T.C.
Dicle Üniversitesi Sosyal Bilimler Enstitüsü
İşletme Ana Bilim Dalı

Yüksek Lisans Tezi

BOWTIE TEKNİĞİ İLE BİLGİ YÖNETİMİNDE SIZINTILARIN ÖNLENMESİNE YÖNELİK BİR MODEL ÖNERİSİ

Müslüm YILDIZ

Diyarbakır 2014

T.C.
Dicle Üniversitesi Sosyal Bilimler Enstitüsü
İşletme Anabilim Dalı

Yüksek Lisans Tezi

BOWTIE TEKNİĞİ İLE BİLGİ YÖNETİMİNDE SIZINTILARIN ÖNLENMESİNE YÖNELİK BİR MODEL ÖNERİSİ

Müslüm YILDIZ

Danışman
Yrd.Doç.Dr.Mehmet METE

Diyarbakır 2014

TAAHHÜTNAME

SOSYAL BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Dicle Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğine göre hazırlamış olduğum "Bowtie Tekniği ile Bilgi Yönetiminde Sızıntıların Önlenmesine Yönelik Bir Model Önerisi" adlı tezin tamamen kendi çalışmam olduğunu ve her alıntıya kaynak gösterdiğimi ve tez yazım kılavuzuna uygun olarak hazırladığımı taahhüt eder, tezimin/projemin kağıt ve elektronik kopyalarının Dicle Üniversitesi Sosyal Bilimler Enstitüsü arşivlerinde aşağıda belirttiğim koşullarda saklanmasına izin verdiğimi onaylarım. Lisansüstü Eğitim-Öğretim yönetmeliğinin ilgili maddeleri uyarınca gereğinin yapılmasını arz ederim.

□ Tezimin tamamı her yerden erişime açılabilir.

□ Tezim sadece Dicle Üniversitesi yerleşkelerinden erişime açılabilir.

□ Tezimin … yıl süreyle erişime açılmasını istemiyorum. Bu sürenin sonunda uzatma için başvuruda bulunmadığım takdirde, tezimin tamamı her yerden erişime açılabilir.

..../..../.....

Müslüm YILDIZ

KABUL VE ONAY

Müslüm YILDIZ tarafından hazırlanan "Bowtie Tekniği ile Bilgi Yönetiminde Sızıntıların Önlenmesine Yönelik Bir Model Önerisi" adındaki çalışma, 07-11-2014 tarihi saat:11:00 'de İİBF toplantı Salonunda yapılan savunma sınavı sonucunda jürimiz tarafından İşletme Anabilim Dalı, İşletme Bilim Dalında YÜKSEK LİSANS TEZİ olarak oybirliği / oyçokluğu ile kabul edilmiştir.

Doç.Dr. Abdulkadir BİLEN (Başkan)

Yrd.Doç.Dr. Mehmet METE (Danışman)

Yrd.Doç.Dr. Mustafa ZİNCİRKIRAN (Üye)

ÖNSÖZ

Kurumların ve İşletmelerin ticari sırları, müşteri bilgileri, finansal bilgileri gibi önemli ve mahrem bilgilerinin istenmeyen ellere geçmesi olarak tanımlanan bilgi sızıntısına engel olmak kurumdaki entelektüel sermayenin korunmasıdır. Son zamanlarda dünyada ve ülkemizde bu konunun gündemde olması ve ilgili alan yazın ulusal ve uluslar arası kaynaklar açısından incelendiğinde konu ile ilgili bütüncül bir başka çalışmaya rastlanılmaması bu çalışmanın temel amacını oluşturmaktadır.

Alan yazın ulusal ve uluslar arası kaynaklar açısından incelendiğinde konu ile ilgili bütüncül bir çalışmaya rastlanılmamıştır. Konu, Türkçe ve yabancı kaynaklardan araştırılmış, 2014 yılının başında Infowatch tarafından yayınlanan 2013 Dünya Sızıntı Raporu incelenerek konunun ne denli önemli olduğu tespit edilerek, sorunun ne olduğu ve alınması gereken tedbirler belirtilmiştir.

Hazırlanan bu tez çalışması ile kurumlar ve işletmeler açısından BowtieXP programı kullanılarak profesyonel bir ‘Güvenli Kurum Ortamı’ oluşturularak kurumların bilgi sızmasını engelleyici bariyerleri nasıl oluşturulabileceği konusunda bir model şekillendirilmiş ve açıklanmıştır. Oluşturulan bu ‘‘Güvenli Kurum Ortamı’’ ın tüm kurum ve şirketler tarafından değerlendirilip gerekli önlemler alındığında, kurumlardaki bilgi kaçaklarının önlenebileceği değerlendirilmiştir.

Konuyu mikro, mezo ve makro planda açıklayacak şekilde ilgili işletme ve kurumlarda dikkate alınarak yoğun bir literatür araştırması yapılmıştır. Son zamanlardaki Wikileaks ve NSA Bilgi Sızıntıları örneklerindeki hatalar irdelenirken, 100 yıldan fazla bir zamandır kendi formülünü saklamayı başaran Coca-Cola gibi firmaların bu sırrı nasıl saklamayı başardığı araştırılmıştır. Bu kapsamda hazırlanan çalışma 4 bölümden oluşmaktadır.

Birinci bölümde; veri, enformasyon ve bilgi kavramları açıklanarak bilgi yönetimi hakkında bilgi verilmiş ve Bilgi Yönetim Sürecinin aşamaları anlatılmıştır.

İkinci bölümde; bilgi güvenliği kavramı ve bilgi güvenliği temel unsurları hakkında bilgi verilmiş ve Bilgi Güvenliği Süreçleri anlatılmıştır.

Üçüncü bölümde, bilgi sızıntı kavramı ve çeşitleri açıklanarak, tarihteki büyük bilgi sızıntı vakaları örnek olarak gösterilmiştir. Ayrıca Infowatch tarafından yayınlanan 2013 Dünya Sızıntı Raporu grafiklerle incelenmiştir.

Dördüncü ve son bölüm ise, Bilgi Sızıntısına neden olan faktörler BowtieXP modeliyle şekillendirilerek, her faktör tek tek değerlendirilip alınması gereken tedbirler sıralanmıştır. Çalışma, sonuç ve öneriler ile sonlandırılmıştır.

Bu çalışmanın hazırlanmasında yardım ve desteğini hiçbir zaman esirgemeyen danışman hocam Yrd.Doç.Dr.Mehmet METE ve değerli fikirleriyle beni yönlendiren arkadaşım Recep ÇAKIR ve yorucu çalışmam sırasında büyük destek gördüğüm fedakar eşim Sema YILDIZ'a, kızlarım Hale ve Kübra'ya sonsuz teşekkürler eder, şükranlarımı sunarım.

Müslüm YILDIZ

Diyarbakır 2014

ÖZET

Bu çalışmanın amacı; içinde bulunduğumuz yüzyılda rekabet avantajı yaratmada en etkin yollardan biri olarak kabul edilen bilginin kurumlar ve şirketler tarafından toplanması, değerlendirilmesi, raporlanması ve paylaşılması süreçlerinin bilgi yönetimi perspektifinde yeniden değerlendirilebilmesidir. İlgili süreçlerde bilgi güvenliğinin sağlanmasına yönelik tedbirler alınırken bilgiyi gizlilik, bütünlük ve erişilebilirlik özelliklerine zarar vermeden sadece yetkililerin kullanımına sunmak, yetkisizlerin erişimlerinden korumak ve bilgi kaybını ise önleyebilmek hedeflenmektedir. Bu yolla yönetimsel etkinliğin artırılacağı güvenlik zafiyetlerinin ise en aza indirgenerek oluşabilecek ekonomik zarar ve kurumsal prestij kaybının önüne geçilebileceği düşünülmektedir.

Alanyazın ulusal ve uluslararası kaynaklar açısından incelendiğinde konu ile ilgili bütüncül bir çalışmaya rastlanılmamıştır. Konu Türkçe ve yabancı kaynaklardan araştırılmış, 2014 yılının başında Infowatch tarafından yayınlanan 2013 Dünya Sızıntı Raporu incelenerek konunun ne denli önemli olduğu tespit edilerek, sorunun ne olduğu ve alınması gereken tedbirler belirtilmiştir.

Hazırlanan bu tez çalışması ile kurumlar ve işletmeler açısından BowtieXP programı kullanılarak profesyonel bir ‘‘Güvenli Kurum Ortamı’’ oluşturularak kurumların bilgi sızmasını engelleyici bariyerleri nasıl oluşturulabileceği konusunda bir model şekillendirilmiş ve açıklanmıştır. Oluşturulan bu ‘‘Güvenli Kurum Ortamı’’ nın tüm kurum

ve şirketler tarafından değerlendirilip gerekli önlemler alındığında, kurumlardaki bilgi kaçaklarının önlenebileceği değerlendirilmiştir.

Konuyu mikro, mezo ve makro planda açıklayacak şekilde ilgili firma ve işletmeler/kurumlarda dikkate alınarak yoğun bir literatür araştırması yapılmıştır. Son zamanlardaki Wikileaks ve NSA Bilgi Sızıntıları örneklerindeki hatalar irdelenirken, 100 yıldan fazla bir zamandır kendi formülünü saklamayı başaran Coca-Cola gibi firmaların bu sırrı nasıl saklamayı başardığı araştırılmıştır.

Anahtar Sözcükler

Bilgi Sızıntısı, Bilgi Kaçağı, Bilgi Güvenliği, Bilgi Yönetimi, Bowtie Modeli

ABSTRACT

The purpose of this study is to reassess the information processes estimated one of the most effective ways creating competitive advantage in the century in which we are. The processes consist of collecting, assessment, reporting and sharing of information by organizations and instutions in the scope of knowledge management. Maintaining security, in these information processes, providing this information to the authorities, avoiding unauthorized access, preserving the confidentiality, integrity and availability and avoiding information loss are targeted. In this way, administrative efficiency is believed to be increased and security vulnerability leading to preventing financial loss and institutional prestige.to be minimized.

A comprehensive study on this subject has not been detected during the study in the national and international resources. The subject has been examined and investigated in national and foreign sources. The importance of the subject has been come out by examining Global Data Leakage Report 2013 published by InfoWatch Analytical Center at the beginning of 2014 and determined what the problem is and what pracautions to be taken.

With this thesis, a model with a professional ‘‘Safe and Secure Organizational Environment’’ for organizations and institutions is constituted by using BowtieXP program showing and defining how the organizations establish barriers to prevent the data leakage.

It is considered that data leakage is to be prevented in the organizations if organizations and instutitons reassess this constituted ‘‘Safe and Secure Organizational Environment’’and take necessary preacutions.

An intensive literature search has been conducted to explain this topic in micro, meso and macro plans considering organizations and instutions. Mistakes are evaluated in the recent examples like Wikileaks and NSA data leakage and the successes in managing to keep its secret formula more than 100 years like Coca Cola, are examined in this study.

Key Words

Information Leakage, Data Leakage, Information Security, Knowledge Management, Bowtie Model

İÇİNDEKİLER

Sayfa No.

İKİNCİ BÖLÜM

BİLGİ GÜVENLİĞİ

ÜÇÜNCÜ BÖLÜM

BİLGİ SIZINTISI

DÖRDÜNCÜ BÖLÜM

BİLGİ GÜVENLİĞİNDEKİ VERİ SIZINTILARININ ÖNLENMESİNE YÖNELİK BİR MODEL ÖNERİSİ

TABLO LİSTESİ

Sayfa No.

ŞEKİL LİSTESİ

Sayfa No.

GRAFİK LİSTESİ

Sayfa No.

KISALTMALAR

CD	Compact Disc (Kompakt Disk-Yoğun Disk)
CIA	Central Intelligence Agency (Merkezi İstihbarat Teşkilatı)
DVD	Digital Versatile Disc (Çok Amaçlı Sayısal Disk)
e-ticaret	Elektronik Ticaret
e-kurum	Elektronik Kurum
e-devlet	Elektronik Devlet
e-imza	Elektronik İmza
e-posta	Elektronik Posta
FBI	Federal Bureau of Investigation (Federal Soruşturma Bürosu)
GSM	Global Positioning System (Küresel Konumlama Sistemi)
IDS	Intrusion Detection System (Saldırı Tespit Sistemi)
IPS	Intrusion Prevention System (Saldırı Önleme Sistemi)
ISO	International Organization for Standardization (Uluslararası Standartlar Teşkilatı)
NSA	National Security Agency (Ulusal Güvenlik Dairesi)
USB	Universal Serial Bus (Evrensel Seri Veriyolu)

GİRİŞ

İnsan hayatını daha kolaylaştırmak maksadı ile yeni teknolojiler üretmek için bir unsur olan bilgi günümüzde gücün sembolü haline gelmiştir. Bilgi teknolojilerini kullanan kuruluşlar, gerek maliyet avantajı elde ederek, gerekse ürün farklılaştırma olanağı ile önemli rekabet avantajı sağlamaktadır.

Kurum içerisinde bilginin iyi bir şekilde muhafazası, güncelliğini koruması, bilgilerin ulaşılabilir olması, gerekli bilginin kurum/şirket çalışanlarıyla rahat bir şekilde paylaşılabilmesi işlemlerini tanımlayan bir sistem olan Bilgi Yönetimi, kurum için kritik önem arz eden en önemli başarı faktörüdür. Bilgi yönetimi, işletmelerde önemli bir varlık olarak kabul edilen entelektüel sermayenin verimli bir şekilde kullanılmasıdır.

İşte, işletmeye rekabet üstünlüğü kazandıracak olan bilginin güvenli bir şekilde muhafazası ve paylaşımında bilgi güvenliği devreye girmektedir. Bilgi güvenliği özellikle hızla gelişen teknoloji ile birlikte son yıllarda kurumların en büyük sorunlarından biri olmuştur. İşletmelerin günümüzdeki en belirgin rekabet dayanağı, icra ettikleri üretim faaliyetlerindeki sahip oldukları bilgi varlıkları ve tecrübeleridir. Günümüz bilişim çağında kurum ve işletmeler rakiplerine üstünlük sağlamak amacıyla bilgiyi ellerinde bulundurmak ve bilgi teknolojilerinden azami derecede faydalanarak güvenliğini sağlamak zorundadır.

Şirketlerin rakiplerine karşı ekonomik avantaj elde etmesini sağlayan formül, tasarım, yasal araç ya da örüntü biçiminde olan ve bazı hukuk sistemlerinde "gizli bilgi" ya da "sınıflandırılmış bilgi" olarak adlandırılan bir bilgi bütünü olan ticari sırların ifşa edilmesi, şirketleri zarara soktuğu gibi itibarını da zedeleyebilmektedir.

Bilgi Yönetimi kapsamında bilginin toplanması, değerlendirilmesi, raporlanması ve paylaşılması süreçlerinde güvenliğin sağlanmasına yönelik tedbir almak, bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek içerden veya dışarıdan kasıtlı ya da kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak, son kullanıcı, idareci, sistem ve veri tabanı yöneticileri ve teknik personelin bilgi sistem ve ağları üzerinde yapacakları çalışmalarda bilgi güvenliği farkındalık, duyarlılık ve teknik bilgi düzeylerinin artırılması ile sistemsel güvenlik açıklarının ortadan kaldırılmasını sağlayarak, insan kaynaklı zafiyetlerin önlenmesi ve gizliliği, bütünlüğü ve erişilebilirliği sağlanmış bilişim alt yapısının kullanılması ve sürdürebilirliğinin temin edilmesi sureti ile; veri ve bilgi kayıplarının önlenmesi bu yolla ekonomik zarara uğranılmaması ve kurumsal prestij kaybı yaşanmaması tezimde ki ana ilke ve amaçlar olarak öngörülmektedir. Bu kapsamda hazırlanan çalışma 4 bölümden oluşmaktadır.

Birinci bölümde; Veri, Enformasyon ve Bilgi kavramları açıklanarak Bilgi Yönetimi hakkında bilgi verilmiş ve Bilgi Yönetim Sürecinin aşamaları anlatılmıştır.

İkinci bölümde; Bilgi Güvenliği kavramı ve Bilgi Güvenliği temel unsurları hakkında bilgi verilmiş ve Bilgi Güvenliği Süreçleri anlatılmıştır.

Üçüncü bölümde, Bilgi Sızıntı kavramı ve çeşitleri açıklanarak, tarihteki büyük bilgi sızıntı vakaları örnek olarak gösterilmiştir. Ayrıca Infowatch tarafından yayınlanan 2013 Dünya Sızıntı Raporu grafiklerle incelenmiştir.

Dördüncü ve son bölüm ise, Bilgi Sızıntısına neden olan faktörler bir risk analiz yöntemi olan BowtieXP modeliyle şekillendirilerek, her faktör tek tek değerlendirilip alınması gereken tedbirler sıralanmıştır. Çalışma, sonuç ve öneriler ile sonlandırılmıştır.

BİRİNCİ BÖLÜM

BİLGİ YÖNETİMİ

Kurumda var olan kayıtlı veya potansiyel bilgi kaynaklarını ortaya çıkarıp iş sürecine dâhil ederek, kişisel ve kurumsal verimliliğe katkı sağlayan, her türlü bilgi kaynağını kurumun amaçları doğrultusunda toplayıp, düzenleyerek ilgili çalışanlara iletmek olarak tanımlanan Bilgi Yönetiminin en önemli yapı taşlarını enformasyon ve bilgi oluşturmaktadır.

1.1.BİLGİ KAVRAMI

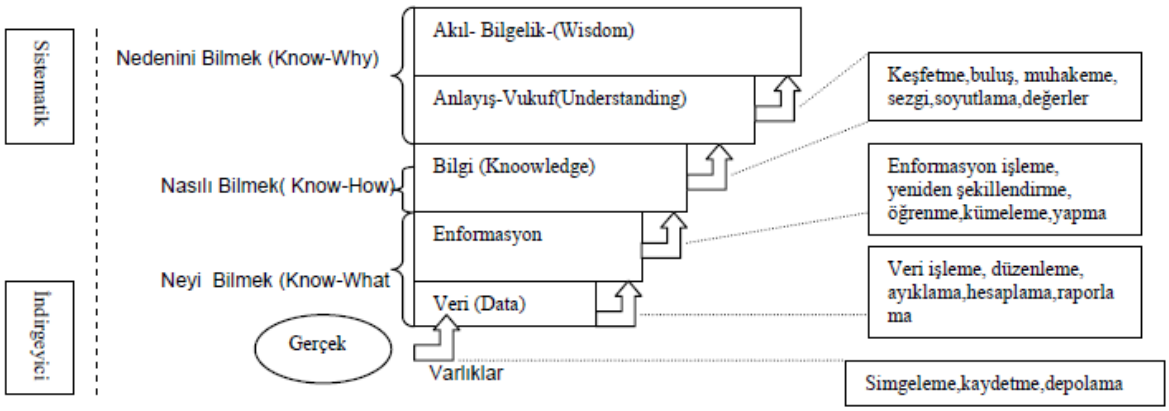
Örgütsel yapılarda ve sosyal hayatımızda beyin gücü, kas gücünün yerini almaya başladıkça, 20.yüzyıla damgasını vuran arazi, işgücü ve sermaye üçlemesine 21.yy'da bilgi (knowledge) kavramı da eklenmiştir. Bilgi, rekabet avantajı yaratmada en etkin yollardan birisidir (Nonaka ve Takeuchi, 1995).

Bilgiyi nelerin oluşturduğu tartışma konusu olmuştur. Bu hususu açıklamak için; veri, enformasyon, bilgi ve bilgelik-akıl arasındaki farklılıkları belirlemek daha yardımcı olacaktır. Veri, enformasyon, bilgi ve bilgelik yukarı doğru bir sıradüzen içinde en çok alıntı yapılan ve veriden bilgeliğe (VEBB-Veri-Enformasyon-Bilgi-Bilgelik) uzanan bir zincirdir (Ackoff,1989,3-9).

Bir bağlamdan çıkarılan rakamlar, kelimeler veriyi temsil etmektedir. Bağlama ilave yapıldığında yani bir katkıda bulunulduğunda veri enformasyona dönüşmektedir. İnsanların tecrübe ve yargılarına dayanarak kullanılan enformasyon ise bilgiyi oluşturur. Bilgelik ise, değişen şartlar çerçevesinde ileriyi görebilme yeteneğine sahip olmadır. Bilgelik, kendi ihtisas alanındaki tecrübelerinin toplamıdır. Bilgelik ayrıca, sağlıklı değerlendirme ve karar verme konusunda bilgiyi nasıl kullanacağının anlayışı olarak da tanımlanmaktadır (Montano, 2004,302).

Molhatra'ya göre ise bilgi, enformasyonun tecrübe, fikir, yorum ve bütün bunların içinde bulunduğu şartlarla bir araya gelmesidir. Bazen sezgiseldir, söze dökülmesi her zaman mümkün olmayabilir (Probst ve Romhardt, 2006: 51).

Şekil 1 incelendiğinde bilginin Veri (Data) den Akıl-Bilgelik (Wisdom) aşamasına geçerken hangi soruların cevanı aradığını görmekteyiz.



Şekil 1- Anlam Şeması
Kaynak: C.C Aktan, İ.Y. Vural, "Bilgi Çağında Bilginin Yönetimi", Bilgi Çağı ve Bilgi Yönetimi ve Bilgi sistemleri ,Çizgi Kitapevi, Şubat 2005, 1. Baskı ,s: 6,

1.1.1.Veri (Data)

Veri, amaçlara bağlı olarak işlemlerin işlenmemiş bir biçimde kaydedilmesidir. Veri, özümlenmemiş ve yorumlanmamış gözlemler, işlenmemiş gerçekler olarak tanımlanabilir. Modern kurumlarda veri, teknolojik sistemlerde saklanır ve çoğu kez bir anlam veya içerik teşkil etmez (Barutçugil, 2002:57).

Bilgi ve iletişim teknolojilerinde veri, "Bir durum hakkında, birbiriyle henüz bağlantısı kurulmamış bilinenler veya kısaca sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri" olarak tanımlanmaktadır.

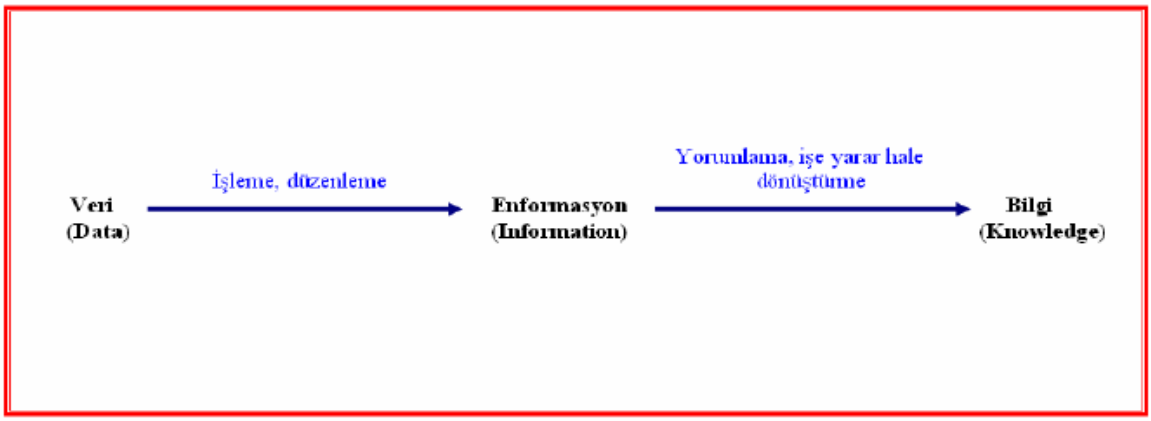
Veri, bir organizasyonda veya fiziki çevrede gelişen hadiseleri temsil eden, insanların anlayabileceği ve kullanabileceği şekle dönüştürülmemiş ham gerçeklerdir. Bu yönüyle veri geçmişten veya gelecekten bağımsız olarak bir olayın veya vakanın münferit olarak tespit edilmesidir (Zaim, 2005).

Veri, özetleme, düzeltme, hesaplama, sınıflandırma ve içerik işlemleri aracılığıyla değer eklenmesiyle enformasyona dönüştürülmektedir. Veri, yorumsuz ve içeriksiz şekiller ve/veya olgulardır (Kalseth ve Cummings, 2001).

1.1.2.Enformasyon

Enformasyonun amacı, alıcının bir konudaki düşüncelerini değiştirmek, değerlendirmesi ya da davranışı üzerinde bir etki yaratmaktır. Enformasyon, alıcısını biçimlendirmek zorundadır, alıcının bakış açısında ya da anlayışında fark yaratmalıdır. Buradan da anlaşılacağı üzere alınan iletinin gerçek bir enformasyon niteliği taşıyıp taşımadığına karar veren alıcıdır. Yani, enformasyonda hâkim konumda olan alıcıdır, gönderici değildir. Enformasyon kuruluş içinde iletişim teknolojisini kullanarak (iletişim ağı, e-posta, İntranet, Extranet gibi.) veya geleneksel yöntemler kullanarak (el yazısıyla not göndermek, bir yazının fotokopisini göndermek gibi) dolaşır (Davenport ve Prusak, 1998).

Enformasyon, düzenlenmiş veri olarak tanımlanabilir. Düzenlenme başkaları tarafından yapılır ve yalnızca ilgili kişi için bir anlam taşımaktadır (Barutçugil, 2002:57). Enformasyon anlamlıdır, amacı vardır konu ile ilgilidir, belirli bir amaç için şekillenmiştir. Enformasyon, çalışanlara ve yöneticilere ağ bağlantıları, internet veya e-mail ile ulaşır (Awad ve Ghaziri, 2004:36). Enformasyon, olay ve objeleri yorumlamak için bir bakış açısı kazandırır ve bilgi oluşturmak için gerekli bir öğedir. Enformasyon, bilgiye katkıda bulunarak onu etkiler (Nonaka, 2004:50). Veri ve enformasyon için kullanılan sorular; "kim-ne-nerede-ne zaman?" sorularıdır, fakat bilgi için sorulan sorular ise "neden?" ve "niçin?"dir (Malhotra, 2000:15). Unutulmaması gerekir ki veri ve enformasyon, bilginin oluşmasında ve kaybolmamasında önemli iki unsurdur. Veri olmadan enformasyona ulaşmak, enformasyon olmadan da bilgi elde etmek zordur (Abdullah ve Diğ., 2005:39). Bu ilişki aşağıdaki gibi gösterilebilir.



Şekil 2: Bilginin Oluşum Süreci
Kaynak: Sotirofski ve Güçlü, 2006:354 **"**Bilgi Yönetimi", Türk Eğitim Dergisi, Cilt:4 Sayı:4,2006,s351-357.

1.1.3.Bilgi

Bilgi (İng. knowledge), enformasyonu yorumlamak için ihtiyaç duyulan kuralların anlaşılmasıdır. Bir başka tanımla; bilgi, enformasyon parçaları ile bunlardan yararlanarak ne yapılabileceği arasındaki ilişkiyi anlama yeteneğidir.

Bilgi insan zihninde, deneyimlerle, değerlerle, gözlemlerle, duyumlarla vs. elde edilmiş enformasyonun sentezlenip içselleştirilerek kişiselleştirilmiş hale gelmesidir. Bilgi, insan beyninde ve/veya zihninde bulunduğundan soyut bir varlığa işaret etmektedir. İnsan zihnindeki bilgiler elektronik ya da basılı bir kayıt ortamına aktarıldığında veya birileriyle paylaşıldığında enformasyona dönüşebilmektedir. "Bilgi ile enformasyon arasındaki bağlantıyı açıklayan kabul edilmiş en iyi tanım, onun sadece ve sadece hayata geçirilebilir enformasyon olduğudur. Eğer bilgiyi nasıl kullanacağınıza karar verirseniz enformasyon da tartışılarak bilgiye dönüşür" (Tiwana, 2003: 77).

Bilgi; belli bir düzen içindeki deneyimlerin, değerlerin, amaca yönelik enformasyonun ve uzmanlık görüşünün, yeni deneyimlerin ve enformasyonun bir araya getirilip değerlendirilmesi için bir çerçeve oluşturan esnek bir bileşimidir. Bilgi bilenlerin beyinlerinde ortaya çıkar ve orada uygulamaya geçirilir. Kuruluşlarda genellikle yalnızca belgelerde ya da dolaplarda değil rutin çalışmalarda, süreçlerde, uygulamalarda ve normlarda kendini gösterir (Davenport ve Prusak, 2001: 27).

Yusuf Has Hacip, Kutadgu Bilig'de bilgiyi, "değeri yok olmayan bir servet" biçiminde tanımlarken, J.J.Rousseau gerek bireysel, gerek toplumsal gelişmenin bilgi ile gerçekleşebileceğini vurgulamıştır.

Gelişmiş ve endüstrisini tamamlamış toplumlar ile gelişmekte olan ülkeler arasındaki en önemli ayrıcalık, "bilgi" olmaktadır. Bilgi üretim faktörleri olarak sayılan emek sermaye doğal kaynak ve teknoloji yanında beşinci etmen olmaya başlamıştır. Gelişmiş toplumların %80'i gibi büyük bir bölümü, bu yeni kaynaktan etkin olarak

yararlanma yeteneği kazandığından, bilginin üretim ve hizmet sektöründe sermayeden daha önemli bir etmen olacağı düşünülmektedir.

Bilginin giderek daha popüler hale gelmesinin arkasında yatan nedenlerin başında; son yıllarda, bilginin toplanması, saklanması, işlenmesi alanlarındaki teknolojik olanakların hızla artmış olmasıdır.

Bilgi yaşamın her alanında kullanılan ve korunması gereken bir güçtür. Günümüzde her alanda yapılan savaşların, rekabet ve yarışların sonucunu bilginin üstünlüğü belirlemektedir. Günümüz ve geleceğin savaşları bilgi savaşına dönüşmüştür. Bilginin üretilme, depolanma, korunma, kullanılma, paylaşılma, yayılma, etkileşme ve artma hızı, bilişim teknolojilerinin gelişmesine bağlı olarak her geçen gün artmaktadır.

Bilgi yaşam için vazgeçilmez bir varlık ve medeniyet yakıtıdır. Bilgi değerli bir varlıktır. Bilgiye sahip olmak emek, zaman ve kaynak harcamayı gerektirir. Bilginin değerinin yüksek olması korunma gereksiniminin ölçüsünü de belirler. Bilgi hayatımızın her alanında yer aldığından içinde bulunduğumuz dönem bilgi çağı olarak adlandırılmaktadır.

Bilgi, kaynağına göre incelendiğinde örtülü ve açık bilgi olmak üzere iki türde yer aldığını görmekteyiz. Sözle ya da yazıyla ifade edilen net söylemler açık bilgi olarak kabul edilirken, aktarımda zorluk olan duyguların, düşüncelerin eylemlere kolayca aktarılamaması ise örtülü bilgi olarak kabul edilirler.

Okuldaki bir öğretmenin öğrencilerine anlattığı ders veya bir ustanın çırağına yaptığı açıklama açık bilgiye örnektir. Örtülü bilgi ise, açık bilginin tersine sözlü veya yazılı olmanın dışında uzun süreli bir birikim ve tecrübe ile kazanılan bir eylemle veya davranışla açığa çıkmaktadır.

1.2.BİLGİ YÖNETİMİ

Bilginin çok önemli olduğu bir ortamda sadece bilgi sahibi olmak yeterli olmamaktadır. Çünkü sahip olunan bilginin örgüt içinde paylaşılması ve karar verme, planlama gibi stratejik öneme sahip konularda doğru ve eksiksiz kullanılabilmesi için iyi bir bilgi yönetim sistemine sahip olunması gerekir. Bilgi Yönetiminin genel amacı, bilginin birden fazla kişinin (örgütün, toplumun vb) kullanabilmesine elverişli, yani paylaşılabilir bir hale gelmesidir (Aktan ve Vural, 2005).

Bilgi Yönetimin en önemli amacı, örgütsel bilgi kaynaklarını kullanarak, örgütsel verimliliği gerçekleştirmeye ve faaliyetleri etkin kılabilmeye yönelik bir ortam yaratmak ve bilgiyi etkinliklerin merkezine yerleştirmektir. Bilginin edinimi, içselleştirilmesi, paylaşımı ve değerlendirilmesi Bilgi Yönetim sürecinin en önemli işlemleri olarak ortaya çıkmaktadır (Yılmaz, 2009).

Bilgi, entelektüel sermayenin bir bileşeni olan insan sermayesinin kurum içerisinde en verimli biçimde kullanılmasını sağlayan bir unsurdur. Bu unsurun kurum içerisinde yönetim tarafından üretken kılınması bilgi yönetiminde yöneticilere düşen en büyük sorumluluktur.

Bilgi yönetiminin uygulandığı örgütlerde liderler, ilk ve öncelikli olarak hem bireysel hem de örgütsel düzeyde öğrenme işinden sorumludurlar. Liderler, organizasyon içinde öğrenme kültürünün oluşturulması, sürdürülmesi konusunda önemli bir role sahiptirler. Liderler bilgiye değer vererek, personel güçlendirme uygulayarak örgüt içinde sorgulama yapma, deneyimlerin geliştirilmesi yönünden çalışanların cesaretlendirilmesi, güvene dayalı bir ortamın yaratılması ve örtülü bilginin deneysel öğrenme vasıtası ile açığa çıkarılmasını kolaylaştırması konusunda da rollere sahiptir (Kılıç,2006:180).

Bilgi yönetiminin temel amaçları şu şekilde belirtilebilir (Özgener,2002: 485 Plunkett, 2001: 15):

- Öğrenme eğrisini hızlandırmak,
- Daha hızlı bir iyileştirmeyi sağlamak,
- Örgüt içerisinde yeni bilgi üretmek,
- Doğru bilginin, doğru insanlara, doğru zamanda ulaşmasını sağlamak,
- Hızlandırılmış transformasyona imkân sağlamak,
- Dış kaynaklardaki değerli bilgiyi örgüte kazandırmak,
- Toplumsal kültür ve özendiricileri ile bilginin büyümesini kolaylaştırmak,
- Bilginin dokümanlar, veri tabanları ve yazılımlar aracılığı ile (mevcut örgütsel bilgi varlıkları ile) sunmak,
- Örgütsel kararlarda ulaşılabilir bilginin kullanılmasını sağlamak,
- Örgütün birimleri içerisinde oluşan bilginin veya başka örgütlerdeki benzer birimlerin birimler arası transferini gerçekleştirmek,
- Örgütsel bilginin kıymetlendirilerek entelektüel sermayeye dönüştürmek ve bilgi yönetimi sayesinde ölçülmesini sağlamak.

Bilgi yönetiminin nihai amacı, entelektüel sermayeden yararlanmak, spesifik olarak bilgi transferini teşvik etmek ve bilgi paylaşımını sağlamaktır (Duffy, 2001: 59).

Bazı örgütlerin bilginin üretken kılınması çabalarına örnek olması amacıyla bilgi yönetimi hedefleri ve uygulamaları Tablo 1'de gösterilmiştir. Bu tabloda Bilgi Yönetiminin hedeflerinin arasında;

- Bilgi paylaşma kültürü oluşturmak
- Bilgiyi yakalamak, saklamak ve bireylerin dolaylı bilgisini ortaya çıkarmak
- Bilgi transferi için küçük çevreler oluşturmak
- Müşterinin bilgisinden faydalanmak
- Mevcut bilgiden yeni gelirler elde etmek
- Bilgi yönetimine dayalı kariyer oluşturmak
- Bilgi üretim sürecini ve görülmez becerilerini ölçmek olduğunu görmekteyiz.

Bilgi yönetimi uygulamalarında Hawlett-Packard tarafından uygulanan; Şirketin tüm basamaklarında bilgi paylaşımı ve risk almayı cesaretlendiren bir işbirlikçi kültürün olması ve hiçbir işe yaramayan bilgi bulanların bile desteklendiği bir yapının oluşması şirketin ürünlerinin çeşitliliğine ve müşteri tatmininde zirveyi yakalamayı sağlamıştır. McKinsey&Bainco danışmanlık firmalarının her işten oluşan tecrübeleri, takım çalışanlarının isimleri ve müşteri tepkilerini içeren 'bilgi veritabanı' geliştirmesi şirketin tecrübelerinin bir havuzda toplanarak bu tecrübelerden daha sonra faydalanılmasını sağlamıştır.

