Dokuz Eylül Üniversitesi
Sosyal Bilimler Enstitüsü Dergisi
Cilt: 11, Sayı:4, Yıl: 2009, Sayfa: 01-15
ISSN: 1302-3284

BİLGİ GÜVENLİĞİ NEDİR, NE DEĞİLDİR, TÜRKİYE' DE BİLGİ GÜVENLİĞİ SORUNLARI VE ÇÖZÜM ÖNERİLERİ

Mete EMİNAĞAOĞLU*
Yılmaz GÖKŞEN**

Özet

Günümüzde Bilgi Güvenliği Yönetimi; uluslararası standartlar, ölçümleme yöntemleri, ilgili ulusal veya uluslararası yasalar, ticari yükümlülükler, gelişen teknolojiler ve değişen iş süreçlerine paralel olarak sürekli değişen ve önemi artan riskleri de kapsayacak şekilde büyük önem kazanmakta ve hem bilişim hem de iş dünyasındaki en öncelikli konulardan birisi haline gelmektedir. Bilgi Güvenliği Yönetimi'nin başarıyla uygulamada gerekli birçok çözümler, yöntemler, teknolojiler ve ürünler hazırda olmasına rağmen, uygulamada birçok yanlışlıklar yapılmakta, bazı konularda yanlış yaklaşımlar sergilenmekte ve bunun sonucunda güvenlik sorunları artarak sürmektedir.

Bu çalışmada, dünyadan ve Türkiye'den en güncel istatistiksel bilimsel verilerle mevcut durum ortaya konularak bilgi güvenliğinde ortak yapılan en yaygın yanlışlara dikkat çekilmekte ve bunlara yönelik olarak kısa ve uzun vadede toplum geneline ve kurumlara uygulanabilecek etkin çözüm önerileri sunulmaktadır.

Anahtar Kelimeler: *Bilgi Güvenliği Yönetimi, Farkındalık Eğitimi, Bilgi Güvenliği Risk Analizi, Bilgi Güvenliği Anketleri.*

INFORMATION SECURITY; WHAT IS AND WHAT IS NOT, INFORMATION SECURITY PROBLEMS IN TURKEY AND SOME RELATED SOLUTIONS

Abstract

In today's challenging and tremendously changing business world, Information Security Management has become one of the most important topics with the relevant trade laws, IT laws, regulations and international standards. Despite all the existing best-practices, years of experience, knowledge, methods, brand-new technologies and tools in information security management domain, everyone seems to be yet at serious stake due to misunderstandings, wrong implementations and unconscious approaches.

In this study, the current situation regarding information security risks and problems are summarized by using the statistical surveys conducted in Turkey and other countries and the most common mistakes related with these problems are analyzed.

* Öğr. Gör., Yaşar Üniversitesi Meslek Yüksek Okulu Bilgisayar Programcılığı Bölümü, mete.eminagaoglu@yasar.edu.tr
** Yrd. Doç. Dr., Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi İşletme Bölümü, yilmaz.goksen@deu.edu.tr

Some effective and practical solutions that can be applied to communities and corporations in the short and long term are also given in this study.

Keywords: *Information Security Management, Awareness Training, Information Security Risk Analysis, Information Security Surveys.*

Journal of Economic Literature (JEL) Classification System

M - Business Administration and Business Economics; Marketing; Accounting
M1 - Business Administration
M15 - IT Management

1. GİRİŞ

21. yüzyılda şirketler, devletler, kurumlar, bireyler ve toplumların tamamının ortak bileşkesi bilgi çağında yaşıyor olmaları ve bilgi çağının gereklerine ayak uydurma zorunda olmalarıdır. Üretim, hizmet veya tüketim sürecinde, bilgi en değerli ve en vazgeçilmez rekabet ve başarı unsuru haline gelmiştir. Aynı zamanda, her türlü örgütsel yapılanmada, iş sürecinde ve kurumda veya şirkette; ilgili her türlü iş sürecinde mutlaka bilgi ilintili işler, parçalar ve unsurlar da vazgeçilmez bir biçimde yer almaktadır. Bu kadar vazgeçilmez ve değerli bir unsur olan bilginin güvenliği ve güvenilirliği de, artık yadsınamaz bir kavram olarak karşımıza çıkmaktadır. İşin niteliği veya sürecin yapısı ne olursa olsun, teknoloji bağlantılı olmayan süreçlerin yönetiminde bile, bilgi güvenliğinin de etkin, sürekli ve başarılı bir şekilde sağlanarak yönetilmesi çok önemli bir gereksinim olmaktadır. İşlerin ve süreçlerin sağlıklı yönetimi aynı zamanda ilgili bilgi güvenliği süreçlerinin de sağlıklı yönetimini zorunlu kılmaktadır. Bilgi güvenliği stratejileri ve bunları yönetecek uygun yöntemleri olmayan kurumlar, sadece güvenlik açısından değil, operasyonel ve diğer her türlü iş süreçlerinin yönetimi açısından da ciddi sıkıntılar, maddi ve/veya manevi kayıplarla yüzleşmektedir (Tipton ve Krause, 2007).

İş yaşamımızda kullandığımız, iş gereği bizimle paylaşılan, çalışmalarımızla, türlü deneyimlerle elde ettiğimiz her bilgi değerlidir ve / veya özeldir. Günümüzde bilgisayar ortamlarında her türlü değerli bilgi tutulmaktadır. İnternet ve elektronik iletişim; banka, alışveriş, eğlence alanlarında yaygın olarak kullanılmaktadır. Öyle ki, artık bir ilkokul öğrencisi de bir emekli de İnternet kullanıcısı olmuştur (Mitnick, 2005).

Kurumların ve çalışanlarının ellerindeki değerleri koruma gerekçeleri olarak; kurum ve işin sürekliliği, başarısı, kamu, toplum, ticari ve bağımsız organizasyonlara karşı yerine getirilmesi gereken sorumluluklar sayılabilir.

"Bilgi güvenliği konusunda kurumlar, bireyler ve toplum ne gibi problemler yaşıyor, bilgi güvenliğinde ne gibi risklerle ve sorunlarla karşı karşıyayız?" soruları artan sıklıkla sorulmaktadır. İlginç olan ise; çözümleri olmasına karşın bu gibi sorunlar her türlü sektörde artarak yaşanmaktadır. Kurumların gizli bilgilerinin, ticari sırlarının dışarı sızdırılmasından tutun da,

yasalara uygun olmayan iş yapış şekilleri, kazalar, afetler, vb. sonucu yaşanan ciddi iş kayıpları, maddi ve manevi (saygınlık, vb) kayıplar olmak üzere çok değişik bilgi güvenliği sorunları bunlara örnek olarak verilebilir.

