadar hapis cezası ile cezalandırılır.

(3) Yukarıdaki fıkralarda yazılı fiillerden biri işlenerek elde edildiği bilinen bilgilerden yarar sağlayan veya bunları başkalarına veren veya diğer kişilerin bilgi edinmelerini temin eden kişi, altı aydan iki yıla kadar hapis ve bin güne kadar adlî para cezası ile cezalandırılır. Bu konuşmaların basın ve yayın yoluyla yayınlanması hâlinde de, aynı cezaya hükmolunur.

Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar

➢Kişisel Verilerin kaydedilmesi

Madde 135:

(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.

(2) Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.

Mal Varlığına Karşı Suçlar

➢ Nitelikli Hırsızlık

Madde 426: **(1)** Hırsızlık suçunun;

…….

e) Bilişim sistemlerinin kullanılması suretiyle,

……

➢ Nitelikli Dolandırıcılık

Madde 158: **(1)** Dolandırıcılık suçunun;

……

f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle,

g) Basın ve yayın araçlarının sağladığı kolaylıktan yararlanmak suretiyle,

……

5651

- İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun

5651

- Bilgilendirme yükümlülüğü
  - MADDE 3- (1) İçerik, yer ve erişim sağlayıcıları … tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlüdür.

    (2) Yukarıdaki fıkrada belirtilen yükümlülüğü yerine getirmeyen içerik, yer veya erişim sağlayıcısına Başkanlık tarafından….. kadar **idarî para cezası** verilir.

5651

- İçerik sağlayıcının sorumluluğu
  - MADDE 4- (1) İçerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur.

    (2) İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur.

Elektronik İmza Kanunu

- İmza oluşturma verilerinin izinsiz kullanımı
  - Madde 16- Elektronik imza oluşturma amacı ile … imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar **bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para** …

    Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

Yargıtay Kararları (1)

- E. 2004/8763, K. 2005/21445, T. 5.12.2005
- E-Posta yolu ile yapılan hakaret ve sövme
- Sözü edilen iletiyi internet servis sağlayıcısından gönderen bilgisayarın (IP) numarasının sorulması, bu yolla bilgisayarın kime ait olduğunun saptanması sonucuna göre;
  - 1-İnternet kafe gibi umuma açık yerlerde bulunan bir bilgisayardan ileti gönderilmiş ise sanığın beraatine,
  - 2- Sanığın evi ya da işyerinde bulunan kişisel bilgisayarından gönderilmiş ise mahkumiyetine,
  - 3- Olayla ilgisi bulunmayan bir üçüncü kişinin kişisel bilgisayarından gönderilmiş ise, bu şahsın tanık olarak dinlenmesi ve sonucuna göre karar verilmesi gerekir.

Yargıtay Kararları (2)

- E. 2007/16405, K. 2007/30241, T. 15.10.2007
- İşyerindeki bilgisayarı şahsi işlerinde kullanmak, iş aktinin hakli feshi
  - Davacı, feshin geçersizliğine ve işe iadesine karar verilmesini talep etmiştir. Davacının şirket bilgisayarını mesai saatleri içinde bir çok kez kişisel mailinde kullandığı ve elektronik ortamda yazılan bir takım yazıları işyerinde çalışan bir çok arkadaşının mailine gönderdiği anlaşılmaktadır. Davacının bu davranışı şirketin iç işleyişi ile ilgili düzenlenen kurala aykırı olduğu gibi, mesai saatleri içinde işyeri bilgisayarını kullanarak iş görme edimini yeterince yerine getirmediği, bu davranışının işyerinde olumsuzluklara neden olduğu, feshin geçerli nedene dayandığı anlaşılmaktadır. Davanın reddi gerekir.

Yargıtay Kararları (3)

- E. 2005/4748, K. 2006/7341, T. 22.6.2006
- İnternet bankacılığı yoluyla dolandırıcılık
  - Bir güven kurumu olarak faaliyet gösteren bankalar objektif özen yükümlülüğünün yerine getirilmemesinden kaynaklanan hafif kusurlarından dahi sorumludurlar.

