T.C.

GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ

SOSYAL BİLİMLER ENSTİTÜSÜ

TELEKOMÜNİKASYON SEKTÖRÜNDE FİRMA İÇİNDEKİ BİLGİ GÜVENLİĞİNİ ETKİLEYEN FAKTÖRLER VE BU FAKTÖRLERİN ÇALIŞANLAR ÜZERİNE ETKİLERİ

ÇİĞDEM YILDIZ

YÜKSEK LİSANS

STRATEJİ BİLİMİ ANABİLİM DALI

DANIŞMANI

DOÇ. DR. SALİH ZEKİ İMAMOĞLU

GEBZE 2009

T.C.

GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ

SOSYAL BİLİMLER ENSTİTÜSÜ

TELEKOMÜNİKASYON SEKTÖRÜNDE FİRMA İÇİNDEKİ BİLGİ GÜVENLİĞİNİ ETKİLEYEN FAKTÖRLER VE BU FAKTÖRLERİN ÇALIŞANLAR ÜZERİNE ETKİLERİ

ÇİĞDEM YILDIZ

YÜKSEK LİSANS

STRATEJİ BİLİMİ ANABİLİM DALI

DANIŞMANI

DOÇ. DR. SALİH ZEKİ İMAMOĞLU

GEBZE 2009

ÖZET

TEZİN BAŞLIĞI: Telekomünikasyon Sektöründe Firma İçindeki Bilgi Güvenliğini Etkileyen Faktörler ve Bu Faktörlerin Çalışanlar Üzerine Etkileri

YAZAR ADI: Çiğdem YILDIZ

Şirketlerde bilgi ve ağ güvenliği konusunda yaşanan problemlerin artışı ve şirketlerin gelir kalemlerinin denetim firmaları tarafından çeşitli uyumluluk süreçleri doğrultusunda denetlenmeye başlamaları, pek çok kurumun önemli miktarlarda kaynağı bilgi ve ağ güvenliğine ayırmaya başlamasına neden olmuş ve şirketlerde bilgi ve ağ güvenliği ekiplerinin varlığı, oluşturdukları prosedürler çalışanlar üzerinde gün geçtikçe etkisini daha çok hissettirmeye başlamıştır.

Bilgi güvenliği ancak kurum içinde belirlenen prosedürlere uyum ile sağlanabilmektedir. Bu prosedürlerin kurum politikasına uygun olarak oluşturulması ve çalışanların prosedürlere uyumunu sağlamak ise Bilgi Güvenliği'nin sağlanmasındaki en önemli unsurlardandır. Bu tez çalışması ile Telekomünikasyon Sektöründe Bilgi Güvenliği'ne kurum içinde uyumu etkileyen faktörleri bazı ana başlıklar altında belirleyerek bu faktörlerin çalışanlara etkileri tespit edilmeye çalışılmıştır. Telekomünikasyon Sektöründe faaliyetlerini sürdüren firmalarda anket yöntemi ile Bilgi Güvenliğini Etkileyen Faktörler ve çalışanlar üzerinde etkilerini inceledik.

Anahtar Kelimeler: Bilgi Güvenliği, Bilgi Güvenliği Kavramları, Bilgi Güvenliği Denetimleri, Telekomünikasyon Sektörü, Bilgi Güvenliğini Etkileyen Faktörler, SOX, ISO 27001, BGYS

SUMMARY

TITLE OF THE THESIS: The Factors that Affect the Information Security within the Company and the Effects of These Factors on Employees in Telecommunication sector.

AUTHOR: Çiğdem YILDIZ

Increase in the problems about information and network security and start of the auditing in accordance with various compliance processes by the audit firms caused many organizations to start to reserve for significant amounts for information and network security. This case, caused an increase in the procedures that are developed by the control of information and network security team,consequently by the day passed the effects of internal information security rules began to be felt on workers more and more.

Information security, can only be achieved by accordance with the procedures identified by appropriate team within the organization. This procedure's creation in accordance with the institutions policy and ensuring employees to comply with procedures is the most important element in providing the Information Security. In this thesis the factors affecting accordance incorporation to the Telecommunications Sector Information Security are specified under main sections, however the effects of these factors on employees were tried to be determined using survey methods.

Key Words: Information Security, Information Security Components, Information Security Audits, Telecommunication Sector, The Factors that Affect the Information Security , SOX, ISO 27001, ISMS

TEŞEKKÜRLER

Yüksek Lisans çalışmam boyunca benden desteğini esirgemeyen aileme, çalışma arkadaşlarıma, anket çalışmasının tamamlanabilmesi için değerli vaktini ayırarak anketi dolduran herkese ve çalışmalarım sırasında yardımlarını esirgemeyen arkadaşlarım; Özlem Tezgel, Görkem Gürel, Özlem Yılmaz, Eda Gençay ve Saime Aydın'a yardımları için çok teşekkür ederim.