Bilgi güvenliği, her organizasyonun sürekliliğinin sağlanmasında büyük önem taşır ve organizasyonun başta elektronik olmak üzere, çeşitli ortamlardaki kritik bilgilerinin ve diğer bilgi varlıklarının korunmasını sağlar. Sadece büyük şirketler, holdingler değil bunun yanı sıra KOBİ'ler, devlet kurumları veya kar amacı gütmeyen herhangi bir organizasyon, okul, vb. de bilgi güvenliği sorunları ve risklerini farklı düzeylerde de olsa sürekli yaşamaktadır. Bu gerçek, dünya genelinde olduğu gibi ülkemizde de sürekli artan boyutlarda ortaya konan bir olgu haline gelmektedir.

2. ÜLKEMİZDE VE DÜNYADA MEVCUT DURUM

CSI ve FBI kurumlarının 2008 yılında ortak yaptıkları bir çalışmanın sonuçlarına göre (Richardson, 2008: 2-4); ABD'deki 522 kurumun (devlet veya özel sektör) %49'unda virüs, truva atı, solucan, vb zararlı kod saldırısı yaşanmış, %42'sinde dizüstü bilgisayar, cep bilgisayarı, vb mobil cihazlar çalınmış, %44'ünde şirket çalışanları İnternet ve diğer yetkilerini, erişimlerini suistimal etmiş ve bir yıl içerisinde bu 522 kurumun toplam maddi kaybı 156 Milyon ABD Doları olmuştur. Bilişim suçlularının değerli bilgi içeren büyük firmalara saldırı olasılığı son yıllarda çok daha fazla olmaktadır ve yapılan araştırmalar sonucu elde edilen istatistiksel veriler de bu savı desteklemektedir.

Dünya genelinde yapılan bir başka araştırma raporunda (Symantec, 2009: 5); 2008 yılı boyunca yeni tehditlerin yayılması ve amacına ulaşmasında Internet ortamı ve web sitelerinin yine ana kaynak olarak kullanıldığını özellikle vurgulanmıştır. Aynı çalışmada, saldırganların bu tehditleri geliştirirken ve kullanıcılara yöneltirken eskisine oranla çok daha fazla "kişiye özel" zararlı kod aktiviteleri düzenlediklerinin de altı çizilmektedir. Dahası, 2008 yılı boyunca Symantec firması tarafından saptanan tüm saldırıların neredeyse %90'ı, kullanıcıya ait kritik bilgilerin çalınması amacını taşımaktadır. Klavye tuş basımlarının kaydedilmesi yolu ile çevrim içi banka hesap bilgileri gibi kritik bilgilerin çalınmasına yönelik aktiviteler, saldırıların %76'sını oluşturmaktadır ki bu oran, 2007 yılında %72 olarak saptanan oranla kıyaslandığında, bir senede yaşanan artışı açıkça ortaya koymaktadır.

Aynı araştırmada ülkemizle ilgili çarpıcı istatistiksel değerler ve bulgular da mevcuttur. Geçmişte herhangi bir saldırı yaşadıklarını ifade eden Türkiye'deki kurumların %50'si, saldırının "sistemin durmasına neden olduğunu" belirtmiştir. Sistemi duran kurumların %50'inde ise 8 saati aşan bir kesinti yaşanmıştır. Herhangi bir saldırıya maruz kalan kurumların % 35'i, bu saldırının "bilgi kaybına" neden olduğunu belirtirken, %10'u ise "sistemin yavaşladığını" belirtmişlerdir.

Bu araştırmanın dikkat çekici bir tarafı da, Türkiye'nin bilgi güvenliğindeki dünyadaki konumuna ait verilerdir. 2008 yılında, Türkiye geneli

güvenlik saldırıları, dünya bazında çok kaygı verici bir düzeyde olduğu bulgulanmaktadır. Örnek vermek gerekirse; 2008 yılında bir önceki yıla göre ülkemizdeki zararlı kod saldırıları 2 misline yakın artmış, dünyadaki tüm zararlı kod eylemlerinin %6'sını oluşturarak genel sıralamada 9. sıraya yükselmiştir.

Çöp (İng. spam) e-posta eylemleri de Türkiye'de bir önceki yıla göre 12 kat artarak dünya genelinde 3., Avrupa-Orta Doğu (EMEA) bölgesinde de 2. sıraya yükselmiştir (Symantec, 2009a; 2009b). Ama diğer dereceye giren ülkelere göre Türkiye'nin Internet hat kullanım kapasiteleri ve Internet kullanıcısı sayısı oranları göz önüne alındığında, aslında Türkiye'nin dünyadaki diğer tüm ülkelerden daha yüksek düzeyde bilgi güvenliği sorunları yaşadığı anlaşılmaktadır.

Aynı araştırmanın ülkemizle ilgili ortaya koyduğu çarpıcı sonuçlardan birisi de, 2008 yılında virüs tipindeki zararlı kodların üretildiği ve yayılma kaynağı olarak çıktığı ülkeler arasında Türkiye, Avrupa-Orta Doğu bölgesi genelinde 2. sırada yer almaktadır (Symantec, 2009: 26).

Sözü edilen istatistiki görünüm Tablo 1., Tablo 2. ve Tablo 3. de özetlenmektedir.

Tablo 1. 2007 ve 2008'de dünya genelinde zararlı kodların tiplerine göre sıralamalar ve genel sıralamalar (Symantec, 2009: 18).