Tablo 1: Şirketlerin Bilgi Yönetimi Hedefleri ve Bilgi Yönetimi Uygulamaları

Şirket Adı	Ülke	Bilgi Yönetimi Hedefleri	Bilgi Yönetimi Uygulamaları
3M	USA	Bilgi paylaşma kültürü oluşturmak.	Yöneticiler, devamlı öğrenme ve geliri birbirine paralel götürür.
McKinsey & Bainco	USA	Bilgiyi yakalamak, saklamak ve bireylerin dolaylı bilgisini ortaya çıkarmak.	Bu iki danışmanlık firması, her işten oluşan tecrübeleri, takım çalışanlarının isimleri ve müşteri tepkilerini içeren "bilgi veritabanı" geliştirmiştir. Her takımın, işi düzenleyecek bir kişi belirlemesi gerekir.
Ford Motor	USA	Bilgi paylaşma kültürü oluşturmak.	Şirket kendini, enformasyon, teknoloji ve bilgiyi kullanan satıcı ağları ile dönüştürmüştür.
Hewlett-Packard	USA	Bilgi paylaşma kültürü oluşturmak. Dolaylı bilgi transferi için küçük çevreler oluşturmak.	Şirketin tüm basamaklarında bilgi paylaşımı ve risk almayı cesaretlendiren bir işbirlikçi kültür vardır. HP aynı zamanda, hiçbir işe yaramayan bilgi bulanları bile destekler.
Honda	Japonya	Dolaylı bilgi transferi için küçük çevreler oluşturmak.	Emek bolluğu ve aşırılık rutin olarak kullanılmakta, insanlara işle ilgili gerekli konularda enformasyon verilmekte. Bu da beklenmeyen kaynaklardan gelen sorumluk ve yaratıcı çözümlere yol açar ve bir kişisel kontrol mekanizması oluşturur.
Benetton	İtalya	Müşterinin bilgisinden faydalanmak.	Renkler ve modellerde en son trendleri yakalamak için karmaşık müşteri kesimlerini takip eder.
General Electric	USA	Müşterinin bilgisinden faydalanmak.	1982'den beri, firma tüm müşteri şikayetlerini bir veritabanında toplamıştır. 1,5 milyon şikayet toplamıştır ve onlara faal çözüm üretmiştir.
Netscape	USA	Müşterinin bilgisinden faydalanmak.	İnternet aracılığıyla, rapor verebilecek ve yeni üretimde destek olabilecek müşteri liderleri ile bağlantı.
National Bicycle	Japonya	Müşterinin bilgisinden faydalanmak.	Müşterinin ağırlık, uzunluk ve renk tercihine göre bir günde bisiklet üretmekte.
Outoku-mppu	Finlandiya	Mevcut bilgiden, yeni gelirler elde etmek.	Madenî arıtım için fabrika kurmak bilgisi, tüm dünyada personel, yönetim ve müşterinin kullanacağı şekilde olmuştur.
IBM	USA	Bilgi yönetimine dayalı kariyer oluşturmak.	Çalışanlar, şirket hakkında daha çok holistik bilgi elde etmek için, profesyonel ve yönetim arasında yer değiştirmek için yüreklendirilir.
Telia	İsviçre	Bilgi üretim sürecini ve görülmez becerileri ölçmek.	İsviçre Telekom şirketi, 1990'dan beri kâr ve zarar tablosunu, insan kaynakları profilini ve insan kaynaklarına yatırımını gösteren bir rapor yayımlar ve bu rapor herkes tarafından okunabilir.

Kaynak: H. Bell. (2001). *Measuring and Managing Knowledge.*

1.3 BİLGİ YÖNETİM SÜRECİ

Bilgi yönetimi süreci bilginin yaratılmasından bilginin kullanılmasına kadar birbirini takip eden bilginin yaratılması/elde edilmesi, bilginin saklanması/organize edilmesi, bilginin yayılması/dağıtılması ve bilginin kullanılması/uygulanması gibi aşamalardan oluşmaktadır (Alavi, 1997).

1.3.1 Bilginin Elde Edilmesi

Bilgi örgütsel düzeyde iç faaliyetlerden veya şirket yapısıyla iletişimi olan dış kaynaklardan elde edilir. Şirketler bu iç ve dış çevreleri ile ilişkileri sırasında ihtiyaç duyduklarında gerekli enformasyonu alarak bilgiye dönüştürür. Bu bilgiyi kendi tecrübeleri, değerleri ve kuralları ile birleştirerek harekete geçerler. Bütün şirketler bilgiyi yaratmak için insan, enformasyon ve mekanizma gibi bileşenlere sahiptir. Bununla birlikte bu temel bileşenlerin nasıl olduğu ve nasıl yayıldığı hakkında farklılıklar vardır. Bu farklılıklar şirketlerdeki elementler arasındaki ilişki kadar bilgiyi yaratma sürecini etkiler (Sena ve diğ., 1999).

1.3.2. Bilginin Saklanması

Firmalar örgütün iç ve dış kaynaklarından elde edilen bilgileri gerekli olduğunda kullanmak için saklamaya ve depolamaya ihtiyaç duyarlar. Bilgiyi saklama, şirketin elde ettiği bilginin kaybını en aza indirgemektir. Bu yüzden tüm insan kaynakları politikaları çalışanlarıyla birlikte değerli bilgilerini kaçırmamak için yüksek personel devir hızından kaçınmaktadır. Bilgiyi saklamak bir firma tarafından benimsenen davranışlardaki değişimlerin muhafaza edilmesi, arındırılması ve firmanın alt bölümleri boyunca bu değişimlerin yayılması olarak açıklanabilir. Bu yayılma sayesinde, bir firma yeni ve eski bilgilerine alan ve zaman bakımından etki edebilir. Örgütler değişik şekillerdeki bellek sistemlerinde bilgiyi saklarlar. Bu sistemler beyindeki özel bir bölümden, fiş kartlarına, sabit disklere, dosyalama kabinlerine, kütüphanelere ve veri ambarlarına uzanır (Perez ve diğ., 2002).

1.3.3 Bilginin Paylaşılması

İşletmelerin sürekliliği için hangi bilginin, nasıl, niçin, ne zaman ve ne kadar paylaşılacağı son derece önemlidir. Bilgiye sahip olmanın çok ayrıcalıklı bir güce sahip olma anlamı taşıması nedeniyle paylaşımının da bu gücün yitirilmesi veya arttırılmasına neden olacağı söylenebilir. Bu çerçevede bilgi paylaşımı konusunda öne çıkan konular bilgi paylaşımının ne olduğu ve bilgi paylaşımını etkileyen faktörlerin neler olduğudur (Köseoğlu ve diğ., 2011:220).

1.3.4 Bilginin Kullanılması

Bilginin uygulanması şimdiye kadar kontrol altında bulunan bilginin şirketin ulaşmak istediği amacını gerçekleştirmek için en hızlı bir şekilde doğrudan kullanılmasıdır. Bu aşamada bilgi kullanılmakta, bu kullanımın sonuçları değerlendirilmekte ve gerekirse bilgi yönetimi süreci yeniden düzenlenmektedir. Firmaya rekabet avantajı sağlayan şey soyut bilgi değil bilginin etkin bir biçimde kullanımı, uygulanmasıdır. Enformasyon teknolojileri firmaya bilgiyi uygulama konusunda pek çok imkân sunmaktadır. İşletmeler belirli konularla ilgili özel çalışma grupları oluşturmak suretiyle de bilginin daha etkin bir biçimde kullanımını sağlayabilirler (Hauschild ve diğ., 2001).

İKİNCİ BÖLÜM

BİLGİ GÜVENLİĞİ

2.1. BİLGİ GÜVENLİĞİ KAVRAMI

Yaşadığımız çağın bir sembolü olarak kabul edilen bilgi, gelişen teknoloji ile toplumların ulaşması kolay fakat korunması o denli zor olan ve kurumların/işletmelerin rakiplerine üstünlük sağlayan değerli bir varlıktır. Günümüzde bilgi teknolojisinde gelişmelerle birlikte, bilginin basılı ortamdan elektronik ortama aktarılması giderek yaygınlaşmış, bilgisayar üzerinden doğrudan bilgiye ulaşmak kolaylaşmıştır. Bilginin elektronik ortama aktarılması ile birlikte bilgiye erişim, analiz etme ve karar destek açısından önemli kolaylıklar sağlamakla beraber, elektronik ortamda saklanan ve paylaşılan bilginin güvenliği çok daha önemli hale gelmiştir. Bilgi güvenliği ise bu değerli varlığın izinsiz kullanıcılar tarafından çalınmasını, kullanılmasını ya da değiştirilmesini engellemektir.

Bilgiye sürekli erişimin sağlanması, bilginin göndericiden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlük içerisinde güvenli bir şekilde iletimi bilgi güvenliği olarak tanımlanabilir (Pfleeger, 1997).

Bilgi güvenliği, “Bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önlemek” olarak tanımlanır. Bilgisayar teknolojilerinde güvenliğin amacı ise “kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin yapılarak gerekli önlemlerin önceden alınmasıdır” (Canbek ve Sağıroğlu, 2006).

Bilgi, fiziksel olarak kâğıt üzerinde yazılı olabileceği gibi elektronik olarak bilgisayarlarda, hard disklerde, USB’lerde, CD ve DVD lerde saklanabilmektedir. Posta ya da elektronik posta yoluyla bir yerden bir yere iletilebilir ya da kişiler arasında sözlü olarak ifade edilebilmektedir. Bilgi hangi formatta olursa olsun, mutlaka uygun bir şekilde muhafaza edilmelidir. Bilgi güvenliğinin sağlanabilmesi bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin yeterli düzeylerde sağlanabilmesi ile mümkündür.

Bilgi güvenliğinin sağlanması için bilgi varlıklarının korunması gerekmektedir. Bir kurum veya kuruluşun kar etmek, katma değer sağlamak, rekabet oluşturmak ve kurumsal sürdürülebilirliğini sağlamak amacıyla sahip olduğu veya sahip olması gereken ürün, pazar, teknoloji ve organizasyona ait bilgilerin tümü bilgi varlıkları olarak tanımlanabilir. Bu bilgi varlıklarının fiziksel olarak korunması için, fiziksel güvenliğin, transfer edilmesi gereken bilgilerin sağlanması için iletişim güvenliğinin, bilgisayar sistemlerine erişimlerin kontrol edilmesi için bilgisayar ve ağ güvenliğinin sağlanması gerekmektedir. Bilgi güvenliğinin yüksek seviyede sağlanabilmesi için bu farklı güvenlik türlerinin tamamının organize bir şekilde sağlanması gerekmektedir (Gümüş, 2010).

Bilgi güvenliği, bilgiyi yetkisiz erişimlerden koruyarak gizliliğini (confidentiality) sağlamak, bilginin bozulmadan tamlığını (bütünlük) ve doğruluğunu (integrity) sağlamak ve istenildiği zaman erişilebilirliğini (availability) garanti etmektir (Isaca, 2009).

Kurumsal bilgi güvenliği ise, kurumların bilgi varlıklarının tespit edilerek zafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerinin alınması olarak düşünülebilir.

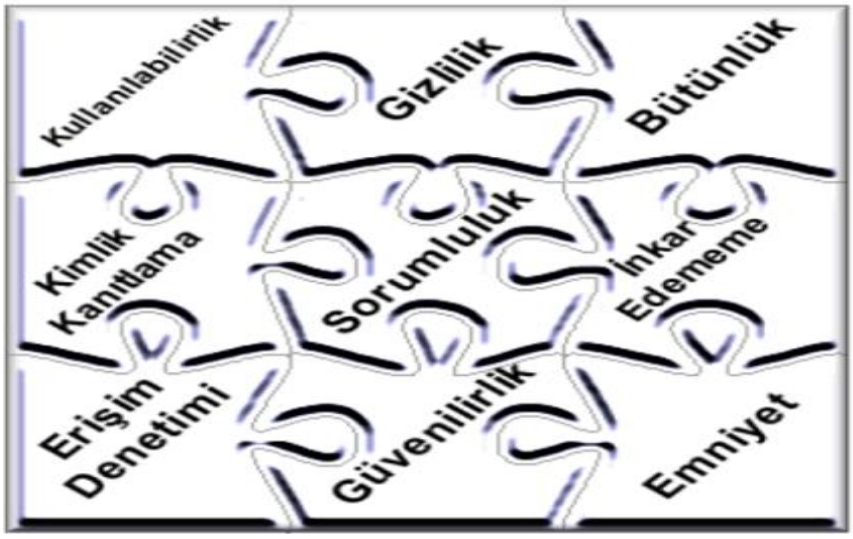
Kurumsal bilgi güvenliğini; bilginin üretildiği, işlendiği ve muhafaza edildiği her ortamda sağlamak zorundayız. Bunun için mevcut yazılımlar, donanımlar, ortamlar ve her şeyden önemlisi insan kaynakları dikkate alınmalıdır. İnsan unsurunun güvenlik halkasındaki zincirin en zayıf halkası olduğu hiçbir zaman unutulmamalıdır.

Kurumsal bilgi güvenliğini sağlamak dinamik bir süreç olduğundan güncel risk analizleri devamlı yapılmalı, ihtiyaca binaen güvenlik politikaları güncellenmelidir. Bilgi güvenliğinin kâğıt üzerinde bir zorunluluktan ibaret olmayıp şirketin itibarını doğrudan etkiliyip kurumun gelir kaybına uğramasına yol açan bir etkendir.

Kurumlarda bilginin gizliliği, bütünlüğü ve ulaşılabilirliğine ilişkin güven ortamının yaratılması ve sağlam bir güvenlik yönetim sisteminin kurulması için TS ISO/IEC 27001 "Bilgi Güvenliği Yönetim Sistemi" standardı oluşturulmuştur. TS ISO/IEC 27001 standartı sayesinde kurumlar bilgi güvenliği yönetim sistemini kurarak gerçek risklerini saptayabilmekte ve bu risklerin giderilmesi için gereken teknoloji, politika ve prosedürleri devreye alabilmektedirler.

2.2 BİLGİ GÜVENLİĞİNİN TEMEL UNSURLARI

Bilgi güvenliği denilince gizlilik, bütünlük ve erişilebilirlik kavramları ön plana çıkmaktadır. Bilginin gizliliği kavramı ile kastedilen, bilgiye sadece o bilgiye erişmesi gereken kişi ya da kişilerin erişimine izin verilmesidir. Bilginin bütünlüğü kavramı ile kastedilen, bilginin tahrif edilmeden, orijinal yapısı bozulmadan olduğu gibi korunmasının sağlanmasıdır. Bilginin erişilebilirliği kavramı ile kastedilen ise, bilgiye istenilen ve makul olan bir zamanda erişilmesi ve bilginin kullanılmasıdır (Baykara ve diğ, 2013).



Şekil 3: Bilgi Güvenliğinin Temel Unsurları
Kaynak: NAZLI, 2011 den uyarlanmıştır. Sistem Yönetimi ve Bilgi Güvenliği http://mikailnazli.blogspot.com.tr/2011/04/guvenlik-gereksinimleri-nasil-saptanir.html

Bilgi güvenliğinin temel unsurları; gizlilik, bütünlük veya bütünsellik, kullanılabilirlik veya istendiğinde hazır bulunma, kimlik kanıtlama veya gerçeklik ve inkar edememe (yadsıma) dır. Bununla birlikte; sorumluluk, erişim denetimi, güvenilirlik ve emniyet etkenleri de bilgi güvenliğini destekleyen unsurlardır. Bu kapsamda;

(1) Gizlilik, bilginin yetkisiz kişiler, varlıklar veya süreçler tarafından kullanılmaması ya da erişilememesinin temini, hem bilgisayar sistemlerinde, hem saklama ortamlarında, hem de ağ üzerinde gönderici ve alıcı arasında taşınırken yetkisiz erişimlerden korunmasıdır.

(2) Bütünlük, verinin işlenmesi, depolanması ve iletilmesi esnasında içeriğinin ve doğruluğunun yetkisiz olarak değiştirilmediğinin garanti edilmesi, veriyi olması gerektiği şekilde tutmak ve korumaktır. Bilginin bozulmasını, değiştirilmesini, yeni veriler eklenmesini, bir kısmının veya tamamının silinmesini engellemeyi hedefler.

(3) Kullanılabilirlik, yetkili bir varlık tarafından talep edildiğinde bilginin erişilebilir ve kullanılabilir olma özelliğinin temini, kullanıcıların erişim yetkileri dâhilinde olan verilere, veri tazeliğini yitirmeden, zamanında ve güvenilir bir şekilde ulaşabilmesidir.

(4) Kimlik kanıtlama, geçerli kullanıcı ve işlemlerin tanınması ve doğrulanması ile bir kullanıcının veya işlemin hangi sistem kaynaklarına erişme hakkının olduğunun belirlenmesi sürecidir.

(5) İnkâr edememe, bir bilgiyi alan veya gönderen tarafların, o bilgiye sahip olduğunu, aldığını veya gönderdiğini inkâr edememesi, iki sistem arasında bir bilgi aktarımı yapılmışsa ne gönderen veriyi gönderdiğini, nede alıcı veriyi aldığını inkâr edememesidir.

(6) Sorumluluk, belirli bir eylemin yapılmasından; kimin, hangi makamın veya neyin sorumlu olduğunu belirleme yeteneğidir.

(7) Erişim denetimi, bir kaynağa erişmek için belirli izinlerin verilmesi veya alınmasıdır.

(8) Güvenilirlik, bilginin üretiminde kullanılan herhangi bir unsurun belirlenen güvenlik süreçlerine kesin bir şekilde uyarak çalışması veya çalıştırılması ve paylaşıldığı tüm ortamlarda bunu çok güvenli bir şekilde yapabilmesidir.

(9) Emniyet, bilgi varlığının bulunduğu her ortamda potansiyel veya bilfiil tehlike oluşturacak etkinlik veya olayları önleme tedbirlerini içermektedir.

Bu unsurların bir veya birkaçının eksikliği, bilgi güvenliğinde aksamalara neden olur. Bu nedenle bilgi güvenliğinin sağlanması iş süreçlerinin bir parçası olmalı, yönetim ve kültür sorunu olarak ele alınmalıdır.

2.3 BİLGİ GÜVENLİK SÜREÇLERİ

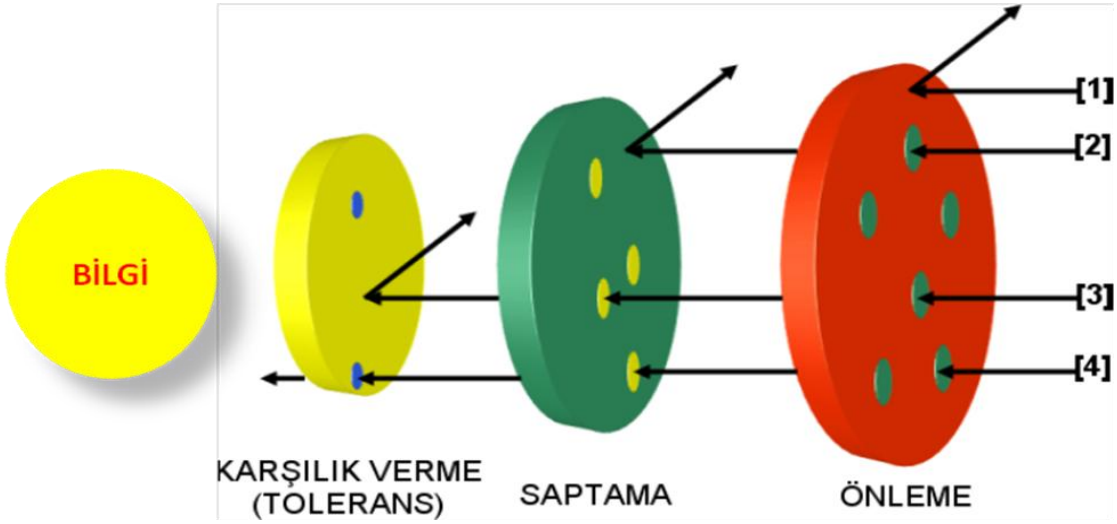
Bilgi güvenliği çerçevesinde kurulacak güvenlik sistemi altyapısının ve politikasının doğru bir şekilde belirlenebilmesi için, korunmak istenen bilginin değerlendirilmesi ve güvenlik yönetiminin doğru ve eksiksiz bir şekilde yapılması gerekir. Güvenlik yönetimi, bilgi ve bilgisayar güvenliğini olumsuz yönde etkileyecek faktörlerinin belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecidir (Canbek ve Sağıroğlu, 2006).

ISO Rehber 73'e göre risk, bir olayın ve bu olayın sonucunun olasılıklarının birleşimi olarak tanımlanmaktadır. Risk yönetiminin bir adımı olan risk değerlendirmesi, risklerin tanımlandığı ve tanımlanan bu risklerin etkilerinin ve önceliklerinin belirlendiği bir süreçtir. Risk yönetimi, kabul edilebilir düzeyde bir riskin belirlenmesi, hali hazırdaki riskin değerlendirilmesi, bu riskin kabul edilebilir düzeye indirilebilmesi için gerekli görülen adımların atılması ve bu risk düzeyinin sürdürülmesidir. Bilgi ve diğer varlıklar, bu varlıklara yönelik tehditler, var olan sistemde bulunan korunmasızlıklar ve güvenlik sistem denetimleri, mevcut riski tayin eden bileşenlerdir. Korunması gereken bilgi ya da varlıkların belirlenmesi; bu varlıkların kuruluşlar açısından ne kadar değerli olduğunun saptanması; bu varlıkların başına gelebilecek bilinen ve muhtemel tehditlerden hangilerinin önlenmeye çalışılacağının ortaya konulması; muhtemel kayıpların nasıl cereyan edebileceğinin araştırılması; her bir varlığın maruz kalabileceği muhtemel tehditlerin boyutlarının tanımlanması; bu varlıklarda gerçekleşebilecek zararların boyutlarını ve ihtimallerini düşürmek için ilk planda yapılabileceklerin incelenmesi ve ileriye yönelik tehditleri asgari seviyede tutmak için atılması gereken adımların planlanması, risk değerlendirmesinin belli başlı safhalarındandır (Jones, A., Ashenden, 2005).

Bilgi ve bilgi sistemleri güvenliğinde düşman; kasıtlı ve kasıtsız olarak yapılan ihlal ve saldırılar ile bunları gerçekleştirenlerdir. Var olan bilgi ve bilgi sistem güvenliğini aşmak veya atlatmak, zaafa uğratmak, kişileri doğrudan veya dolaylı olarak zarara uğratmak, sistemlere zarar vermek, sistemlerin işleyişini aksatmak, durdurmak, çökertmek veya yıkmak gibi kötü amaçlarla yapılan ve çok farklı teknikler içeren girişimler saldırı

olarak adlandırılmaktadır. Saldırı türlerinin bilinmesi, doğru bir şekilde analiz edilmesi ve gereken önlemlerin belirlenmesi, bilgi güvenliği için büyük bir önem arz etmektedir. Bilgi güvenliğinin ideal yapılandırılması üç süreç ile gerçekleştirilir. Bu süreçler, önleme (prevention), saptama (detection) ve karşılık vermedir (response ya da reaction).

Şekil 4'de güvenlik süreçlerine bir örnek verilmiştir. Bu şekilde, 4 farklı saldırı [1]-[4] ile gösterilmiştir. Şekilden de açıkça görülebileceği gibi, [1] numaralı saldırı, hemen önleme safhasında engellenirken; [2], [3] ve [4] numaralı saldırılar bu safhada önlenememiştir. Önleme sürecini atlatan bu saldırılardan [2] numaralı saldırı, saptama aşamasında tespit edilip, bertaraf edilirken; [3] ve [4] numaralı saldırılar, saptama aşamasından da geçebilmiştir. Belirlenen tolerans ile tasarlanmış son aşama olan karşılık verme safhasında, [3] numaralı saldırı önlenirken; bütün aşamaları atlatıp geçen [4] numaralı saldırı, bütün güvenlik süreçlerini geçip, sisteme zarar vermiştir. Takip eden kısımda güvenlik süreçlerinin her biri, temel özellikleri ile açıklanmaktadır (Canbek ve Sağıroğlu, 2006).



Şekil 4: Bilgi Güvenliği Süreçleri ve Saldırılara Tepkileri
Kaynak: CANBEK ve SAĞIROĞLU, 2006 dan uyarlanmıştır. Bilgisayar Sistemlerine yapılan saldırılar ve türleri, Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi 23, 2007.

2.3.1 Önleme

Önleme, güvenlik sistemlerinin en çok üzerinde durduğu ve çalıştığı süreçtir. Bir evin bahçesine çit çekmek, çelik kapı kullanmak gibi güncel hayatta kullanılan emniyet önlemleri gibi, bilgisayar sistemlerine yönelik tehdit ve saldırılara karşı, sistemin yalıtılmış olması için çeşitli önlemler geliştirilmektedir.

Kişisel bilgisayar güvenliği ile ilgili, virüs tarama programlarının kurulu olması, bu programların ve işletim sistemi hizmet paketlerinin ve hata düzeltme ve güncellemelerinin düzenli aralıklarla yapılması, bilgisayarda şifre korumalı ekran koruyucu kullanılması, bilgisayar başından uzun süreliğine ayrı kalındığında sistemden çıkılması, kullanılan şifrelerin tahmininin zor olacak şekilde belirlenmesi, bu şifrelerin gizli tutulması ve belirli aralıklarla değiştirilmesi, disk paylaşımlarında dikkatli olunması, İnternet üzerinden indirilen veya e-posta ile gelen dosyalara dikkat edilmesi, önemli belgelerin parola ile korunması veya şifreli olarak saklanması, gizli veya önemli bilgilerin e-posta, güvenlik sertifikasız siteler gibi güvenli olmayan yollarla gönderilmemesi, kullanılmadığı zaman İnternet erişiminin kapatılması, önemli bilgi ve belgelerin düzenli aralıklarla yedeklerinin alınması gibi önlemler, basit gibi gözükebilecek ama hayat kurtaracak önlemlerden bazılarıdır.

Kurum giriş çıkışlarının kontrol altına alınması, akıllı kart ya da manyetik kartla çalışan turnikeli elektronik geçiş kontrol sistemlerinin kullanılması, bilgisayar, cep telefonu, kamera, USB bellek, CD,DVD, vb.elektronik veri kaydedicilerin ve İnternet bağlantı cihazlarının (Kablolu/Kablosus modem, GSM modemler, uydu internet bağlantılı modemler vb.) giriş ve çıkışlarının engellenmesi veya kontrollü hale getirilmesi Önleme kapsamında alınacak en büyük tedbilerlerdendir.

Aslında önleme sürecinde belirlenen işleyiş mükemmel olabilseydi, daha sonraki süreçlere hiç ihtiyaç duyulmazdı. Yapılan bütün saldırılar en baştan önlenmiş olurdu. Fakat hiç bir güvenlik ürünü kusursuz veya eksiksiz değildir. Ayrıca, hemen hemen her gün, işletim sistemleri, İnternet servisleri, web teknolojileri ve güvenlik uygulamalarında çeşitli

açıklar tespit edilmektedir. Bu açıdan bakıldığında saptama ve karşılık verme süreçlerini kullanmak şarttır (Canbek ve Sağıroğlu,2006).

2.3.2 Saptama

Güvenlik, sadece önleme ile sağlanabilecek bir mesele değildir. Örneğin bir müzede iyi bir korunmanın sağlanmış olması, müzenin çevresinin çitlerle çevrili olması, kapıların kapalı ve kilitli olması, o müzede geceleri bekçi kullanılmamasını gerektirmez. Aynı şekilde bilgisayar sistemlerinde de saldırı girişimlerini saptayacak yöntemlerin de kullanılması şarttır. Önleme, saldırıları güçleştiren (ama imkânsız kılmayan) veya saldırganların cesaretini kıran (ama yok etmeyen) bir engel inşa etmeyi sağlar.

Saptama ve karşılık verme olmadan önlemenin ancak sınırlı bir faydası olabilir. Sadece önleme ile yetinilseydi, yapılan çoğu saldırıdan haberdar bile olunamazdı. Saptama ile daha önce bilinen veya yeni ortaya çıkmış saldırılar, rapor edilip, uygun cevaplar verebilir. Saptamada ilk ve en temel basamak, sistemin bütün durumunun ve hareketinin izlenmesi ve bu bilgilerin kayıtlarının tutulmasıdır.

Bu şekilde ayrıca, saldırı sonrası analiz için veri ve delil toplanmış olur. Güvenlik duvarları, saldırı tespit sistemleri (intrusion detection system), ağ trafiği izleyiciler, kapı (port) tarayıcılar, bal çanağı (honeypot) kullanımı, gerçek zamanlı koruma sağlayan karşı virüs ve casus yazılım araçları, dosya sağlama toplamı (checksum) kontrol programları ve ağ yoklayıcı (sniffer) algılayıcıları, saptama sürecinde kullanılan en başta gelen yöntemlerden bazılarıdır (Canbek ve Sağıroğlu, 2006).

2.3.3 Karşılık Verme

Bekçiler, köpekler, güvenlik kameraları, algılayıcılarla donatılmış bir yerin, hırsızların dikkatini çekmesi gibi, gerçek zamanlı saptama sistemlerine sahip bilgisayar sistemleri de bilişim korsanları ve saldırganlara cazip gelir. Hızlı karşılık verme, bu saldırıları püskürtmek için güvenlik sistemini tamamlayan esaslı bir öğe olarak ortaya çıkmaktadır. Karşılık verme, önleme süreci ile baş edilemeyen ve saptama süreçleri ile

belirlenmiş saldırı girişimlerini, mümkünse anında veya en kısa zamanda cevap verecek eylemlerin ifa edilmesi olarak tanımlanabilir.

Saldırı tespit sistemleri, bu tespite cevap verecek birilerinin veya bir sistemin olması ile anlam kazanabilir. Aksi takdirde bu durum, hiç kimsenin duyup da önemsemediği bir araba alarmının getireceği faydadan öteye gitmez. Bu açıdan karşılık verme güvenlik sürecini tamamlayan önemli bir halkadır. Saldırı tam olarak önlenmese bile; sistemin normal durumuna dönmesine, saldırıya sebep olan nedenlerin belirlenmesine, gerektiği durumlarda saldırganın yakalanmasına, güvenlik sistemi açıklarının belirlenmesine ve önleme, saptama ve karşılık verme süreçlerinin yeniden düzenlenmesine olanak verir. Saldırı tespit edilince yapılması gereken işlerin, daha önceden iyi bir şekilde planlanması, bu sürecin etkin bir şekilde işlemesini ve zaman ve para kaybetmemeyi sağlayacaktır. Yıkım onarımı (disaster recovery), bu aşama için gerçekleştirilen ve en kötü durumu ele alan esaslı planların başında gelir (Canbek ve Sağıroğlu, 2006).

Bilgi güvenliğini sağlayacak çözümleri sadece teknik sistem güvenliği veya bilişim teknolojileri ile ilişkilendirmemek gerekmektedir. Bilgi güvenliği, kurumlardaki iş süreçlerinde bilginin devreye girdiği her noktada ve her aşamada yer almaktadır. Bilgi güvenliği ve bilgi güvenliği yönetimi, insan, süreç ve teknoloji üçlüsünün birlikte uyumlu ve birbirini destekler biçimde hareket etmesiyle başarılmaktadır (Mitnick, 2005).

ÜÇÜNCÜ BÖLÜM

BİLGİ SIZINTISI

3.1 BİLGİ SIZINTISI KAVRAMI

Son yıllarda bilgisayar ve internet kullanımının hızla yaygınlaşarak artması sonucu, kişiler, kurumlar ve kuruluşlar işlerini artık çok büyük oranda elektronik ortamlarda gerçekleştirmektedirler. Bunun sonucu olarak e-ticaret, e-kurum, e-devlet, e-imza, e-posta gibi kavramlar hızla klasik çalışma biçimlerinin yerini almaktadır. Bu değişim, kurumların ticari faaliyetlerinde ve bireylerin günlük yaşantısında neredeyse her alanda görülebilmektedir. Ancak, günümüzde bilişimde yaşanan müthiş gelişim hızı ile beraber kişiler ve kurumlar; yazılımlar ve bilgisayarların kullanılmasıyla yapılan sahtekârlıklar, bilgi hırsızlığı, bilgisayar korsanları, elektronik saldırılar, bilgi sızdırma ve ilgili kuruluşların kendi çalışanlarınca oluşturulabilecek potansiyel iç saldırılar gibi çok çeşitli tehditlerle karşı karşıyadır (Rost ve Glass, 2011). Özellikle yazılımlardaki güvenlik açıklarından yararlanılarak yapılan saldırılar, bilgisayar virüsleri, bilgisayarları ağ üzerinden ele geçirerek bilgisayarlara zarar veren kişilerin kullandığı yöntemler, kişisel ve kurumsal bilgilerin izinsiz olarak elde edilmesi veya değiştirilmesi konusundaki tehditler artarak sürmekte olup, kişiler ve kurumlar bu tehlikeler karşısında giderek daha riskli bir duruma gelmektedir. Hizmetlerin internet ortamında sunulma eğiliminin artması, açık ve

özel ağlar arasındaki geçişler, bilgilerin halka açık sistemlerle paylaşılması gibi uygulamaların artması sonucu bilgilere erişimin yetkilendirilmesi ve denetlenmesi güçleşmektedir (Calder ve Watkins, 2008).

Bilgi Sızıntısı, özel ya da hassas nitelikteki bilgilerin yetkisiz kişi ya da kurumlara isteyerek veya kazara ulaştırılması olarak tarif edilir. Kurum ya da şirketler için hassas nitelikli bilgiler, Entelektüel sermaye, finansal bilgiler, patent bilgileri, personel kredi kartı bilgileri ya da buna benzer kurum için önemli olan bilgilerdir. Bilgi sızıntısı şirketi maddi zarara uğratabileceği gibi şirketin prestij kaybına neden olabilir (Shabtai ve diğ.2012).

Kurum için önem arz eden gizli bilgilerin yetkisiz ellere geçmesi olarak tanımlanan Bilgi Sızıntısı kurum içinden ya da kurum dışından kötü niyetle veya gayri ihtiyari olarak meydana gelebilir. Kurum için önemli bilgilerin dışa yayılması kurumu zora sokacaktır. Kurum sızan bilgiden doğrudan ve dolaylı yollarla zarar görecektir. Doğrudan zarar görme maddi olarak kuruma yansımasıyla olacaktır. Diğer taraftan dolaylı yollarla zarar görme ise prestij kaybı ve akabinde müşteri kaybı vb. olarak uzun bir zamana yayılmasıyla olacaktır. Bu kuruma daha fazla zarar verecektir (Bunker ve King, 2009).

Bilgi sızıntısı kısaca kurumdaki bilginin dışarıdaki kuruma ya da alıcıya yetkisiz bir şekilde iletimidir. Bu elektronik olarak olduğu gibi fiziksel yöntemlerle de olabilmektedir. Veri kaçağı ile Bilgi Sızıntısı eş anlamlıdır (Gordon, 2007).

Bilgi sızıntısı kasıtlı ya da kazara personel kimlik bilgilerinden, korunur entelektüel sermaye ve ticari sırlara kadar hassas bilgilerin ifşa edilmesidir (Miller, 2009).

Kurumun kendi bünyesinde kullandığı hassas bilgi ve bilgi sistemlerinin ciddi teknik bilgi gerektiren yöntemlerle ya da bilinçsiz bir şekilde çok basit hatalarla kurum dışına çıkarılarak, kurum tarafından belirlenmiş “bilgi güvenliği” politikalarının ihlalidir. Bu durum kurumda geri dönülmez hasarlara sebep olabilmektedir. Dışarıya veri akışının mümkün olduğu her ağda, veri sızıntısı riski bulunmaktadır.

Bilgi sızıntısı bireysel olarak bizlerin kişisel bilgilerimizin ve kurumsal olarak ticari bilgilerin yetkisiz ellere geçmesini sağlamaktadır. Özellikle kimlik bilgileri, sağlık bilgileri ve kredi kartı bilgileri gibi kişisel verilerin serbest piyasada işlem gören bir mal haline gelmesidir.

Datamonitor firmasının yaptığı bir araştırmaya göre, büyük şirketlerde yaşanan her bilgi sızıntısı olayı ortalama 1,8 milyon dolar maliyet oluşturuyor. Üstelik aynı araştırma bu şirketlerin %77'sinin, bilgi sızıntısı olaylarını tespit etme yeteneğinden de yoksun olduğunu gösteriyor. Dolayısıyla bilinmeyen bu maliyet hesaplanan ortalamaya katılamamıştır. Avrupa, Ortadoğu ve Afrika bölgesinde ise 2000 adet küçük ve orta boy şirkette yapılan bir araştırma, bu şirketlerdeki bilgi sızıntısı maliyetinin olay başına ortalama 200.000 pound olduğunu gösteriyor (Oğuz, 2010).

Başka bir önemli nokta ise, bilgi sızıntısı olaylarında müşterilerin özel bilgilerinin de sızıyor olmasıdır. Müşteriler şahsi olarak zarar gördüğü için bu durum,"hacker" saldırılarından çok daha büyük prestij kaybına yol açıyor. Firmalar doğrudan maliyetlerin ve itibar kaybının yanında, iş ortakları ve müşterileri tarafından açılan davalar sonucunda da yüklü cezalar ödemek zorunda kalıyorlar. Gün geçtikçe çalışanlar arasında kullanımı yaygınlaşan Facebook gibi sosyal ağ servisleri ve bilgi paylaşımını kolaylaştıran her türlü platform şirketler için riskleri arttırıyor. Yakın bir zamana kadar bir çalışan stratejik bir bilgiyi sızdırdığında yapabileceği en kötü şey bu bilgiyi rakip şirketlere ulaştırmasıydı. Ancak bugün bir çalışan şirketinizin her türlü bilgisini kazara veya kötü niyetle sosyal ağ ortamlarında ve diğer internet ortamlarında binlerce hatta milyonlarca kişi ile paylaşabilir (Oğuz, 2010).