    Bu nedenle; banka müşterisinin hesabında bulunan paranın, müşterinin haberi olmadan bilgisayar korsanlığı yoluyla başka bir hesaba aktarılmasının önlenmesi konusunda ek güvenlik tedbirleri almayan bankanın hafif kusurundan dahi sorumlu olduğu dikkate alınarak, müşterisinin zararını ödemek zorunda olduğu sonucuna varılmalıdır. Ayrıca belirtmek gerekir ki, bankanın hafif kusurundan dahi sorumlu olduğu bu olayda müşterinin müterafik kusurundan söz edilemez.

Yargıtay Kararları (4)

- E. 2005/6376, K. 2007/2551, T. 16.4.2007
- E-posta ile virüs göndererek bilişim sistemine zarar vermek
  - Gerçeğin kuşkuya yer vermeyecek şekilde belirlenebilmesi için; öncelikle e-posta yoluyla virüs gönderilerek sistemine zarar verilmiş bir bilgisayarda incelemenin olaydan hemen sonra yapılması yada inceleme yapılacak bilgisayarın olaydan sonra inceleme anına kadar hiç kullanılmamış olması; bilgisayarda virüslü dosya üzerinden inceleme yaparken ilk işlem olarak, söz konusu dosyanın birebir yedeğinin alınması, ikinci olarak birebir yedeğin değiştirilip değiştirilmediğinin tespitine yarayacak zaman ve bütünlük kontrolü imkanı sağlayan değerin (hash) belirlenmesi; bir e-postanın kimden geldiğinin tespiti için de, ilk olarak e-postayı gönderen İP adresinin bulunması, daha sonra da bulunan IP adresinin belirtilen tarih ve saatte hangi abone tarafından kullanıldığının ve o abonenin kimlik ve açık adres bilgilerinin talep edilmesi, bulunan IP adresini kullanan abonenin sanıkla bağlantısının araştırılarak tespiti gerekir.

BT Standartları, Çerçeveler ve Modeller

- SOX
- ISO 27001
- COBIT
- ITIL
- BS 2599
- …

Sermaye Piyasaları ve Bilgi Teknolojileri

- Borsalara uzaktan erişim imkanı
  - İşlem hızlarının artması
  - İşlem maliyetlerinin azalması
- İnternetin yaygınlaşması ve geniş bir yatırımcı kitlesi
- Aracısızlaşma, online işlemler
- Bilgiye hızlı ve rahat erişim
- e-imza uygulamaları, ispat ve geri bildirim şekilleri vb.
- Uzaktan gözetim ve denetim, iç kontrol, operasyonel risk

Sermaye Piyasaları ve Bilgi Teknolojileri

- KAP
- KAF
- SERYET
- eCAS
- Elektronik tebligat
- …

Sermaye Piyasaları ve Bilgi Teknolojileri

- Sermaye piyasalarında yaşanan gelişmeler, yeni bilgi ve iletişim teknolojileri, internetin artan kullanımı, finans piyasalarındaki ürün ve hizmetlerdeki değişimler aracı kurumları önemli ölçüde etkilemektedir.
- Özellikle internet üzerinden yoğun işlem yapan, merkez dışı birim sayısı ve işlem hacmi yüksek olan aracı kurumlarda bu etki daha çok görülebilmektedir.