2008 tüm saldırı tipleri Dünya Sıralaması	2007 tüm saldırı tipleri Dünya Sıralaması	Ülke	2008 Yılı Tüm Saldırı Tipleri içinde oranı	2007 Yılı Tüm Saldırı Tipleri içinde oranı	Zararlı Kod	Spam Yayıcı Sistem	Phishing Web Siteleri	Bot Sistemler	Tüm Saldırılar Geneli
1	1	A.B.D.	23%	20%	1	3	1	2	1
2	2	Çin	9%	11%	2	4	6	1	2
3	3	Almanya	6%	7%	12	2	2	4	4
4	4	İngiltere	5%	4%	4	10	5	9	3
5	8	Brezilya	4%	3%	16	1	16	5	9
6	6	İspanya	4%	3%	10	8	13	3	6
7	7	İtalya	3%	3%	11	6	14	6	8
8	5	Fransa	3%	4%	8	14	9	10	5
9	15	**Türkiye**	**3%**	2%	15	**5**	24	8	12
10	12	Polonya	3%	2%	23	9	8	7	17

Tablo 2. Dünya geneli ve Avrupa-Orta Doğu bölgesinde çöp (spam) e-posta oranları ve sıralamaları (Symantec, 2009: 39).

2008 Avrupa ve Ortadoğu Sıralaması (spam)	2007 Avrupa ve Ortadoğu Sıralaması (spam)	2008 Dünya Geneli Sıralama (spam)	Ülke	2008 Avrupa ve Ortadoğu Oranları (spam)	2007 Avrupa ve Ortadoğu Oranları (spam)
1	3	2	Rusya	14%	10%
2	8	**3**	**Türkiye**	**13%**	4%
3	1	6	İngiltere	7%	15%
4	4	7	Almanya	6%	9%
5	5	8	İtalya	6%	6%
6	2	9	Polonya	6%	10%
7	6	10	İspanya	5%	6%
8	7	13	Fransa	5%	6%
9	20	19	Romanya	3%	1%
10	10	20	Hollanda	3%	1%

Tablo 3. Truva atı, virüs, arka kapı ve solucan tipinde zararlı kod saldırılarında ilk 3 sıradaki ülkeler (Symantec, 2009: 26)

	Zararlı kod türlerinde ilk 3 sıra (Avrupa ve Ortadoğu bölgesi geneli)			
Sıralama	**Arka Kapı**	**Truva Atı**	**Virüs**	**Solucan**
1	İngiltere	İngiltere	Mısır	Suudi Arabistan
2	İspanya	Fransa	**Türkiye**	İngiltere
3	Fransa	Almanya	İngiltere	İspanya

Deloitte firmasının TMT (Teknoloji, Medya, Telekomünikasyon) Küresel Güvenlik Araştırması 2009 raporuna göre (Deloitte, 2009: 15), teknoloji şirketlerinin güvenliğe daha fazla kaynak ayırması gerekirken, son bir yıldır yaşanan küresel ekonomik kriz nedeni ile bu alandaki yatırımların ciddi bir şekilde azaldığını ortaya koymaktadır. Son yıllarda çoğu kurumsal verinin ve içeriklerin hızla bilgisayar ortamına taşınması nedeniyle güvenlik yatırımlarının kurumsal bilgi teknolojileri (BT) bütçeleri içindeki payının artması beklenmektedir. Oysa Deloitte TMT Güvenlik Araştırması'na yanıt verenlerin sadece %6'sı toplam BT bütçesi içinde güvenliğe %7 veya daha fazla kaynak ayırdığını bildirmiştir (Bir önceki yılki araştırmada bu oranın %36 olduğu vurgulanmaktadır).

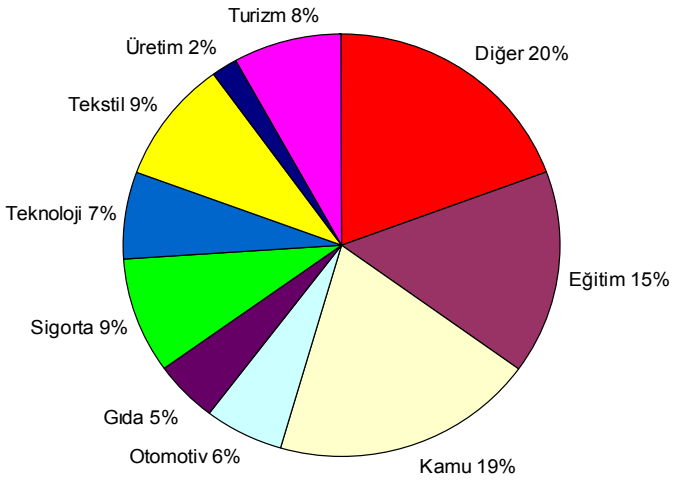
Öte yandan, aynı araştırmanın sonuçlarına göre; dünya genelindeki kurumların %41'inin son 12 ayda kurum içinden kaynaklanan en azından bir tehditle uğraşmak zorunda kaldıkları açıklanmıştır. Aynı araştırmadan elde edilen bir başka sonuçta ise, bu kurumların %70'inden fazlasının zararlı kod saldırısı, gene aynı orana yakın düzeyde kazayla bilgi kaybı ve hizmet kesintisi saldırıları yaşadıkları ve zarar gördükleri (kurumların %5 civarında bir oranının 1 ile 5 milyon ABD Doları arasında kayıp yaşadığı) kaydedilmiştir. Bilgi güvenliği tehditleri ve risklerinin yarattığı zararlar arttığı halde, ekonomik kriz veya bütçe

sorunlarında ilk kısıtlanan veya vazgeçilen masraf kaleminin bilgi güvenliği olması da oldukça düşündürücüdür. Bu durum, başta yöneticiler olmak üzere bireyler ve toplumların hala bilgi güvenliğini tam olarak algılayamadığının somut bir örneği olmaktadır.

Yabancı kuruluşların yanı sıra, sadece ülkemizi kapsayacak şekilde bazı ulusal araştırmalar da önceki yıllarda yapılmıştır. Bu konuda Koç.net şirketinin yapmış olduğu ilgili çalışmalar örnek verilebilir. 1025 ADSL kullanıcısı ve 850 şirketin kapsandığı Rizikometre 2005 Türkiye Internet Güvenliği Araştırması Sonuçları'na göre (Koç.net, 2005: 1):

- ADSL erişimlerinin %65'inin güvenlik duvarı (İng. firewall) kullanmadığı saptanmıştır.
- Web sunucularının %43'ünün bilgileri kolaylıkla çalınabilir, ana sayfaları değiştirilebilir veya bir başka adrese yönlendirilebilir durumda risk altındadır.
- Şirketler ve ADSL kullanıcılarının sadece %30'u casus yazılımlara (İng. spyware) karşı korunmaktadır.
- Alan adı hizmeti (İng. DNS) sunucularının %22'sindeki açıklardan dolayı şirket e-postaları ele geçirilebilir veya çalışanların internet üzerinden eriştiği bankacılık vb. işlemlerde kullanılan şifreler çalınabilir durumdadır.
- Kritik güvenlik açıklarının oranı tüm açıkların tamamının %19'u, orta düzey açıkların oranı da tüm açıkların %28'idir; başka bir deyişle araştırmaya katılanların yaklaşık yarısı internet' ten gelecek güvenlik tehditlerine karşı kayda değer düzeyde risk altındadır.
- Kamu, Eğitim, Turizm, Tekstil ve Sigorta sektörleri risk altındadır.