Bilgi sızıntısı olaylarını diğer bilgi güvenliği olaylarından ayıran başka bir nokta ise, kötü niyetli kişilerin yanı sıra personelin yaptığı kazara aktiviteler de bu tip olaylara sebep olabiliyor. Proofpoint firmasının yayınladığı bir araştırmaya göre bilgi sızıntısı olaylarının %80' i çalışanların kurumun bilgi güvenliği politikasını bilmemesinden kaynaklanmaktadır. Aynı araştırmaya göre İngiltere'de bulunan kuruluşların %66'sında

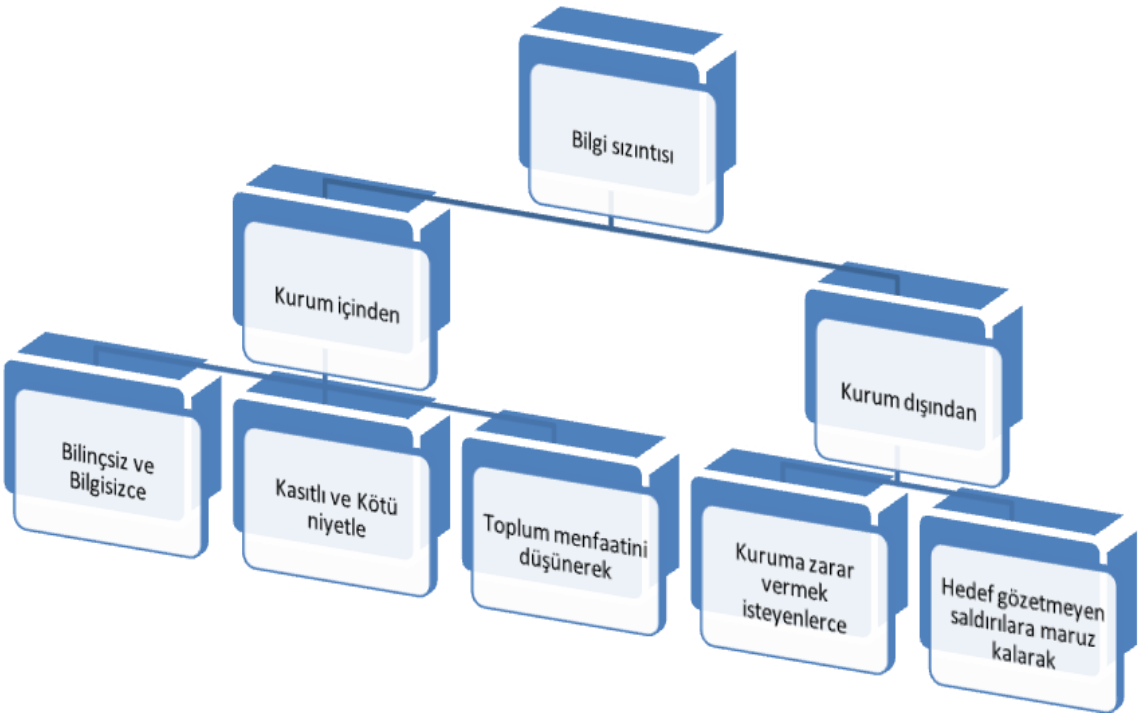
çalışanlar bilinçli veya bilinçsiz e-posta yoluyla bilgi sızdırmıştır. Ayrıca bu kurumlardaki tüm e-postaların %12'lik kısmının yasal sorunlara yol açabileceği saptanmıştır (Oğuz, 2010).

Bilgi çağında en önemli gücün bilginin kendisi olduğunu düşününce kurumların ellerinde bulundurdukları bilgileri korumak istemesi son derece doğaldır. Burada en büyük sorun ise bunu sağlamanın kolay olmamasıdır. İşlerin yürümesi için kurum bünyesinde çalışanların kuruma ait bilgilere erişim imkânına sahip olması gerekiyor ama diğer yandan bu bilgilerin dışarı sızmasını engellemek gerekiyor. Kazara kurum dışına sızdırılan bilgi müşteriye ait kimlik bilgileri, sağlık bilgileri, banka hesap bilgileri olabileceği gibi, ülkenin güvenliğini tehlikeye düşürecek gizli bir bilgi ya da kurumun itibarına zarar verecek bir bilgi de olabilir.

Bazen kurumdan sızan bilgi, sonuç kurum için felaket olsada bilgiyi sızdıran kişi tarafından iyi niyetle yapılmaktadır. Bu şekilde sızan bilgi kurum menafaatinin yerine toplum menfaatinin tercihidir. Bunun ne kadar etik ne kadar etik olmadığı yıllardır tartışılmaktadır. Susmak yerine karşılaştıkları yasa veya etik dışı davranış ve durumları ilgili mercilere bildiren kişiler 'ifşa eden (açığa çıkaran)' olarak adlandırılırken; gerçekleştirilen bu ifşa eylemi, ahlaki olmayan davranışların duyurulması (whistleblowing) olarak isimlendirilmektedir. Kısaca ahlaki olmayan davranışların duyurulması, göz göre göre susmak yerine, ıslık çalarak işletmedeki etik/yasa dışı bir olaya katılmayı reddetmek ve bu kötü olayı durdurmaya çalışmak anlamına gelmektedir. Bu nedenle, vicdani, insani ve yapılması gereken bir davranıştır. Tamamen iyi niyetle yapılan bir açığa çıkarma eylemi olmasından dolayı, bu eylemi gerçekleştiren kişileri, kötü olarak nitelendirmek son derece yanlıştır (Bouville, 2008:579-584).

Alınan tüm önlem ve tedbirelere rağmen bilginin yeterince korunmadığının ortaya çıkması, bir yandan Kurum ve İşletmelerin güvenilirliğini, itibarını ve inanırlığını aşındırmakta, diğer yandan alınan ilave tedbirler nedeniyle iş süreçlerini olumsuz etkileyerek yavaşlatmakta ve gayret israfına sebep olabilmektedir.

3.2 BİLGİ SIZINTISI ÇEŞİTLERİ



Şekil 5: Bilgi Sızıntı Çeşitleri (Sızıntıya Sebep Olana Göre)

Bilgi kurumdan 2 şekilde sızar.

a. Kurum içinden – Bilgi Sızıntılarının tahmini olarak %80'i kurum içinden sızar.

1. Bilgisiz ve Bilinçsiz kullanımla: Kullanıcılardaki bilgi güvenliği bilinci eksikliği tüm sistemi zafiyetli hale getirebilmektedir.

2. Kasıtlı ve kötü niyetli olarak: İşten çıkarılan bir çalışanın intikam alma arzusundan, maddi/manevi kazanç sağlamak isteyen profesyonel çalışanına ve hatta rakip firma personelinin kurum içinde kiraladığı personel vasıtasıyla bilişim sistemlerini kullanarak kurum için önem arz eden bilgileri sızdırmak olarak tanımlanabilir.

3. Toplum menfaatini düşünerek: Kurumdaki ahlaki olmayan davranışların duyurulması olarak nitelenen Whistleblowing, etik-dışı olay, davranış ve faaliyetlerin, gerekli önlemlerin alınması amacıyla gerek işletme içi, yeterli gelmediği takdirde de işletme dışına bildirilmesidir. Uygunsuzluğun ortadan kaldırılması ya da mimize edilmesi için yapılan bu açığa çıkarma eylemi, vicdani bir faaliyet olarak nitelendirilebilir.

b. Kurum dışından - Bilgi Sızıntılarının tahmini olarak %20'si kurum içinden sızar

1. Kuruma zarar vermek isteyenlerce: Endüstri ve Teknoloji casusları, rakip firmalar ya da yabancı istihbarat teşkilatları tarafından kurumun sahip olduğu değer ve bilgilere izinsiz erişmek, zarar vermek, maddi/manevi kazanç sağlamak için bilişim sistemleri kullanarak yapılan her türlü saldırı olarak tanımlanabilir.

2. Hedef gözetmeyen saldırılara maruz kalarak – Hacker lar tarafından hedef gözetmeden kurumlara virus, solucan ve Truva atı arka kapıları ile yapılan saldırılardır.

Bilgi güvenliği tehditleri arasında, organizasyon bünyesinde çalışan kişilerin oluşturabileceği bilinçli veya bilinçsiz tehditler olarak tanımlayabileceğimiz iç tehditler çok önemli bir yer tutmaktadır. Bilinçli tehditler iki kategoride ele alınabilir. Birinci kategori, organizasyonda çalışan kötü niyetli bir kişinin kendisine verilen erişim haklarını kötüye kullanmasını içerir. İkinci kategori ise bir kişinin başka birine ait erişim bilgilerini elde ederek normalde erişmemesi gereken bilgilere erişerek kötü niyetli bir aktivite gerçekleştirmesini kapsar. Veri tabanı yöneticisinin, eriştiği verileri çıkar amacıyla başka bir firmaya satması ilk kategoriye verilecek örnektir. Veri tabanı yöneticisi olmayan ve normalde veri tabanına erişim hakkı bulunmayan birisinin erişim bilgilerini bir şekilde elde ederek verileri elde etmesi ve bunu çıkarı için kullanması ikinci kategoriye örnektir. CSI (Computer Security Institute) tarafından yapılan ankete göre katılımcıların %44'ü 2008 yılı içerisinde iç tehditlere maruz kalmışlardır. .
https://www.hlncc.com/docs/CSIsurvey2008.pdf, Erişim Tarihi:25.04.2013)

3.3 INFOWATCH TARAFINDAN YAYINLANAN 2013 DÜNYA SIZINTI RAPORUNUN İNCELENMESİ

Kurum ve şirketlerde veri kaybı önleme/koruma, Entelektüel Sermayenin korunması ve Risk yönetimi gibi konularda öncü ve yenilikçi bir teknoloji şirket grubu olan InfoWatch tarafından 2014 yılının başında, 2013 Dünya Bilgi Sızıntı Raporu yayınlanmıştır. (Yayınlanma tarihi: 27 Mart 2014, The Global Data Leakage Report for the 2013 by InfoWatch Analytical Labs.)

2013 yılında, InfoWatch Analytical Center 1143 gizli belge ve bilginin kurum dışına sızma vakasını tespit etmiştir. Bu sayının 2012 yılındaki rakamlarla kıyaslandığında %22 oranında bir yükselme gösterdiği görülmüştür.

2013 yılında sızan belgeler personel şahsi bilgileri ve finansal bilgileri dâhil olmak üzere toplam 561 milyon belgeden oluşmaktadır.

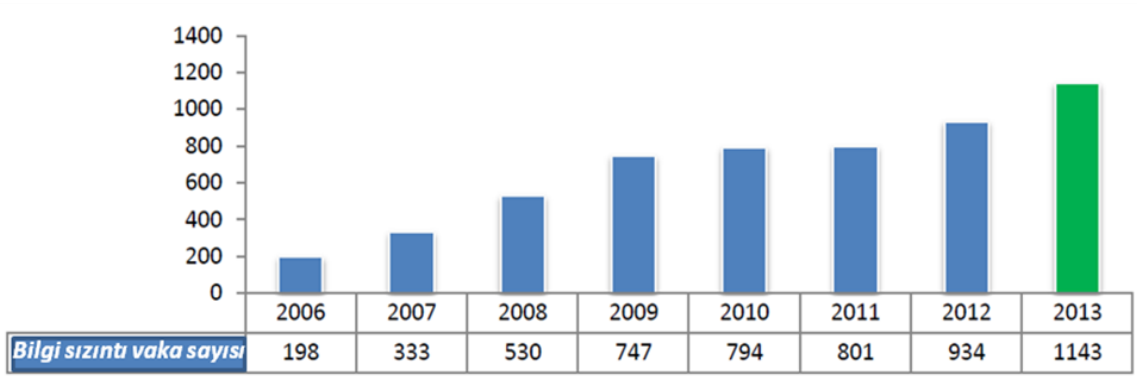
679 bilgi sızıntı vakası ile Amerika ilk sırada yer alırken (%59,41), Rusya 134 bilgi sızıntı vakası ile ikinci sırada yer almaktadır. (İngiltere-80, Almanya-48 ve Kanada-33)

Kamu kurum ve kuruluşları ile beraber kamu hastaneleri kişisel veri sızıntı vakalarının olduğu yerlerin başında gelmektedir. Bilgi sızıntılarının büyük çoğunluğunu %85 ile kişisel veriler oluşturmaktadır.

Basın ve medya raporlarına göre 2013 yılında kurum ve kuruluşların bilgi sızıntılarından dolayı hukuki sürecin işlemesi ve tazminat ödemelerinden dolayı 7.79 milyar dolar kurumlar zarara uğramışlardır.

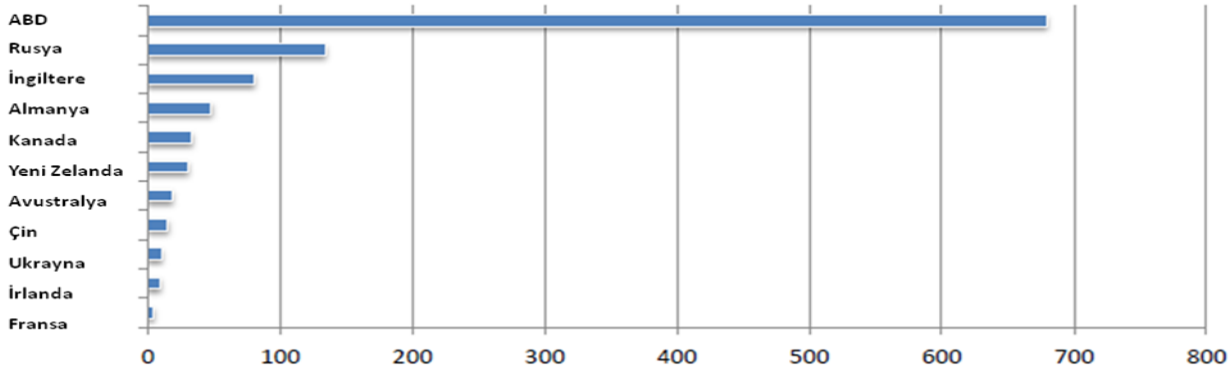
2013 yılında, InfoWatch Analytical Center tarafından 1143 Gizli Bilgi Sızıntı vakası tespit etmiştir. (Günlük 3,1 ve Aylık 95,2) Bu rakam 2012 yılından %22,3 daha fazladır (934). Artış trendinin 2012 yılına oranla %5,7. 2011 yılına oranla %16,6 olduğu gözlemlenmiştir.) 2013 yılı 1000 den fazla gizli bilgi sızıntı vakasının olduğu ilk yıldır.

2006 yılından 2013 yılına kadar olan bilgi sızıntı vaka sayılarına baktığımız zaman bu sayının her geçen gün arttığını görmekteyiz. Teknolojinin gelişmesiyle bilginin paylaşımı artmış ve sızıntıya engel olacak tedbirler alınmasına rağmen bu oranın arttığı gözlemlenmiştir. Grafik 1'de InfoWatch tarafından tespit edilen kayıtlı bilgi sızıntı sayılarını, Grafik 2'de ise Bilgi Sızıntıların hangi ülkelerde meydana geldiğini görmekteyiz.



Grafik 1. 2006-2013 Yılları Arasındaki Kayıtlı Bilgi Sızıntı Sayısı

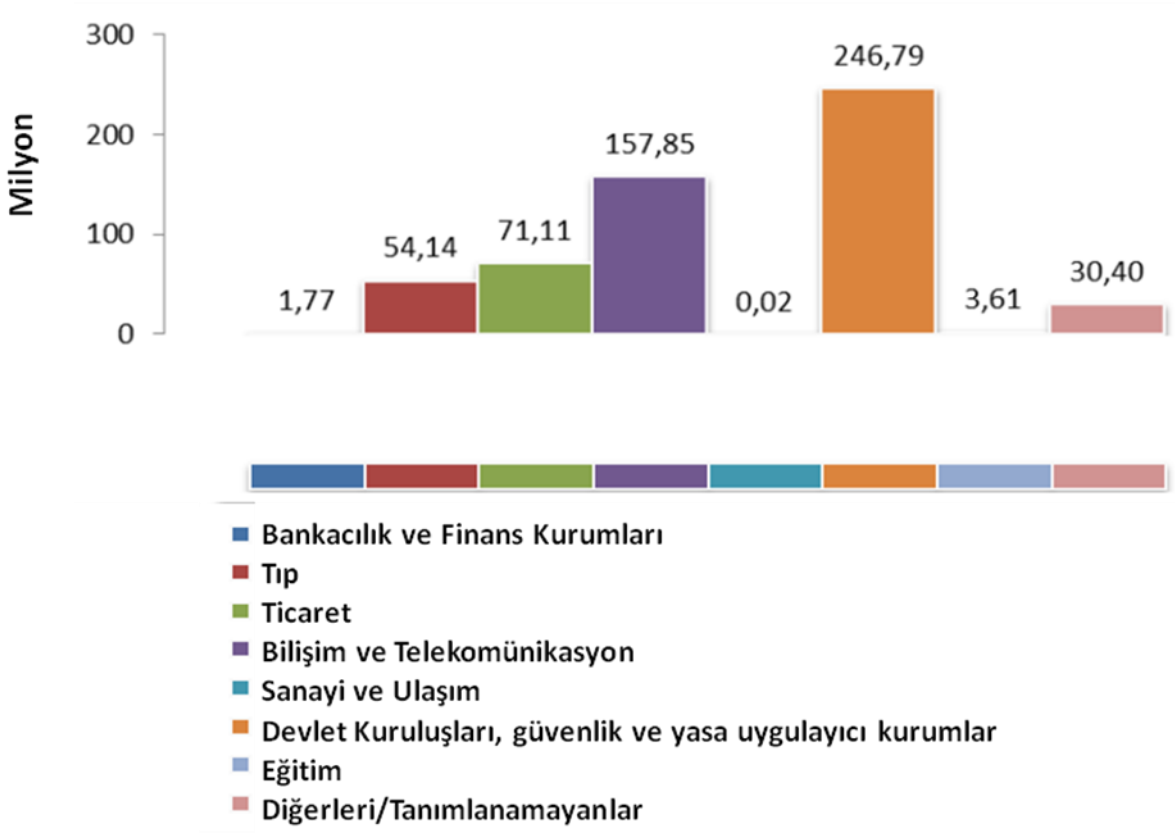
Kaynak: InfoWatch Analytical Center, Global Data Leakage Report 2013, https://infowatch.com/analytics/reports/3641



Grafik 2. Bilgi Sızıntılarının Ülkelere Göre Dağılımı:

Kaynak: InfoWatch Analytical Center, Global Data Leakage Report 2013, https://infowatch.com/analytics/reports/3641

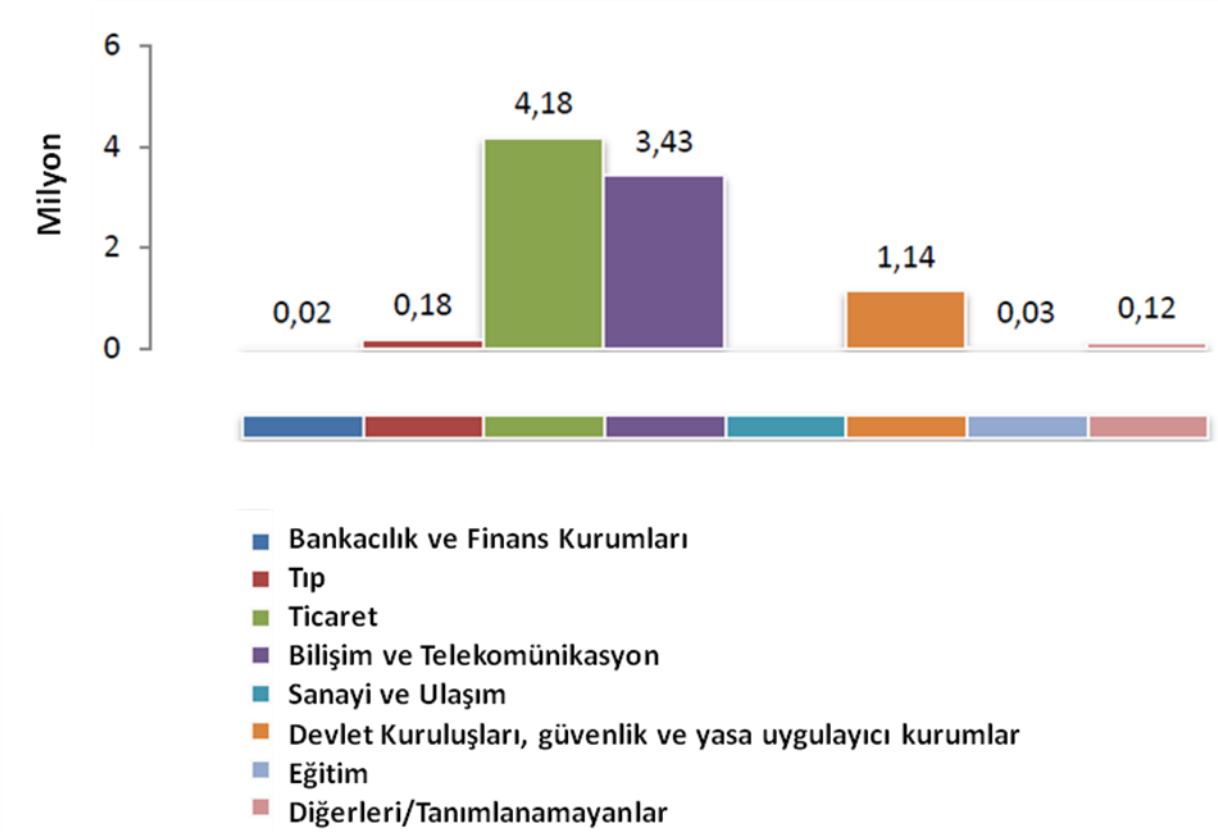
Sektör bazında kişisel verilerin sızdığı sektörler ve sızan belge miktarı Grafik 3'de tabloda gösterilmiştir. 246,79 milyon belge ile Devlet Kuruluşları, savunma ve yasa uygulayıcı Kurumların ilk sırada olduğu gözükmektedir. Bilişim ve Telekominikasyonda 2'nci sırada yer almaktadır.



Grafik 3. Sektör Bazında Kişisel Verilerin Sızdığı Sektörler ve Sızan Belge Miktarı

Kaynak: InfoWatch Analytical Center, Global Data Leakage Report 2013, https://infowatch.com/analytics/reports/3641

Sektör bazında her bir Bilgi sızıntı vakasındaki ortalama kayıp belge sayısı Grafik 4'te gösterilmiştir. İlk sırada Ticaret sektörü bulunmaktadır ve her vaka da 4,18 milyon belgenin sızdığı tespit edilmiştir.



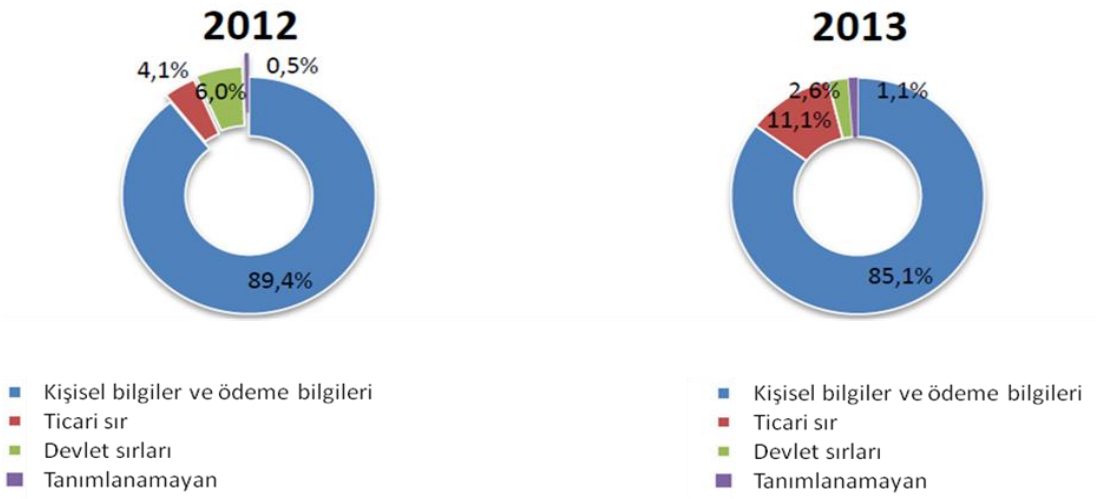
Grafik 4. Sektör Bazında Her Bir Bilgi Sızıntı Vakasındaki Ortalama Kayıp Belge Sayısı

Kaynak: InfoWatch Analytical Center, Global Data Leakage Report 2013, https://infowatch.com/analytics/reports/3641

2012 ve 2013 Yıllarına Ait Bilgi Sızıntılarının Kurumsal olarak dağılımında, 2013 yılında Ticari bilgi sızıntılarının 2012 yılına kıyasla arttığı gözlemlenmiştir. Ticari bilgi sızıntılarının muhteviyatının kişisel bilgiler ve ödeme bilgileri olduğu tespit edilmiştir.

Grafik 5. 2012 ve 2013 Yıllarına Ait Bilgi Sızıntılarının Kurumsal Olarak Dağılımı

Kaynak: InfoWatch Analytical Center, Global Data Leakage Report 2013, https://infowatch.com/analytics/reports/3641



Grafik 6. Bilgi Sızıntısında Sızan Bilginin Muhteviyatı

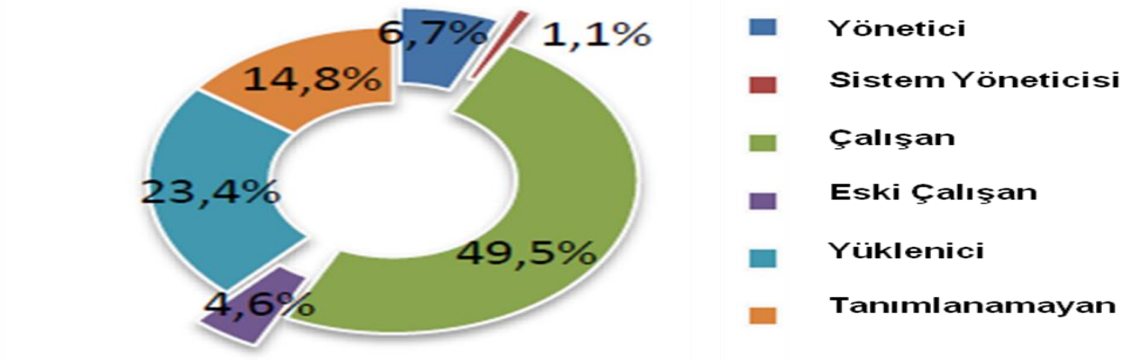
Kaynak: InfoWatch Analytical Center, Global Data Leakage Report 2013, https://infowatch.com/analytics/reports/3641

2013 yılında tespit edilen bilgi sızıntıların %45,7 si istemeyerek-kazara olurken, %44,1 i kasıtlı olarak yapılmış, %10,2 lik kısmı ise tanımlanamamıştır.

Grafik 7. Bilgi Sızıntısının Şekli (Yapan Kişi Olarak)

Kaynak: InfoWatch Analytical Center, Global Data Leakage Report 2013, https://infowatch.com/analytics/reports/3641

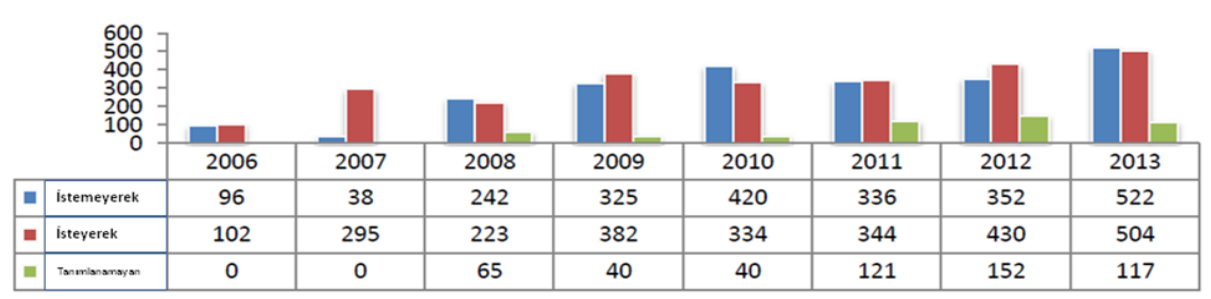
2013 yılında bilgi sızıntısını gerçekleştirenlerin oranına bakıldığında %50 den fazlasını mevcut çalışanlar (%49,5) ve kurumun eski çalışanları (%4,6) olduğu görülmektedir. Kuruma sözleşme ile belirtilen zaman aralığında hizmet sağlayan veya iş yapan firma personelinin de bu oranda büyük payı aldığı (23,4) tespit edilmiştir.



Grafik 8. 2013 yılında Bilgi Sızıntısını Gerçekleştirenlerin Profili

Kaynak: InfoWatch Analytical Center, Global Data Leakage Report 2013, https://infowatch.com/analytics/reports/3641

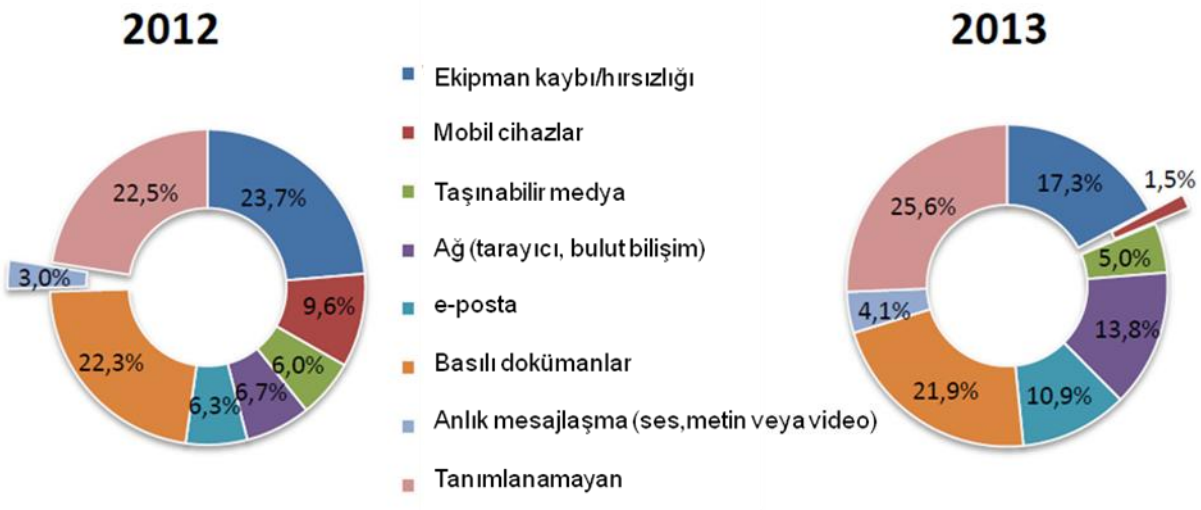
Grafik 9'da 2006 yılından 2013 yılına kadar kazara ya da kasıtlı bilgi sızıntı oranları görülmektedir.



	2006	2007	2008	2009	2010	2011	2012	2013
İstemeyerek	96	38	242	325	420	336	352	522
İsteyerek	102	295	223	382	334	344	430	504
Tanımlanamayan	0	0	65	40	40	121	152	117

Grafik 9. 2006-2013 Yılları Arasında Bilgi Sızıntısını Gerçekleştirenlerin Durumu

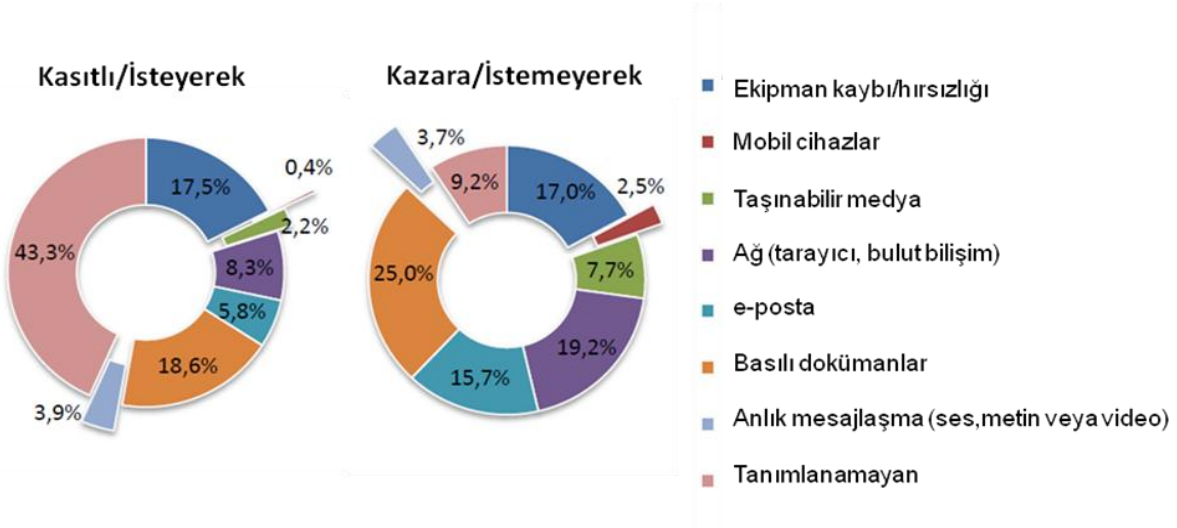
Kaynak: InfoWatch Analytical Center, Global Data Leakage Report 2013, https://infowatch.com/analytics/reports/3641



Grafik 10. Sızan Bilginin Sızıntı Kanalları

Kaynak: InfoWatch Analytical Center, Global Data Leakage Report 2013, https://infowatch.com/analytics/reports/3641

Bilgi sızıntı kanalları önceki yıl ile kıyaslandığında network 7,1 oranında, e-mail in 4,6 oranında artış gösterdiği görülmektedir.



Grafik 11. 2013 yılında gerçekleşen Bilgi Sızıntılarının yapan kişi bakımından sızıntı kanalları

Kaynak: InfoWatch Analytical Center, Global Data Leakage Report 2013, https://infowatch.com/analytics/reports/3641

Kazara bilgi sızıntısında Network (%19,2) ve e-mail (%15,7) ile göze çarpmaktadır.

3.4. TARİHTEKİ BİLGİ SIZINTI VAKALARI

3.4.1 Watergate Skandalı

Amerika Birleşik Devletleri'nin başkenti Washington'da 1972-1974 yılları arasında gelişen ve Başkan Richard Nixon'ın istifa etmesiyle sonuçlanan siyasi bir skandaldır.

17 Haziran 1972 günü ABD'nin başkenti Washington'da Demokrat Parti genel merkezinin de olduğu Watergate adlı iş hanına girmeye çalışan 5 kişinin tutuklanmasıyla başlayan süreçte, zanlıların Demokrat Parti merkezini dinlemek için dinleyici yerleştirdiği ortaya çıkmıştı. Sürdürülen soruşturma hırsızların Nixon'ın partisi olan Cumhuriyetçi Parti ile bağlantılı olduklarını ve amaçlarının Demokratik Parti'nin telefonlarını gizlice dinlemek üzere mikrofonlar yerleştirmek olduğunu ortaya koydu.

Yaklaşık 2 yıl süren araştırma ve mücadeleler sonucunda dinleme emrini dönemin ABD başkanı Cumhuriyetçi Partili Richard Nixon'ın verdiği ortaya çıkınca, Nixon 8 Ağustos 1974 tarihinde istifa ederek, Amerikan tarihinde başkanlıktan istifa eden ilk ve tek başkan olmuştur.

Washington Post gazetesi muhabirleri Woodward ve Bernstein, Watergate'in dinlendiği haberini yayınlayan ilk gazeteciler olarak tarihe geçtiler. İki muhabir sonraki 2 yıl boyunca da skandal ile ilgili çok özel bilgileri yayınlayarak, Nixon'un istifasına giden sürecin hazırlanmasının en önde gelen kahramanları oldular. İkili o dönemdeki tüm haberlerini, adını "Deep Throat (derin gırtlak)" diye yazdıkları bir kaynağa atfen yayınladılar.

FBI'da ikinci adam olarak görev yapan William Felt'in yıllar sonra FBI Başkanı olamamaktan duyduğu kırgınlık üzerine bilgileri sızdırdığı ortaya çıktı. Watergate krizinde, William Felt tarafından Washington Post'ta çalışan gazeteciler Bob Woodward ile Carl Bernstein'a sağlanan sızdırmalar yaygın bir medya ilgisine yolaçmış; Kongre oturumlarının televizyonda yayımlanarak milyonlarca izleyici tarafından izlenmesine ve aynı zamanda, önde gelen siyasi kişiliklerin başkan ve suç ortakları hakkında cezai soruşturma yapılması

çağrılarına sebep olmuştu. Bu süreç Nixon'u Ağustos 1974'te istifa etmek zorunda bırakmıştır.

"Derin Gırtlak" esrarı, gazetecilik tarihinin en iyi korunan sırlarından biri olarak görülüyordu. Haber kaynağı, Woodward'a verdiği ipuçları aracılığıyla araştırmacı gazeteciyi yönlendirmiş, soruşturmanın derinleşmesini sağlamıştı. Derin Gırtlağın kimliği, yıllardır spekülasyonlara neden olmuş, çeşitli isimler ortaya atılmış, ancak son açıklamalara kadar doğrulanmamıştı. Watergate skandalı, 1972 seçimleri öncesinde, Demokrat Parti'nin Washington'daki Watergate binasında bulunan genel merkezine dinleme cihazı yerleştirmeye çalışan kişilerin cumhuriyetçi parti ve CIA'yle bağlantıları olduğu iddiasının soruşturulmaya başlamasıyla ortaya çıktı. Skandal nedeniyle istifa etmemekte direnen Başkan Richard Nixon soruşturmayı örtbas etmeye çalıştığının ortaya çıkmasının ardından görevinden ayrılmak zorunda kalmıştı. Skandal, Amerikan tarihinde ilk bir Başkan'ın görevinden istifa etmesine neden olan olay olarak da anılmaktadır.

3.4.2 Wikileaks Olayı

Julian Assange önderliğindeki WikiLeaks organizasyonu, ABD Dışişleri Bakanlığı ve dünya genelindeki ABD büyükelçilikleri arasındaki ayrıntılı yazışmalardan oluşan 251.287 gizli belgenin bir önbelleğini elde etti ve belgeleri yayınladı. Belgeleri beş büyük gazetenin (El País, Le Monde, Der Spiegel, The Guardian ile The New York Times) desteği altında dağıttı ve ilk 220 diplomatik belge 28 Kasım 2010 tarihinde yayımlandı. Belgelerin yaklaşık 100 bini "hizmete özel" (confidential), 15 bini "gizli" (secret) olarak sınıflandırılırken, "çok gizli" (top secret) sıfatını taşıyan hiçbir belge yayınlanmadı. ABD Dışişleri Bakanlığı'nın toplam 270 büyükelçilik ve konsolosluklarla günlük yazışmalarına dayanan belgeler içinde Washington'dan sonra 7918 belge ile en fazla belge ABD Ankara büyükelçiliği tarafından hazırlananlardan oluşmaktadır. Belgelerin çoğu, ABD ile Orta Doğu ülkeleri arasındaki diplomatik ilişkilere dayanmaktadır.