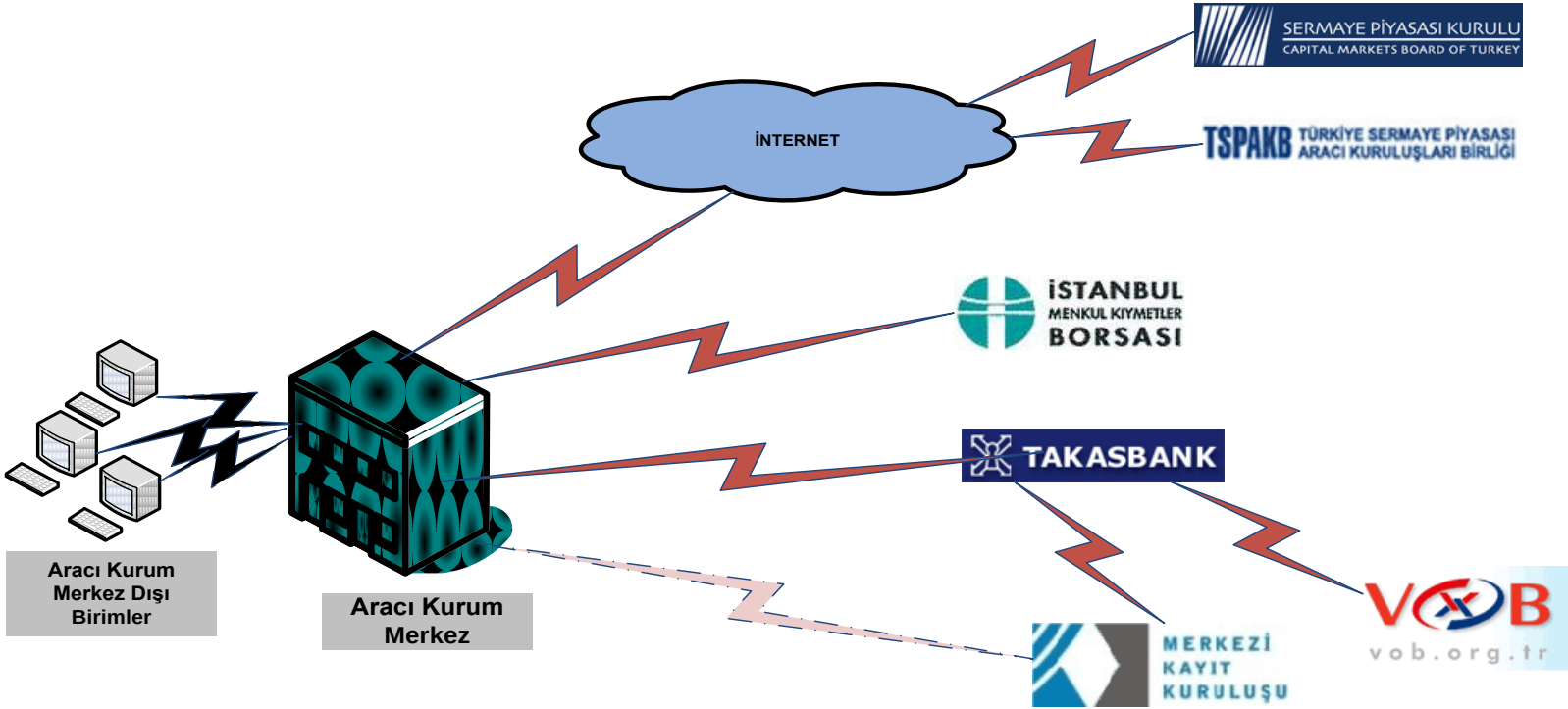
Aracı Kurumlar ve Bilgi İşlem Personeli

	2008	2009
Toplam Aracı Kurum Sayısı	98	89
Banka Kökenli Aracı Kurum Sayısı	31	30
Banka Kökenli Olmayan Aracı Kurum Sayısı	67	59
İnternet Üzerinden İşlem Yapan Aracı Kurum Sayısı	69	64
Bilgi İşlem Çalışanı Bulunan Aracı Kurum Sayısı	62	62
Toplam Çalışanların Bilgi İşlem Departmanında Bulunma Oranı	%3,6	%3,9
Aracı Kurumlarda Ortalama Bilgi İşlem Çalışan Sayısı	3	3