Şekil 1. Şirketlerdeki yüksek düzeydeki güvenlik açıklarının sektör bazında dağılımları (Koç.net, 2005: 5).



Bu araştırmada altı çizilmesi gereken bir başka nokta da, ilgili çalışmanın sadece Internet üzerinden ve dışarıdan yapılabilecek tehdit ve saldırıları kapsamış olmasıdır. Bir başka deyişle, kurumlardaki diğer sistemlerin ve içeriden olabilecek saldırılar ve risklerin de kapsama alınması durumunda elde edilecek sonuçların çok daha kötümser bir tablo ortaya koyması beklenebilir.

Türkiye'nin de kapsama alındığı diğer bir başka uluslararası araştırmaya göre (Ernst & Young, 2008); genel amaçlı bilgi sistemlerinin kurulumunda bilgi güvenliği birimleri süreçlere büyük oranda katılırken insan kaynakları sistemlerinin kurulumunda katılımın yarı yarıya azaldığı görülmektedir. (Bu oran dünyada %69 iken Türkiye'de %53 seviyesinde bulunmaktadır.) Ayrıca, Türkiye'deki kurumların sadece %31'inin iş sürekliliğine yönelik planları olduğu ve bilgi sistemlerinin krizlere, felaketlere hazırlıklı olduğu, dünya genelinde de bu oranın %40 civarında olduğu bulgulanmıştır.

3. BİLGİ GÜVENLİĞİNDE YAPILAN ORTAK HATALAR

Aslında bilgi güvenliği konusunda, ülkemizde de dünyada da birçok teknolojik veya süreçsel çözümler, yöntemler, standartlar, yasalar, yönetmelikler bulunmaktadır (Tipton ve Krause, 2007; T.S.E., 2006; Scholtz vd., 2006; ISO, 2005). Buna rağmen, bir önceki bölümde sayılarla da örneklendiği gibi, bilgi güvenliğinde kayıplar, zararlar, açıklar, sorunlar artarak sürmekte ve bilgi güvenliği riskleri yeterli düzeyde azaltılamamakta veya kontrol edilememektedir. Çünkü temel sorun, bu konuya bireylerin ve toplumun bakışı, algılama ve yaklaşım tarzındaki hatalar ve yetersizliklerdir. Bilgi güvenliğine bireylerin, toplumların ve kurumların bakış açısının öncelikle değişmesi gerekmektedir. Kurumlardaki üst yöneticilere, yazılı ve görsel basınımıza, kanun ve yönetmelikleri düzenleyen yetkililere bu konuda ciddi görevler düşmektedir. Güvenliğin teknolojiden önce insana yatırım yapılmasıyla, bilinçlendirmeyle, kurumların en tepeden başlayarak bu gibi konularda bilgilenmesi, desteklemesi ve önemsemesi ile sağlanacağı ve güvenliğin sürekli yönetilecek bir süreç olduğu unutulmamalıdır (Eminağaoğlu, 2008).

Günümüz koşullarında, bilgi hırsızlığı ve sanayi casusluğunun; özel istihbarat birimleriyle, pahalı teknolojilerle veya çok usta bilişim korsanlarının desteğiyle yapılması bir zorunluluk olmaktan çıkmıştır. Son dönemlerde kullanımı kolay ve masrafsız olan birçok bilgi hırsızlığı teknolojisi, donanım ve yazılımlar mevcuttur ve ne yazık ki bu teknolojiler herkesin kolaylıkla ulaşabileceği bir noktaya gelmiştir. Sanayi casusluğu, vb eylemler kurumların dışarısından daha çok kurumların içindeki sistemler ve insanlar kullanılarak yapılmaktadır (Schneier, 2008; Mitnick, 2005). Kurum içerisinden bilgi güvenliğine zarar veren saldırılar veya kasıtsız eylemler; dışarıdan yapılanlara göre risklerin ve kayıpların çok daha yüksek düzeyde gerçekleşmesine neden olmaktadır.

En önemli çelişkilerden ve sorunlardan birisi de kurumların en değerli ticari sırlarının USB bellek, DVD, avuç içi veya dizüstü bilgisayarlarda, vb. de,

yani çok kolay çalınabilecek, kaybolabilecek aygıtlarda koruma önlemleri alınmadan sıkça taşınması ve kullanılmasıdır.

Daha da önemlisi, bu gibi aygıtları kullanan insanların neredeyse %70'inin ilgili güvenlik risklerinin ve yüklenmiş oldukları sorumlulukların farkında olmamalarıdır (Eminağaoğlu, 2008).

Kurumlarda "bilmesi gerektiği kadar, en az yetki, erişmesi gerektiği kadar" gibi ilkelere en öncelikli uyması gereken gruplar yöneticiler ve bilişimcilerdir. Oysa tam tersine bu ilkelerin en az uygulandığı ve en riskli eylemlerin yaşandığı (zorunlu veya keyfi, bilinçli veya bilinçsiz) birimler de bu iki gruptaki çalışanlardır. Kurumlarda en değerli ve en gizli bilgileri kullanan, taşıyan, kaydedenlerin çoğunlukla bu iki gruptaki çalışanlar olduğu bilinmektedir. Ayrıca, işlerinin niteliği gereği kurum genelinde en sık örnek alınan ve daha çok dikkat çeken birimler de gene bu iki birimdir. (Tipton ve Krause, 2007).

Kurumlardaki üst yönetimin bilgi güvenliğini önemsemeye başlamış olduğu durumlarda da, genelde bir başka hata yapılarak acele ve günü kurtarıcı çözümlere başvurulduğu ve sadece teknoloji temelli çözümlere odaklanıldığı da gözlemlenmektedir (Richardson, 2008: 28).