ABD'li diplomatların Washington'la yazışmalarını Lady Gaga CD'sine kaydederek birçok ülke ve lider hakkında çirkin ifadeleri içeren gizli belgeleri 'Wikileaks' aracılığıyla

dünyaya duyuran ABD ordusunda görev yapan sıradan bir er olan Onbaşı Manning olmuştur. Onbaşı Manning ABD'nin 250 elçilik ve konsolosluğuna ait 251 bin 287 gizli belgeyi www.wikileaks.org adlı siteye göndererek bu bilgilerin tüm dünyaya yayılmasını sağlamıştır.

ABD, 11 Eylül saldırılarının ardından kurumlar arasında bilgi akışında bir boşluk olmaması için orduya ait Secret Internet Protocol Router Network (SIPRNet) adlı internet sistemini elçiliklerin de kullanımına açtı ve tüm arşivleri birleştirdi. Irak'ta görev yapan 22 yaşındaki onbaşı Bradley Manning SIPRNet üzerinden ABD'nin gizli diplomat yazışmalarını ve belgelerini bir CD'ye kopyalayarak, Wikileaks'a ulaştırmıştır.

Manning, bilgileri nasıl ele geçirdiğini arkadaşıyla yaptığı bir internet sohbetinde "Lady Gaga CD'sine benzer bir CD ile geldim. Müziği sildim. Sonra da dosyaları sıkıştırdım. Kimse bir şeyden şüphelenmedi" diye anlatmıştır.

Wikileaks 26 Temmuz'da Amerikan ordusunun 2004-2009 yılları arasında Afganistan Savaşı'nda tutmuş olduğu 92 bin belgeyi The Guardian, The New York Times ve Der Spiegel gazeteleriyle birlikte açıkladı. Bireysel olaylar da dâhil olmak üzere dost ateşi ve sivil kayıplar hakkında ayrıntılı bilgileri içeren belgelerin dünyaya yayılmasının hemen ardından Manning, görev yaptığı Kuveyt'deki Camp Arfijan üssünde tutuklandı. Şu anda Virjinya'da hapishanede bulunan Manning, askeri sırları açıkladığı için 52 yıl hapis cezası ile yargılanmaktadır.

İlk önce Wikileaks olayı özelinde bilgi sızıntısının nasıl gerçekleştiğini incelemek gerekmekte. WikiLeaks olayında içeriden sızmalara karşı gerekli önlemler alınmadığı için sızmaların tamamı bilinemiyor. Sadece Bradley Manning adındaki ABD ordusunda görevli istihbarat uzmanı, arkadaşı olduğunu düşündüğü birinin ihbarı sonucunda yakalanmıştır.

Ancak Wikileaks ile ilgili diğer sızmaların da içeriden yapıldığına kesin gözüyle bakılıyor. Zira sızan bilgiler, SIPRNet adındaki internetten bağımsız ve dışarıdan saldırılara karşı en üst düzeyde güvenli olan ABD devletine ait bir ağdan çalındı. Bu da gösteriyor ki

dışarıdan gelen tehditlere yönelik mevcut güvenlik çözümleri ne kadar sofistike olursa olsun bilgi sızıntısı söz konusu olduğunda bu önlemler tamamen yetersiz kalıyor. Bilgileri sızdıran istihbarat görevlisi Bradley Manning ise şu şekilde bir açıklama yapıyor. ”Üzerinde 'Lady Gaga' gibi bişey yazan bir yeniden yazılabilir CD ile geleceğim... müziği sil... sonra ayrı bir sıkıştırılmış dosya yap. Kimse hiçbir şeyden şüphelenmedi... Muhtemelen ABD tarihinin en geniş bilgi döküntüsünü sızdırırken Lady Gaga'nın “Telephone” şarkısını dinleyip dudaklarımı oynatıyordum.” (Oğuz, 2012).

3.4.3.Edward Snowden’in Sızıntıları

Amerikalı bilgisayar uzmanı, eski Merkezi İstihbarat Teşkilatı (CIA) ve eski Ulusal Güvenlik Dairesi (NSA) çalışanı olan Edward Joseph Snowden Haziran 2013 te NSA’ye ait gizli belgeleri ifşa ederek ABD tarihindeki en önemli sızıntıya imzasını atmıştır.

Tam adı Edward Joseph Snowden olan 1983 doğumlu ve Amerikan Ulusal Güvenlik Dairesi (NSA) ve Merkezi Haberalma Teşkilatı (CIA) görevlisi olan Edward Snowden’ın dünya siyasetinin gündemine oturmasının temel sebebi; Amerikan devletinin bu iki güvenlik kurumunda teknik eleman (sistem mühendisi ve benzeri görevler) olarak görev yapan Snowden’ın Amerikan ve İngiliz istihbarat servislerinin kullandığı kitle takip programlarını kamuoyuna açıklamasıdır.

2013 Yılının Haziran ayında The Guardian Gazetesi ile başlayıp toplamda binlerce gizli dokümanları basına sızdıran Amerikan Bilgisayar Uzmanı, eski Merkezi İstihbarat Teşkilatı (CIA) ve eski Ulusal Güvenlik Dairesi (NSA) çalışanı olan Edward Joseph Snowden vasıtasıyla daha önce CIA, FBI gibi sık duymadığımız bir İstihbarat kuruluşunu tanımış olduk.

Ortaya saçılan bilgilerle NSA’nın Amerikan filmlerinden çok da aşina olduğumuz CIA ve FBI gibi İstihbarat kuruluşlarından üstün, Gölge bir Örgüt ve bünyesinde 50.000 personeli çalıştıran, kimsenin bilmediği, hâkim olmadığı bir güce sahip olduğunu ve

Amerika’nın içinde ve dışında operasyon yapabilen, yasalar karşısında korunan ve demokrasinin ulaşamadığı bir güce sahip bir örgüt olduğunu öğrendik.

2013 yılından itibaren, Snowden vasıtasıyla yıllardır sır olarak kalan bu kurumun organize yapısı ve işlevleri su yüzüne çıkmaya başlamıştır. Bu kurumun; 35 devlet başkanı, IMF Başkanı ve Papa dâhil 66 dil ve lehçeleriyle milyonlarca insanı öylesine ileri bir teknoloji ve öylesine küresel bir güçle kimseye fark ettirmeden dinlediği ortaya çıkınca bu kurum herkesin dikkatini çekmeye başlamıştır.

ABD'nin en çok istihbarat toplayan teşkilatı olduğu tahmin edilen bu teşkilatın bünyesinde çalıştırdığı entelektüel sermaye olan insanın, Bilgi Güvenliğine bu denli önem verip 60 yıldan fazla bir zamanda kurumun yapısını ve işlevlerini dışarı ifşa etmeme konusundaki başarısındaki etkenler gözlerden kaçmamıştır.

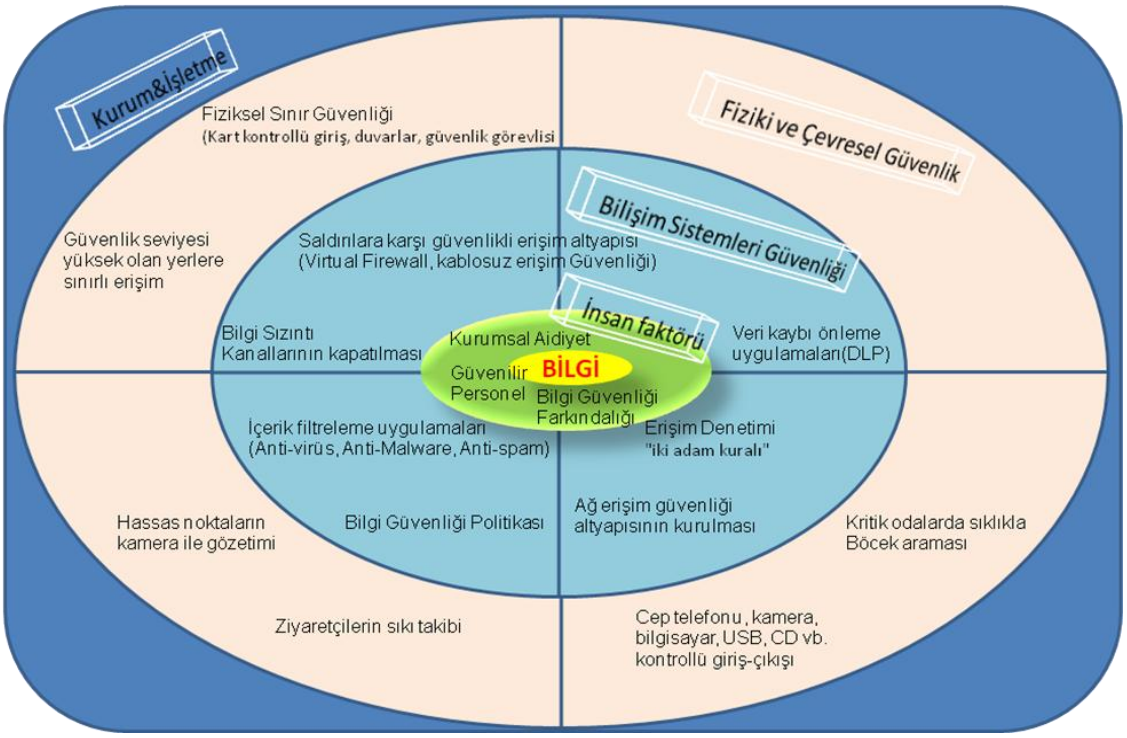
Bunun yanı sıra böylesine ileri teknoloji ve küresel güce sahip olan bu kurumun Bilgi Güvenliğindeki hassasiyetine rağmen Entelektüel bir Sermaye olan insan, Snowden örneğinde olduğu gibi Kurumdaki en gizli bilgileri ifşa edebilecek yeteneğe sahip olduğu görülmüştür.

DÖRDÜNCÜ BÖLÜM

BİLGİ GÜVENLİĞİNDEKİ VERİ SIZINTILARININ ÖNLENMESİNE YÖNELİK BİR MODEL ÖNERİSİ

4.1 MODELİN ÖNEMİ VE AMACI

Kurumlar için prestij ve maddi kazanç anlamına gelen bilginin yetkisiz kişiler tarafından erişimine engel olmak için alınması gereken birtakım önlemler vardır. Bugüne kadar tespit edilen kurumlardaki bilgi sızıntılarının sebepleri incelendiğinde İnsan güvenliği, fiziki ve çevresel güvenlik ve bilişim sistemlerinin güvenliği olmak üzere 3 temel faktörün göze çarptığı görülmektedir. Aşağıdaki şekilde bir kurumun içerisindeki bilginin muhafaza edildiği katmanlar ve bu katmanlardan sızmaması için alınması gereken ana tedbirler gösterilmiştir.



Şekil 6: Kurumdaki Bilginin Muhafaza Edildiği Katmanlar

Bilgi sızıntısı ile ilgili bugüne kadar yapılan çalışmalar incelendiğinde, her çalışmanın bir ya da birkaç konu üzerinde yoğunlaştığı görülmektedir. Bilgi sızıntısının kurumlardan uzak tutulmasına yönelik; hataların neler olduğu ve muhtemel sonuçların kuruma verdiği zararlar hakkında bir risk değerlendirme çalışmasının olmadığı görülmektedir.

Bugüne kadar sağlık, havacılık ve farklı sektörlerde kullanılan bir risk değerlendirme modülü olan Bowtie modeli ile bilgi güvenliğindeki sızıntıların neler olduğu ayrıntılı bir şekilde incelenmiş ve bu sızıntıları önlemek için ne gibi tedbirlerin alınması gerektiği görsel olarak sıralanmıştır. Elde edilen bu modülün kurumlarda veya işletmelerde uygulanması ile bilgi sızıntılarının azalacağı değerlendirilmektedir.

4.2 BOWTİE RİSK DEĞERLENDİRME METODU

Kurumlarda bilgi güvenliği yönetimi sisteminin etkin ve başarılı bir biçimde oluşturulması ve yönetilmesinde, risk yönetimi zorunlu ve hayati yapı taşlarından birisi olmaktadır. ISO 27001 başta olmak üzere, ilgili tüm bilgi güvenliği standartları ve yönetmeliklerinde, bilgi güvenliği risk analizi, ölçümü ve değerlendirmesi en öncelikli ve önemli aşamalardan birisi olarak kabul edilmektedir (Dhillon, 2007).

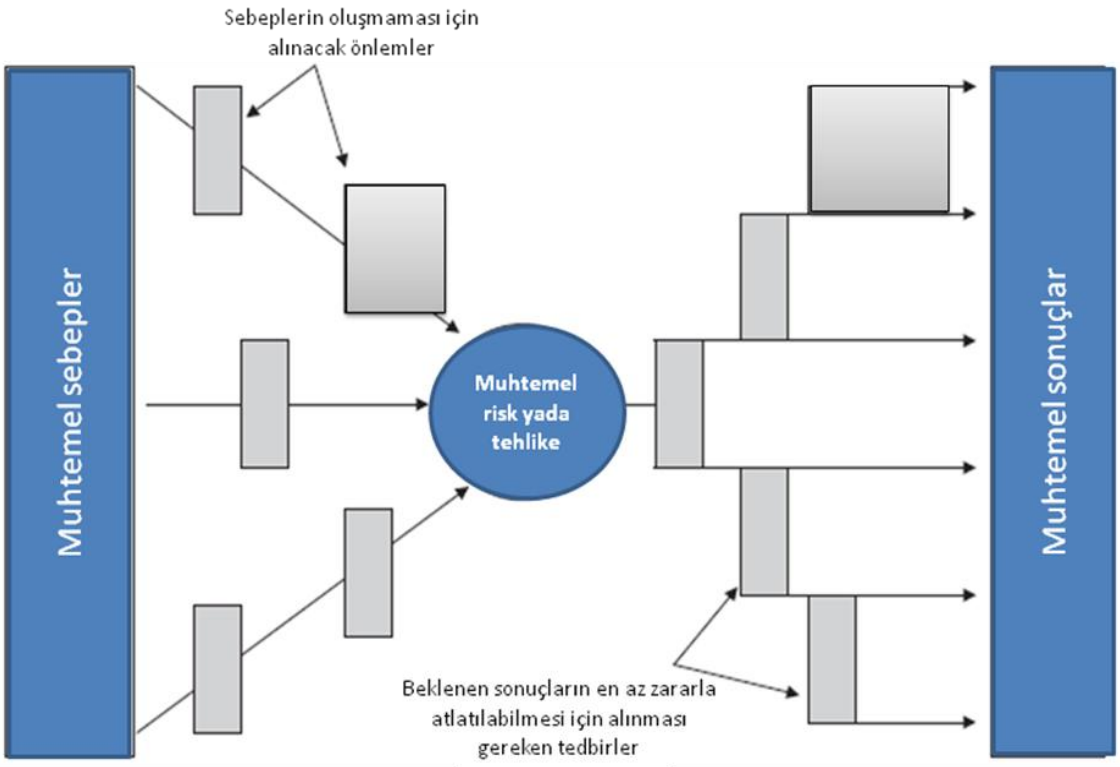
Risk yönetimi, risklerin oluşma olasılıklarını veya oluşan risklerin etkilerini azaltacak ya da riskleri tamamen ortadan kaldıracak her türlü eylem olarak tanımlanabilir. Bir başka deyişle, risk yönetimi karar vericilerin riski azaltmak veya ortadan kaldırmak üzere yararlandıkları yol veya yöntemlerdir (Cadoğlu, 2000). Bu tanım, risk yönetiminin hedeflerini de ortaya koymaktadır. Risk yönetimi iki önemli aşamadan oluşur. Mevcut durumun incelenmesi, bilgi varlıklarının gizlilik, bütünlük ve kullanılabilirlik bileşenlerine karşı zarar verebilecek tehditlerin belirlenmesi ve bu tehditlerin kullanabilecekleri zayıf noktaların ortaya listelenmesinden oluşan risk analizi birinci aşamadır. İkinci aşamada risk alma isteğine bağlı olarak risk işlemesi süreci yer alır. Risk işlemesi içinde dört farklı seçenek yer almaktadır. Riskten kaçınma, riske neden olan tehdidin ortadan kaldırılarak riskin tümüyle yok edilmesidir. Riski azaltma, ilgili tehdidin ortaya çıkma olasılığını ve/veya ortaya çıkması durumunda kuruma olan olumsuz etkisinin azaltılmasıdır (ISO / IEC, 2005).

Papyon Şeması olarak Türkçeye çevirebileceğimiz Bowtie risk analiz şeması, bir tehlike ya da risk oluşmadan önce risklerin tanımlanarak bunlar için alınması gereken tedbirlerin bir şemada gösterilmesidir.

Papyon diyagramı işletmelerde balık kılçığı, hata ağacı metodolojisi ve olay ağaç analizi gibi risk analiz yöntemlerinden birisidir. Dünyada Shell gibi birçok büyük işletmelerde kullanılan ve olumlu sonuçların alındığı görsel ve anlaşılır bir diyagramdır. Diyagramın merkezinde muhtemel tehlike veya risk vardır. Papyonun sol tarafı, bahsi geçen tehlike ve riske neden olabilecek muhtemel sebeplerin toplamını gösterir.

Diyagramin sol tarafına eklenen dikey bariyerler, tehlike veya risk oluşumunu engelleyen ya da kontrol altına alan faktörleri içerir. Papyonun sağ tarafı ise, muhtemel tehlike ve riskin sonuçlarından doğabilecek istenmeyen sonuçların grafiksel görüntüsü bulunmaktadır. Diyagramin sağ tarafına eklenen dikey bariyerler, istenmeyen sonuçları engelleyen, sınırlayabilen ya da kontrol altına alan faktörleri içerir. Kısaca, meydana gelmesini arzu etmediğimiz olası olayın sebep ve sonuçlarının analiz edilerek gerekli tedbirlerin alınmasından ibaret olan bowtie modeli merkezinde kritik olay, solunda hata ağacı ve sağında olay ağacının bulunduğu yöntem olarak ifade edilir.

Burada merkezde gösterilen bir tehlike veya bir risk olabilir. Risk analizinin en önemli görevi bu başlangıç olayını iyi bir şekilde tanımlamaktır. Şekil 7'nin sol tarafında olayının olmasına sebep olabilecek unsurlar yer alırken, sağ tarafında ise olayının olası sonuçları yer almaktadır. Sol tarafta dikey olarak yazılı olanlar sebeplerin oluşmasına engel olabilecek ya da olma olasılığını azaltabilecek tedbirlerdir. Sağ tarafta dikey olarak yazılı olan bariyerler ise olayın olası ciddi sonuçlarından kaçınabilmek için alınabilecek tedbirleri belirtmektedir.



Şekil 7: Örnek Bowtie (Papyon) Diyagramı

Kaynak: The Bowtie Model in Medication Safety Risk Analysis den uyarlanmıştır. Application of the Bowtie Model in Medication Safety Risk Analysis Consecutive Experience in Two Hospitals in the Netherlands, Peter C. Wierenga,1 Loraine Lie-A-Huen, Sophia E. de Rooij, Niek S. Klazinga, Henk-Jan Guchelaar and Susanne M. Smorenburg.

Bugüne kadar kurumlarda ve işletmelerde gerçekleşen bilgi sızıntı vakaları ve istatislikler incelendiğinde ve bilgi sızıntı nedenlerinin ayrıntılarına inildiği zaman aşağıdaki 10 etkenin sızıntıya neden olan temel faktörler olduğu gözlemlenmiştir. Bunlar;

1. İşe alırken doğru ve güvenilir personelin alınmaması

2. Fiziki ve Çevresel Güvenlik Zaafiyeti

3. Kurumda Bilgi Güvenliği Farkındalığının Oluşmaması

4. Örgütsel Sinizmin Kurumda Hâkim Olması

5. Kurumsal Aidiyetin Oluşmaması

6. Cezai Müeyyidelerin Bilinmemesi veya Önemsenmemesi

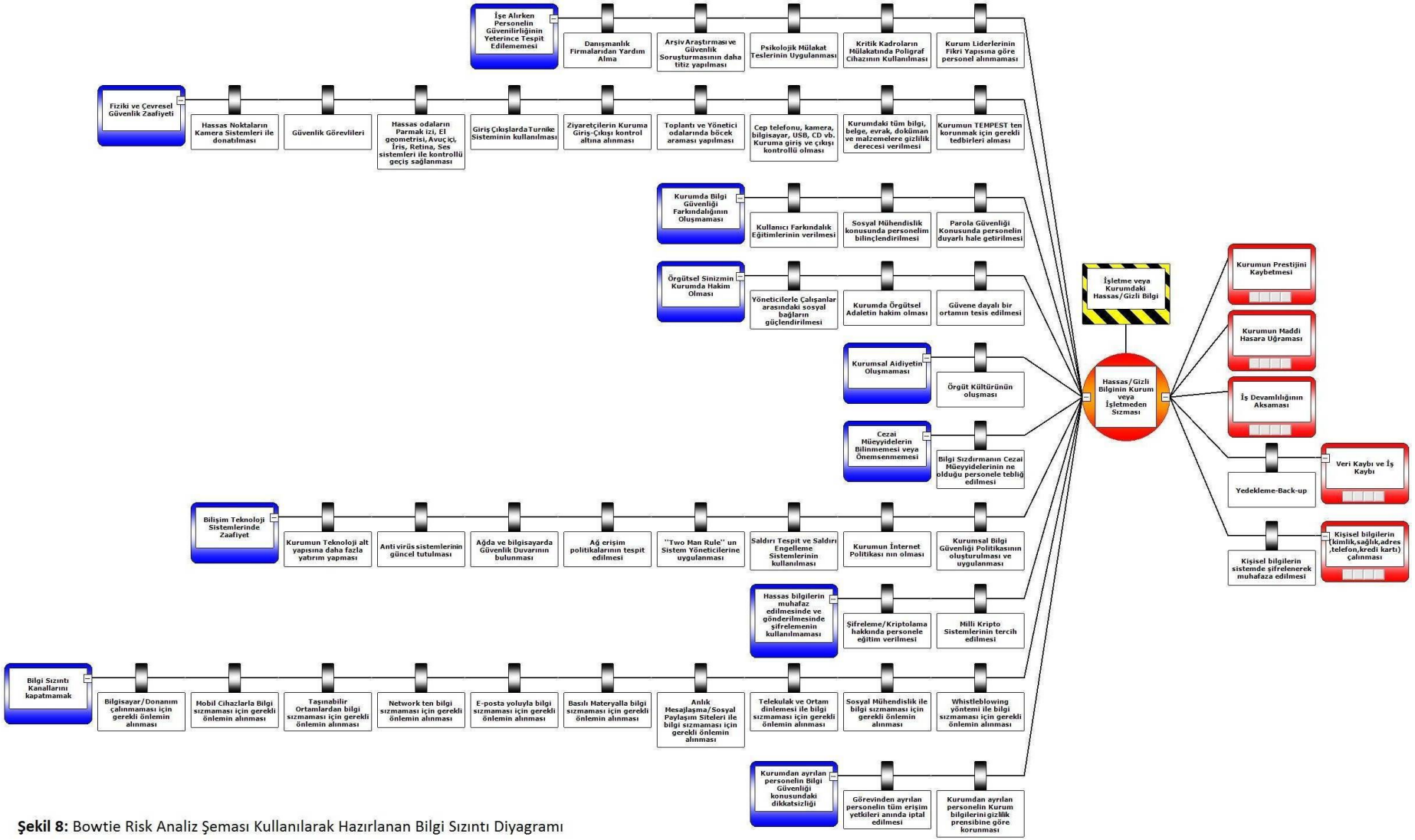
7. Bilişim Sistemlerindeki Zaafiyet

8. Bilgi Sızıntı Kanallarını Kapatmamak

9. Hassas Bilgilerin Sistemde Kriptolu/Şifreli Olarak Bulunmaması

10. Kurumdan Ayrılan Personelin Bilgi Güvenliği Konusunda Dikkatsizliği

Kurumlardaki bilgi sızıntısına sebep olan bu 10 faktör Bowtie risk analiz şeması ile risk analizi yapılmış ve alınması gereken tedbirler aşağıdaki şemada gösterilmiştir.



Şekil 8: Bowtie Risk Analiz Şeması Kullanılarak Hazırlanan Bilgi Sızıntı Diyagramı

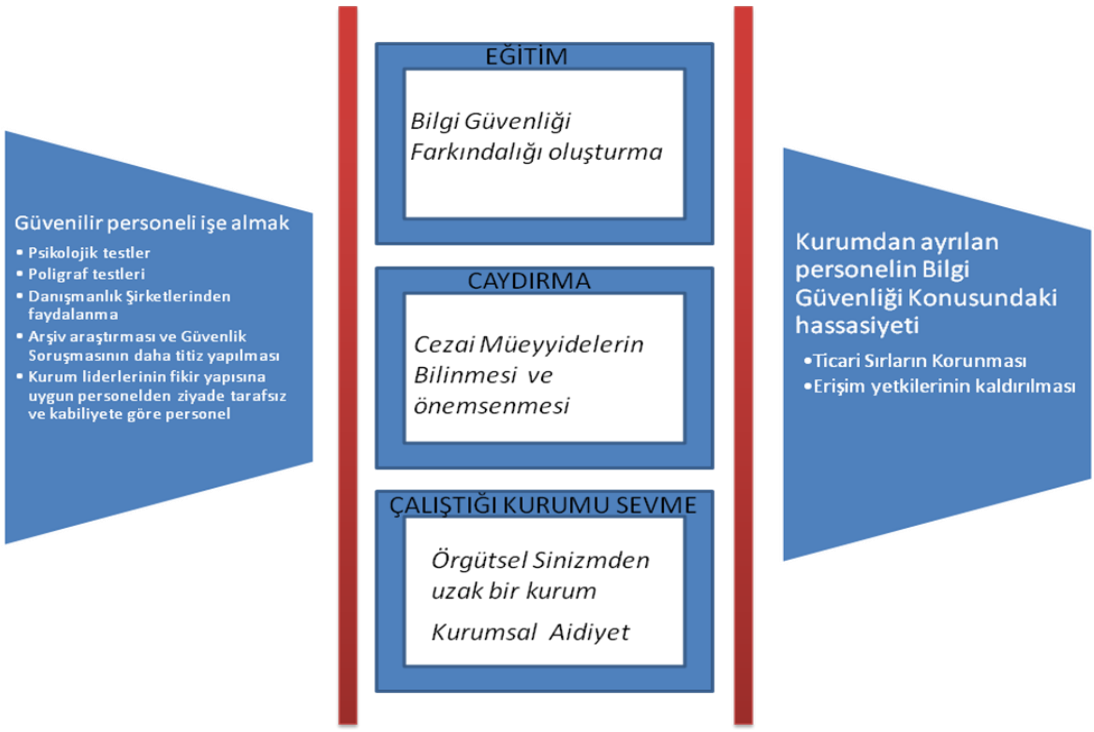
4.2.1 İşe Alırken Personelin Güvenilirliğinin Yeterince Tespit Edilememesi

Bilgi güvenliği ile ilgili olarak yazılım, donanım ve fiziki teknik önlemlerin alınmasının yanında, güvenlikte en önemli faktör olan insan faktörü de göz önüne alınmalıdır. Güvenlik sistemlerinin en zayıf noktasını oluşturan insan faktörü, bilgi güvenliğinde güvenlik zincirinin en zayıf halkasını oluşturmaktadır.

Kurum tarafından, personelin istihdam öncesi, çalışma esnasında ve istihdamın sonlandırılması veya değiştirilmesi aşamalarında alması gereken tedbirlerin neler olduğu belirlenmelidir.

Doğru ve güvenilir personelin kuruma alınması, personelin bilgi güvenliği ve farkındalık ile ilgili kurumda gerekli eğitimleri alıp uygulaması, bilgi güvenliği ihlallerinde maruz kalacağı cezai müeyyideleri bilmesi, örgütsel sinizmden uzak ve güvene dayalı işleyen kurumundan tatmin olması, çalıştığı kurumuna karşı aidiyetin oluşmuş olması ve en son olarak da kurumdan ayrılırken bilgi güvenliği konusunda göstermiş olduğu hassasiyetle insan faktörünün vereceği zararları asgariye indirebiliriz.

Bilgi sızıntısına engel olmak için güvenilir insan faktörünün kurumdaki yeri Şekil 9'da gösterilmiştir. Güvenilir personeli işe almakla başlayan süreç, 3 temel unsur (Eğitim, Ceza, Kurumu sevme) üzerine kurulan kurum ortamından Bilgi Güvenliğindeki hassasiyeti kurumdan ayrılırken de devam ettiren personelle neticelenmektedir.



Şekil 9: Bilgi Sızıntısına Engel Olmak İçin Güvenilir İnsan Faktörünün Kurumdaki Yeri

Teknik güvenliğin en üst seviyede tutulduğu kurumların mutlaka kaliteli, iyi yetişmiş ve seçilmiş insanlara ihtiyacı vardır. İşletmenin stratejik amaçlarına ve beklentilerine ulaşmasında büyük bir yer teşkil eden personel seçimi ve alımı işletme için çok büyük öneme haizdir. Profesyonel kişilerce yapılan doğru ve adil bir personel seçimi, doğru işler için doğru adayların tespit edilmesini ve kurumsal performansın artmasını sağlayacaktır. İşletmelerin personel seçimlerinde en sık kullandıkları yöntemlerden biri de mülakattır. Adayların belirli özelliklerinin saptanması için yapılan bu görüşmenin zekâ, bilgi, dikkat, karar verme ve sorun çözme gibi niteliklerin yanı sıra güvenilirlik, örgüte bağlılık ve duyarlılık gibi nitelikleride ortaya çıkarması işletmenin personelden en üst düzeyde yararlanmasını sağlayacaktır. Tespit edilmesi zor olan bu özelliklerin açığa çıkartılabilmesi için, insan davranışının sayısız boyutlarını ölçmek amacıyla geliştirilen psikoteknik yöntemlerden personel seçiminde faydalanmak gerekmektedir.

İnsan kaynakları yönetiminin belki de en önemli fonksiyonlarından birisi personel seçme sürecidir. İçinde yaşadığımız bilgi çağında yüksek nitelikli insan kaynağının örgütler açısından önemi son derece artmıştır. Son yıllarda özellikle bilgi işçiliğine ve entelektüel sermayeye verilen önem, insanı en önemli üretim faktörü haline getirmiştir. İnsanın en önemli rekabet dayanağı haline gelmesiyle örgütler, bu yükselen değeri elde etme ve tutma çabalarını yoğunlaştırmaktadırlar. Seçme işlemiyle verilecek olan kararın doğru ya da yanlış olması yalnızca işe alınan kişiyi değil, tüm örgütü etkileyecektir. Bu etki özellikle yönetim kademesine alınacak personel de daha da belirginleşir. İş için uygun niteliklere sahip personelin işe alınmasıyla, bu kişinin diğer personele, işine ve genelde örgüte karşı tutum ve davranışları olumlu ve yapıcı yönde olurken, uygun olmayan seçim ve atamalar, genellikle huzursuzluğa, moral bozukluğuna ve sonuç olarak işten ayrılmalar nedeniyle yüksek bir personel devir oranına yol açmaktadır (Yelboğa,2008).

Bir örgütün en önemli unsuru olan personelin, nitelik ve nicelik bakımından iş ve işyerine uygunluğu, o örgütün başarısında etkin bir rol oynar. Bu nedenle, örgütler kendilerine en uygun nitelik ve sayıdaki elemanın kazandırılması konusunda politikasını belirlemeli ve personel seçim sistemini kurmalıdırlar. Seçim sürecinin başarıyla yürütülmesi ve en uygun adayın işe alınması, kişi-iş uyumunun gerçekleştirilmesi işletmenin temel hedeflerinden birisi olmak durumundadır. Bu hedefe ulaşabilmek için batı ülkelerindeki işletmelerin birçoğu yeni yaklaşım ve teknikleri uygulamakta ve uzun yıllardan beri psikolojik testlerden faydalanmaktadırlar. Testler psikolojik ölçme araçlarıdır ve bireylerin şimdiki davranışlarını ölçerek gelecekteki davranışları ile ilgili kestirimde bulunurlar (Yelboğa,2008).

Her alanda ihtiyaç duyulan personel seçimi ve alımı, kurumun/kuruluşun amaçları ve hedefi doğrultusunda temel ve tartışmasız çok önemli bir konudur. Doğru anlaşılması, uygun metodların seçilmesi ve uygulanması durumunda kurumun/kuruluşun stratejik amaçları ve beklentilerine ulaşması için büyük bir öneme sahiptir (Altun ve Kovancı,2004).

İfşa edilmesiyle ülkenin güvenliğini tehlikeye düşürecek Savunma, Güvenlik ve İstihbarat kadrolarında görev alan veya alacak kişilerin güvenilirliklerini ve uygunluklarını belirlemek için kuruma personel alımlarında yalan makinası uygulaması dâhil değişik teknik ve yöntemler kullanılmalıdır.

NSA gibi istihbarat teşkilatları uzun süredir poligrafı (yalan makinası) kuruma başvuran tüm adayların iş görüşmelerinde kullanmaktadır.

CIA, FBI ve büyük istihbarat teşkilatlarının da poligrafı kullandıkları bilinmektedir. Hükümet yetkililileri tarafından Amerika'da yılda yaklaşık 70.000 personelin iş başvurusunda ya da mahkeme tarafından taleple yalan makinası tarafından mülakata tabi tutuldukları belirtilmektedir.

Yalan makinası ya da diğer adıyla poligraf temel olarak kan basıncı ve nabız atışındaki artış gibi adrenalin yan etkilerini ölçerek personelin yalan söyleyip söylemediğini tespit etmeye çalışan bir alet olarak tanımlanabilir. İş görüşmelerinde personele bağlanarak sorulan sorulara vermiş olduğu cevaplardaki vucudunun tepkisiyle şahsın doğruluğu sorgulanabilmektedir.

Çok yakın zamanlara kadar ve bugün yetkili bir yere gelmenin yolu, çoğunlukla bir siyasi ya da bir parti yetkilisine, çıkar birliği için kurulmuş bir derneğe ya da benzer bir kuruluşun etkisine, bazen kişisel ilişkilere, hatta rüşvet ve karşılıklı çıkar ilişkisine dayalıdır. İnsanlık tarihi, doğru bilgi ve beceriyle donatılmamış insanlara verilen yetkilerden dolayı çekilen acılarla doludur. Tarih kitaplarımız, özellikle Osmanlı döneminde, yeteneksiz ve bilgisiz yöneticilerin neden olduğu toplumsal felaketlerin öyküleriyle motiflenmiştir (Demirsoy, 1995).

Toplumlarda bireylerin iyi yetiştirilmesi tartışmasız özlenecek bir durumdur. Fakat bundan daha önemlisi, bilgili ve yaratıcı insanların seçilerek, olması gereken yerlere ulaşmaları için uygun sistemin kurulmasıdır. Çağdaş ve gelişmiş ülkelerde, toplumu yönlendirecek ve lokomotif görevi yapacak yerlere yetenek ve beceri ve keza bilgi birikimi

bakımından üstün insanlar girerken, az gelişmiş toplumlarda çok defa bilgiyle değil kurnazlığıyla ön plana çıkanlar girer. Böylece bilgi göz önüne alınmadığı için bir yandan doğru seçim yapılamaz, yetenek göz önüne alınmadığı için de diğer taraftan yaratıcı tip oluşturulamaz ve sonuçta toplum sorunlarını çözemez, hatta bilgisizliğin ve kurnazlığın doğurduğu yeni sorunlarla boğuşmaya başlar. (Demirsoy, 1995). Bu sakıncanın ortadan kaldırılması ve toplumun doğru yönlendirilmesi için bilgili ve yetenekli insanların seçimi konusunda liyakata dayalı bir sistemin kurulması gereklidir.

Kurum ve kuruluşların personel alımlarında siyasi istismarlardan kurtarılarak tamamiyle görevin gerektirdiklerini yerine getirebilecek liyakata, yetenek ve beceriye sahip personelin seçimine dayalı bir sistemin kurulması sağlanmalıdır.

Kurum liderlerinin fikri yapısına uygun personel alma gayreti güvenilir personel arayışını arka plana itmektedir. Personel seçimlerinin kurum liderlerinin fikri yapısına uygunluktan ziyade yetenek ve kadronun gerektirdiklerini yerine getirebilecek kabiliyette güvenilir personelin seçilmesi ile sağlanmalıdır. Bunun aksi gerçekleştiğinde kurum fikir yapısı aynı olan ya da aynı gibi gözüken yeteneksiz ve güvensiz personel yığınına dönerek kurum asıl işlevini yerine getirmekte zorluk çekecektir.

Adayın iş için gerekli olan niteliklere ne ölçüde sahip olduğunu tespit etmeye çalışan mülakatı yapacak kişilerin profesyonel olmaları gerekmektekdir. Üst düzey yönetici alımlarında Danışmanlık Şirketlerin uzman personelinden faydalanılmalıdır. Amerika'da bu tür mülakatlarda McKinsey&Company gibi danışmanlık şirketleri tarafından tarafsız bir şekilde doğru işlere uygun personel seçimi yapılmaktadır.