Aracı Kurumlar ve Bilgi İşlem Personeli

İşlem Hacmi (milyar TL)	2008	2009	Değişim (2007-2009)
Toplam Hisse Senedi İşlem Hacmi	665	965	%24
İnternet Üzerinden Hisse Senedi İşlem Hacmi	62	137	%149
Toplam VOB İşlem Hacmi	378	587	%178
İnternet Üzerinden VOB İşlem Hacmi	73	151	%529

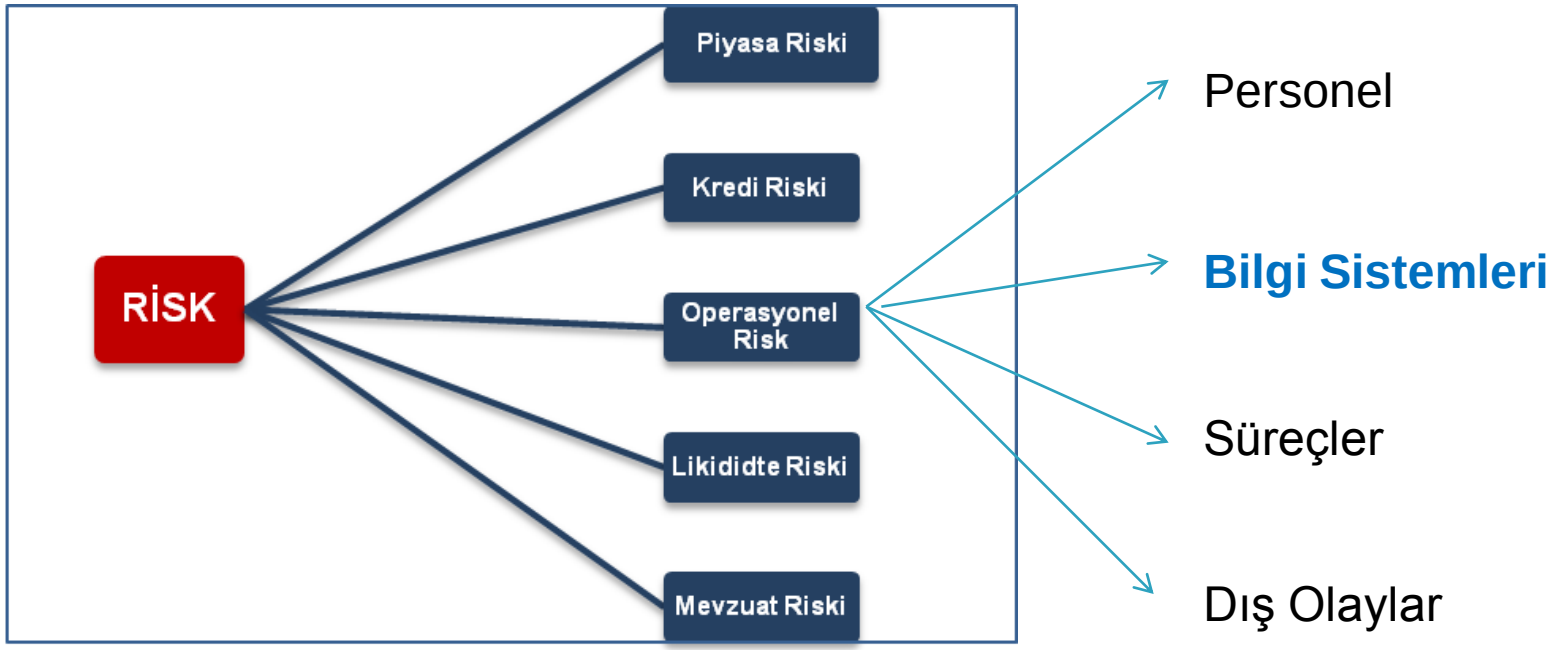
Aracı Kurumların Bilgi Sistemleri



Aracı Kurumların Bilgi Sistemleri

- Emir iletim sistemleri (Ex-API)
- İşletim sistemleri (windows)
- Muhasebe uygulamaları (Geneks, IDB, TradeSoft)
- Kayıt sistemleri (analog)
- Web sayfaları
- KAP, KAF vb.
- …