Bilgi güvenliğinde yaşanılan sorunların çözümü genelde bilişimci personelin üzerine yüklenmekte ve sadece teknolojik güvenlik yatırımlarıyla sorunların hallolacağı yanılgısı çok sık yaşanmaktadır. Oysa belki de ilgili riskin ve sorunun çözümü sadece teknolojik olmayabilir veya belki de öncelikli çözüm güvenlik teknolojileriyle sağlanmayabilir. Bilgi güvenliği yönetiminde, insan ve sürecin hemen her aşamada teknolojiyle birlikte düşünülmesi gerektiği unutulmamalıdır (T.S.E., 2006; ISO, 2005). Birçok kurumda; "Acaba hangi teknoloji o şirketin kurum kültürüne ve iş süreçlerine uygun? Hangisi altyapımızla en kolay şekilde bütünleşebilir?" vb kritik sorular sorulmaktadır. Bu soruların en sağlıklı yanıtı olan risk ve gereksinim analizleri göz ardı edilip yakın çevredekilerin önerdiği en düşük maliyetli seçenek aceleyle seçilir ve yatırım yapılırsa başarısız sonuçlar alınacak ve düş kırıklığı yaşanacaktır. Kurumlardaki üst yönetimler, bilgi güvenliğini bilişim personelinin çözmesi gereken teknik bir iş ve basit bir yatırım gibi gördüğü sürece sorunlar ve riskler azalmamakta, tam tersine katlanarak artmaktadır (Mitnick, 2005).

Bruce Schneier, bir çalışmasında şu yorumu yapmaktadır; "Eğer güvenliği, o ürün / sisteme hal-i hazırda bütünleşik şekilde son kullanıcıya sunarsanız, insanları memnun eder ve kazanırsınız, aksi takdirde insanların güvenlik özelliklerini kullanması / benimsemesi için sürekli zaman, enerji, para harcamak zorunda kalır ve güvenliği başarılı bir şekilde pazarlayamazsınız." (Schneier, 2008).

En pahalı ve en karmaşık çözüm, her zaman en güvenli çözüm değildir. Daha önceki bölümlerde açıklanan nedenlerden ötürü, her kurumun kendisine en uygun ve en doğru çözümü seçmesi ve uygulaması gerekmektedir. Basit ve düşük maliyetli bir güvenlik çözümü bazı kurumlar için belki yetersiz kalabilir ama aynı çözümün bir başka kurum için yeterli ve etkili olabileceği de unutulmamalıdır.

Bilgi güvenliği, başlanıp bitirilecek bir çalışma, bir iş değildir. Bilgi güvenliği yönetimi, kurumlar ve bilgiler var olduğu sürece sürekli yönetilmesi, denetlenmesi gereken bir yaşam döngüsüdür (ISO, 2005).

Teknolojik çözümlerin, o kurumun kendi iş yapma şekillerine, özgün kurum kültürüne, iş süreçlerine en uygun şekilde uyarlanması gerekmektedir. Ayrıca, bu çözümlerin kurum süreçleriyle uyumlu tutacak şekilde sürekli gözlenip yönetilmesi ve değişiklik yönetiminin sağlanması büyük önem kazanmaktadır. Hiçbir güvenlik sistemi, üzerinde hazır gelen ayarlarıyla kendi başına ilgili kuruma ve iş süreçlerine uygun olmamaktadır.

Yaygın olarak yapılan bir başka yanlış, kurumlardaki projelerde güvenlik etmeninin en baştan itibaren projeye katılmaması ve bu nedenle analiz, tasarım, uyarlama, test ve kontrol süreçlerinde güvenliğin düşünülmemesidir. Oysa bilgi güvenliği projelerin son aşamasında hızla yapılacak ek bir yama değildir. Bu şekilde bir yaklaşım, kurumların projelerinde çoğunlukla başarısızlığa uğramasına neden olacaktır. Başta bilişim projeleri olmak üzere, projelerde bilgi güvenliği risk analizleri ve güvenlik gereksinimleri projenin en başından itibaren sürece katılmalıdır.

"%100 güvenli" ve "0 risk" kavramları günlük yaşamda gerçekçi ve uygulanabilir değildir. Bilgi güvenliği hiçbir veriyi, iş sürecini tamamen güvenli kılamaz veya risklerini sıfırlayamaz. Gerçekçi bir bilgi güvenliği yaklaşımı; o kurum veya o toplum için güvenliği gereken düzeyde sürekli sağlamak, risk analizlerinin sonucuna göre ilgili riskleri olabilecek en alt düzeye indirgemek ve kalan riskleri de kontrollü bir şekilde izleyerek yönetmektir. Sağlık, finans, vb sektörlerin süreç yönetiminde olduğu gibi bilgi güvenliği yönetiminde de risk odaklı yaklaşım esastır (Tipton ve Krause, 2007).

4. ÇÖZÜM ÖNERİLERİ

Bilgi güvenliği yönetiminin kurumlarda etkin ve etkili biçimde sağlanabilmesi için; üst düzey yöneticilerin maddi ve manevi destek vererek bilgi güvenliği süreçlerini sahiplenmeleri gerekmektedir. Bilgi güvenliği uygulamalarının kurumlardaki tepe yöneticilerden başlayıp daha alttaki kademelere yaygınlaştırılarak kurum genelinde benimsetilmesi çok büyük önem taşımaktadır. Bu süreci uygularken ISO 27001 ve diğer benzeri bilgi güvenliği yönetimi standart ve mimarilerinin temel alınmasında büyük yarar vardır. Güvenlik süreçlerinin denetlenen, geliştirilen, desteklenen ve yaşatılan bir yapıya oturtulması gerekmektedir. Bilgi güvenliğinin sadece teknoloji veya bilgisayar güvenliği olmadığı gerçeğinin anlaşılması da büyük önem taşımaktadır. Bilgi güvenliği bir maliyet veya ek bir yük olarak görülmemeli, kurumun ticari stratejileri ve iş geliştirme vizyonu kadar önemli ve belirleyici bir yerde konumlanmalı, bir kurum kültürü haline getirilmelidir (ITGI Inst., 2007; Tipton ve Krause, 2007).