Emniyet, İstihbarat, Askeri Kurumlar ve Dışişleri gibi kritik kadrolara personel alımlarında yürütülen arşiv araştırması ve güvenlik soruşturmasının daha kapsamlı yapılması sağlanmalıdır. Her ne kadar kuruma girdiğinde tüm bu engelleri aşan personel bir süre sonra kurum içerisinde çalışıpta başka ülke, rakip kurum ve örgütlerin maşası olabilmektedir. Yabancı istihbarat örgütleri tarafından ya da rakip firma tarafından, hedef kurum içerisinde çeşitli ideolojik, para, cinsellik, makam-mevki vb. usulleri kullanılarak

zaafı olan insanlar tespit edilir ve bunlar vasıtasıyla kurumdan bilgi sızdırmaları sağlanır. Bunun için bu araştırma ve soruşturmanın kuruma girdikten sonrada devam etmesi gerekmektedir. Zaman zaman gerek duyulan personelin güvenirliği değişik tekniklerle yeniden gözden geçirilmelidir.

4.2.2 Fiziki ve Çevresel Güvenlik Sistemindeki Yetersizlikler

En hassas bilgileri içinde barındıran bir kurum/işletme için bilginin muhafazası oldukça önem arz etmektedir. Bilgi güvenliğinin başlangıç noktası sayılan fiziki ve çevresel güvenlikte almış olduğumuz sıkı tedbirler kurumdaki bilgiye ulaşmayı daha da zorlaştıracaktır.

Kurumdaki bilgi güvenliğinin ilk aşaması olan fiziki ve çevresel güvenliğin amacı kuruma yetkisiz erişimlerin engellenmesi ve bilgi varlıklarının hırsızlığa ve her türlü tehlikelere karşı korunup gerekli tedbirlerin alınmasıdır.

Bu kapsamda hassas/gizli veri ve bilgilerin muhafaza edildiği ortamların güvenlik kameraları ile 24 saat izlenerek kurum içerisinde belli yerlere sadece yetkili personelin girişine izin verecek şekilde kontrol mekanizmaları kurulmalıdır. Bilginin muhafaza edildiği yerin, bilginin içeriği ve gizlilik derecesiyle doğru orantılı bir koruma tedbirlerinin alınması gerekmektedir. Bilginin korunduğu bölgeye giriş ve çıkışta bilginin içeriği ve gizlilik derecesine uygun sınırlamaların getirilmesi gerekir. Bu bölgelere giren ve çıkarılan evrak, doküman ve elektronik kopya imkânı sağlayan malzemelerin sıkı kontrol altına alınması sağlanmalıdır. Ziyaretçilerin kuruma giriş ve çıkışları kontrol altına alınmalı ve hassas bilgilerin bulunduğu alanlar ziyaretçilerin erişimine kapatılmalıdır.

Kuruma giriş ve çıkışların kontrol altına alınması maksadıyla fiziki güvenliğin kartlı geçiş imkânı sağlayan turnike sistemleri ile desteklenmesi gerekmektedir. Güvenlik seviyesi yüksek olan yerlere sadece girmeye yetkili personele sınırlı erişim tanınmalıdır.

Cep telefonu, kamera, bilgisayar, USB, CD vb. malzemelerin kuruma giriş ve çıkışı kontrollü olmalıdır.

Toplantı ve yönetici odalarına şirket sırlarını öğrenmek isteyenler tarafından habersiz ve gizli bir şekilde yerleştirilen ve böcek diye tabir edilen casus sistemlere karşı sık sık böcek araması yapılmaldır.

Elektrikle çalışan her cihaz elektromanyetik yayılımda bulunduğundan bu yayınlanan dalgaların ele geçirilmesi prensibine dayanan araştırmaların bütününü içeren TEMPEST in çok gizli ve hassas bilgilerini korumak isteyen kurum ve işletmelerin çok dikkat etmesi gereken bir unsurdur. TEMPEST kaçaklar uzak mesafelerden elde edilip gerekli çözümlemesi yapıldığı zaman ortaya anlamlı bir bilgi çıkabilir.

TEMPEST konusu, bu kaçakların kontrol edilmesini ve bu nedenle oluşabilecek güvenlik ihlallerinin asgari seviyelere indirilmesini sağlar. Bu nedenle gizli nitelikli bilgileri işlerken TEMPEST standart ve yönergelerine azami riayet edilmelidir. Özellikle gizlilik dereceli bilgilerin yoğun olarak işlendiği kurumlarda TEMPEST farkındalığının yaratılması maksadıyla eğitimler verilmeli ve bu kurumların TEMPEST denetimleri, oluşturulacak denetleme birimleri tarafından düzenli olarak yapılmalıdır. Bina TEMPEST değerlerine uygun cihazlar seçilmeli, oluşabilecek elektromanyetik kaçaklara karşı filtreleme ve ekranlama teknolojileri ile gerekli tedbirler alınmalıdır (Sevim ve diğ,2013).

Kurumlarda ve işletmelerde kullanılan bilgi, belge, evrak, doküman ve malzemelerin, rakip firma ya da düşmanın eline geçmesine veya yetkili olmayan personel tarafından nüfuz edilmesini öğrenmek için bu belgelere gizlilik derecesi verilmeli ve buna göre işlem yapılmalıdır.

4.2.3 Kurumlarda Bilgi Güvenliği Farkındalığının Oluşmaması

Bir kurumun bilişim güvenliği açısından karşı karşıya bulunduğu riskleri azaltmada kullanılması gereken ana yöntemlerden biri eğitimdir. Bilgi sistemlerini kullanan kullanıcıların, bilgi güvenliği konusunda eğitimlerle bilinçlendirilmesi, onların bir güvenlik boşluğu olmasını ve kurum açısından risk oluşturacak bir etken olmaları olasılığını en aza indirecektir (Moffett, 1990).

Kurumlardan bilinçsiz bir şekilde sızan bilgi sızıntı oranı azımsanmayacak oranda olunca bununla ilgili tedbirlerin alınması kurumun menfaatine bir çalışmadır. Bilgi eksikliğinden kaynaklanan insan hatalarını minimize edecek, teknolojinin yanlış kullanılma riskini azaltacak, bireylerin bilgi güvenliği tehditlerinden haberdar edecek bir bilgi güvenliği farkındalığı oluşturmak kurum için kritik bir öneme sahiptir. Farkındalık ile kurumun yöneticisinden en alt kademede çalışanına kadar bilgi güvenliği bilinci oluşturularak, kurumun ticari sırların neler olduğu, hangi bilgilerin korunması gerektiği, bunların ne tür tehditlere karşı nasıl korunması gerektiği hususunda bilinçlendirme sağlanır. Bu donanıma sahip personelin bilinçsiz hata yaparak kurumdan bilgi sızdırması oldukça zorlaşacaktır.

Bunu sağlamanın yolu kurumsal bir farkındalık programı oluşturmak ve bunu belirli dönemlerde veya farklı yöntemlerle çalışan zihinlerde aktif bir şekilde tutacak şekilde bilinçlendirme çalışmalarını yapmaktan geçmektedir. Kurumlarda bilginin paylaşıldığı bireylerin yapabilecekleri çok küçük hatalar, dikkatsizlikler, bilinçli ya da bilinçsiz yapılabilecek her türlü suistimaller teknik anlamda alınan tüm güvenlik önlemlerini boşa çıkaracaktır. Bu nedenle kurumlar, günümüz şartlarına uygun bir farkındalık oluşturmak zorundadırlar (Şahinaslan ve diğ.,2009).

2007 yılındaki kurum içinde bilinçli ya da bilinçsiz bir şekilde yapılan güvenlik istismarları %59' den 2008 yılında bu durum bilgi güvenliği farkındalık çalışmaları ile %44'de kadar düşürülebildiği gözlemlenmektedir. Yine etkin bilgi güvenlik olaylarına ait yüzdelik dilimler incelendiğinde en büyük tehdit unsurunu iç tehditler olduğu görülmektedir. Bu durum insan faktörünün kurum için önemini açık bir şekilde göstermektedir (2008 CSI Computer Crime & Security Survey).

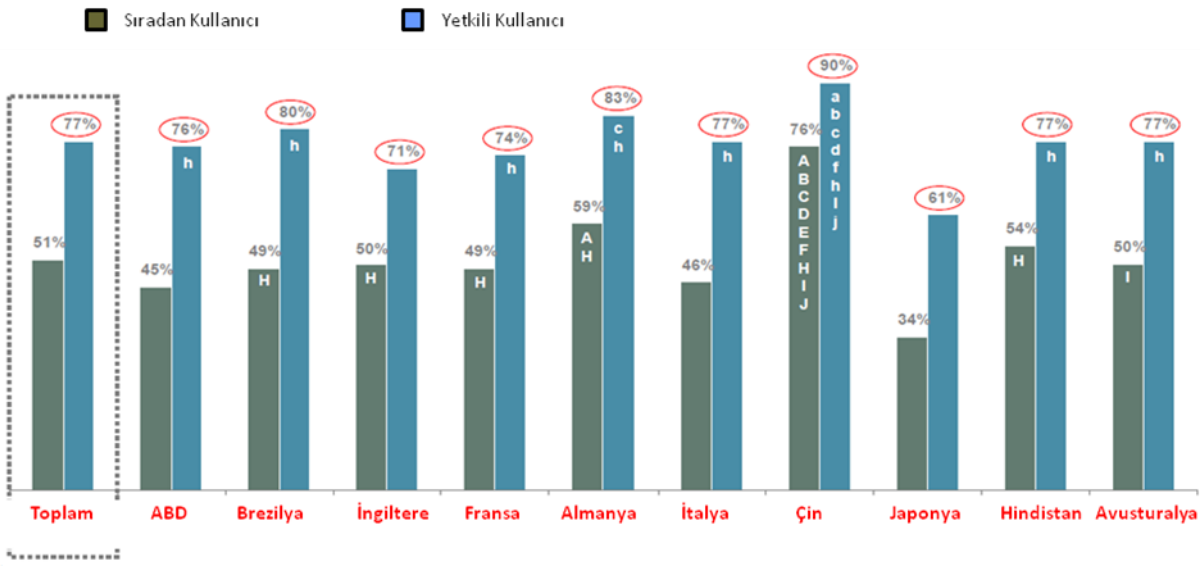
Bilgi Güvenliği farkındalığını oluşturmanın ana yolu kurumda en üst seviyedeki yönetimden en alt seviyedeki çalışana hatta tedarikçilere kadar çalışanların görev ve pozisyonları da dikkate alınarak ihtiyaç ve beklentilere göre farklı eğitim ve farkındalık programları hazırlanmalı ve eğitimler düzenlenmelidir. Bu eğitimler bir çalışan ise

başladığında verilen oryantasyon eğitimlerinin ayrılmaz bir parçası olarak düşünülmeli ve mutlaka her çalışana en az bir kez verilmelidir. Daha sonraki dönemlerde ise çalışana planlanmış alması gereken diğer eğitimler düzenli olarak verilmedir (Şahinaslan ve diğ.,2009).

Kurumlarda uygulanan bilgi güvenliği farkındalık eğitiminin kurumun bilgi güvenliği politikasının ne olduğu, ticari sırların neler olduğu, sosyal mühendislik konusunda nelere dikkat edilmesi gerektiği, virüsler vb. konularını ihtiva etmesi gerekmektedir.

Personelin parola güvenliği konusunda duyarlı olması sağlanmalıdır. Özellikle kolay tahmin edilmeyen güçlü parolaların kullanılması gerektiği, kullanılan parolaların başkaları ile paylaşılmaması gerektiği ve parolaların unutulmaması için her hangi bir yerde yazılma yanlışından uzak durulması gerektiği bu eğitimlerde vurgulanmalıdır.

10 Temmuz- 4 Ağustos 2008 tarihleri arasında kurumlarda ve işletmelerde bilgi teknolojilerini kullanan personelin bilgi güvenliğindeki farkındalığını tespit etmek maksadı ile 10 farklı ülkede 1009 sıradan kullanıcı ve 1011 yetkili kullanıcı ile bir ağ teknolojileri şirketi olan CISCO tarafından online olarak anket yapılmıştır. Yapılan bu anket neticesinde Çin'deki sıradan ve yetkili kullanıcıların bilgi güvenliği konusunda daha duyarlı oldukları tespit edilmiştir.



Grafik 12. Dünya Bilgi Güvenliği Farkındalığı Oranları

Kaynak: CISCO Systems, Data Leakage Worldwide: The Effectiveness of Corporate Security Policies, August 2008

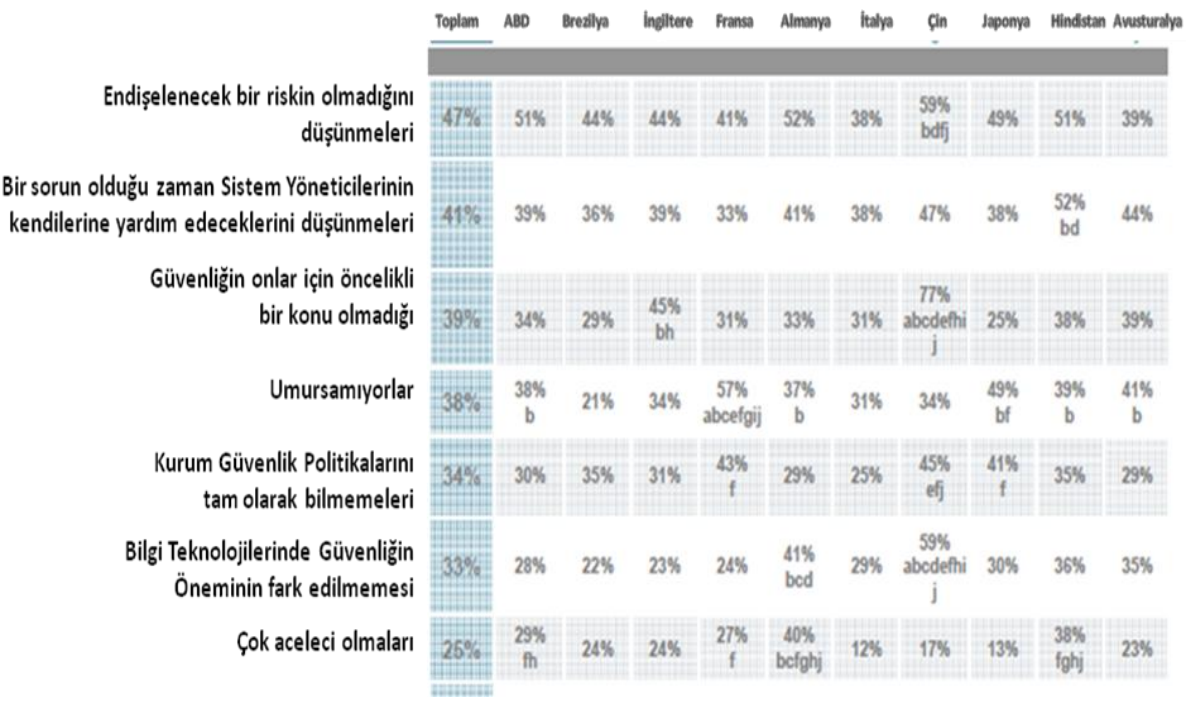
Yapılan bu ankete göre; bilgi güvenliği politikalarındaki ihlallerin en sık rastlanan neticesinin sisteme virüsün bulaşması ve bilgiye yetkisiz erişim olduğu tespit edilmiştir.

	Toplam	ABD	Brezilya	İngiltere	Fransa	Almanya	İtalya	Çin	Japonya	Hindistan	Avustralya
Sisteme virüsun bulaşması	65%	62%	74% dj	63%	57%	66% j	64%	68% j	67% j	74% dj	49%
Bilgiye Yetkisiz erişim	45%	39%	51% df	39%	35%	46% f	26%	68% abcdefij	54% df	49% f	41%
Elektronik posta ve ağın içerideki kullanıcı tarafından istismarı	39%	51% be	18%	38% be	41% be	17%	47% be	64% bcdefhij	34% be	43% be	37% be
Laptop ya da mobil sistemlerin çalınması	29%	37% bf	11%	41% bf	36% bf	28% bf	14%	46% befhij	25% b	27% bf	28% bf
Müşteri bilgilerinin kaybı ya da çalınması	20%	21% ef	13%	11%	11%	8%	8%	59% abcdefhij	21% ef	30% bcdefj	15%
Kablosuz ağın yetkisiz Kişilerce istismarı	19%	46% bcdefhij	14%	17%	13%	7%	16%	34% bcdefhj	11%	21% e	10%
Phishing Saldırısı	19%	21% eh	18%	14%	16%	8%	18%	33% bcdefhj	8%	34% bcdefhj	11%
Hizmet alamama	16%	17% e	15% e	17% e	12% e	2%	10% e	30% abcdefhj	11% e	27% defh	15% e
Bilgisayara kötü amaçlı Yazılımlar kurmak	15%	9%	16% d	10%	5%	8%	18% d	38% abcdefhij	15%	16% d	8%
Dışarıdan sisteme girilmesi	13%	9%	6%	4%	5%	13%	6%	38% abcdefhij	10%	22% abcdfj	8%
Haydut kablosuz erişim noktası	12%	7%	16% dej	7%	3%	6%	13% dj	33% abcdefhij	16% dej	8%	4%
Telekom dolandırıcılığı	11%	5%	5%	3%	11%	8%	10%	26% abcdefhj	8%	19% abcej	6%
Finansal Dolandırıcılık	10%	11% be	2%	4%	5%	2%	4%	28% abcdefhj	11% be	22% bcdefj	10% be
Website sinin zarar görmesi	9%	5% d	8% df	6% d	0%	6% d	1%	29% abcdefhij	10% df	16% adfj	4%
Diğerleri	3%	4%	1%	7% gi	1%	7% gi	1%	0%	3%	0%	8% bgi

Grafik 13. Bilgi Güvenliği Politikalarındaki İhlallerin Neticeleri

Kaynak: CISCO Systems, Data Leakage Worldwide: The Effectiveness of Corporate Security Policies, August 2008

Anket neticesinde sistem yöneticilerine göre sıradan kullanıcılarının bilgi güvenliği politikalarını ihlal etme nedenlerinin arasında ilk sırayı ‘‘endişelenecek bir riskin olmadığını düşünmeleri’’ almaktadır.



	Toplam	ABD	Brezilya	İngiltere	Fransa	Almanya	İtalya	Çin	Japonya	Hindistan	Avusturalya
Endişelenecek bir riskin olmadığını düşünmeleri	47%	51%	44%	44%	41%	52%	38%	59% bdfj	49%	51%	39%
Bir sorun olduğu zaman Sistem Yöneticilerinin kendilerine yardım edeceklerini düşünmeleri	41%	39%	36%	39%	33%	41%	38%	47%	38%	52% bd	44%
Güvenliğin onlar için öncelikli bir konu olmadığı	39%	34%	29%	45% bh	31%	33%	31%	77% abcdefhij	25%	38%	39%
Umursamıyorlar	38%	38% b	21%	34%	57% abcefgij	37% b	31%	34%	49% bf	39% b	41% b
Kurum Güvenlik Politikalarını tam olarak bilmemeleri	34%	30%	35%	31%	43% f	29%	25%	45% efj	41% f	35%	29%
Bilgi Teknolojilerinde Güvenliğin Öneminin fark edilmemesi	33%	28%	22%	23%	24%	41% bcd	29%	59% abcdefhij	30%	36%	35%
Çok aceleci olmaları	26%	29% fh	24%	24%	27% f	40% bcfghj	12%	17%	13%	38% fghj	23%

Grafik 14. Sistem yöneticilerine Göre Sıradan Kullanıcılarının Bilgi Güvenliği Politikalarını İhlal Etme Nedenleri

Kaynak: CISCO Systems, Data Leakage Worldwide: The Effectiveness of Corporate Security Policies, August 2008

4.2.4 Örgütsel sinizmin Kurumda Hâkim Olması

Küreselleşmenin, tüm dünyayı sardığı ve ülkeler arasındaki sınırların ortadan kalkarak, adeta dünya genelinde bir yerelleşmeye doğru gidildiği günümüzde artık örgütler her zamankinden daha zor koşulları barındıran bir rekabet ortamında faaliyetlerini sürdürmektedirler. Yaşanan siyasal, ekonomik ve sosyal gelişmeler, bu süreci daha da zorlu ve sıkıntılı bir süreç haline getirmektedir. Böylesi bir küresel rekabet ortamının hüküm sürdüğü bir ortamda misyonu ve vizyonu ne olursa olsun her örgütü, başarıya götürecek unsurların başında insan kaynağının geldiği düşünülmektedir. Bu nedenle örgütler, her

zamankinden daha fazla insan kaynağına yatırım yapmaktadırlar. Örgütler için önemi bu kadar büyük olan insan unsurunun da elbette ki istek, ihtiyaç ve beklentileri de olacak ve bu sayılanlar, insan unsurunun performansını büyük ölçüde etkileyebilecektir. Dolayısıyla örgütlerin, çalışanlarının ihtiyaç ve beklentilerini karşıladıkları müddetçe başarılı sonuçlara daha yakın oldukları söylenebilir. Tersi durumda ise yani örgütler, çalışanlarının ihtiyaç ve beklentilerini yeterince karşılamazlar ve bunu karşılama noktasında herhangi bir çaba göstermezler ise, bu durum, çalışanların mutsuz olmalarına, düşük performans sergilemelerine ve örgütlerine karşı birtakım olumsuz tutum ve davranışlar içerisine girmelerine yol açabilecektir. Örgütsel sinizm söz konusu bu olumsuz tutum ve davranışlar arasında yer alan bir kavram olarak karşımıza çıkmaktadır. (Dean ve diğ.,1998).

Son zamanlarda dünyada ve ülkemizde meydana gelen kasıtlı bilgi kaçaklarını yapan kişilerin bunu kurumlarına karşı duydukları öfke, kızgınlık, hayal kırıklığı, ümitsizlik gibi negatif duygulardan yaptıkları tespit edilmiştir.

Örgütsel sinizm kavramı, bir çalışanın örgütüne karşı geliştirdiği negatif tutumlar olarak tanımlanmakta ve örgütün dürüstlükten yoksun olduğuna dair inanç, örgüte yönelik negatif duygu ve bu inançlar ve duygularla tutarlı olarak, örgüte yönelik aşağılayıcı ve eleştirel davranma eğilimi olmak üzere üç boyutunun olduğu ifade edilmektedir (Dean ve diğ., 1998:345).

Örgütsel sinizmin ilk boyutu, öfke, hor görme ve kınama gibi olumsuz duygularla ortaya çıkan, örgütün dürüstlükten yoksun olduğuna dair inançtır**.** Bu açıdan sinizm, eylemlerin ve insan güdülerinin iyiliği ve samimiyeti ile ilgili inançsızlığa olan eğilimdir. Bu nedenle sinikler; adalet, dürüstlük ve samimiyet gibi prensiplerin eksikliği nedeniyle, örgütlerinin uygulamalarıyla kendilerine "ihanet" ettiklerine inanmaktadırlar. Bir nesneye karşı gösterilen duygusal tepkiler örgütsel sinizmin ikinci boyutunu oluşturmaktadır. Sinizm, düşünce ve inançların yanı sıra örgüte yönelmiş objektif bir yargı içermeyen hor görme ve öfke gibi güçlü duygusal tepkileri de içermektedir. Hatta örgütsel sinizm düzeyleri yüksek bireylerin örgütlerini düşündükleri zaman sıkıntı, tiksinti ve utanç bile

hissedebilecekleri belirtilmektedir. Örgütsel sinizmin son boyutu olumsuz davranışlara yönelme eğilimidir. Bu davranışların çoğu, örgütün samimiyet ve dürüstlükten yoksun olduğuna dair ifadelerdir. Bu boyut güçlü eleştirileri, karamsar tahminleri, alaycı mizah gibi unsurları ve örgütle ilgili hakir görmeleri ve eleştirel ifadeleri de kapsamaktadır (Özgener ve diğ., 2008: 56; Kutaniş ve Çetinel, 2010:188).

Örgütsel sinizm; kişi, grup, ideoloji, sosyal yetenekler veya kurumların güvensizliğine yönelme ve kızgınlık, ümitsizlik, hayal kırıklığı ile karakterize edilen genel veya spesifik tutumlar olarak tanımlanmaktadır (Andersson, 1996:1397-1398). Bir diğer tanımla, örgütsel sinizm, "bireylerin örgütlerinin ahlaki bütünlükten yoksun olduğu ve hakkaniyet, dürüstlük ve samimiyet gibi ilkelerin örgütsel çıkarlar lehine feda edildiği yönündeki inançları" dır (Bernerth ve diğ., 2007:311).

Çalışanlar örgütlerinde yaptıkları ve etkiledikleri işler ile ilgili kontrolü kendilerinde hissetme isteğine sahiptirler. Bu kontrolü, kendi fikir ve tercihlerini ortaya koyabildikleri durumda kendilerinde hissederler. Kendilerini ifade etme fırsatları sağlanmadığında kontrol duygusu ortadan kalkacaktır. Eğer çalışan bu kontrol duygusunun eksikliğini yaşarsa fizyolojik veya psikolojik yılgınlık, vazgeçme, stres tabanlı huzursuzluk, tatminsizlik ve motivasyon düşüşleri hatta sabotaj gibi zararlı etkilere yol açabilir (Ehtiyar ve Yanardağ, 2008: 58). Genel olarak, sinizmin temelinde insan doğasına karşı olan güvensizlik yatmaktadır (Eisinger, 2000:55).

Bireylerin birbirlerine karşı düşünce ve davranışlarıyla ilgili olumlu duyguları içeren güven kavramı, bireylerarası ilişkileri geliştirmede en etkili faktörlerden birisidir. Güven duygusunun belki de en önemli özelliği karşılıklı olmasıdır. Yani bir kişinin bir başka kişiye güvenmesi tek başına anlamlı ve yeterli değildir. Eğer bir örgütten söz ediyorsak, bu örgütte yer alan herkesin önce örgüte, daha sonra da örgüt içindekilere güven duyması ve bu güvenin karşılıklı olması gerekmektedir. Örgütsel güvenin sağlanması, örgütte çalışan bireylerin, olumlu duygulara sahip olmasıyla sonuçlanmaktadır (Özler ve diğ.,2010).

Örgütlerde güven ilişilerinin oluşturulması, çalışanlar ve yöneticiler arasında güvene dayalı ilişkilerin varolması örgütsel davranış açısından büyük önem taşımaktadır. Güven ilişkilerinin örgütler için sonuçları gerek alan araştırmaları ile gerekse teorik düzeyde tartışma alanı bulmaktadır. Bireylerin birbirine duydukları güven, yönetsel sorun çözme etkinliğini belirgin bir biçimde arttırmaktadır. Bireyler arası güvenin düşük olduğu gruplarda, bireyler arası ilişkiler problemlerin algılanmasında hata ve çarpıtmalara yol açacak nitelikte olmaktadır. Buna karşılık güven düzeyi yüksek gruplarda, toplumsal belirsizlikler oluşmamakta, problemler daha etkili bir şekilde çözülmektedir (Zand, 1972:238).

Güvenin kurumlardaki temel işlevleri arasında, kurumdaki işlem maliyetlerini azaltması, üyeleri arasında işbirliğine, özgeci davranışlara, fazladan gerçekleştirilen rol davranışlarına yönelik gönüllülük yaratması; kurum kurallarına uymayı kolaylaştırması ve çatışmaları azaltması sayılabilmektedir. Çalışanlar arasındaki güven iklimi, bağlılık ve tutarlılığın oluşmasını sağladığı gibi, yeni fikirlerin ve yaratıcı şekilde düşünmenin gelişimini sağlar. Çalışan ve yönetici arasındaki güven ilişkisi, çalışanların işlerine yoğunlaşmasına yardım eder. Böylece kurumsal verimlilik artar. Çalışanlar güvenin olmadığı bir ortamda, işbirlikçi davranışa daha az istekli olurlar. Kurumların güven sağlamada başarılı olabilmeleri için, yapılarının güvene göre tasarlanması gerekmektedir.

Kurumlarda iletişimin açık olması ve denetimin paylaşılması, güven oluşumunu arttıran unsurlardandır. Açık iletişimin, önemli bilgileri paylaşmanın, karar almaya katılımın kurum içinde güven oluşturduğu ve çalışan memnuniyetini artırdığı bilinmektedir. Çalışanlar kurumsal karar ve eylemlerle ilgili bilgilere ulaşamaz ve bilginin saklı olduğuna ya da kendinden saklandığıyla ilgili şüphe duyduğunda yönetime güveni yok olur. Buna ek olarak, kurumun yapısı da güven durumunu etkilemektedir. Merkezileşme ve biçimselleşmenin yüksek olduğu, temel odağı verimlilik olan mekanik örgütler, güvenin kurumda oluşumunu kısıtlamaktadır. Merkezileşme ve biçimselleşme düzeyi düşük olan ve etkinlik üzerine odaklanan organik örgütlerde ise yöneticiler açık iletişim ortamı sağlayacaklardır. Böylece güvenin oluşacağı bir ortam oluşacaktır (İşçi, 2010).

Güven tanımları ile birlikte kavrama ilişkin bir değerlendirme yapıldığında güvenme durumunda belirginleşen ortak davranış, durum ve noktaların var olduğu gözlenmektedir. Bu saptamalar; güvenin gelişmesi durumunda güvenen kişinin açıklığında ve savunmasızlığında bir artış olması, güvenilen kişinin davranışlarının güvenen kişi tarafından ya hiç kontrol edilmemesi ya da daha az kontrol edilmesi, güvenin risk ve zarar görme ihtimali içermesi, buna karşın risk alma isteğini doğasında bulundurması, iki veya daha fazla insanın etkileşimi ile biçimlenmesi, karşılıklı bağımlılığı zorunlu kılması ve zamanla gelişmesi olarak sıralanabilecektir. Güven tanımlarından çıkan bir diğer önemli çıkarım da güvenin olumlu yönde bir beklenti ve inanç içermesi, bu olumlu beklentinin karşı tarafa ilişkin iyi niyetlilik, dürüstlük gibi bazı özelliklerin varlığından ve bunlara yönelik değerlendirme ile algılardan etkilenmesidir (Zand, 1972: 230; Hosmer, 1995: 390-393; Bhattacharya ve vd., 1998: 462; Mayer ve ark., 1999; Tschannen-Moran ve Hoy, 2000: 552-555; Arı,2003: 20-23).

Güven tanımları paralelinde, bireyler arası güven ilişkileri üzerine düşünüldüğünde akla ilk gelen sorulardan birisi, bir kişiye güvenmeyi sağlayan unsurların neler olduğu ve karşıdaki kişinin hangi özelliklerinin ona güvenilmesini sağladığıdır. Güvenen tarafa ilişkin özellikler, bireyin güvenme eğilimi olarak ifade edilmekte ve ilişkinin başında güvenme üzerinde etkili olduğu düşünülmektedir (Rotter, 1971; Mayer ve vd., 1999). Güvenilene ilişkin özellikler üzerinde ise yazındaki ilk çalışma Gabarro'nun (1978) 4 işletmede 33 ast-üst çifti ile yaptığı görüşmeler sonucunda güvenin dayanakları olarak nitelendirdiği özellikleri ortaya koyduğu araştırmasıdır. Gabarro (1978: 295-298) araştırmasında karşıdaki kişiye güvenmeyi sağlayan özellikler olarak karakter, yetkinlik ve yargı başlıkları altında bazı özellikler belirlemektedir. Bu çerçevede karaktere dayalı özellikler; niyet ve amaçlarının karşı tarafa zarar vermeyecek ölçüde olumlu olmasını ifade eden dürüstlük; tutarlılık ve tahmin edilebilirlik; açıklık; güvenen tarafından verilen ve ortaya çıktığında güvenene zarar verici olabilecek bilgiyi korumak anlamında ketumluk olarak belirlenmektedir. Yetkinliğe dayalı özellikler olarak; bireyin işinde gereken bilgi ve donanıma sahip olması; bireyler arası iletişimde, ilişkilerinde ve iş yaşamında akıl ve tecrübeden kaynaklanan yetkinlik güven dayanakları olarak nitelendirilmektedir. Son

olarak araştırmada, bireyin davranışlarında ve işe ilişkin konularda yargıya varma ve karar almadaki yetkinliği güveni oluşturan özellikler olarak belirlenmektedir. Yazar, yapılan görüşmelerde yöneticiler ve astlar açısından güven oluşumunda etkili olan bu unsurlar arasında bir öncelik sıralaması yapıldığında, yöneticinin astına güveninde öncelik sırasının; dürüstlük, yetkinlik ve davranışlarda gösterilen tutarlılık olarak belirlendiğini ortaya koymuştur. Astın yöneticiye güveninde ise dürüstlük, yöneticinin niyet ve amaçları ile açıklık sıralaması yapılmıştır (Gabarro, 1978: 298).

David R.Hannah, Coca Cola ve Kentucky Fried Chicken gibi ticari sırlarını patent yolu ile korumaktansa kendi belirlemiş olduğu gizlilik politikaları ile yıllarca korumayı tercih eden firmaların bunu nasıl başardığını araştırdığında çalışanlara güvenin ön planda geldiğini söylemektedir. Bu firmalar, çalışanların ticari sırlarla ilgili olarak eğitimlerinde ticari sırların ifşa edilmesinde ne gibi cezalara maruz kalacakları tehditlerine odaklanmaktadırlar. Bu yaklaşım tamamiyle ters etki yapmaktadır. Bu konu ile ilgili yapılan araştırmalar güven duyulmayan çalışanların güven duyulan çalışanlara nazaran ticari sırları açıklamaya daha yatkın olduklarını tespit etmiştir (Hannah, 2006).

4.2.5 Kurumsal Aidiyetin Oluşmaması

Günümüzde en önemli üretim faktörü olarak kabul edilen bilginin saklanması, paylaşılması ve transferinde sağladığı olanaklar ile işletmelere çok büyük fayda ve avantajlar sağlayan bilişim teknolojileri, işletmeler için önemli maddi finansal ve itibar kaybına neden olabilecek bazı güvenlik tehditlerini de beraberinde getirmektedir. İşletmelerde bilgi güvenliği ile ilgili tedbirler alınırken, sadece teknik önlemlerin yerine getirilmesi güvenliğin sağlanmasında yeterli olmamaktadır. Bilgi güvenliği ile ilgili olarak yazılım, donanım ve fiziki teknik önlemlerin alınmasının yanında, güvenlikte en önemli faktör olan insan faktörü de göz önüne alınmalıdır. İşletmeler, bilgi güvenliği ve örgüt kültürünü birleştiren bir strateji izlemeli ve sadece dışarıdan gelecek saldırılara odaklanmayarak, işletme içindeki kapalı ve çoğu zaman bilinçsizse olabilen insan ve insan ilişkilerine de önem vermesi gerekmektedir (Chang & Lin, 2007).

Kurum içerisinde insan ilişkilerinin iyi olabilmesi için personelin kendini kurumuyla özdeşleştirmesi, kurumlarına bağlılık duymaları ve bireysel niteliklerini kurumun başarısına en fazla katkı sağlayacak şekilde kullanmaya gayret etmesi ile mümkündür. Çalışanların kurumlarına duyacağı güçlü bağ, kurumsal aidiyetin yüksek olması ile ilgilidir. Bu bağın güçlü olması personelin kurum için fedakârlıkta bulunabileceği, kurumsal kimlikle özdeşleşeceği, kurumsal amaç ve değerleri özümseyeceği anlamına gelmektedir. Bu bağın zayıflaması personelin performans düşüklüğüne, geç kalma, devamsızlık, işten ayrılma gibi olumsuz sonuçlar doğurabilecektir. Kendini kurumun bir parçası olarak hissetmeyen personel kurumun itibarını zedelemek ya da maddi hasara uğratmak adına bilgi sızdırmaya meyillidir.

Kurumsal aidiyetin bir kurumda oluşması için çalışanların bir arada yaşamalarının bir sonucu olarak kendilerine özgü değer ve normlardan oluşan bir kültürün oluşmuş olması gerekir. Oluşan bu kültüre örgütsel kültür denilmekte ve tanımı; ‘‘bir örgütteki insanların davranışlarını yönlendiren normlar, davranışlar, değerler, inançlar ve alışkanlıklar sisteminden ibarettir’’ olarak yapılmaktadır. (Dinçer ve Fidan, 1996: 401).

Örgüt kültürü, bir örgütte bulunan değerler, normlar ve inançlar sisteminin, tüm çalışanlar tarafından yürekten benimsenmesiyle kuvvetlenir. Kabul edilmiş ve yaşanan bir örgüt kültürü, üyelerinin davranışlarının yönlendirilmesinde ve üyeler arasında uyumun sağanmasında etkili olmakta, işbirliğini, güven duygusunu ve iletişimi geliştirmektedir. Örgüt kültürünü oluşturan ortak değerleri, varsayımları ve normları paylaşan üyeler kendini bir bütünün parçası gibi hisseder. Bu duygu üyelerin birbirlerine ve örgüte olan bağlılığını arttırır, aidiyet duygusu sağlar, çatışmaları azaltır ve ekip ruhunu geliştirir (Tozkoparan ve Türker, 2001: 203).

Sağlıklı bir örgütsel kültür örgütlerde güvenlik bilincinin temelini oluşturmada önemli ve gerekli olan faktörlerdir. Fakat bu konuda çalışma koşulları da önemli bir rol oynamaktadır. Çalışanların iş tatminsizliği etik olmayan davranışlara sebep olabilmekte ve

bu durum da çeşitli güvenlik tehditlerinin ortaya çıkmasına neden olabilmektedir (Siponen, 2000).

Kurumsal aidiyetin sağlanması kurumda çalışan insanların birbirlerini daha yakından tanımalarına bu da bilgiyi sızdırmaya meyilli insanları bu eylemi gerçekleştirmeden tespit etmeye faydası olabilir. Aynı zamanda kurumdaki ekonomik, psikolojik ve sosyal sorunlu insanların tespit edilip gerekli önlemleri almak için bize imkân tanıyabilir.