Risk


RİSK
Piyasa Riski
Kredi Riski
Operasyonel Risk
Likididte Riski
Mevzuat Riski
Personel
Bilgi Sistemleri
Süreçler
Dış Olaylar

Düzenlemeler ve Standartlar

Örnek bir düzenleme:SEC 17a-3/4

- Menkul kıymet işlemlerine yönelik kayıtlarla ilgili düzenleme
- Elektronik iletişim ve mesajlaşma (E-posta ve anlık mesajlaşma gibi kayıtlar) dahil
- Kayıtların, inceleme ve denetimlere uygun şekilde oluşturulması ve saklanması
- 17a-3: Kayıtların nasıl oluşturulacağı
- 17a-4: Kayıtların nasıl saklanacağı
- Benzer düzenleme: NASD 3010/3110

Düzenlemeler ve Standartlar

Örnek bir düzenleme:SEC 17a-3/4

- Yasaya uyum konusu çok sıkı ve cezalar çok ağır
- Yatırım bankalarının bazılarının istenilen bu gereklilikleri sağlamamasından dolayı aldığı ceza : 8 milyon $'dan daha fazla

Düzenlemeler ve Standartlar

Örnek bir düzenleme:SEC 17a-3/4

Company	Fine	Violation	Date
SG Cowen	$100,000	E-mails deleted before retention period expired.	May-03
Deutsche Bank Securities	$1.65 mil	Violated SEC 17a-4, NYSE 440 and NASD 3110.	Dec-02
Goldman Sachs	$1.65 mil	Violated SEC 17a-4, NYSE 440 and NASD 3110.	Dec-02
Morgan Stanley	$1.65 mil	Violated SEC 17a-4, NYSE 440 and NASD 3110.	Dec-02
Salomon Smith Barney	$1.65 mil	Violated SEC 17a-4, NYSE 440 and NASD 3110.	Dec-02
U.S. Bancorp Piper Jaffray	$1.65 mil	Violated SEC 17a-4, NYSE 440 and NASD 3110.	Dec-02

Source: Connor, Deni. "Confusion reigns over data archiving." Network World, 06/23/03.

Bilgi Sistemleri İncelemeleri

İSTANBUL MENKUL KIYMETLER BORSASI

VADELİ İŞLEM VE OPSİYON BORSASI
VOB

TAKASBANK

SPK

İnceleme alanları

- Kurumun IT süreçleri
- Bilgi güvenliği
- Kurum yönetimi ve personel yapısı
- Dışarıdan alınan hizmetler
- Güvenlik Taraması Hizmeti
- SLA
- Ağ ve Sistem
- Veritabanı
- Uygulama Geliştirme

İnceleme alanları

- Yedeklilik ve yedekten dönme
- Dokümantasyon
- Risk analizi
- Acil Durum Planları
- Ayrıcalıklar Yönetimi
- İç denetim
- Uyum, Yasal yükümlülükler
- ...

Sermaye Piyasası Mevzuatından...

Mevzuat…

- Düzenlemeler
  - İç Denetim Tebliği (Seri:V, No:68)
  - Aracılık Faaliyetleri Tebliği (Seri:V, No:46)
  - Belge ve Kayıt Düzeni Tebliği (Seri:V, No:6)
  - Bağımsız Denetim Tebliği (Seri:X, No:22)
  - Sermaye Yeterliliği Tebliğ (Seri:V, No:34)
  - …
- İMKB, TSPAKB, …

Aracı Kurumlarda Mevcut İç Kontrol Sistemi

- 15.12.1999/4487 sayılı Kanun
  - *“aracı kurumların, işlemlerinin sermaye piyasası ilkelerine ve mevzuata uygunluğunu denetlemek üzere yeteri kadar müfettiş çalıştırmaları zorunludur”*

Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ

- “Bağımsız denetçi, işletmenin bilişim teknolojilerinden kaynaklanacak risklere karşı nasıl önlem aldığı hususunda bilgi sahibi olmak zorundadır.”
- “Bilişim teknolojilerine ilişkin kontroller, bilgi sistemlerinin uygun bir şekilde işlemesine katkıda bulunan uygulamalar ve uygulamaların etkinliğini sağlayan usul ve esaslardır.”
- “…Genel bilişim teknolojilerine dayalı kontrollerin etkinliği…”
- “…Genel bilişim sistemi kontrolleri ve uygulama kontrolleri gibi, hizmet sağlayıcının bilgi sistemleri ile ilgili kontrollere ilişkin ulaşılabilir bilgiler...”
- …

Aracılık Faaliyetinde Belge ve Kayıt Düzeni Hakkında Tebliği

- “...internet üzerinden alınan emirlerde tarih, zaman ve müşteri bazında olmak üzere emri ileten müşterilere ilişkin kayıtlarının ….”
- “… elektronik ortamda diğer şekillerde alınan emirlerde emri veren kaynağı gösterecek şekilde gerekli elektronik log kayıtlarının emri alan aracı kuruluşlarca tutulması zorunlu...”

Aracı Kurumlarda Uygulanacak İç Denetim Sistemine İlişkin Esaslar Hakkında Tebliğ

- “...Aracı kurumların bilgi sistemlerinin güvenliğine yönelik olarak aracı kurum personelinin görev tanımları dikkate alınarak yetkilendirmeler yapılır. Erişim ve yetkilendirme işlemleri ile sistemin sürekliliğini temin edecek yedekleme işlemleri dahil olmak üzere, bilgi sistemleri ile ilgili faaliyetlere ilişkin tüm hususlar belirlenir...”

Aracı Kurumlarda Uygulanacak İç Denetim Sistemine İlişkin Esaslar Hakkında Tebliğ

- “...Aracı Kurumlar, Teftiş kurulunda görev yapacak müfettişlerde mesleki yeterlilik aramak zorundadırlar...lisans ve mesleki tecrübe...müfettişlerden bilgi teknolojileri denetimi icra edeceklerin bilgi teknolojileri ile bilgi teknolojilerine dayalı denetim teknikleri konularında.....”

Genel Değerlendirme

- Bilgi ve iletişim teknolojilerindeki ilerlemeler, internetin artan kullanımı, finans piyasalarındaki ürün ve hizmetlerdeki değişimler aracı kurumları bilgi teknolojilerine dayalı kuruluşlar haline getirmiştir.
- Aracı kurumların güvenilir bir ortamda çalışması sermaye piyasasında istikrarı sağlamak için gerekli koşullardan biridir. Bu koşulun sağlanmadığı ortamda tasarruf sahipleri zarar görebilecek, sermaye piyasasına duyulan güven sarsılabilecek ve tasarruf oranı azalarak finansal sektör ile reel sektör arasındaki aracılık süreci bozulabilecektir.
- Bu nedenle sermaye piyasasında bir güven kurumu olarak faaliyet gösteren aracı kurumların bilgi sistemlerinden kaynaklı operasyonel risklerinin yönetilmesi gerekmektedir.

Genel Değerlendirme

- Aracı kurumlardan gerek kuruluş aşamasında gerekse faaliyetlerini yürütürken bilgi sistemleri ile ilgili kontrolleri tamamlamaları, etkin sistemler kurmaları ve bu hususları yazılı hale getirmelidirler.
- Kurumsal yönetimin en önemli süreçlerinden biri de BT Yönetimi (IT Governance) olup, iş hedeflerini destekleyecek BT yönetimi oluşturulmalıdır.
- Bilgi sistemlerinden kaynaklı risklerin yönetildiği aracı kurumlar sayesinde sermaye piyasalarına olan güven artacak, süreçlere hız, gizlilik, süreklilik, bütünlük, izlenebilirlik gibi hususlar eklenebilecektir.

Teşekkürler...

gozbilgin@gmail.com