Bilgi güvenliğinde kritik başarı faktörlerinden birisi ve belki de en önemlisi insandır. Başarılı ve uzun soluklu bir bilgi güvenliği yönetimi; insanların bilgi

güvenliği konusunda farkındalık eğitimleri almaları, bilgilenmeleri ve bilinçlenmeleriyle sağlanabilecektir.

Bilgi güvenliğine uzun soluklu ve vizyoner bakabilen kurumların çoğu bankacılık, vb finans sektörü ile iletişim ve yazılım firmaları, devlet kurumları ve büyük holdingler arasından çıkmaktadır. Oysa bu yaklaşımın genele yayılarak tüm sektörleri ve irili ufaklı her kurumu kapsaması gerekmektedir ki, bu da ancak zamanla ve toplumların bilinçlenmesiyle olabilecektir. Bireylerin ve toplumun iş dışı günlük yaşamlarında da kablosuz ADSL, Internet, cep telefonu, vb kullanımları göz önüne alınırsa, sadece iş amaçlı değil, bireysel kullanımda da bilgi güvenliği çözümlerinin hızla yaygınlaştırılması gerekmektedir (Swaminatha ve Elden, 2003).

Sonuçta günümüzde bilgiyi ve teknolojiyi hiç kullanmadan işletilen herhangi bir şirket, kurum, örgüt, vb olamayacağına göre, bilgi güvenliği de değişik oranda ve düzeyde olsa bile herkes için gerekli bir unsur haline gelmektedir.

Hiçbir risk tamamen sıfırlanamayacağı gibi aynı sektörde çalışan iki farklı şirketin aynı konuda farklı riskleri ve zaafları olabilmektedir. Bu nedenle her kurum kendine özgü risk değerlemesini ve yaklaşımlarını sağlamak veya danışmanlık alarak sağlatmak zorundadır.

Öncelikle, "ilgili kurumun ne gibi riskleri var ve bunların kuruma etkileri neler, ne kadar maddi kayıp yaratır, hangi riskleri gidermek kurum için önemli?" vb. soruların değerlendirilmesi, sonra da karar verilen en öncelikli çözümlerin planlanıp aşamalı bir şekilde uygulatılması gerekmektedir. En basitinden bir örnek vermek gerekirse, bir kurumda ticari sırların kağıt çıktı olarak çalınması önlenmek isteniyorsa, hemen özel baskılı mürekkep teknolojisine yatırım yapmak veya o bilgilerin çıktısının alınmasını yasaklamak gibi acele kararlar ve çözümlere geçmemeli, önce risk ölçümü ve değerlendirmesi yapılmalıdır. Belki de ilgili kurumun iş yapış şeklinden ötürü, bu riskler mecburen azaltılamayabilir veya belki de aslında çok daha riskli ve gizli kalmış başka sorunları bulgulayıp önce onların çözümlenmesi gerekebilir. Bir başka örnek; kablosuz ağların veya kablolu telefon hatlarının şifrelenmesi kurum için uygun bir çözüm olabilir ama başka bir kurum için, belki iş yapış şeklinden ötürü veya bazı ticari kurallardan ötürü bu uygun bir çözüm olamayabilir.

Bilgi güvenliği risk ölçümü ve değerlendirmesi için, çok çeşitli yöntemler ve bu yöntemleri kullanan çeşitli yazılım ve araçlar da mevcuttur. Öncelikle, risk ölçüm ve değerlemesi yapılacak ilgili varlıkların (İng. asset) yaklaşık bilgi değerleri ele alınmalıdır. Bu değerlere, hangi olasılıkla, hangi güvenlik açıkları veya zayıflıklarının (İng. vulnerability) sonucunda, hangi tehditlerin (İng. threat) ne ölçüde olumsuz etki yapacağı denklemlerle irdelenir ve toplam olası risk değeri, yani riskin gerçekleşmesi durumunda, o bilgi değerinin göreceği olası zarar (İng. impact) hesaplanır. Tüm bu hesaplar ve ölçümlerde, niceliksel (İng. quantitative) veya niteliksel (İng. qualitative) parametreler ve yöntemlerden birisi veya ikisi birlikte kullanılabilir. Tüm riskler bu şekilde hesaplandıktan sonra da, bu risklerin

hangilerinin kurum için öncelikli olduğu ve ne düzeyde riskin azaltılması gerektiği saptanır ve istenen düzeye düşürmek için yapılması gereken çözümler, önlemler, kontroller belirlenir ve bu çözümleri uygulamanın maliyetleri de analiz edilir. Böylece risk azaltıcı önlemin ne kadar uygulanır ve etkin olduğu da irdelenir. (Karabacak ve Soğukpınar, 2005; Tan, 2003; Wawrzyniak, 2008). Niceliksel bir bilgi güvenliği risk analizini basit şekilde aşağıdaki gibi örnekleyebiliriz:

Bir avuç içi bilgisayardaki bilgilerin değeri 5000 TL ve bu bilgilerin bir defalık çalınması durumunda yaşanacak tüm kaybın (İng. Single Loss Expectancy) 4000 TL olduğu hesaplandığı varsayılsın (bilgi kaybına ek olarak imaj kaybı, vb hesaba katılacaktır). Bu olay son 4 yıl içinde 1 kere gerçekleşmiş ise, bir yıl içinde gerçekleşme ve tekrar etme katsayısı da (İng. Annual Rate of Occurence) 0.25 olacaktır ve yıllık toplam beklenen kayıp (İng. Annual Loss Expectancy) 1000 TL olacaktır. Eğer, özel bir güvenlik takip teknolojisi yatırımının yıllık maliyeti 800 TL ve bu yatırım sonrası kalan olası yılık risk katsayısı 0.01 olursa, bu risk etkin bir şekilde azaltılmış olacak ve risk analizi tamamlanmış olacaktır. Çünkü kalan risk ve ilgili kayıp (İng. residual risk) yılda ortalama 40 TL ye düşecek ve güvenlik yatırımının maliyeti de hesaba katılınca, sonuç negatif çıkmayıp 160 TL olacağı için risk azaltıcı çözüm etkin ve kabul edilebilir olacaktır.

Risk azaltıcı teknolojik veya süreçsel çözümler yanı sıra, kurumun iş yapış şeklini düzenleyecek politikalar, prosedürler, kurallar tam uyum sağlanacak şekilde uygulatılmalıdır.