4.2.6 Cezai Müeyyidelerin Bilinmemesi ve Önemsenmemesi

Şirket veya kurumların ticari sır olarak muhafaza ettikleri projeler, know-how bilgileri, formüller, çalışanlar ve müşteriler hakkında özel bilgiler, muhasebe kayıtları, raporlar, teklifler, sözleşmeler, üretim teknikleri, pazarlama teknikleri, tedarikçi kayıtlarının başka şirket veya kurum tarafından ele geçirilmesi o şirket için bir kâbus olabilmektedir. Bu derece önemli olan ticari sırların bilerek ya da bilmeyerek ifşasının bir suç teşkil ettiği ve ağır cezalarının olduğu personel tarafından bilinmediğinden ya da umursanmadığından kurumlardaki bilgi sızıntısı her geçen gün artmaktadır.

Kurumsal açıdan cezai yaptırımlarının bireyleri suç işlemekten caydırdığı yapılan araştırmalarda tespit edilmiştir. Bu caydırıcı özelliğin tam olarak hayata geçirilmesi için personelin bilgi sızdırmasının kendisine nelere malolacığı ve bu eylemlerin karşılığında ne gibi cezaların olduğu anlatılmalıdır.

Kurumlar yeni aldıkları personele ticari sırların neler olduğunu ve kurumun bilgi güvenliğine zarar verdiği zaman ne gibi cezaların uygulanacağını sözleşmelerinde belirtmeleri gerekmektedir. Personel işe girdiğinde bu tebliğ edilmeli ve senede 2-3 defa bu konu ile ilgili eğitimler verilmelidir.

Ceza konusunda bilgilenen personel, bilinçsiz bilgi sızma konusunda daha duyarlı hale geleceğinden bu konudaki bilgi kaçakları cezanın caydırıcı etkisiyle minimize edilmiş olunacaktır.

Bu alanda yapılan ilk araştırmalar, caydırıcı hipotezi doğrular yönde gerçekleşmiştir. Örneğin Gibbs (1975) yaptığı çalışmada, adam öldürme ile cezalandırmanın ağır olması ve kaçınılmazlığı unsurları arasında negatif bir ilişkiyi saptamıştır (Liska, 1987:97). Diğer bir ifade ile Gibbs, Birlesik Devletlerde adam öldürme suçu için cezalandırmanın kesinliği ve ağırlığının etkisini incelediği çalışmasında, yakalanmanın/tutuklanmanın görece kesin/kaçınılmaz ve cezaevi tutuklama koşullarının da ağır olduğu yerlerde/bölgelerde daha az sıklıkta işlendiği bulgusunu elde etmiştir (Gibbons, 1987:471). Bu araştırma, ceza korkusu veya riskinin suç davranışı üzerinde caydırıcı bir etkiye sahip olduğunu ortaya koymuştur (Hagan, 1985:302).

Suç oranları üzerinde cezanın caydırıcı etkisini inceleyen diğer bir araştırmacı olan Chamblis (1971: 196-204) de, Midwestern Üniversitesi kampüsünda yaptığı araştırmada, park ihlallerine karşı cezaların ağırlaştırılması ve kesinliğinin arttırılmasından sonra park ihlallerinin önemli ölçüde azalma gösterdiği bulgusunu elde etmiştir.

Ceza, bir davranışın suç olarak tanımlanıp tanımlanmayacağını belirleyen hukuksal bir terimdir. Diğer bir ifade ile ceza, hangi davranışın suç olduğunu ve belirlenen suç davranışı için öngörülen yaptırımın ne olduğunu belirleyen yasal bir tanımlamadır. Genel olarak cezanın/cezalandırmanın amacı, daha önceden suç işlemiş olan bireylerin yeniden suç işlemelerini engellemek ve suç işleme eğiliminde olan bireyleri de bu davranışı gerçekleştirmekten caydırmaktır. Bu yaklaşım, cezalandırmanın önde gelen temel amacının caydırıcılık olduğunu göstermektedir. Caydırıcılık, bireyin ceza alacağı veya hapsedileceği korkusuyla suç işlemekten kaçınmasını tanımlamaktadır. Suç eylemine verilen uygun bir cezanın hem suçlu hem de potansiyel suçlu açısından bir caydırma görevini görmesidir. Diğer bir deyişle, suç işleyen bir suçluya verilen ceza, onun yeniden suç işleme olasılığını azalttığı gibi, toplumda da suç işleme eğiliminde olan bireyleri de suç işlemekten caydırmaktadır. İlkinde ceza, bireysel/öznel anlamda bir caydırıcı rolünü yerine getirirken, ikincisinde de genel önleme açısından bir fonksiyonu yerine getirmektedir (İçli ve Öğün, 1999: 25-26).

Caydırıcı teorisinin önde gelen teorisyenlerinden Bentham, suç için öngörülen cezanın vereceği acının, hazdan daha fazla olması gerektiğini ileri sürmektedir. Diğer bir deyişle bireylerin suç işlemeleri ile elde edecekleri faydanın, suçun maliyetinden daha az olması durumunda ceza caydırıcı olabilecektir. Ayrıca suç davranışı için potansiyel cezanın ağırlığının yanında cezanın kesinliği ve ivediliğinin arttırılması da suçlulukta caydırıcıdır (Pogarsky ve Piquero, 2004:373).

4.2.7 Bilişim Teknoloji Sistemlerinde Zaafiyet

Bilgi güvenliği, bilginin gizliliği, bilginin bütünlüğü ve bilginin erişilebilirliğine gelebilecek zararlardan korunulmasıdır. Günümüz bilgi ve bilişim teknolojileri ilişkisi düşünüldüğünde, bilgi güvenliğinin sağlanmasının, bilişim teknolojilerinin güvenliği ile yakından ilgili olduğu anlaşılmaktadır. Bilişim teknolojileri güvenliği içerisine, donanım, yazılım, bilgi ve iletişimi kapsayan bilgi sistemlerinin gizlilik, güvenlik, bütünlük ve her zaman çalışır vaziyette olmasının sağlanması girmektedir (Onwubiko & Lenaghan, 2007).

Bilişim teknolojilerinin sağladığı fayda ve olanaklar nedeniyle günümüzde çoğu işletme, faaliyetlerini gerçekleştirmek için bilişim teknolojilerine bağımlı hale gelmiştir. İşletmelerin bilişim teknolojilerine bağlılığı arttıkça bu teknolojilerde meydana gelebilecek arızalara ve saldırılara karşı duyarlılığı da artmaktadır. İşletmenin bilgi işlem sistemine yapılacak bir saldırı ciddi miktarda para, zaman, itibar ve değerli bilgi kaybına sebep olabilmektedir (Dayıoğlu, 2002).

İşletmelerin sahip oldukları sınırlı kaynakları da bilgi güvenliğinin sağlanmasında bir kısıt oluşturmaktadır. İşletmelerin bilgi güvenliği harcamaları, işletmeden işletmeye ve sektörden sektöre değişmektedir. Karşılaşılabilecek güvenlik tehditlerinin çokluğuna karşın, işletmelerin güvenlik harcamaları sınırlıdır. Ayrıca, güvenlik uzmanları için "Ne kadar güvenlik yeterli?", cevaplaması zor bir sorudur (Johnson & Goetz, 2007).

Gartner ve Deloitte gibi bağımsız araştırma kuruluşlarının raporları incelendiğinde kurum ve kuruluşların güvenlik teknolojilerine yeterli ölçüde yatırım yapmadıkları

görülmektedir. Deloitte firmasının 30 ülkede 2006 yılında gerçekleştirdiği araştırmada kurumların 73'nün güvenlik yatırımı yaptığı, yatırım yapan firmaların bilgi işlem müdürlerinin %54'nün ise bu yatırımları yetersiz buldukları belirtilmiştir (Kudat,2007).

Bugün şirketlerin elindeki en büyük değer, eşya, araç, gereç ve bina gibi sabit değerlerden çok değer yaratan bilgi, patentler, ticari marka, telif hakkı, ticar sırlar, çalışanlarda ve süreçlerde vucut bulan fikirler olarak tanımlanan entelektüel sermayedir. Bu entelektüel sermayenin büyük bir kısmının muhafaza edildiği yer kurumun bilişim teknoloji sistemleri olmaktadır. Verilerin bulunduğu veritabanının kaçaklara ve dışarıdan gelecek olan tehlikelere karşı güvenilir olması kurumun rekabet avantajını sağlayacaktır. Güvenilirlik, verinin toplanıp bilgi haline gelmesinden, işlenmesine, depolanmasına, kurumun ağ sistemlerini kullanarak bir noktadan başka bir noktaya iletilip son kullanıcıların hizmetine ve kullanımına sunulmasına kadar olan safhalardaki iletişim teknikleri ve bilgisayarlar dâhil tüm bu teknolojileri kapsamaktadır.

Bilgisayar veya aktif cihazlara fiziksel olarak erişebilen saldırganın cihazın kontrolünü kolaylıkla alabileceği unutulmamalıdır. Ağ bağlantısına erişebilen saldırgan ise kabloya özel ekipmanla erişerek (tapping) hattı dinleyebilir veya hatta trafik gönderebilir. Açıkça bilinmelidir ki fiziksel güvenliği sağlanmayan cihaz üzerinde alınacak yazılımsal güvenlik önlemlerinin hiç bir kıymeti bulunmamaktadır. Kurumun ağını oluşturan ana cihazlar ve hizmet sunan sunucular için alınabilecek fiziksel güvenlik politikaları kurum için belirlenmelidir (Karaarslan, 2002).

Kurum bilgisayar ağındaki gelen ve giden ağ trafiğini kontrol ederek bilgisayar ağına yetkisiz ve istenilmeyen kişilerin çeşitli yollardan erişim sağlamasını engellemeye yarayan bir yazılım ve donanım olan Güvenlik Duvarı (Firewall) Kurumunuz için olmazsa olmazların arasındadır. Güvenlik Duvarı sayesinde hacker ların veya solucanlar gibi zararlı yazılımların ağ veya internet üzerinden kurumunuzdaki bilgisayarlara erişmesine engel olmaktadır.

Veri kayıplarına ve veri bozulmalarına neden olan kötü amaçlı yazılımlar olan virüslerin geri dönüşümü mümkün olmayan zararlarından korunmak için kurumdaki tüm bilgisayarlarda güncel ve lisanslı bir antivirüs programının bulunması gerekmektedir.

Erişim politikaları kullanıcıların ağa bağlanma yetkilerini belirler. Her kullanıcının ağa bağlanma yetkisi farklı olmalıdır. Erişim politikaları kullanıcılar kategorilere ayrıldıktan sonra her kategori için ayrı ayrı belirlenmelidir. Bu kategorilere sistem yöneticileri de girmektedir. Sistem yöneticisi için erişim kuralları belirlenmediği takdirde sistemdeki bazı kurallar sistem yöneticisinin yetkisine bırakılmış olacağından, bu sistem üzerinde istenmeyen güvenlik açıkları anlamına gelebilecektir (Karaarslan ve diğ, 2002).

Kurumda muhafaza edilen çok gizli ya da ifşası kurumu sıkıntıya sokacak hassas bilgilerin erişimi ve işlenmesi "iki adam kuralı" (Two-Man Rule) ile kurumdan çıkması oldukça zor hale gelecektir. Edward Snowden'in National Security Agency den binlerce bilgi sızdırdıktan sonra Komiteye açıklama yapan NSA Director'ü Keith Alexander 18 Haziran 2013'te İki yetkili görevlinin eş zamanlı bilgiye erişimi olarak nitelendirilen "iki adam kuralı" nın gelecekte bu tür sızmaları önleyebileceğini beyan etmiştir.

Özellikle istihbarat ve güvenlik kurumlarında sistem yöneticilerinin bu kuralla çalışması kurumdaki bilgilerin daha emin ellerde olmasını sağlayacaktır.

Son zamanlarda artan ve ciddi zararlara yol açan sistem saldırılarının tespit edilmesinde ve önlenmesinde önemli rol oynayan IDS **(**Intrusion Detection System**)** ve IPS **(**Intrusion Prevention System**)** olarak adlırılan Saldırı Tespit ve Saldırı Engelleme sistemlerinin kurumsal bilgisayarlarda kullanılması sistemin güvenli bir şekilde işlemesine yardımcı olur ve Sistem Yöneticilerinin Sistemi güçlü bir şekilde izlemesine yardımcı olmaktadırlar.

Kurumsal menfaatler gereği, kurum içi İnternet politikası oluşturulmalıdır. Kurumda internete girmek için ayrı bilgisayarlar tahsis edilmeli ve bununda web erişiminin denetim altında tutulması gerekmektedir. Bunu yapmak kurumumuzdaki bilgilerin virüs

veya truva atı gibi zararlı yazılımlardan uzak tutulmasına, personelin iş verimine engel olmamasını sağlayacaktır.

Bilgisayar tabanlı bilişim sistemlerinin her geçen gün iş ve özel hayatımıza daha fazla girmesiyle elektronik ortamlarda bulunan kamu ve özel bilgilerin sayısı artmaktadır. Bu bilgilerin güvenliğinin sağlanması kendimiz ve kurumumuz için önem arz etmektedir. Evimizdeki bilgisayarların güvenliğini virüs programları ile korurken, kurumuzdaki bilgisayarları ise kurumun bünyesinde uygulanması zorunlu olan bilgi güvenliği politikaları ile sağlayabiliriz.

Bilgi sızıntılarının engellenebilmesi için öncelikle kurumun bir bilgi güvenliği politikasına ihtiyacı vardır. Bu politikada kurumda hangi bilgi tiplerinin işlendiği, bu bilgilerin nerelerde tutulduğu ve gizlilik derecelerinin neler olduğu, kimlerin bu bilgilere erişebileceği, bu kişilerin görev ve sorumluluklarının ne olduğu, hangi koşullarda bilgilerin diğer kişi veya kuruluşlarla paylaşılabileceği mutlaka yer almalıdır. Bu politikanın sadece bilgi işlem personeli değil tüm personeliniz tarafından benimsenmesi ve gerekli iç ve dış denetim mekanizmalarının oluşturulması politikanın başarılı olması için gereklidir (Oğuz, 2010).

Etkin bir bilgi güvenlik yönetim sisteminin oluşturulması amacıyla hazırlanmış olan TS ISO IEC 27001 standartlarından faydalanılmalıdır. Bu standart, işletmeler içerisinde bilgi güvenliği yönetimini başlatmak, gerçekleştirmek, sürdürmek ve iyileştirmek için genel prensipleri ve yönlendirici bilgileri ortaya koyar.

Güvenlik politikaları kurum veya kuruluşlarda kabul edilebilir güvenlik seviyesinin tanımlanmasına yardım eden, tüm çalışanların ve ortak çalışma içerisinde bulunan diğer kurum ve kuruluşların uyması gereken kurallar bütünüdür (Kalman,2003,36-37).

Her şeyden önce, kurumlar kendi içlerinde bilgi güvenliği politikası içeren bir belge oluşturmak zorundadır. Veriler sınıflandırılmalı ve gizlilik dereceleri belirlenmelidir. Hangi veriye kimin nasıl ulaşacağı saptanıp buna göre erişim yetkileri düzenlenmelidir. Şifre ve

parolaların sık sık değiştirilmesi zorlanmalıdır. Tüm veri sistemlerinin hem en güçlü unsuru olan, hem de en zayıf halkası olan insan faktörü unutulmamalıdır (Ahi, 2003).

İyi bir güvenlik politikası, kullanıcıların işini zorlaştırmamalı, kullanıcılar arasında tepkiye yol açmamalı, kullanıcılar tarafından uygulanabilir olmalıdır. Politika, kullanıcıların ve sistem yöneticilerinin eldeki imkânlarla uyabilecekleri ve uygulayabilecekleri yeterli düzeyde yaptırım gücüne sahip kurallardan oluşmalıdır. Alınan güvenlik önlemleri ve politikaları uygulayan yetkililer veya birimler yaptırımları uygulayabilecek idari ve teknik yetkilerle donatılmalıdır. Politika kapsamında herkesin sorumluluk ve yetkileri tanımlanarak kullanıcılar, sistem yöneticileri ve diğer kişilerin sisteme ilişkin sorumlulukları, yetkileri kuşku ve çelişkilere yer bırakmayacak biçimde açıkça tanımlanmalıdır. Politikalar içerisinde uygulanacak olan yasal ve ahlaki mahremiyet koşulları ile elektronik mesajların ve dosyaların içeriğine ulaşım, kullanıcı hareketlerinim kayıt edilmesi gibi denetim ve izlemeye yönelik işlemlerin hangi koşullarda yapılacağı ve bu işlemler yapılırken kullanıcının kişisel haklarının nasıl korunacağı açıklanmalıdır (Vural ve Sağıroğlu,2008).

Kurumlar, olağanüstü durumlar için sistem backuplarını, mutlaka kurumun dışında, uzakta, fakat gün içerisinde erişilebilir konumda, ısı, nem ve manyetik korumalı ideal saklama koşullarında saklamalı ve kurumun belirleyeceği sıklıkta teslim ve değişimini sağlaması gerekmektedir.

Dalgalar, elektrik yükleri ve manyetik durumlar olarak elektromanyetik tayfta bulunan elle tutulamayan veri ve yazılımlar olarak nitelenen Siber Uzaydan (Galbstein ve diğ. 2003) gelebilecek ataklara/tehditlere karşı kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan politikalar, güvenlik kavramları, risk yönetimi yaklaşımları, faaliyetleri oluşturan siber güvenlik konusunda gerekli hassasiyet gösterilmelidir.

2007 yılında Estonya ya yapılan siber saldırılar ülkenin başkanlık ve parlemonta sitelerini, bütün bakanlık sitelerini, siyasi partilerin sitelerini, medya kuruluşlarını ve birçok

devlet kurumunun resmi sitelerine zarar vererek siber güvenliğin önemi konusunda tüm dünya için bir milat olmuştur.

2008 yılında Gürcistanın Rusya ile çatıştığı Güney Osetya savaşında maruz kaldığı siber saldırılarda çatışmanın çok kritik aşamalarında Gürcistan hükümetini zayıf düşürmeye yönelik siber saldırılardı.

2010 yılında ABD ve İsrail'in ürettiği tahmin edilen ve İran'ın nükleer çalışmalarını sekteye uğratmak maksadı ile kullanılan bir solucan yazılım olan Stuxnet, sadece internete bağlı bilgisayarları değil herhangi bir veri girişi yapılan (USB, CD vb. aracılığıyla) bilgisayarı ele geçirip kendine yönelik kullanabilmesi yöntemiyle dış dünyaya kapalı sistemlerin de siber saldırılarda hedef olabileceğini göstermesi açısından oldukça önemli bir yere sahiptir.

Siber tehditleri önlemenin veya en azından etkisini azaltmanın en etkin yollarından biri eğitimdir. Gerek bireysel olarak kendimizi gerekse kurumsal olarak personeli siber güvenlik konusunda eğitmek ve son bilgilerle donatmak artık kaçınılmaz hale gelmiştir. Bununla paralel olarak kurumlardaki ve bireysel kullanımdaki bilgisayarlar en son teknoloji ve güvenlik yazılımları ile donatılmalıdır. Kurumlarda mutlaka risk değerlendirmesi yapılmalı ve olası saldırı ve aksaklık durumunda uygulanacak hareket şekli belirlenmelidir. Yedek planlar oluşturulmalıdır.

Ulusal düzeyde oluşturulanların yanında kurumlarda da siber güvenlikle ilgili birimler oluşturulmalı ve bunlar aracılığıyla gerekli tedbirler alınmalı, farkındalık meydana getirilmeli ve eğitim verilmelidir. Siber güvenlik olayları ile ilgili saldırı şekilleri ve bunlara karşı korunma tedbirlerinin kaydedildiği ve gerektiğinde ilgililerce erişilebilecek bir veri tabanı oluşturulması benzer saldırılar meydana gelmesi durumunda iş gücü ve zaman kaybının azaltılmasını ve hatta ortadan kaldırılmasını sağlamak açısından son derece önemlidir (Öğün ve Kaya, 2013).

4.2.8 Hassas bilgilerin muhafaza edilmesinde ve gönderilmesinde şifrelemenin kullanılmaması

Bilgiye artan saldırılar karşısında anlık koruma sağlayan çözümler yetersiz kalmış, özellikle büyük kurumların sahip olduğu verilerin korunması için bilgilerin şifrelenmesi vazgeçilmez bir çözüm olmuştur.

Teknolojinin hızla ilerlemesi ve internet kullanımının her alanda yaygınlaşması kriptolojinin önemini giderek arttırmıştır. Başlangıçta çok dar bir alanda kullanılan kriptoloji internet kullanımının yaygınlaşması ile kurumların gizli bilgilerini muhafazasında ya da bir noktadan başka bir noktaya sorunsuz bir şekilde ulaştırılmasında kullanılmasıyla kullanım alanı gelişmiştir.

Sistemler arası bağlantılarda ya da herhangi iki nokta arasındaki haberleşmede verinin güvenli bir şekilde gittiğinden emin olmak gerekir. Bunun sağlanması ise gönderilen verinin şifrelenmesi ile olur. Böylece açık haberleşme kanalları kullanılarak verinin güvenli bir şekilde ulaştırılması sağlanır. İletişimde, açık bir haberleşme kanalı kullanılıyorsa gizli tutulmak istenen bilginin yetkisiz bir kişi tarafından dinlenebileceği veya haberleşme kanalına girip (araya girme) veriyi bozabileceği ya da değiştirebileceği (yanlış verinin gönderilmesi) düşüncesi her zaman için önemli bir problem oluşturur.

Şifreleme, askeri ve diplomatik iletişimde (haberleşmede) güvenliği sağlamak için bin yıldır kullanılmaktadır. Ancak bugün artık özel sektörde de gereksinim duyulmaktadır. Sağlık hizmetleri, finansal işler (örneğin: kredi oranları) gibi konularda bilgisayarlar arasındaki haberleşmede açık kanallar kullanılarak yapılmaktadır. Bu açık kanalların kullanılması sırasında yukarıda sayılan işlerin güvenli ve gizli bir şekilde yapılabilmesi için şifrelemeye gerek duyulmaktadır (Yerlikaya ve diğ.,2006).

Kurumların gizli haberleşmelerinde belgenin şifrelenerek/kriptolanarak gönderilmesi belgenin istenilmeyen kişilerin eline geçmesine bir engel koyar. Bunun milli kripto sistemi ile olması dış güçlerin buna erişmesini neredeyse imkansız hale sokacaktır.

Kurum içerisindeki ağda kişisel ve gizli bilgilerin muhafazasında muhakkak şifreleme/kriptolama tercih edilmesi gerekir. Gizli bilgilerin veri şifreleme programları vasıtasıyla şifrelenmesi sağlanmalıdır. Bu konu ile ilgili personele eğitim verilmeli ve kural ihlallerinde gerekli cezai işlem uygulanmalıdır. Kurumda çalışan personelin kuruma ait bilgileri kendi bilgisayarında muhafaza etmesi gerektiğinde TruCrypt veya PGP gibi şifreleme programlarının kullanılması kurumun bilgilerinin yetkisiz şahıslara geçmesini engellemek adına doğru bir karardır.

4.2.9 Bilgi Sızıntı Kanallarını Kapatmamak

Bilgi Sızıntı kanalı, bilgi üzerindeki kontrolün kaybı ya da gizliliğinin ihlaline neden olan her türlü metodun kullanılmasıyla gerçekleştiğinden tam olarak bunu sınıflandırmak kolay değildir. Bilgi sızıntısı, bugüne kadar gerçekleşen bilgi sızıntı vakaları incelendiğinde 9 temel sızıntı kanalının ve birde toplumun menfaatlerini kurumun menfaatlerine tercih etme yoluyla bilgi sızdırma olan whistleblowing yönteminin olduğu tespit etmiştir.

9 temel sızıntı kanalları şu şekildedir.

1. Basılı Materyal
2. Taşınabilir Ortamlar
3. E-Posta
4. Sosyal Paylaşım Siteleri
5. Ortam Dinlemesi
6. Bilgisayar, Donanım Çalınması
7. Sosyal Mühendislik
8. Network
9. Mobil Cihazlar

Şekil 10: Bilgi Sızıntı Kanalları

4.2.9.1 Bilgisayar/Donanım Çalınması:

Kurum Bilgisayarı, Dizüstü bilgisayar ve veri depolama cihazlarının fiziksel olarak çalınması ya da yanlışlıkla bir yerde unutulması kurum için büyük bir tehlike oluşturmaktadır. Bu Kurumdaki fiziksel tedbirlerin yeterince alınmamasından kaynaklandığı gibi personelin bu konudaki dikkatsizliğinden de kaynaklanabilir. Mümkün olduğunca kurum bilgisayarları kurumdan çıkartılmamalı, çıkartılıyor ise bu konuda gerekli tedbirler alınmalıdır.

Credant Technologies deki araştırmacılara göre kurumlardaki dizüstü bilgisayarların %25 i çalışma ofislerinden ya da kullanıcının arabasından çalınırken, %14'üde havaalanlarında ya da uçaklarda kaybolmaktadır (Kitteringham, 2008).

Oran bu kadar yüksekse bu konu ile ilgili kurumlar ciddi önlemler almalıdırlar. Önlemlerin başında dizüstü bilgisayarların içerisine mümkün olduğunca gizli belge konulmamalı, konulması gerekiyorsa da kriptolanarak muhafaza edilmelidir.

4.2.9.2 Mobil Cihazlar

İş ve işlemlerin elektronik ortamlarda yapılmaya başlanmasıyla, hayatımız kolaylaşmakta, yaşam kalitemiz artmakta, iş ve işlemler hızlanmakta ve iş verimliliği artışı sağlanmaktadır. Fakat karşılaşılan sıkıntılar, beklenmeyen durumlar ve maddi ve manevi kayıplar elektronik ortamlarda meydana geldikçe bu ortamlar bizleri çoğu zamanda hayal kırıklığına uğratabilmekte ve sonuç olarak bu ortamlarda güvensizliği ortaya çıkmaktadır (Sağıroğlu ve Alkan, 2005).

Akıllı telefon ve tablet gibi içeriğinde her türlü programı çalıştıracak kapasiteye sahip cihazlar mobil cihazlar olarak adlandırılmaktadır. Şu anki teknoloji ile telefonun uzaktan yönetilen programlarla ses kayıt cihazına dönüşebileceği ve yer konum bildiren bir GPS cihazı olarak kullanılıp ortam dinlemesi ve mevki belirlemede kullanılabileceği bilgi güvenliği eğitimlerinde personele anlatılmalıdır. Hatta farkındalığı arttırmak adına görsel olarak konunun uzmanları vasıtasıyla sunulmalıdır.

Hassas bölgelerine mobil cihazlarla girilmemesi için gerekli önlemler alınmalıdır. Kuralın herkes tarafından uygulanması sağlanmalı, kuralın ihlal edilmemesi için hassas bölgelerden personelin yakınları ile yapılacak telefon görüşmelerinin kurum imkânları ile kolaylıkla yapılması sağlanmalıdır.

4.2.9.3 Taşınabilir ortamlar: (CD,DVD ve USB)

Kurumdaki en gizli bilgi ve belgelerin kısa bir zaman içerisinde CD ve USB lere kopyalanıp kurumdan çıkarılması olayı en son Bradley Manning'in Amerika Birleşik Devletlerinin çok gizli diplomatik belgelerini yayınlayarak tüm dünyanın bildiği WikiLeaks'in ortaya çıkmasını sağlamıştır. Manning bu çok gizli belgeleri sistemden aldıktan sonra bir CD'ye kopyalayarak kurumdan çıkarttığını itiraf etmiştir. Binlerce hatta milyonlarca belgenin CD, DVD veya USB ye atılarak tüm kurumun itibarının zedeleneceği göz ardı edilmeden, donanımsal olarak herkese kısıtlı yetki verilmelidir. Kısıtlı yetki ihlal edildiğinde kurumsal yöneticiyi uyaracak sistemler kurulmalıdır.

4.2.9.4 Kurumsal Bilgisayar Ağı:

Bilgisayarlar arasında veri/bilgi aktarımı ve etkileşimini sağlayan, fiziki ağ yapısı ile bunu destekleyen ve kullanımını gerçekleştirmeye yarayan tüm donanım ve yazılımların oluşturduğu sistem olarak tanımlanan kurumsal bilgisayar ağının iç ve dış tehditlerden korunması için gerekli tedbirler alınmalıdır.

Kurumlar ve işletmeler; internet aracılığı ile ticaretin yaygınlaşmasıyla yerel ağlarını geniş ağa ve internete açtıklarında birçok tehlike ve risklere de kapılarını açmış olurlar. Rakiplerine üstünlük sağlamak ve teknolojinin imkânlarından tamamen yararlanmak isteyen bir kurum, geniş alan ağ bağlantılarından ve internet erişiminden vazgeçemeyeceği için gerekli güvenlik önlemlerini de almalı ve gerekli yatırımları yapmalıdır. Dışarıdan gelen tehlikelerin yanı sıra içeriden kuruma yapılan saldıralar da ağ güvenlik sistemleri sayesinde çözülebilir. Ağ trafiğinin izlenmesinden başlayan bu çözümler, tüm ağ trafiğinin kontrolüne ve raporlamasına kadar uzanır. Donanım ve yazılım tabanlı paketlere, bilgi sistemleri artı değerini katarak yerel ağ güvenliğinizi sağlar.

Kurumlarda mümkün olduğunca kablosuz ağlardan uzak durulmalıdır. Kablosuz ağın zorunlu olduğu durumlarda ise sadece yetkili kişilerin ağa şifreli bir şekilde erişebilmesi için kurulum yapılmalıdır. Kablosuz ağlardaki en temel güvenlik problemi

verilerin havada transfer edilmesidir. Kablosuz ağlarda güvenlik açıkları ağa saldırılara neden olabilir. Kablosuz ağa giren saldırgan ağdaki kullanıcıların yapabilecekleri her şeyi yapabilecektir. Bilgisayarlardaki dosyaları dizinleri kopyalayabilir, zararlı programları bilgisayara kurabilir.

Ağ güvenliğini sağlamak ve ağı dış saldırılardan korumak için ağ güvenlik duvarı (network firewall) oluşturulmalı, sunucuya gelen e-postaları bir süzgeçten geçirerek istenilmeyen e-postaları tespit etmek ve kullanıcının gelen kutusuna (inbox) düşmesine engel olmak için spam filtresi kullanılmalı, güvenlik açıklarına karşı yazılımlar güncellenmeli, istenmeden açılan pencerelerin açılmasını engellemeli ve sistemde kullanılan antivirüs programlarının güncellenmesi sağlanmalıdır.

Kısaca, erişim noktaları arasında ortak bilgi ve hizmet paylaşımını sağlayan platform olarak tanımlanan Bulut Bilişim son zamanlarda uzaktan erişim kolaylığı, donanım ve yazılım maliyetlerinin az olması, yüksek bant genişliği ve yüksek işlemci gücünden şirketlerin tercih sebebi olmuştur. Fakat veri güvenliği ve gizliliği konusunda arzu edilen seviyede olmaması ticari sırların ifşa edilir endişesi ile bazı kurumlarında uzak durması gereken önemli bir unsur olmuştur.

Sayısal çağ olarak isimlendirilen 21inci yüzyılın ilk on yıllık döneminde, sayısal ortamların büyük bir hızla sosyalleşmesi gözlenirken, veri saklama ve hesaplama hizmetlerine donanaım ve fiziksel mekândan bağımsız erişim sağlayan bulut bilişim uygulamaları da yaygınlaşmaktadır. Bilgisayar ağ altyapısında erişilen sürat ve yaygınlaşmaya paralel olarak, veri ve hizmetlerin ağ üzerinden kullanılması daha cazip hale gelmektedir. e-ticaret, e-bankacılık, e-devlet ve uzaktan eğitim gibi geniş kullanıcı kitelesine hitap eden hizmetler internet ağı üzerinde başarılı bir şekilde kullanılmaktadır. Bütün bu gelişmelerin yanında bulut bilişim yaklaşımı özellikle hizmet maliyetlerinin düşürülmesi ve yüksek erişilebilirlik özellikleri ile yeni fırsatlar yaratmaktadır. Yapılan stratejik değerlendirmeler, bulut bilişim uygulamalarının yaygınlaşacağını ve bu alanda ekonomik gelişmeler yaşanacağını ve bu alanda ekonomik gelişmeler yaşanacağına işaret

etmektedir. Dünya genelinde bu alandaki pazarın 2010 yılında 21,5 milyar dolar olduğu belirtilirken, 2015 yılı için bu rakamın 73 milyar dolara ulaşacağı öngörülmektedir (Fox, 2012).

Bulut bilişim konusunda yapılan inceleme ve araştırmalar güvenlik ve kişisel bilginin korunması boyutlarının bu teknolojinin yaygınlaşmasının önünde en önemli engelleri oluşturduğu konusunda hem fikirdir (Khatıbı,2012).

4.2.9.5 E- posta:

Kurumsal ya da özel e-posta sistemi üzerinden gizli bilgilerin kasıtlı ya da gayri ihtiyari sızdırılması kurumların en çok maruz kaldıkları sızıntı yöntemlerindendir. Kasıtlı kuruma ait gizli belgelerin gönderilmesi genelde bilgisayardaki hedef belgenin ismini değiştirerek olmaktadır. Gayri ihtiyari sızıntı ise, yanlış dosyanın gönderilmesi, e-postanın yanlış kişiye gönderilmesi, sosyal mühendislik saldırılarına maruz kalma (Spam, sahte vb. zararlı olduğu düşünülen e-postalara yanıt verme) şeklinde olmaktadır.

Personel bu konularda eğitilmeli ve bu tür saldırılara maruz kaldığı zaman sistem yöneticisine bilgi vermelidir.

4.2.9.6 Basılı Materyal:

Gizli olan basılı materyallerin (evrak, belge, doküman, mesaj vb.) çalınması, fotokopisinin çekilmesi ya da fotoğrafının çekilmesi yöntemiyle sızdırılması kurumun bilgi ve belgelerini tamamiyle elektronik ortama aktaran kurumların bir yönden rahat oldukları bir bilgi sızdırma metodudur.

Kurum için hassas olan basılı materyallerin fiziki olarak emniyetli yerlerde kilit altında muhafaza edilmesi gerekir. Yetkisiz personelin bu materyallere nüfuz etmesini engelleyecek tedbirler alınmalıdır.

Bu belgelerin kurumdan sızması genellikle fotokopisi çekilerek, dökümanın kendisi alınarak ya da fotoğrafı çekilerek olmaktadır. Bu konuda alınması gereken tedbirler; yetkili personelin fotokopi çekimini sağlayan yetkilendirilmiş kartla çekim, evrak çalınmasına karşı gerekli önlemlerin alındığı kurumsal arşiv politikasının belirlenmiş olması ve gizli dökümanların bulunduğu yere fotoğraf makinası ve fotoğraf çekme özelliği olan telefonların bu bölgelere girmemesidir.

4.2.9.7 Anlık Mesajlaşma/ Sosyal Medya:

Anlık mesajlaşma, bir bilgisayar programı sayesinde, üye olarak, listenize eklediğiniz kişilerle gerçek zamanlı görüşme olanağıdır. Program özelliğine bağlı olarak görüntülü ve sesli görüşme olanağı da olabilir. En bilinen anında mesajlaşma programları Facebook, Twitter, ICQ, Yahoo Messenger, MSN Messenger ve Google Talk dır.

Mayfield, (2010:6)'e göre, sosyal medya "en yüksek derecede paylaşımın gerçekleştiği, online medyanın yeni bir türü olarak fırsatlar sunduğu en yeni fikirlerden biridir." ve kullanıcılarına karşılıklı paylaşım imkanı sağlamaktadır.

Sanayi toplumundan bilgi toplumuna geçişle birlikte, iletişim alanındaki gelişmeler, bilginin üretimi, depolanması, paylaşılması ve eleştirilmesini zamandan ve mekândan bağımsız hale getirmiştir. Sanayi toplumunda bilginin üretilmesi ve paylaşılması hemen hemen her ülkede medya kartellerinin kontrolünde gerçekleşmekteydi. Ancak bilgi toplumuna geçişle birlikte, bilginin üretilmesi ve paylaşılmasıyla ilgili kaynaklar hem çeşitlendi, hem de bilgisayar ve mobil cihaz (akıllı telefon, tablet bilgisayarlar vs…) teknolojisindeki gelişmelere bağlı olarak mekâna bağlılıktan ve periyodik olmaktan kurtuldu. Başka bir ifade ile bilgi belli odakların tekelinden ve iletişim de tek yönlü olmaktan çıktı. Dolayısıyla kitle iletişim araçlarının kullanımının tabana yayılmasıyla (blog, kişisel siteler) bilgi kaynağı çeşitliliği ve bireysel tecrübelerin çok kolay ve hızlı bir şekilde aktarımı sağlanmış oldu. Fakat son dönemde özellikle facebook ve twitter gibi sosyal paylaşım ağlarının ortaya çıkması ve yaygınlaşması, iletişim biçimini, söz konusu klasik anlamından köklü biçimde koparark, iletişim sürecinin yapısal bir dönüşüme

uğraması sonucunu doğurdu. Böylece iletişim tam olarak, interaktif, çok boyutlu ve karşılıklı bir etkileşim sürecine dönüştü. Soysal medya alanındaki bu hızlı ve esaslı gelişme, bireyden başlayarak bir ülkedeki veya toplumdaki her unsuru daha görünür ve kolay ulaşılır hale getirmiş, yani onlara ait sırları (bunlar devlet sırrı olabilir) ve gerekli bilgileri (bunlar firmaların stratejileri olabilir) erişilebilir kılmıştır. Bu durum bir yönüyle şeffaflaşma ve karşılıklı kolay bilgi alışverişi anlamına gelmekte; fakat diğer yönüyle de art niyetli kişilerin elinde bireyler ve toplum için bir tehlikeye dönüşme riski taşımaktadır (Eren ve Aydın,2014).

Genel olarak internet ya da iletişimi kolaylaştırmak için tasarlanmış mobil tabanlı sosyal alanlarda, işbirliği ve ağlar arası ilişkileri anlatan sosyal ağlar her geçen gün üye sayılarını arttırarak daha geniş kitlelerle buluşmaktadır. Bu ağlar arasında en yüksek üye sayılarıyla sırasıyla Facebook, Twitter ve Linkedin göze çarpmaktadır (Tablo 2). Bu ağların varlığı ve üye sayılarının artması, giderek daha fazla bilginin bireyler arasında paylaşılması anlamına gelmektedir (Eren ve Aydın, 2014).

Sosyal medya, iş dünyasında özellikle çalışanların zamanlarını, enerjilerini ve dikkatlerini çaldığı için ekonomik zararlara da yol açmaktadır. Ayrıca devletlerin ve şirketlerin mahrem bilgilerinin üçüncü kişilerin eline geçmesine olanak sağladığı için de sosyal medya bir risk faktörü olarak değerlendirilebilir. Dünya çapında 1000 den fazla çalışana sahip 1225 firmanın yetkilileri ile görüşülerek hazırlanan bir rapora göre sosyal medya bir yıl içerisinde firmalarda ortalama 4,3 milyon dolarlık zarara neden olabiliyor. Araştırmalarda firmaların sosyal medya kullanımının taşıdığı en büyük riskleri şu şekilde ifade ettikleri görülmüştür: Çalısanların çok fazla bilgi paylaşıyor olması (%46), şirket içi gizli bilgilerin kaybedilmesi/açığa çıkarılması (%41), marka imajının zedelenmesi (%40), artan davalara maruz kalma (%37), kötü amaçlı yazılım (%37) ve düzenleyici kuralların ihlal edilmesi (%36) (slideshare.net).

Tablo 2 : Dünyada Sosyal Ağ Sitelerinde ilk 10 sıralama

Sıra	Sosyal Ağ	Üye Sayısı
1	Facebook	900.000.000
2	Twitter	310.000.000
3	Linkedln	255.000.000
4	Pinterest	250.000.000
5	Google Plus +	120.000.000
6	Tumblr	110.000.000
7	Instagram	100.000.000
8	VK	80.000.000
9	Flickr	65.000.000
10	Vine	42.000.000

Kaynak : Top 15 Most Popular Social Networking Sites / October 2014
http://www.ebizmba.com/articles/social-networking-websites

Son zamanlarda medyada çıkan haberlere göre sosyal paylaşım siteleri aracılığı ile kurumun gizli ve hassas bilgilerini sızdıran çalışanların sayısı artmıştır. Örneğin, bir İsrail askerin 2010 yılında yapılacak olan operasyon yer ve zaman bilgilerini Facebook ta paylaşması operasyonun iptal edilmesine sebep olmuştur.

Buna benzer olaylar İngiltere de Savunma Bakanlığı çalışanları tarafından İngiliz ordusunun askeri bilgilerini Facebeook ve Twitter vasıtasıyla paylaşılmasıyla defalarca kez yaşanmıştır.

Amerika Birleşik Devletlerinde ise, Hem Parlamenter hem de Amerika Meclisi İstihbarat Komitesi üyesi olan Peter Hoekstra Bağdat'a gerçekleştirdiği gizli bir ziyareti

Tweeter vasıtasıyla paylaşmış ve gerçekleştirmiş olduğu gizli ziyareti saat saat sosyal medyada paylaşmıştır. Bu bilgiler düşman için fayda sağlarken kuruma da zarar verecektir.

Sosyal medya günümüzde şirketler için ürün geliştirme, geri bildirim, müşterinin süreçlere katılabilmesi açısından anahtar bir görev üstleniyor. Ayrıca şirketler arası ilişkileri, müşteri ilişkilerini, işveren, tedarikçi ve kural koyucu ilişkilerini yeniden yapılandırmış durumda. Eskiden günler süren süreçleri de dakikalara indirerek kısaltılmasını sağlıyor. Ancak sosyal medya marka bilinirliğini kısa sürede yukarı çekebildiği gibi aynı hızda da çökertebiliyor (Dede,2013).

Sosyal Medya çoğumuzun artık hayatında bir bağımlılık haline geldiğinden bu bağımlılığın kurumda da devam etmesi personeli ve kurumu olumsuz olarak etkileyecektir. Personelden daha fazla verimlilik almak ve kurum bilgisayarlarını dışarıdan gelecek tehditlere karşı korumak için, iş amaçlı kullanılan kurum bilgisayarlarına sosyal paylaşım site ve programları kurulmamalıdır.

Sosyal medya, bireylere toplumsal yaşam ve devlet yönetimine katılmadan, eğitim ve ticarete kadar birçok alanda değişik olanaklar sunmakla birlikte; birey, toplum, kamu düzeni ve devlet açısından önemli tehditleri de içinde barındırmaktadır. Bu tehditlerin en başında sosyal mühendislik saldırılarıyla bir ülkenin yönetimini etkileme veya değiştirme faaliyetlerine olanak sağlaması gelmektedir. Diğer yandan sosyal medya, provokasyona, dezenformasyona ve bilgi kirliliğine neden olma potansiyeli yüksek bir ortamdır. Ayrıca bu ortam niteliği gereği, bağımlık, ailevi sorunlar, tehlikeli bilgi paylaşımı ve manipülasyonlar, ekonomik kayıplar, mahrem sırların deşifre olması, özel hayatın gizliliğinin ortadan kalması gibi birçok riski içinde barındırmaktadır.

Sosyal ağların kişisel ve kurumsal tehditlerini azaltabilmek için alınması gereken önlemler arasında, sosyal ağlarda kişisel bilgilerin korunması için kullanıcıların bilgi güvenliği farkındalığının artırılması, korumaya dayalı sosyal ağ modelleri geliştirilmesi, sosyal paylaşım sitelerinin uygulama katmanı güvenliğinin standartların ötesinde yeniden ele alınarak gerekli düzenlemelerin yapılması sayılabilir. “Devlet sırrı” niteliğindeki

bilgilerin korunabilmesi için kamu kurumlarının ve kamu görevlilerinin bu alandaki bilgi birikimlerini artırmaları da büyük önem taşımaktadır. Kişi ve kurumların tehdit ve tehlikeleri dikkate alarak öncelikle kısa, orta ve uzun vadeli stratejilerini belirlemeleri ve bu ortamları ona göre kullanmaları veya bilgilerini ona göre paylaşmaları şarttır. Sosyal ortamda bulundurdukları veya bulunduracakları bilgileri gözden geçirdikten sonra bu ortamlarda yayımlamalarının daha faydalı olacağı, konu hakkında bilgisi olmayan kurumların ise bu konuda danışmanlık almalarının daha faydalı olacağı değerlendirilebilir (Eren ve Aydın, 2014).

4.2.9.8 Ortam Dinlemesiyle ya da Bilişim Sistemlerine Girilerek Dinleme

Telekulak veya yasadışı dinleme olarak Türkçe ye geçen telephone tapping ya da wiretapping üçüncü şahıslar tarafından internet ve telefon görüşmelerinin gizli metodlarla dinlenmesi ve kaydedilmesidir. Bu yasal yollarla yapıldığı zaman adı yasal dinleme olmaktadır.

Bir ağ veya kanal üzerinden iletilen verinin, kötü niyetli üçüncü kişiler tarafından araya girilerek alınmasıdır. Bu saldırı tipinde, hatta kaynaktan hedefe giden verinin arada elde edilip, değiştirilerek hedefe gönderilmesi bile mümkündür. İngilizce "eavesdropping" (saçak damlası) olarak adlandırılan bu saldırının, sanıldığının aksine çok farklı uygulama alanı bulunmaktadır. Hiç bir bilgisayarla etkileşimi olmayan tek başına çalışan bir bilgisayar bile, mikroçip, ekran veya yazıcı gibi elektronik parçalarından yayılan elektrik veya elektromanyetik yayılım takip edilerek gizlice dinlenebilir. Bu cihazların bu tür dinlemelere olanak vermemesi için, Amerikan hükümeti 1950'li yılların ortasından başlayarak TEMPEST adında bir standart geliştirmiştir (Canbek ve Sağıroğlu,2007).

Tarih boyunca, insanlar özel görüşmeler yaptıkça muhakkak kişisel merakından ya da farklı maksatlarla bu özel görüşmeleri dinlemeye çalışan birileri olmuştur. Salon ya da oturma odalarındaki gizli konuşmalar binanın dışında saçakların altında gizlice dinlendiğinden, saçakdamlası olarak tabir edilen eavesdropper lar konuşulanları dinleyen kişilerdir. Günümüzde salon dinlemelerinin yerini teknolojik imkânları kullanarak telefon,

internet ve ortam dinlemeri saçakdamlalarının yerini aldı. Bunları yapanlarda konunun uzmanları çoğu zamanda ajanlar olmuştur.

Kimi zaman birbirleri hakkında istihbarat toplamak için ülkeler çapında, kimi zaman siyasi emeller için ülkenin politik alanında kimi zaman da şantaj yapmak için insanlar birbirlerini dinlemişlerdir.

Yakın tarihte bilinen en büyük dinleme skandallarından olan Watergate Skandalı, 1974 yılında Richard Nixon'un ABD tarihinde başkanlıktan istifa eden ilk başkan olmasına sebep olmuştur. 17 Haziran 1972'de 5 hırsızın Washington DC'deki Watergate adlı binaya girerken yakalanmasıyla ortaya çıkan bu skandalla, Başkan Nixon'un Demokratları dinlemek için mikrofonlar yerleştirdiği belirlenince halkın desteğini kaybederek 1974 yılında istifasıyla sonuçlanmıştır.

Son yıllarda gündem yaratan olaylara neden olan gizli kamera kayıtları, ortam dinlemesi ve telefon dinleme olaylarında genellikle ev veya ofis eşyalarının tercih edildiği ortaya çıkmıştır. En çok elektrik prizi, oda spreyi, hediye çiçekler, duvar saati, resim tabloları, kalemlik, mouse, klavye, hoparlör, masanın altına yerleştirilen micro ortam dinleme cihazı ve benzeri ürünler ortam dinlemesinde ve gizli kamera kayıtlarında kullanılmaktadır.

Ortam dinlemeleri GSM bazlı, RF bazlı, Lazerli, Çanak antenli şekilde yapılmaktadır. Bu tür dinlemelere engel olabilmek için GSM Sinyal Kesici Jammerlar ya da Full Band Jammer ların kullanılması yeterli olmaktadır.

4.2.9.9 Sosyal Mühendislik Kullanılarak Bilgi Sızdırma & Gafil Muhbir

Sosyal mühendislik insanların zaaflarından faydalanıp istenilen bilgi ya da veriyi elde etme sanatı olarak tanımlanır. Diğer bir tanımda, normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanmaktadır. Sosyal mühendisler teknolojiyi kullanarak ya da kullanmadan bilgi edinmek için insanların zaaflarından faydalanıp, en çok etkileme ve ikna yöntemlerini kullanmaktadırlar.

“Yalnızca iki şey sonsuzdur, evren ve insanoğlunun aptallığı, aslında evrenin sonsuzluğundan da o kadar emin değilim.” diyen Albert Einstein insanın zaafından faydalanılarak her şeyin elde edilebileceğini ima etmiştir.

Bilgisayar sistemlerinde karşılaşılan güvenlik ile ilgili birçok olay, insan faktörünün kasten veya bilerek devreye girmesiyle meydana gelmektedir. Bilgisayar güvenliğinde sosyal mühendislik, bir bilgisayar korsanının, ilgilendiği bilgisayar sistemini kullanan veya yöneten meşru kullanıcılar üzerinde psikolojik ve sosyal numaralar kullanarak, sisteme erişmek için gerekli bilgiyi elde etme tekniklerine verilen genel addır. Özellikle telefon ile kullanıcı ve şifre bilgilerini elde etme, buna en tipik örnektir. Korsan sıradan bir şirket kullanıcısı gibi sistem yöneticilerinden bu tür bilgileri edinebilir. Bu konuda birçok taktik düşünülebilir ve tüm bu taktiklerden yara almadan çıkmak için yapılması gereken en önemli şey; kullanıcıların düzenli olarak eğitilmesi ve sistem yöneticileri dâhil tüm kullanıcıların istisnasız güvenlik politikalarını uygulamasıdır (Barwinski, 2005).

Kurumlardan sızan bilgilerin büyük bir çoğunluğunun bilgisayarlar vasıtasıyla sisteme sızılarak elde edildiği düşünülmektedir. Oysaki gerçekte hiç de bu işler düşünüldüğü gibi bilgisayar vasıtasıyla yapılmamaktadır. Sosyal mühendislik dediğimiz yöntemlerle kurum için can alıcı bilgiler bilgisayar kullanılmadan elde edilebilmektedir.

Bu kadar öneme haiz bir konunun kurum yöneticileri tarafından göz ardı edilmemesi gerekmektedir. Personelin sosyal mühendislik konusunda bilinçlendirilmesi büyük önem taşımaktadır. Şirket yöneticileri sosyal mühendislik yöntemiyle yapılabilecek saldırılara karşı çalışanları eğitmelidirler. Yöneticiler bu konuda profesyonellere başvurarak personelin bu konuda bilgilendirilmesini sağlayabilirler.

Sosyal mühendislikte kullanılan ilginç yöntemler, risk alanı, korsanın uyguladığı taktik ve bunlara karşı mücadelede yapılması gerekenler Granger tarafından Tablo 3’de listelenmektedir. Listeden de görülebileceği gibi sosyal mühendislik, bir bilgisayar kullanıcısını, bilgisayarını kullanırken arkasından hissettirmeden gözetlemekten, iş yerinde

kâğıt atıkları arasında işe yarar belge aramaya kadar, akla gelmeyecek çeşitli yöntemleri kullanmaktadır.

Tablo 3: Yaygın Sosyal Mühendislik Taktikleri ve Önlemler

Risk Alanı	Korsan Taktiği	Mücadele Stratejisi
Telefon (Yardım Masası)	Taklit ve inandırma	Çalışanların ve yardım masasının telefonla hiç bir şekilde şifre veya diğer gizli bilgilerin verilmemesi için eğitilmesi
Binaya giriş	Yetkisiz fiziksel erişim	Sıkı kimlik kartı güvenliği, çalışanların eğitilmesi ve güvenlik görevlilerin çalıştırılması
Ofis	Omuz sörfü (Klavye ile yazı yazarken çevredeki birinin sizi gözetlemesi)	Sizden başka birinin ortamda bulunduğu durumlarda şifrenizi girmeyin. Zaruri durumlarda hızlı bir şekilde tuşlara basınız.
Telefon (Yardım Masası)	Yardım masası aramalarında taklit etme	Bütün çalışanlara yardım masası desteği alabilmesi için tekil bir PIN numarası atanması.
Ofis	Kimsenin olmadığı açık odalar bulabilmek için koridorlarda dolaşma	Bütün misafirlere işyerinden bir refakatçi sağlanması
Posta odası	Sahte notların sokulması	Posta odasını kilitle ve izlemeye tabi tut
Makine odası – Santral	Erişmeye teşebbüs, cihazların kaldırılması ve gizli bilgileri elde edebilmek için bir protokol analizcisi eklenmesi	Santral, sunucu odaları v.s. her zaman kilitli tut ve cihazların güncel envanterini tut
Telefon ve PBX	Telefon görüşme ücreti erişimi çalma	Şehirlerarası, milletlerarası ve cep telefonu aramalarını kontrol et, konuşmaları izle, aktarmaları reddet
İş yeri atık deposu (dumpster)	Çöplük karıştırma	Bütün çöp kutularını güvenli ve izlenen alanlarda tut. Önemli belgeleri kesme makinesiyle yok et, manyetik ortamdaki verileri sil.
İntranet - İnternet	Şifre araklamak için İntranet veya İnternet üzerinde sahte yazılımların oluşturulması ve konulması	Sistem ve ağ değişikliklerinden sürekli haberdar olma, şifre kullanımı eğitimi
Ofis	Hassas belgelerin çalınması	Belgelere gizlilik derecesi ver ve bu belgeleri kilitli yerlerde sakla
Genel - Psikolojik	Taklit ve ikna	Bütün çalışanları sürekli uyanık tutarak ve eğitim programlarına tabi tutarak bilinçlendirme

Kaynak: Granger S., Social Engineering Fundamentals, Part I: Hacker Tactics, SecurityFocus Infocus, Article No: 1527. 2001.

Sosyal Mühendislerin kurumlardan bilgi elde etmek için kullandıkları insan profilinde ilk sırada gafil muhbirler gelir. Şirket ya da kuruma ait bilgileri olur olmadık yerde konuşan gafil muhbirlere hemen her yerde rastlanılabilir. Gafil muhbirler, aslında bunu yaparken kötü bir şey yaptıklarını, şirket ya da kuruma ait bir güvenlik ihlaline neden olduklarını düşünmezler. Bu nedenle, bir şirket ya da kurum hakkında elde edilmek

istenilen bilgilerin bir kısmı şirket ya da kurum çalışanı ile irtibata geçilerek, onların güveni ve sempatisi kazanılarak yapılmaktadır.

Phishing, sosyal mühendislikte en çok kullanılan yöntemlerden bir tanesidir. Bu yöntem, internet üzerinde genellikle e-posta yoluyla kullanılan, saldırgan tarafından kurbana güvenilir ya da doğruluğu sorgulanamaz bir kaynaktan gönderilen özel kodlar ya da program parçalarını kullanarak kurbana ait özel bilgilerin elde edilmesidir. Örnek: Saldırgan öncelikle kurbanın internet bankacılığını kullandığı bankayı tespit eder. Daha sonra o bankanın internet bankacılığı giriş arayüzü ile oturum açtıktan sonraki diğer sayfaların kodlarını tamamen kendisinin kontrolünde olan bir web sunucu üzerinde taklit eder. Daha sonra kurbana, kendi kontrolündeki bankanın internet bankacılığı web arayüzünün kodlarını "internet bankacılığı bilgilerinizi güncelleyiniz" isimli bir e-posta ile gönderir ve e-posta açıldığında kurbanın internet bankacılığını kullandığı bankanın giriş sayfası ekrana gelir. Oysa ekrana gelen sayfa saldırganın kontrolündeki web sunucudaki sayfadır ve kurbanın bundan sonra girdiği tüm bilgiler saldırganın web sunucusu üzerine kaydedilir. Saldırgan bu bilgileri kullanarak kurbana ait banka hesabını boşaltabilir.

Türkçeye kimlik avı, internet sazanı avlama ve yemleme olarak giren phishing, kimlik hırsızlığı (identity theft) adı verilen banka hesap numaraları, kredi kartı numaraları gibi kişisel bilgilerin, banka gibi resmi bir kurumdan gerçekten gönderilen resmi bir mesaj gibi gözüken e-postalarla kişilerden elde edilmesidir. Sosyal mühendisliğin bir uygulama alanı olan bu tür sahte e-postalarını alan kişi, istenilen gizli bilgileri göndererek, bu bilgilerin kötü niyetli üçüncü şahısların eline geçmesine ve akabinde oluşabilecek zararlara maruz kalınmasına neden olacaktır.

Önümüzdeki yıllarda çok yüksek teknik bilgiler üzerine kurulu saldırılardan ziyade bilgi güvenliği bilincine haiz olmayan kişilerin kandırılması sonucunda ortaya çıkan güvenlik açıklarının saldırganlar tarafından ustaca kullanılacağı tahmin dilmektedir. Literatürde yaşanan önemli olaylardan görüleceği üzere kurumsal bilgi güvenliğinin üst seviyede sağlanabilmesi için bilgi güvenliğinin devamlılık gerektiren bir süreç olduğu ve

bu sürecin kurumsal bilgi güvenliği standartları çerçevesinde yönetilmesi gerektiği unutulmamalıdır. Sazan avlama saldırılarıyla kullanıcıların kandırılmasını önlemenin yegâne yolunun kurumsal bilgi güvenliği yönetim sistemleri çatısı altında yapılacak olan eğitim ve bilinçlendirme çalışmalarının olduğu unutulmamalıdır (Vural ve Sağıroğlu,2008).

Gelmiş geçmiş en büyük hacker olarak kabul edilen Kevin Mitnick, Sosyal Mühendislik tanımıyla bütünleşmiştir. 1995 te FBI tarafından yakalanmıştır. Fujitsu, Motorola, Nokia ve Sun Microsystems gibi şirketlerin bilgisayar ağlarına izinsiz girmekten suçlu bulunarak 5 yıl hapis cezası almıştır. Şu anda dünya çapında pek çok firmaya güvenlik danışmanlığı yapan Kevin Mitnick, sızmış olduğu sistemlerin çok büyük kısmına Sosyal Mühendislik kullanarak sızmış bulunmaktadır. Kullandığı en sık yöntemin hedef kişiyle dost olmak, hedef kurumdan teknik destek talebi almak ve kendisini olmayan birisi gibi göstermek (özellikle bir şeylere kızmış üstleri gibi konuşup onlardan bilgi almak) olduğunu ifade etmektedir.

4.2.9.10 Whistleblowing Yönetimi

Kurum menfaati veya bireysel çıkarlar yerine kamu ve toplum yararına bilgi sızdırma olarak tanımlanan Whistleblowing in literatürde karşılığı ‘düdük çalma’ olarak geçiyor. Kimsenin farkına varmadığı bir yanlışı işaret etme olarak tanımlanabilir. Daha çok devlet kurumlarında çalışırken bilgisi dâhiline girmiş ciddi bir yanlışı ortaya çıkaran kişi de Whistleblower denir yani düdük çalıcıdır.

Irak’ta görevli Amerikalı asker Bradley Manning ile Avusturyalı gazeteci Julian Assange işbirliği ile Wikileaks olayının, Edward Snowden’in NSA den elde ettiği gizli belgeleri tüm dünyaya yayınlamasının temelinde whistleblowing vardır. Sonuçları yayınlanan kurum ve ülke için felaket olsa da ortaya saçılan belge ve bilgilerden tüm dünya memnun kalıp ona göre tedbirlerini almaya çalışmaktadır. Böyle olunca whistleblower çoğuna göre Kahraman ilan edilirken, kurum ve zarar verdiği ülke için Vatan Haini ilan edilebilmektedir.

Whistleblowing Türkçe'de tam karşılığı bulunmayan bir kavramdır. Kelimenin karşılığı bir faul olduğunda çalınan bir düdükle oyunun durdurulması; ya da, bir suç işlendiğinde polisin düdük çalarak halkın dikkatini çekmeye çalışmasıdır. Kavram özellikle Anglo-Sakson literatüründe "ortak bir yanlış olduğunda kamuoyuna başvurmak" anlamında kullanılmaktadır (Aydın, 2002-2003, 81).

Whistleblowing, örgütte yer alan bilgi veya veriye erişim hakkı bulunan bir kişi tarafından gerçekleştirilen ve bu kişinin haksızlığı düzeltme potansiyeli olan örgüt dışındaki bir kişi veya kuruma, herhangi bir zorunluluk olmaksızın, bilerek örgütün kontrolü altında olan veya örgütü içeren, gerçek/şüpheli/öngörülen bir haksızlık veya azımsanamayacak bir hukuka aykırılık ile ilgili kayıtlara geçirilecek bir ifşa etme (açığa çıkarma) davranışında bulunmasıdır (Jubb, 1999, 78).

Diğer bir deyişle whistleblowing, bir örgüt içerisindeki yanlış davranışların örgüt içindeki veya dışındaki kişilere rapor edilmesidir (Eaton-Akers, 2007, 67). Bir başka tanıma göre ise whistleblowing, şimdiki ya da daha önceki örgüt üyelerinin, örgüt liderlerinin kontrol alanı içerisinde gerçekleştirdikleri illegal, gayri-etik veya meşru olmayan faaliyetlerini; bunu düzeltmek için harekete geçmeye istekli ve yeterli kişi ya da kurumlara rapor etmektir (Keenan, 2007, 85).

Çalıştığı kurumdaki yanlış, etik olmayan ve yasalara aykırı olduğu düşünülen olumsuz davranışların herhangi bir kişisel menfaat gözetmeksizin, olası istenmeyen sonuçlarını önlemek maksadı ile tespit edilen yanlışlıkları örgüt içindeki veya dışındaki ilgili ve yetkili kişilere iletilmesi şeklinde tanımlanan whistleblowing kurumun onarılması güç problemlerle baş başa kalmasına sebep olabilir.

Ahlaki olmayan davranışların duyurulması (Whistleblowing);

* İddia edilen bir suçu (sahtekârlık, hırsızlık vb.), ayrımcılığı (ırk, din, milliyet, cinsiyet vb.),

* Bir yasaya, bir düzenlemeye, bir devlet politikasına, ahlaki değerlere, etik kurallara veya terbiyeye aykırı oluşumu,

* Özellikle de toplumun sağlığını ve güvenliğini tehlikeye sokan durumları, açığa çıkartmak ya da şikayet etmek amacıyla yapılan, bir kamu kuruluşundaki ya da özel sektördeki bir kişiyle, kurumla veya örgütle yapılan sözlü veya yazılı iletişimdir (Gerçek, 2005:30).

Rothwell ve Boldwing (2006), işletmelerde arkadaşlık ve takım ikliminin olmasının whistleblowing yapma düzeyini azalttığı sonucuna ulaşmışlardır.

Normatif etik açısından, bireyler örgütsel yaşam içinde hem birbirlerinin hem de örgütün çıkarlarının yanı sıra, en üst düzeyde kamusal yararı da göz önünde bulundurmalı ve örgüt içinde tüm bu tarafların yararına uygun olacak şekilde genel ahlak kurallarına uygun davranmalıdır. Böyle bir durumda, whistleblowing sürecine gerek kalmayacaktır. Eğer normatif etiğe aykırı bir durum gerçekleşir ve haksız ya da etik dışı bir durum yaşanırsa, bu durumda söz konusu ortamda bulunan ve olayı gözlemleyen kişiler bunun düzeltilmesi için ilgililere başvurmalıdır (Özler ve diğ.,2010).

Kurumda görülen her hatanın anında kurum dışına şikâyet edilmesi ne etik ne de ahlaki kurallara uygun bir davranış olacaktır. Bu konuda bir süreci takip etmek daha akıllıca olacaktır.

Whistleblowing sürecinde yer alan aşamaları aşağıdaki şekilde sıralamak mümkündür (Trevino-Nelson, 2004, 80-83):

• İlk olarak ilgili yöneticiye başvurmak,

• Ailenizle bu konuyu tartışmak,

• İlgili yöneticinin soruna duyarsız kalması sonucu diğer kademedekilerle ilişkiye geçmek,

• Örgütünüzdeki etikle ilgili görevli ya da ombudsman (örgüt içinde yasa-dışı ve/veya etik dışı iddiaları soruşturacak ve raporlayacak büro) ile ilişki kurmak,

• Örgüt dışında ilgililerle iletişime geçmeyi düşünmek,

• Örgüt dışındaki ilgili herhangi bir kişiye ya da kuruma başvurmak ve işten ayrılmak.

Whistleblower'lığa konu olan eylemler; gereksiz zarar verme, insan haklarını ihlal, yasal olmayan işlemler, örgütsel amaçlara aykırılık gibi nedenlerle ve tamamen etik amaçlarla ilgili olmalıdır. Yoksa birilerine zarar vererek bundan kişisel fayda temin etmek şeklinde yapılan bir bilgilendirmenin halk arasında ispiyonculuk olarak adlandırılan davranıştan bir farkı kalmayacaktır. Whistleblowing sonucunda etik olmayan durum ya da eylemin ortadan kalkacağına emin olunmalıdır. Aksi halde etkili olmayacağı bilindiği halde kamuyu, kendisini ve ailesini zarara sokmanın bir anlamı kalmayacaktır (Arslan, 2001, 103-104).

Kurumun yanlış uygulamalarından rahatsız olan kişinin öncelikle kurum içindeki ilgili kişi ile görüşmesi buradan bir netice alınmadığı zaman kurum dışına yönelmesi gerekmektedir.

Sadakatsizliğin etik olmayan bir davranış olduğu düşünüldüğünde sadakat mi yoksa yanlışları görmezden gelmemek ve bildirmek mi daha etiktir? Gerçekten bu noktada çözülmesi güç bazı çelişkiler karşımıza çıkmaktadır. Örgütte yanlış birtakım uygulamalara şahit olan bir birey bunu ilgililere bildirdiğinde mi daha etik davranmaktadır? Yoksa bildirmediğinde mi? Ya da yanlış bir uygulamayı bildirdiğimizde mi vicdanımız daha çok rahat eder? Arkadaşımızın bir yanlışını görmezden geldiğimizde mi? Vicdani olarak rahat olmak mı, psikolojik olarak arkadaşımıza karşı suçluluk duygusuna kapılmamak mı? Aslında cevaplanması gereken temel sorulardan belki de en önemlileri bunlardır. Bunun yanında etik ilkelerin evrenselliğinin sorgulanması da işin içine girdiğinde olay tam bir çıkmaza girmektedir. Kişilere, örgütlere ve toplumlara göre etik kuralların değişebilmesi

örgütlerde karşılaşılan etiğe uygun olmayan whistleblower'lığa konu olabilecek yanlış uygulamalarında değişebileceğini göstermektedir. Yani bir kişiye göre iş, çalışma, meslek ve işletmecilik etiğine aykırı olduğu düşünülen bir davranış bir başka kişi açısından etik olarak ya da nötr bir şekilde değerlendirilebilecektir (Özler, Şahin ve Atalay, 2010).

Ahlaki olmayan davranışların duyurulması (whistleblowing), etik-dışı olay, davranış ve faaliyetlerin, gerekli önlemlerin alınması amacıyla gerek işletme içi, yeterli gelmediği takdirde de işletme dışına bildirilmesi şeklinde tanımlanabilir. Uygunsuzluğun ortadan kaldırılması ya da minimize edilmesi için yapılan bu ifşa (açığa çıkarma) eylemi, vicdani bir faaliyet olarak nitelendirilebilir. Etik/yasa-dışı davranışlara şahit olan örgüt çalışanlarının, kamu yararını düşünerek yukarıda belirtilen paragraflardaki olumsuz örnek olayları engellemeye çalışmak amacıyla ifşada bulunması konunun özünü oluşturmaktadır (Sayğan ve Bedük, 2013).

İnsanın içinde yer aldığı gruptaki bazı kişilerin aleyhine olacka bir davranışta bulunması kolay değildir. Yapılan iş istenildiği kadar hukuka ve toplum menfaatine aykırı olsun, ihbarcılar genel olarak hoş karşılanmaz, 'ispiyoncu', 'jurnalci', 'ajan', 'gammaz' gibi hakaretamiz ifadelerle anılır, tecrit ve işten çıkarılma tehdidi ile karşılaşırlar. Bu baskı karşısında insanlar susup kalınca da toplumsal zararı büyük olan birçok olayın ortaya çıkması çok mümkün olmaz. Topluma verilecek zararlara engel olunması adına bu tür olayların ortaya çıkması isteniyorsa, insanların gördükleri yanlışlıklar karşısında susup kalmak yerine, karşı gelme konusunda cesaretlendirilmesi gerekir (Doğru, 2010).

"Ahlaki olmayan davranışların duyurulması" (whistleblowing), her ne kadar gerçekleştirilmesi zor bir davranış olsa da, gerçeklerin ortaya çıkması, suçlu olmayanların zarar görmemesi ve kamu yararının sağlanması açısından oldukça önem arz eden bir olgudur. Gönüllü olarak yerine getirilen bir davranış olan ifşa etme eylemi, yolsuzlukların ve haksız kazançların önlenmesi ve insan sağlığının zarar görmemesi açısından mühimdir (Sayğan ve Bedük, 2013).

İşletmeler örgüt çıkarı veya bireysel çıkarlar yerine kamu yararını gözetmekle yükümlüdürler. Kurumlarda şikâyet ve ihbar mekanizmasının tam olarak işlememesi; neleri, kime hangi süreci takip ederek bildirileceği, bu noktada örgüt içinde muhatap alınacak kişi ya da tarafların kim ya da kimler olduğunu tam olarak bilememe çalışan her bir bireyi potansiyel whistleblower yapar.

Kurumda çalışan personelin kurumdaki yanlış uygulamaları ve tespit etmiş oldukları olumsuzluklarla karşılaştıklarında izlemesi gereken yol ve yöntemlerin neler olduğu personel tarafından bilinmelidir. Bu konuyla ilgili verilen eğitimlerde personel işini kaybetme gibi tehditlerle korkutulmamalı, yanlış uygulamalarını kurum içindeki ilgili personele bildirildiğinde bu konuda gerekli eylemlere girişileceğine personel inandırmalıdır.

4.2.10 Kurumdan Ayrılan Personelin Bilgi Güvenliği Konusundaki Dikkatsizliği

Personelin emeklilik, istifa, işten çıkarılma gibi nedenlerle, işten ayrılma ve aylıksız izin, askerlik, doğum izni gibi uzun süreli işe ara vermelerde kurum personelinin sisteme erişim yetkilerinin dondurulması veya kaldırılması sağlanmalıdır. Personelin kurumdan ayrıldığında kuruma ait gizli bilgilerin ifşasının kendisi için hukuki bir sorumluluk getirdiği tebliğ edilmelidir.

İşten çıkma ya da çıkarılma olaylarının son zamanlarda arttığı günümüzde kuruma kızan eski çalışan tarafından gerçekleştirilen veri sızıntısı veya gelecekteki kariyer fırsatları için kurum verilerini beraberinde götüren personel kurum için tehlike arz etmektedir. Çalışanlara işlerine son verildiği bildirildiğinde sisteme erişim yekisi ve e-mail yetkisi kaldırılmadığından personel öfke ve kızgınlığını kurumdaki ticari sırları ya da kurum için önem arz eden bilgi ve belgeleri özel bir hesaba e-postayla yollayarak veya taşınabilir bir cihaza kopyalayarak ilerde kullanmak üzere yanına almaktadır. Çalışanların işine son verilmesinin veri güvenliğine etkisinin eski çalışanın müşteri listeleri ve çalışan kayıtlarının da dâhil olduğu kurumsal verileri almaya meyilli oldukları değerlendirilmektedir.

Kurumda mutsuz olup başka kurumlarda çalışmak isteyen personel rakip firmaların işine yarayacak bilgi ve belgeleri iş başvurularında sunmaya meyilli olduklarından bu belgelerin muhafazası için gerekli tedbirler alınmalıdır. Personelin işten çıkarılma bilgisi kendisine duyurulmadan önce e-posta ve sisteme erişim yetkilerinin kaldırılması ve CD, DVD ve USB kopyalama özelliklerinin kaldırılması kurumun menfaatine olacaktır.

4.2.11 Bilgi Güvenliğinin İşletmeler İçin Önemi ve Bowtie Modelinin Uygulanması

Gücün sembolü haline gelen bilgi, günümüzde işletmelere finansal kazanç ve itibar kazanmak gibi çok büyük fayda ve avantajlar sağlamaktadır. En önemli üretim faktörü olan bilginin, kurum içerisinde bilgi yönetiminin süreçleri olan elde edilmesi, saklanması, paylaşılması ve kullanımı aşamalarında gerekli güvenlik tedbirleri alınmadığında kurumu tehdit eden bazı sorunlar ortaya çıkacaktır. Küreselleşen dünyada bilim ve teknolojide yaşanan gelişmeler işletmelerin bilgi-iletişim teknolojilerinde yaşanan ilerlemeleri yakından takip etmelerini, dünya piyasalarında kalıcı ve güçlü bir pozisyon elde edebilmek için elektronik ticaret yöntemini uygulama zorunluluğu getirmiştir. İşletmelerin bilişim teknolojilerine bağımlı hale gelmesi bilgi güvenliği konusunu göz ardı edilmeyecek bir unsur haline getirmiştir.

Günümüzün gelişmiş bilişim teknolojileri, kişisel kullanıcılara ve işletmelere önemli faydalar sağlamasının yanında korsanlık yetkisiz erişim ve bilgi hırsızlığı gibi yasal ve etik olmayan faaliyetlerin ortaya çıkmasına ve yaygınlaşmasına da olanak sağlamıştır (Banerjee ve diğ.,1988).

Bilgi güvenliği, bilginin gizliliği, bilginin bütünlüğü ve bilginin erişilebilirliğine gelebilecek zararlardan korunulmasıdır. İşletmelerde bilgi güvenliğinin sağlanması, sadece bilişim uzmanlarını ilgilendiren teknik bir konu olmayıp, işletmede çalışan herkesin bilgi güvenliğinin sağlanmasında sorumluluğu bulunmaktadır (Johnson & Goetz, 2007). Bilgi güvenliğini tehlikeye sokan en önemli tehditler, sanıldığı gibi dışarıdan gelen saldırılar değil, çalışanların yanlış işlem ve davranışlarıdır (Thomson, Solms & Louw, 2006).

Çalışanların bilgi güvenliğinin önemine inanması ve bilgi güvenliği bilincine sahip olması, işletmelerde bilgi güvenliğinin sağlanmasında en önemli faktörlerdendir. Bilgi güvenliği ile ilgili tedbirlerin kullanılmaması, yanlış yorumlanması veya yanlış kullanılması güvenlik tedbirlerinin geçerliliğini kaybetmesine neden olmaktadır (Siponen, 2000). Maslow'un ihtiyaçlar hiyerarşisinde güvenlik gereksinimi, fizyolojik gereksinimlerden sonra ikinci sırada anılsa da bilgi güvenliği söz konusu olduğunda bu sıralamaya uyulduğu söylenemez. İnsanlar, bilgi güvenliği ihlalleri sonucu genelde hayati zararlarla karşılaşmasalar da karşılaşabilecekleri kimlik hırsızlığı, kişisel bilgilerinin çalınması, işletme sırlarının çalınması, bilgilerinin silinmesi, değiştirilmesi ve yetkisiz olarak kullanılması vb. sorunları öngöremeyebilmektedirler (Siponen, 2000).