Özellikle, kurumun iç sistemleri ve verilerine erişen diğer her türlü kurum, kişi (stajyer, geçici sözleşmeli personel, dış kaynaklı firmalar, iş ortaklığı firmalar, vb) ile gizlilik anlaşmaları yapılmalı ve çok ciddi cezai yükümlülükler yer almalıdır. Ayrıca, sadece hizmet alınan dış kaynak firma değil, belki onun da ilgili kuruma verdiği hizmeti başka bir alt yüklenici firmaya devredeceği durumlarda, alt yüklenici firmaları da yükümlü kılacak şekilde bu anlaşmalar düzenlenmelidir.

Bu çalışmaları yürütmeden önce tüm personelin, en başta yöneticiler olmak üzere, bilgi güvenliği konusunda mutlaka eğitilip bilinçlendirilmeleri sağlanmalıdır. Ayrıca, bilgi güvenliğini insanların ciddiye alıp sahiplenmesinde sadece yaptırımlar, yasaklar ve caydırıcı kurallar yeterli olmaz, bunun yanı sıra mutlaka insanları bu konuya teşvik edecek ödüllendirme mekanizmaları da olmalıdır.

Kurumlarda başta bilişim personeli olmak üzere, ilgili tüm paydaşlar bilgi güvenliğinin; "kayıpları azaltan ama aynı zamanda, maddi ve manevi kazanç sağlayan ve ticari güç unsuru olan stratejik bir üst yönetim silahı" olduğunu üst yönetimlere, somut kanıtlar ve sayılarla göstermeleri gerekmektedir. Yöneticilerin de sürece katılmaları sağlanarak bilgi güvenliği yönetimini insan, süreç ve teknolojinin bütünleştiği bir yapıya elbirliğiyle dönüştürülmesi gerekmektedir.

Ülkemizdeki ilgili yasaların daha yaygın ve etkin biçimde uygulanması, ayrıca yazılı ve görsel basında bu konuya daha çok yer verilmesi, (araştırma - yazı dizileri, büyük kurumların üst yöneticilerinin başarı öyküleri ve röportajları, vb) sağlanabilir. Yaşanan olumsuz deneyimlerin başkalarına da ders olmasını

sağlayacak haberlerin kamuoyunda yaygınlaşması da uygulamadaki eksikliklerin azalmasına ve bilgi güvenliğine daha doğru yatırımlar yapılmasına katkı sağlayacaktır.

Kurumun tüm çalışanlarına; bilgi gizliliği, ticari sırların korunması gibi konulara yönelik cezai yaptırımların da açıkça yer aldığı ve çalışanların yükümlülüklerini açıkça belirten bir bilgi güvenliği belgesi imzalatılmalıdır.

Kurum dışına veri iletimi, transferi, vb süreçlere özellikle odaklanmalı ve bu aşamalardaki olası tüm risklerin en aza indirgenmesi hedeflenmelidir.

Bu konuya ilişkin bir örnek vermek gerekirse; Çalışanların çoğu Internet, vb iletişim sistemleri üzerinden iletilen verinin güvenliğine öncelikle odaklanır ama şirket dışına çıkması gereken yedek dosyalar, arızalanmış veya atıl duruma gelmiş ama içinde hala gizli şirket verisi taşıyan bilgisayar, CD, yedekleme kartuşu, vb.nin güvenliği genelde göz ardı edilir. Oysa bu gibi cihazlar ve içindeki veriler de mutlaka kontrol edilmeli ve gizli bilgiler imha edildikten veya şifrelendikten (İng. encryption) sonra kurum dışına çıkarılmalıdır.

Çözüm önerilerinin ve önlemlerin teknoloji boyutundaki yapılabilecekleri kısaca özetlemek gerekirse; ilgili her türlü ağ, iletişim, bilgisayar, elektronik kayıt, arşiv, yedek ve ayrıca yazılı belgeler, yazıcı, faks, vb. araçların kullanımında olabildiğince en güncel kimlik doğrulama ve yetkilendirme teknolojileri tercih edilmelidir. Buna ek olarak, belli noktalarda, cihazlara kaydedilen ve/veya ağlar üzerinden iletilen veriler için şifreleme teknolojileri de mutlaka kullanılmalıdır.

Biometrik, e-imza, tek kullanımlık parola, vb. teknoloji seçeneklerinden hangisinin kullanılacağı, hangi şifreleme yazılımı ve hangi anahtar uzunluğu ile şifreleme yapılacağı, vb. soruların yanıtlarının ilgili risk analizleri sonucunda belirlenmesi gerekmektedir. Bir kurum, bütçesinden yüksek miktarda TL'sini bu iş için ayırıp en pahalı ve en karmaşık teknolojiye parasını harcasa bile doğru güvenlik yatırımını yapmış olduğunun garantisini alamayacaktır.

Kurumlar kendi içlerinde belli birimleri ve bu konuda yetkin personelini görevlendirip belli zamanlarda iç güvenlik denetimleri yaptırmalı ve bunun yanı sıra yılda en az iki kez de kurum dışı güvenlik danışmanlık firmalarından dış denetim hizmeti almalıdır.

Şirket yöneticileri; Türkiye'deki ilgili T.C.K. bilişim suçları, fikir ve sanat eserleri, elektronik veri ve iletişim gizliliği, sınai mülkiyet hakları, patent, vb konulara ilişkin yasalar ve ilgili maddelerinin kendilerini nasıl ve ne şekilde sorumlu kıldığını veya koruduğunu bilmeli, şirketlerinin hukuk birimlerine bu konuları takip ettirmelidir. Özellikle, yazılım ve elektronik verilerin telif hakları, ticari sırlar, marka, gizli kurum verileri, vb sınai değerlerin bu tarz yasal çözümlerle koruma altına alınması sağlatılmalıdır.

Kurumlardaki istihdam süreçlerinde uygulanan bazı yöntemler ve önlemler, bilgi güvenliğinde etkin ve uzun vadeli çözümler sağlanmasına katkı yapmaktadır. Kurumun içerisinde ticari sırları ve gizli bilgileri en yoğun olarak kullanacak personellerin işe alım süreçlerinde adli sicil, güvenlik kontrolleri,

referans araştırmaları, kişilik testleri, adayın güvenilirliğinin irdelenmesi, vb çalışmalar kapsamlı bir şekilde yapılmalıdır.

Kurum geneli uygulanacak her çeşit projede, ister bilgi teknolojileri ile ilgili olsun, ister örgütsel yapılanma veya iş süreçlerinin değişimi ile ilgili olsun, bilgi güvenliği projelerin en başından itibaren sürece katılmalıdır ve projenin her aşamasında güvenlikle ilgili kısımlar da irdelenmelidir.

En küçüğünden en büyüğüne tüm şirketlerde, devlet kurumlarında ve toplum genelinde bilgi güvenliği farkındalık eğitimleri, bilinçlendirme çalışmaları ve eğitsel projeler yapılarak, personelin bilgi güvenliği konularında mutlak surette aydınlatılması gereklidir. Sadece şirketlerde değil, devlet kurumlarında, okullarda ve tüm ülke genelinde eğitim, bilinçlendirme ve farkındalık artışı sağlanmalıdır. Bu konuda, devlete olduğu kadar özel sektöre, basın yayın organlarına, üniversite ve ortaöğretim kurumlarına büyük iş ve sorumluluk düşmektedir.

5. SONUÇ

Günümüz dünyasında her geçen gün bireyler, şirketler, kurumlar ve devletler için "bilgi = daha çok güç" haline geldiği gibi, bilgi teknolojileri geliştikçe güvenlik sorunları da artmaktadır. Altı çizilmesi gereken nokta; bilişim toplumu haline gelinmesine rağmen risklere karşı korunmanın yolu bilişime çok para harcamak ve güvenlik teknolojilerini daha sık kullanmaktan değil, önce insanların bilinçlenmesi ve doğru güvenlik çözümlerinin ve stratejilerinin doğru yerde, doğru zamanda kullanılmasından geçmektedir.

Başarılı ve etkin bir bilgi güvenliği yönetimi; üst yönetimin desteği ve sahiplenmesi, çeşitli eğitimler ve yönetimsel düzenlemelerle tüm çalışanların bilinçlendirilmesi, kurum için öncelikli riskler ve bu riskleri azaltacak uygun çözümlerin belirlenmesi, bu çözümlerin o kuruma en uygun şekilde uygulatılması, bu uygulamaların periyodik olarak denetlenmesi ve bunların sonucunda gerekli iyileştirmelerin yapılarak sürekli gelişim ve değişim sonucunda sağlanabilir.

Birçok konuda olduğu gibi, bilgi güvenliğinde de en kritik başarı faktörü istekli, bilinçli ve bilgili insanlardır. Bilgi güvenliği yönetiminde nihai hedef, bilgi güvenliğinin zaman içinde bir kurum kültürü haline dönüşmesi olmalıdır. En deneyimli bilişim suçlularının kurum dışından yapacakları saldırılardan daha riskli ve zararlı olanının; kurum içindeki art niyetli veya bilinçsiz, dikkatsiz personel olduğu unutulmamalıdır.

Bilgi güvenliği yönetimi, sürekli yaşatılması gereken, değişimlere uyum sağlayarak sürekli gelişime açık olması gereken bir süreçtir. Bilgi güvenliği, sadece teknoloji veya sadece bilgisayar güvenliği değildir. Bilgi güvenliği; insan, süreç ve teknoloji üçlüsünün birlikte uyumlu bir şekilde çalışması gereken bir yönetim sistemidir. Özetle bilgi güvenliği, özel hayatta ve iş yaşamında kanıksanması, öğrenilmesi, rutin hale gelmesi gereken bir süreçtir. Bilgi güvenliği ve güvenlik tehditleri gibi bir konuda bile; insanların korkuyla değil, ancak sevgiyle ve eğitimle kazanılabileceği önemle vurgulanmalıdır.

KAYNAKÇA

Bowen P., Hash J., Wilson M. (2006). *Information Security Handbook: A Guide for Managers,* USA: NIST Publishing.

Carey A. (2006). *2006 Global Information Security Workforce Study*, USA:IDC.

Deloitte. (2009). *Losing Ground; 2009 TMT Global Security Survey Full Report,* Netherlands: Deloitte Touche Tohmatsu.

Eminağaoğlu M. (2008). Dikkat Casus Var!, Bilgi Güvenliği Yazı Dizisi. *İstanbul:Tekborsa Dergisi,* Sayı: 15-21 Haziran 2008.

Ernst & Young. (2008*). Global Information Security Survey 2008*. EGYM Limited.

ISO International Organization for Standardization. (2005). *ISO/IEC 27001:2005*.

ITGI Inst. (2007). *Cobit 4.1; Framework, Control Objectives, Management Guidelines and Maturity Models*. USA: ITGI Publishing.

Karabacak B., Soğukpınar İ. (2005). ISRAM: Information Security Risk Analysis Method. *Elsevier, Computers & Security* (24): 147-159.

Koç.net. (2005). *Rizikometre 2005 - Türkiye Internet Güvenliği Araştırma Sonuçları.* İstanbul: KoçNet A.Ş.

Mitnick K. D. (2005). *Aldatma Sanatı.* ODTÜ Geliştirme Vakfı Yayıncılık, 1. Basım.

Richardson R. (2008). *2008 CSI/FBI Computer Crime & Security Survey*. CSI.

Schneier B. (2008). *Schneier on Security*. USA: John Wiley & Sons Inc.

Schneier B., "A blog covering security and security technology", http://www.schneier.com/blog /archives/2008/08/terrorists_usin.html (08.07.2009).

Scholtz T., Byrnes F. C., Heiser J. (2006). *Best Practices and Common Problems for Information Security Programs*. Gartner.

Swaminatha M., Elden C. R. (2003). *Wireless Security and Privacy: Best Practices and Design Techniques*. Addison-Wesley.

Symantec. (2009). *Global Internet Security Threat Report 2008,* vol.XIV. Symantec Corporation.

Symantec. (2009). *EMEA Internet Security Threat Report 2008*, vol.XIV. Symantec Corporation.

Tan D. (2003). *Quantitative Risk Analysis Step by Step.* Sans Institute InfoSec Reading Room.

Tipton H. F., Krause M. (2007). *Information Security Management Handbook.*Auerbach Publicaions.

T.S.E. (2006). *Türk Standardı TS ISO/IEC 27001*. Ankara: T.S.E.

Wawrzyniak D. (2008). Information Security Risk Assessment – The Development. *5th International Scientific Conference Business & Management 2008:* 759-764.Lithuania.