Bilgi güvenliği ile ilgili çevresel-fiziki tedbirler ve bilişim teknolojileri konularında alınan tedbirlerin yanı sıra güvenlik zincirinin en zayıf halkası olan insan faktörü de göz önüne alınmalıdır. İşletmelerin bünyesinde bulundurduğu bilginin gizliliği, bütünlüğü ve ulaşılabilirliğine ilişkin güven ortamının tesis edilmesi sadece çalışanların katılımı ile değil, aynı zamanda müşteriler, iş ortakları ve hissedarlarla birlikte olması gerekir.

Bilgi güvenliğini sağlamak, teknolojik çözümlerle birlikte sağlam bir güvenlik yönetim sistemi ile olmalıdır. İşletmelerin güvenlik konusunda yapmış oldukları risk analizi kurumun bu konuda yaşayacağı riskleri yok etmek adına etkin ve başarılı bir yöntemdir. ISO 27001 başta olmak üzere, ilgili tüm bilgi güvenliği standartları ve yönetmeliklerinde, bilgi güvenliği risk analizi, ölçümü ve değerlendirmesi en öncelikli ve önemli aşamalardan birisi olarak kabul edilmektedir.

İşletmelerde riskleri belirleyip gerekli önlemlerin alınarak riski minimize etme yöntemlerinden olan balık kılçığı ve hata ağacı gibi modeller ürün tasarımı ve kalite hatalarının engellenmesinde aktif rol oynamıştır. Tüm kurum ve işletmeler için dizayn edilen bowtie modeli ile kurum ve işletmelerin hassas gizli bilgilerinin muhafazasının sağlanacağı daha önce yapılan akademik çalışmalarla desteklenerek bir diyagram haline getirilmiştir.

Bowtie modelinin, insanların ihtiyaçlarını karşılamak maksadıyla üretim faktörlerini şuurlu ve sistemli bir şekilde bir araya toplayarak işleyen ve işleten her iktisadi birim olan işletmelere uygulama aşamasında göz önünde bulundurulacak hususlar şu şekildedir:

İnsan kaynakları yönetiminin en önemli fonksiyonlarından birisi olan personel seçiminde bowtie modelindeki kriterler göz önüne alındığında, doğru işe doğru personelin alınmasına, liyakat sahibi personelin işletmeye dâhil edilmesine, işletmedeki entelektüel sermayenin artmasına ve düşük bir personel devir oranı ile işletmenin çalışmasına vesile olacaktır. Seçim sürecinin başarı ile yürütülmesi en uygun adayın işe alınmasına ve kişi-iş uyumunun gerçekleşmesine sebep olacaktır.

Ticari sırlar, müşteri özel bilgileri, finansal bilgiler gibi işletmeler için önem arz eden hassas bilgilerin istenmeyen kişi ya da rakip firmalara ulaşması işletmeyi maddi ve manevi zarara sokacağından bilgi güvenliğinin başlangıç noktası olan fiziki ve çevresel güvenlikte alınan tedbirler işletmedeki bilgilere ulaşmayı zorlaştıracaktır. Fiziki ve çevresel güvenliğin amacı kuruma yetkisiz erişimlerin engellenmesi ve bilgi varlıklarının hırsızlığa ve her türlü tehlikelere karşı korunup gerekli önlemlerin alınmasıdır.

Bilgi sızıntılarının büyük bir oranının bilinçsiz bir şekilde yapılmasından dolayı, İşletmede istihdam edilen personelin eğitilmesi önem arz etmektedir. Bilgi sızıntısı risklerini azaltmada yapılan araştırmalar eğitimin ilk planda geldiğini göstermektedir. Bilgi güvenliği konusunda çalışanların eğitimle bilinçlendirilmesi bu konudaki güvenlik açığını kapatacaktır.

İşletmelerden sızan bilginin büyük bir oranının iç tehditler tarafından ve bilinçsiz bir şekilde sızması işletmelerin bu konu ile ilgili tedbirler almasını zaruri hale getirmiştir. Bilgi eksikliğinden kaynaklanan insan hatalarını minimize edecek, teknolojinin yanlış kullanılma riskini azaltacak, bireylerin bilgi güvenliği tehditlerinden haberdar edecek bir bilgi güvenliği farkındalığı oluşturmak işletme için kritik bir öneme sahiptir. Bilgi güvenlik farkındalığı ile işletme yöneticisinden en alt kademede çalışanına kadar bilgi güvenliği bilinci oluşturularak, işletmenin ticari sırların neler olduğu, hangi bilgilerin korunması

gerektiği, bunların ne tür tehditlere karşı nasıl korunması gerektiği hususunda bilinçlendirme sağlanır. Bu farkındalık eğitimi ile personelin bilinçsiz hata yaparak işletmeden bilgi sızdırması oldukça zorlaşacaktır.

İşletmeler için çok büyük bir entelektüel bir sermaye olan insanın işletme içerisinde ihtiyaç ve beklentilerinin karşılanması personelden alınan verimi arttıracaktır. İşletmeler çalışanlarını kurum içerisinde mutlu ettiği ve beklentilerini yerine getirdiği müddetçe insan faktöründen endişe etmeyecektir. Yapılan araştırmalar işletmenin içerisinde örgütsel adaletin hakim olmasının, güvene dayalı bir ortamın tesis edilmesinin, yöneticilerle çalışanlar arasındaki sosyal bağların güçlü olmasının, kurumsal aidiyet duygusunun oluşmasının ve örgütsel kültürün oluşmasının çalışanların işletmeye karşı olumsuz tutum ve davranış içerisine girmemesine sebep olduğunu göstermektedir. Bu unsurların çalışanları kendilerine bir bütünün parçası gibi hissettirerek ve işletmede bir ekip ruhunun oluşmasını sağlamaktadır.

Cezaiyi müeyyidelerin suçun oluşmasına engel olması yönüyle çalışanların bilgi güvenliği konusundaki dikkatsizliklerinin ya da kasıtlı bilgi sızdırmalarının nelere mal olacağı tam olarak anlatılmalıdır. İşletmede çalışanların başka şirket veya kurum tarafından ele geçirilmesi o şirket için bir kâbus olan işletmenin ticari sırlarının neler olduğunu bilmesi bu konudaki umarsamazlığı ortadan kaldıracaktır. Bu sırlar genellikle işletmede muhafaza edilen projeler, know-how bilgileri, formüller, çalışanlar ve müşteriler hakkında özel bilgiler, muhasebe kayıtları, raporlar, teklifler, sözleşmeler, üretim teknikleri, pazarlama teknikleri ve tedarikçi kayıtları olabilmektedir.

Bilişim teknolojilerinin sağladığı fayda ve olanaklar işletmeleri bilişim teknolojilerine bağımlı hale getirdiğinden, bu konulara yapılan yatırımın artması bilgi sızıntı kanallarını kapatarak güvenli bir bilişim katmanında işletmenin faaliyetlerini sürdürmesine yardımcı olacaktır.

SONUÇ VE ÖNERİLER

Günümüzde gücün sembolü haline gelen ve medeniyetin yakıtı olarak tabir edilen bilgi, insan hayatını kolaylaştırdığı kadar kurumlar ve işletmeler açısından da rekabet avantajı sağlayan en önemli unsurlardan birisidir.

Bilginin değerli hale gelmesi kurum ve işletme içerisinde paylaşım kanallarının açık olması ve planlama ve karar verme aşamalarında etkin bir şekilde kullanım imkânı sağlayan doğru bir bilgi yönetim sistemi ile olabilmektedir. Etkin bir bilgi yönetimi kurum içerisinde bilginin artmasına, bilgi paylaşma kültürünün oluşmasına ve entelektüel sermayeden yararlanarak bilgi transferini teşvik etmeyi sağlamaktadır.

Bilgi Yönetimindeki aksaklıklar, kurum içerisindeki hassas ve gizli bilgilerin yetkisiz ellere geçmesine ve nihai sonuçların kurum için maddi hasar, prestij ve müşteri kaybı olabileceği görülmektedir. İşte burada Bilgi Güvenliği devreye girmektedir. Bilginin bir varlık olarak hasarlardan korunması ve istenmeyen kişiler tarafından elde edilmesini engellemek olarak tabir edilen Bilgi Güvenliği, doğru teknoloji ve eğitilmiş doğru personel sayesinde gerekli önlemlerin alınmasıyla bertaraf edilebilir.

Bilgi güvenliğinde meydana gelen zafiyet kimi zaman ülke başkanlarını koltuğundan ederken, kimi zaman ülkelerin ya da çok güvenilir kurumların prestijini alt üst ederken kimi zamanda ülkeler ve kurumlar için ağır maddi hasarlara yol açabilmektedir.

Yakın tarihte Julian Assange önderliğinde onbaşı Bradley Manning vasıtası ile Amerika'nın büyükelçiliklerle yapılan gizli yazışmaların ortaya saçılması, Amerika'nın birçok ülke ile diplomatik kriz yaşamasına yol açmıştır. Bunun yanı sıra kimileri tarafından gelmiş geçmiş en büyük bilgi sızıntısı olarak kabul edilen NSA sızıntısıda, Amerika'nın yıllardır sürdürdüğü gizli istihbarat yöntemlerinin tüm dünyaca bilinmesine neden olmuştur. Buna benzer sızıntıların ülkemizde de son dönemlerde oldukça yaygın olması bu konunun hem uluslararası hem de ulusal platformda önem arz ettiğinin bir göstergesi olmuştur.

Kurum, işletme ya da ülke için önem arz eden gizli-hassas bilgilerin yetkisiz ellere geçmesi olarak bilinen bilgi sızıntısı, 2013 Dünya Bilgi Sızıntı Raporu incelenerek konunun dünya genelinde ne denli önemli olduğu istatistiklerle ortaya konmuştur. Yayınlanan bu raporda dikkat çeken noktalar şunlardır;

Sızma vakalarının her geçen gün artığı, 2013 yılında tespit edilen sızma vakalarının 2006 yılından günümüze kadar hep artarak devam etmesinden anlaşılmaktadır.Sızma vakalarının en çok Amerika, Rusya, İngiltere ve Almanya'da meydana gelmesi yüksek teknolojinin sızmalar için yalnız başına bir önlem olmadığı, insan unsurunun güvenlik halkasındaki zincirin en zayıf halkası olduğu görülmüştür. Teknolojinin gelişmesiyle bilginin paylaşımı artmış ve sızıntıya engel olacak tedbirler alınmasına rağmen bu oranın arttığı tespit edilmiştir.

Basın ve medya raporlarına göre 2013 yılında kurum ve kuruluşların bilgi sızıntılarından dolayı hukuki sürecin işlemesi ve tazminat ödemelerinden dolayı 7,79 milyar dolar kurumların zarara uğratıldığı tespit edilmiştir.

Bilgi Sızıntısını gerçekleştirenlerin büyük bir çoğunluğunun istemeyerek/kazara bilgiyi sızdırdığı tespit edilmiştir. Yayınlanan bu rapora göre sızıntı kanalları; ekipman kaybı/hırsızlığı, mobil cihazlar, taşınabilir medya, ağ (tarayıcı, bulut bilişim), e-posta, basılı dokümanlar, anlık mesajlaşma (ses, metin veya video) ve tanımlanamayan olarak tespit edilmiştir.

InfoWatch Analytical Center ın yayınladığı rapor Bilgi Sızıntısının önemini gözler önüne sermiş fakat bu bilgi sızıntılarının önlenmesine yönelik alınması gereken tedbirler belirtilmemiştir. Grafiklerde bilinmeyen ya da tanımlanamayan olarak belirtilen oranların neler olduğu ulusal ve uluslararası yazın çalışması ile tespit edilmeye çalışılmıştır.

Kurum ve İşletmelerdeki hassas/gizli bilginin sızmasına neden olan faktörler şu başlıklar halinde oluşturulmuştur.

-İşe başlarken, personelin güvenilirliğinin yeterince tespit edilememesi,

-Fiziki ve çevresel güvenlik zaafiyeti

-Kurumda bilgi güvenliği farkındalığının oluşmaması

-Örgütsel sinizmin kurumda hakim olması

-Kurumsal aidiyetin oluşmaması

- Cezai müeyyidelerin bilinmemesi veya önemsenmemesi

-Bilişim teknoloji sisteminde zaafiyet

-Hassas bilginin muhafaza edilmesinde ve gönderilmesinde şifrelemenin kullanılmaması

-Bilgi sızıntı kanallarını kapatmamak

-Kurumdan ayrılan personelin bilgi güvenliği konusundaki dikkatsizliği

Kurum ve İşletmelerdeki hassas/gizli bilginin sızmasının kurum ve işletme için;

-Kurumun prestijini kaybetmesine

-Kurumun maddi hasara uğramasına

-İş devamlılığın aksamasına

-Veri kaybı ve iş kaybına

-Kişisel bilgilerin (kimlik, sağlık, adres, telefon, kredi kartı) çalınmasına sebep olabileceği değerlendirilmektedir.

Tespit edilen tüm bu çalışmalar bir risk analiz programı olan Bowtie modeli ile şekillendirilerek, bu modelde Bilgi Sızıntısına sebep olacak tüm faktörler ve alınması gereken tedbirler bariyerlerle gösterilmiştir.

Teknoloji kaynaklı bilgi sızıntı kanallarının neler olabileceği Şekil 10 da gösterilmiş ve alınması gereken tedbirler belirtilmiştir.

Alınan her türlü tedbire rağmen en zayıf halka olan insanın bilgi sızdırmaya meyilli olabileceği değerlendirilerek, teknolojiye yapılan yatırımdan daha fazlası entelektüel sermaye olan insana yapılmalıdır. Güvenilir insanın kurumdaki yeri 3 aşamada belirlenmiştir.

1'nci aşamada; Kuruma faydalı doğru ve güvenilir personelin alınması değişik test ve metodlar kullanılarak ve tarafsız bir şekilde olmalıdır.

2'nci aşamada; Kurumda çalışmaya başlayan personelin kurumundan tatmin olup, kurumuna zarar vermemesi; öncelikli olarak Bilgi Güvenliği farkındalığını eğitimle kazandırmak, cezai müeyyidelerle bir nevi personelin korkutularak sızma teşebbüslerini engellemek ve en önemlisi de personelin kurumundan tatmin olması için kurumsal aidiyetin oluşması, güvene dayalı bir iş ortamının tesisi ve kurumun örgütsel sinizmden uzak bir kurum haline gelmesi ile olacaktır.

3'ncü aşamada; Personelin kurumdan ayrılırken Bilgi Güvenliği konusunda göstermiş olduğu hassasiyetle insandan kaynaklanabilecek sızıntıların önüne geçilmiş olacaktır.

Alınan bütün tedbirlere rağmen insandan kaynaklanan sızıntılara engel olunamamasının diğer bir nedeni de kurum menfaati veya bireysel çıkarlar yerine kamu ve toplum yararının düşünülmesi kurumu zarara soksada toplumu kazançlı hale getirecektir. Vicdani bir faaliyet olarak nitelendirilen Whistleblowing, uygunsuzluğun ortadan kaldırılması ya da minimize edilmesi için bir ifşa eylemi olsa da bunun kurum için etik ve ahlaki kurallara uygun bir davranış şekli olmayacağı da bazı akademisyenler tarafından belirtilmektedir. Hem kurum hem de toplum menfaatini dengede tutacak hareket tarzının öncelikli olarak kurumda ilgili yöneticilerle görüşerek çözüm bulmak buradan bir netice elde edilemediği zaman örgüt dışına çıkmanın daha uygun olacağı değerlendirilmektedir.

Bowtie risk analiz modeli ile şekillendirilen, Bilgi Sızıntısına sebep olan faktörlerin Bilgi Yönetimi süreci kapsamında değerlendirildiğinde;

Bilginin elde edilmesi sürecinde; Kurum ve işletmeler kendi kurumlarında çalışanların deneyimleriyle ya da bilgi düzeyi yüksek ve güvenilir elemanları kendi kurumlarına transferiyle yeni bilgilerin kuruma kazandırılmasını sağlamaktadır. Kurumlarda örtülü bilgi olarak mevcut olan bilginin tüm kurum çalışanlarına kolektif bir şekilde yayılması kurumsal aidiyet ve güven duygusunun artması ile ortaya çıkarken, güvensizlik ve örgütsel sinizmde bunun ortaya çıkmasına engel olacaktır. Dış kaynaktan bilgi edinme yöntemi olan yeni personel temini ya da belli bir süreliğine kiralanması büyük güvensizlik ve risk içeren bir yöntemdir. Bu yöntemin bilimsel ve tarafsız metotlarla yapılması kurumumuza doğru personeli kazandıracağı gibi, kurum liderlerinin fikri yapılarına uygun ve görevin gerektirdiklerini yerine getirebilecek liyakatten uzak personelin seçilmesi de kurumumuzu maddi manevi zora sokacağı değerlendirilmektedir.

Bilginin saklanması; Kurumsal hafıza ya da Örgütsel Bellek, kurumların sahip oldukları geçmişten gelen bilgi, tecrübe ve deneyimlerin istenilen zamanda kullanılmak üzere saklanmasıdır. Kurumsal hafızanın ve yeni bilginin mevcut bilgi tabanında saklanması, bilgi kayıplarının önlenmesi ve bilginin ilgisiz ve yetkisiz kişilerce kullanımını mümkün olduğunca engellenmesi bu aşamada ki en önemli hedeflerimizdir. Bunun yanı

sıra bilgiye ulaşmak isteyen yetkili kişilerinde bu bilgiye kısa zamanda erişmesi saklanan bilginin değerlenmesine katkı sağlamaktadır. Bilgi sızıntı kanallarının kapatılması bilgi kayıplarının önlenmesinde büyük katkı sağlayacağı değerlendirilmektedir.

Bilginin paylaşılması; Kurumların yaşadıkları sorunlardan biri olan; çalışan personelin örtülü bilginin açık bilgiye dönüştürülerek düzenlenmesi ve kurum içerisinde çalışanların kullanımına sunulmasında yaşanan zorluklardır. Takım çalışması yapılması, kişilerarası diyaloglarla tecrübe ve deneyimlerin paylaşılması ve proje grupları bilgi paylaşımına büyük destek sağlayacağı öngörülmektedir.

Bilginin kullanılması; Kurum ve İşletme içerisinde üretilen, paylaşılan ve yapılandırılan bilgi kullanılmadıkça hiçbir işe yaramayacağından bilgi teknolojilerini kullanarak bunu elde edebiliriz. Bilginin etkin bir şekilde kullanımı işletmelere rekabet avantajı sağlayacağı öngörülmektedir.

Bowtie modelindeki tüm bariyerler dikkatli bir şekilde kurum ve işletmelerde uygulandığında;

- Kurum ve işletmelerdeki gizli ve hassas bilgiler güvenilir bir şekilde muhafaza edilir,
- Yöneticiler ve çalışanlar arasında karşılıklı güvene dayalı bir örgüt iklimi oluşturulur,
- İşe alım sürecinde, iş tanımında belirtilen gerekli güvenlik kriterlerine uygun olarak personel temini sağlanır,
- Bilgi Güvenliğinde zaafiyet oluşturabilecek her türlü fiziki ve çevresel etkenler ortadan kaldırılmış olur,
- Bilgi Güvenliği Farkındalığı yaratılarak Bilgi sızıntısına sebep olacak olan etmenler ortadan kaldırılır,

- Bilişim teknoloji sistemlerinde bilgi sızıntısına sebep olacak olan etmenler ortadan kaldırılır,

- Birey merkezli oluşabilecek her türlü güvenlik zaafiyetlerini önlemeye yönelik cezai müeyyide tanımları yapılmış olur,

- Böylelikle hassas/gizli bilginin sızması engellenerek kurumsal prestijin kaybedilmesinin, maddi hasara uğranılmasının, iş devamlılığının aksamasının, veri ve iş kaybının yaşanmasının önüne geçilerek verimliliğin arttırılması sağlanır.

- Bilgi Güvenliğine yönelik yapılan araştırmanın sonuçları irdelendiğinde süreçlerin daha çok savunmaya ve bilgi sızıntısını önlemeye yönelik olduğu görülmektedir.

- Kurumlar ve işletmeler tarafından vizyonlarına ve stratejik planlamalarına uygun olarak üretilecek ve elde edilecek önemli bilginin tasnifi ve değerlendirmesi yapılarak rekabet avantajı kapsamında tanımlanan hassas bilgiler için proaktif bir strateji oluşturulmalıdır.

KAYNAKÇA

Ackoff R.L. (1989). "*From Data to Wisdom*", Journal of Applied System Analysis, 1989, Vol.16, p:

Ahi, M. (2013). Digital Age, Nisan 2013

Aktan C. ve Vural İ.Y. (2005). "*Bilgi Çağı, Bilgi Yönetimi ve Bilgi Sistemleri*", Çizgi Kitabevi, Şubat 2005, 1. Baskı,

Alavi, M. (1997). "Knowledge Management and Knowledge Management Systems", December,http://www.rhsmith.umd.edu/is/malavi/icis–97KMS/sld018.htm, 12.05.2011.

Altun, A. ve Kovancı A (2004). "Personel Seçiminde Mülakat ve Mülakat Yöntemleri", Havacılık ve Uzay Teknolojileri Dergisi, Ocak 2004, Cilt 1, Sayı 3 (55-61).

Andersson, Lynee. M. "Employee Cynicism: An Examination Using A Contract Violation Framework", Human Relations, , 49:11, 1996, 1395-1418.

Arslan, M. (2001). *İş ve Meslek Ahlakı*, Ankara: Nobel Yayın Dağıtım.

Awad, E. ve Ghaziri, H. (2004). Knowledge Management. New Jersey: Prentice Hall Publishing.

Aydın, U. (2002-2003). İş Hukuku Açısından İşçinin Bilgi Uçurması (Whistleblowing), Sosyal Bilimler Dergisi, 79-100.

Banerjee, Debasish; Cronan, Timothy Paul&Jones, Thomas W. ‘‘Modeling IT Ethics-A Study in Situatioal Ethics’’,MIS Quarterly, 22:1, 1988,31-60.

Barutçugil, İ. (2002). Bilgi Yönetimi, İstanbul: Kariyer Yayıncılık, 2002.

Barwinski, M. A. (2005). Taxonomy of Spyware and Empirical Study of Network Drive-By-Downloads, Thesis, Naval Postgraduate School, Monterey, California, 37, September 2005.

Baykara M., DAŞ R. ve KARADOĞAN İ. (2013). Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi, 1st International Symposium on Digital Forensics and Security 20-21 May 2013

Bell, H. (2001). Measuring and Managing Knowledge. Singapore: McGraw-Hill Pub.

Bernerth Jeremy B. & Armenakis Achilles A. & Feild Hubert S. & Walker H. Jack. (2007). “Justice, cynicism, and Commitment A Study of Important Organizational Change Variables”, The Journal of Applied Behavioral Science, 43:3, September 2007, 303-326.

Bhattacharya, R., Devinney ve T. M. ve Pillutla, M. M. (1998), “A Formal Model of Trust Based on Outcomes.” Academy of Management Review, 23 (3), 459-472.
Bouville, M. (2008). Whistle-Blowing and Morality, Journal of Business Ethics, 81, 579-585.

Bunker,G. (2009). Data Leaks for dummies Guy Bunker, Gareth Fraser-King 2009 1.st edition

Cadoğlu, K., (2000). Risk Yonetimi ve TSK’daki Uygulamalar. Harp Akademileri Basım Evi, İstanbul, Turkiye.

Calder, A. ve Watkins, S. (2008). IT Governance A Manager’s Guide to Data Security and ISO27001/ISO 27002, 4th edition. Kogan Page Ltd., UK.

Canbek, G. ve Sağıroğlu Ş. (2007). Bilgisayar Sistemlerine yapılan saldırılar ve türleri, Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi 23, 2007

Canbek G. ve Ş. Sağıroğlu Ş. (2006). "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", Politeknik Dergisi, 9(3):69-72. S.165-174, 2006

Chambliss, William J. (1971), "The Deterrent Influence of Punishment" Theories of Punishment (ed. Stanley E. Grup), Bloomington: Indiana Univ. Press.

Chang, S.E. ve Lin C.S. (2007). "Exploring organisational security culture for information security management", Industrial Management & Data Systems, 107: 3, 2007, 438–458.

Davenport T.H. (1998). Prusak L.,Working Knowledge: Managing What Your Organisation Knows, Harvard Business School Pres, Boston,MA 1998

Davenport, Thomas H. ve Prusak L. (2001). İş Dünyasında Bilgi Yönetimi: Kuruluşlar Ellerindeki Bilgiyi Nasıl Yönetirler. (Çev. Günhan Günay). İstanbul: Rota Yayınları.

Dayıoğlu, B. (2002). "Ağ ve işletim sistemi güvenliği", Türkiye Bilişim Derneği 9. Bilgi İşlem Merkezi Yöneticileri Semineri (İMY9), Belek/Antalya, 2002.

Dean, James W.; Pamela B ve Dharwadkar R. (1998). "Organizational Cynicism", Academy of Management Review, 23(2), 341-352.

Dede, M.B, (2013). Technologic | 07 Ocak 2013, 2:27 http://yenisafak.com.tr/teknoloji-haber/bilgi-sizintisi-alarmi-07.01.2013-453059

Demirsoy, A. (1995). Son İmparatora Öğütler, 'Bilim Toplumu', Ankara

Dhillon, G., (2007). Principles of Information Systems Security. John Wiley & Sons Inc., USA.

Dinçer, Ö. ve Fidan, Y. (1996). İşletme Yönetimi, I. Baskı, Beta Yayın, İstanbul.

Duffy, J. (2001). "Knowledge Management And its Influence on the Records and Information, Manager', Information Management Journal, Praide Village, July

Doğru, H. (2010). Whistleblower hain mi erdemli kişi mi? – Halil DOĞRU-02.06.2010-Referans Gazetesi

Eaton, T. V. ve Akers, M. D. (2007). Whistleblowing and Good Governance, The CPA Journal, 77(6), 66-71.

Ehtiyar, R. ve Yanardağ M, (2008). Organizational Silence: A Survey On Employees Working in Chain Hotel, Tourism and Hospitality Management, 14(1), 51-68.

Eisinger, Robert M. (2000). "Questioning Cynicism", Society, 37:5, 2000, 55-60.

Eren V. ve Aydın A. (2014). Sosyal Medyanın Kamuoyu Oluşturmadaki Rolü ve Muhtemel Riskler ISSN:2147-7833, KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi 16 (Özel Sayı 1): 197-205,2014

Fox B. (2012). Cloud computing a "game-changer" for EU economy

Gabarro, J.J. (1978), "The Development of Trust, Influence, and Expectations", (Eds.) A.G.Athos ve J.J. Gabarro, Interpersonal Behavior Communication an Understanding in Relationship içinde, New Jersey: Prentice Hall Inc., 290-303.

Gelbstein, E., Kurbalija, J., Baldi, ve S., Hacktivism (2003). Cyber-Terrorism and Cyberwar, the Activities of the Uncivil Society in Cyberspace, Diplo Foundation

Gerçek, H. (2005). Mühendislikte Etik Sorunların Ele Verilmesi. Madencilik Dergisi, 44 (4), 29-38.

Gibbons, Don C. (1987). Society, Crime, And Criminal Behavior, Englewoods Cliffs: Prentice- Hall.

Gibbs, Jack P. (1975). Crime, Punishment, and Deterrence, Social Science Quarterly, 48.

Gordon Peter, (2007). Data Leakage-Threats and Mitigation,

Granger S. (2001). Social Engineering Fundamentals, Part I: Hacker Tactics, SecurityFocus Infocus, Article No: 1527. 2001.

Gülmüş M. (2010). "Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği ", Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, 2010.

Jubb, P. B. (1999). Whistleblowing: A Restrictive Definition and Interpretation, Journal of Business Ethics, 21(1), 77-94.

Hagan, J. (1985). Modern Criminology: Crime, Criminal Behavior, And Its Control, USA: McGraw-Hill Pub.

Hannah David R. (2006). Keeping Trade Secrets Secret- Magazine: Spring 2006 Opinion & Analysis April 01, 2006

Hauschild, S., W. Stein ve T. Licht, (2001). "Creating a Knowledge Culture", The Mckinsey Quartely, Number 1, pp. 74–81.

Henkoğlu T., Külcü Ö. (2012). Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir inceleme, Bilgi Dünyası, 2013, 14 (1) 62-86

Hosmer, L.T. (1995), "Trust: the Connecting Link Between Organizational Theory and Philosophical Ethics", Academy of Management Review, 20 (2), 379- 403.

Isaca, Cisa Review Manual (2009). Isaca Press, Rolling Meadows, 2009

ISO/IEC, (2005). ISO/IEC 27001:2005. International Organization for Standardization, Geneva, Switzerland.

İşçi, E.(2010). Kuruma Güven Kavramı 8 Ekim 2010

Johnson, M. E. ve Goetz, E. (2007). "Embedding Information Security into the Organization", IEEE Security & Privacy, May/June 2007, 16–24.

Jones, A. ve Ashenden, D. (2005). Risk Management for Computer -Security, First Edition: Protecting Your Network & Information Assets, Elsevier, 2005.

Kalman, S. (2003). "Web Security Field Guide", Cisco Press, Indianapolis, sf.36, 37, 2003.

Kalseth, K. ve Cummings, S. (2001). "Knowledge Management: Development Strategy or Business Strategy?", Information Development, V.17, N.3, pp.163–172.

Karaarslan, E., Teke A. ve Şengonca H.(2003) Bilgisayar Ağlarında Güvenlik Politkalarının Uygulanması, İletişim Günleri 2003

Karaarslan E. (2002). "Network Cihazlarının ve Sistemlerinin Güvenliği", inet-tr 2002 Konferansı

Keenan, J. P. (2007). Comparing Chinese and American Managers on Whistleblowing, Employ Respons Rights, 19, 85-94.

Khatibi V, Khatibi E. (2012). Issues on Cloud Computing: A Systematic Review, International Conference on Computational Techniques and Mobile Computing (ICCTMC'2012) December 14-15, 2012 Singapore, pages 212-216

Kılıç, S. (2006). Bilgi Yönetiminde Liderliğin Rolü Üzerine Bir Araştırma. Yükseklisans Tezi. Niğde. Niğde Üniversitesi Sosyal Bilimler Enstitüsü.

Kıngır, S.(2006). İsletme becerileri grup çalısması. İstanbul: Türkmen

Kitteringham G. (2008). Crisp Report Lost Laptops-Lost Data

Köseoğlu MA, Gider Ö. ve Ocak S. (2011). ''Bilgi Paylaşımı Tutumunu Etkileyen Faktörler Nelerdir? Bir Kamu Hastanesi Örneği' Eskişehir Osmangazi Üniversitesi İİBF Dergisi, 6(1), 215-243

Kudat, B.(2007). "Kötü adamların hızına yetişen daha güvenli", BThaber, 604:15, 2007.

Kutaniş R.Ö. ve Çetinel E. (2010). "Adaletsizlik Algısı Sinisizmi Tetikler mi?: Bir Örnek Olay", Dumlupınar Üniversitesi Sosyal Bilimler Dergisi, 1:26, Nisan 2010, 186-195.

Liska, Allen E. (1987), Perspectives on Deviance, USA: Prentice-Hall.

Malhotra, Y. (2000). Knowledge Management and New Organization Forms: A Framework for Business Model Innovation. Knowledge Management and Virtual Organizations. USA: Idea Group Publishing, 2-19.

Mayer, R. C., ve Davis, J. H. (1999), "The Effect of The Performance Appraisal System on Trust For Management: A Field Quasi-Experiment", Journal of Applied Psychology, 84,123–136.

Mayfield, A. (2010). What is Social Media, iCrossing, e-book, s. 6. Erişim Tarihi: 02.02.2010.

Miller, C. (2009). Data Leakage for Dummies, Sophos Special Edition by Lawrence, CISSP

Mitnick, K. D., (2005). Aldatma Sanatı. ODTU Yayıncılık, Ankara, Turkiye.

Moffett, J. (1990). Network security management. Security and Networks, IEE Colloquium on , 4- 6

Montano, B. (2004). "Innovations of Knowledge Management", IRM Press, 2004, s: 302,

Nonaka, I. (2004). The Knowledge –Cretaing Company. Hitotsubashi on Knowledge Management. Singapore: John Wiley&Sons Pub.

Nonaka,I. ve Takeuchi, H. (1995). The Knowledge Creating Company. Newyork: Oxford University Press.

Onwubiko, C. ve Lenaghan A.P. (2007)., "Managing Security Threats and Vulnerabilities for Small to Medium Enterprises", 2007 IEEE International Conference on

Intelligence and Security Informatics, New Brunswick, NJ, A.B.D., 23-24 May 2007, 244-249.

Oğuz, B. (2010). Çatlaktan Sızıntılar- -TMMOB Elektrik Mühendisleri Odası Ankara Şubesi Haber 2010/6

Öğün M.N. ve Kaya A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler, Güvenlik Stratejileri Dergisi, Yıl 2013, Cilt 9, Sayı 18

Özgener, Ş. (2002). "Global Ölçekte Değer Yaratan Bilgi Yönetimi Stratejileri", 1.Ulusal Bilgi, Ekonomi ve Yönetim Kongresi, Mayıs.

Özgener, Ş,, Öğüt A. ve Kaplan M. (2008). "İşgören-İşveren İlişkilerinde Yeni Bir Paradigma: Örgütsel Sinizm", İçinde Özdevecioğlu, M. ve Karadal, H., (Ed.) Örgütsel Davranışta Seçme Konular: Organizasyonların Karanlık Yönleri ve Verimlilik Azaltıcı Davranışlar, Ankara: İlke Yayınevi, 2008, 53-72.

Özler D., Atalay C. ve Şahin M. (2010). Örgütlerde Sinizm Güvensizlikle mi Bulaşır? Organizasyon ve Yönetim Bilimleri Dergisi Cilt 2, Sayı 2, 2010

Özler D., Atalay C. ve Şahin M. (2010). Teorik bir çerçevede Whistleblowing Etik İlişkisi, Aralık 2010- Cilt 11 Sayı 2

Perez, M. P., A. Sanches, M. P. Carnicer ve M J. V.Jimenez, (2002). "Knowledge tasks and teleworking: a taxomony model of feasibility adoption", Journal of Knowledge Management, V. 6, N. 3, pp.272-284.

Pfleeger, C.P. (1997). The fundamentals of information security. Software, IEEE ,14 (1,14)

Plunkett, P. T. (2001). "Managing Knowledge&Work: An Overview of Knowledge Management", Knowledge Management Working Group of the Federal Chief lnformation Officers Council, August.

Probst, G. J. B., Raub, S., & Romhardt, K. (2006). Wissen managen: Wie Unternehmen ihre wertvollste Ressource optimal nutzen (5th ed.). Wiesbaden: Gabler.n

Rost, J., Glass, R. L., (2011). The Dark Side of Software Engineering, Evil on Computing Projects. IEEE Computer Society, John Wiley & Sons, Inc.,Hoboken, New Jersey, USA.

Rothwell, G. R., Baldwin, N. J. (2006). Ethical Climate Theory, Whistle-blowing, and the Code of Silence in Police Agencies in the State of Georgia, Journal of Business Ethics, 70, 341-361.

Rotter, J. B. (1971). "Generalized Expectancies for Interpersonal Trust", American Psychologist, 44,

Ruiu D (2006). Learning from Information Security History. IEEE Security & Privacy 4 (1):77-79

Rusli A, Selamat H. ve diğ.. (2005). A Framework for Knowledge Management System Implementation in Collaborative Environment for Higher Learning

Sağıroğlu Ş. ve Alkan Mustafa, (2005). Her Yönüyle Elektronik İmza, Grafiker Yayınları, Ankara

Sayğan, S. ve Bedük, A, (2013). Ahlaki olmayan Davranışların Duyurulması (Whistleblowing) ve Etik İklimi İlişkisi Üzerine Bir Uygulama

Sena, J. A. ve A.B. (Rami) Shani, (1999). "Intellectual Capital and Knowledge Creation : Towards an Alternative Framework", Knowledge Management Handbook, Edited by Jay Liebowitz, CRC Press, Washt., D. C.

Sevim, A., Altıner H, Ünek O.S ve Şam M. (2013). Kurumsal Yapılarda Bilişim Güvenliği TEMPEST Problemi

Shabtai, A., Y.Elovic ve L.Rokach (2012). A Survey of Data Leakage Detection and Prevention Solutions, 2012

Siponen, Mikko T. (2000). "A conceptual foundation for organizational information security awareness", Information Management & Computer Security. 8/1, 2000, 31–41.

Şahinaslan E., Kantürk A, Şahinaslan Ö. ve Borandağ E. (2009). Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri Akademik Bilişim '09 – XI. Akademik Bilişim Konferansı Bildirileri

Tiwana, Amrit. (2003). Bilginin Yönetimi. (Çev. Elif Özsayar). İstanbul: Dışbank.

Trevino, K. L., Nelson, A. K. (2004). Managing Business Ethics, America:John Wiley & Sons.

Tschannen-Moran, M. ve Hoy, W.K. (2000). "A Multidisciplinary Analysis of the Nature, Meaning and Measurement of Trust", Review of Educational Research, 70 (4), 547-593

Vural, V. ve Sağıroğlu Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları üzerine bir inceleme, 2008, Gazi Üniv.Müh.Mim.Fak.Der. Cilt 23, No 2

Yelboğa Atilla (2008). Örgütlerde Personel Seçimi Ve Psikolojik Testler Journal of Social Sciences, 5(2), December 2008

Yerlikaya T., Ercan Buluş ve Nusret Buluş (2006). Akademik Bilişim Konferansları, 2006 Kripto Algoritmalarının Gelişimi ve Önemi

Yılmaz, M. (2009). Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi 49,1

Zaim H. (2005). " Bilginin Artan Önemi ve Bilgi Yönetimi", İşaret Yayınları 2005, s.67

Zand, D.E. (1972). 'Trust and Managerial Problem Solving' Administrative Science Qarterly, 17, 229-239