Tez çalışmam süresinde bana yol gösteren ve anket sonuçlarının analizi konusunda destek olan danışman hocam Doç.Dr. Salih Zeki İmamoğlu başta olmak üzere derslerini aldığım tüm hocalarıma ayrıca teşekkür ederim.

İÇİNDEKİLER DİZİNİ

SİMGELER VE KISALTMALAR DİZİNİ

BG :Bilgi Güvenliği

BGYS :Bilgi Güvenliği Yönetim Sistemi

ISMS :Information Security Management System

BT :Bilgi Teknolojileri

IT :Information Techologies

BS :Bilgi Sistemleri

PUKO :Planla – Uygula- Kontrol Et- Önlem Al

UEKAE :Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

BTK :Bilgi Teknolojileri ve İletişim Kurumu

ISO :Uluslararası Standartlar Örgütü

BTK :Bilgi Teknolojileri ve İletişim Kurumu

SOX :Sarbanes Oxley Act

COBIT :Control Objectives for Information and Related Technology

CIO :Chief Information Officer

SEC :Amerikan Serbest Piyasa Kurulu

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

1. GİRİŞ

Peter Drucker “Kapitalist Ötesi Toplum” adlı kitabında günümüz dünyasını şu şekilde açıklanmaktadır: Yaşamakta olduğumuz bilgi toplumunda, merkez olan kişidir. Bilgi, para gibi kişinin dışında olan bir şey değildir. Bilgi bir kitabın, bir veri bankasının, bir yazılım programının içinde bulunan ve orada kalan bir şey de değildir. Oradakiler yalnızca enformasyondur. Bilgi her zaman insanın içindedir, bir insan tarafından öğrenilir ve öğretilir, doğru ya da yanlış kullanılır. Böyle olunca bilgi toplumuna geçiş kişiyi merkeze yerleştirmektedir. Bu da ortaya, bilgi toplumunun temsilcisi "eğitimli insan"la ilgili olarak yeni zorluklar, yeni sorunlar, eski ve yeni, ama örneğine rastlanmamış sorular çıkarmaktadır (Drucker, 1994).

Drucker'a göre, bilgi toplumunun çekirdeğinde “eğitimli kişi” kavramının yatması zorunludur. Bunun evrensel bir kavram olması da zorunludur; çünkü günümüz toplumu bir bilgi toplumudur, globaldir. Hem parasında, hem ekonomisinde, hem mesleklerinde, hem teknolojisinde, hem ana sorunlarında, hepsinden çok da enformasyonunda globaldir (Drucker, 1994).

Bu çalışmanın amaçlarının daha iyi anlaşılması için, bilgisayar tabanlı enformasyon sistemleri güvenliğinin tarihi üzerine kısa bir tarihi özet yapmamız faydalı olacaktır. 1960'ların başlarında kriptografik algoritmalar ve güvenli işletim sistemleri üzerinde çalışmalar yapılmaya başlandı. Takip eden yıllarda 1980'lerin ortaları ile beraber sektörün odağını kriptografik protokollere kaydıran bilgisayar haberleşmelerine sızılma olaylarının olduğu bir dönem başladı. Üçüncü dönem ise 90'ların ortalarında internetin yaygınlaşması ile mevcut enformasyon sistemlerinin günümüzdeki ağ odaklı-internet merkezli daha iyi enformasyon sistemlerine dönüşümü ile gerçekleşti (Prusak and Thomas, 2000, 3).

İçinde bulunduğumuz son dönemde iş süreçleri, enformasyon teknolojisi (IT) ile çalışanlar arasındaki güçlü ve birbirinin içine geçmiş yapıdan dolayı bilgi güvenliği kurumlar içinde belirgin bir biçimde ön plana çıktı. Güvenlik ile ilgili konular ayrıca uluslararası standartlar ile de tanımlandı. Bu alandaki temel standart

BS7799'dur. Uluslararası Standartlar Organizasyonu ISO tarafından 2000 yılında ISO27001 olarak duyurulmuştur ve günümüzde ISO27002 hali ile uygulanmaktadır. Günümüzde artık enformasyon sistemleri güvenliği sadece bir teknoloji ve organizasyon problemi değil aynı zamanda yasal süreçler, ilişkilerdeki bağımlılıklar ve diğer başlıklardan oluşan bir konu olarak düşünülmektedir.

Bu çalışma dört bölümden oluşmaktadır. Birinci bölümde bilişim çağında bilgi güvenliğinin önemini ortaya koymak için bilgi yönetimi literatüründe farklı perspektiflerden veri, enformasyon ve bilgi kavramları açıklanmıştır. Bilgi kavramının öneminin aktarılmasının ardından bilgi yönetimi bölümüne geçilerek literatür çalışması ile oluşturulan Bilgi Yönetimi kavramı ve bu kavramın önemi açıklanmıştır.

İkinci bölümde öncelikle bilgi güvenliği tanımları ve bilgi güvenliği kavramları olan Gizlilik, Bütünlük ve Kullanılabilirlik konuları incelenmiş ve bilgi güvenliğinin kurum için neden gerekli olduğu açıklanmıştır. Bilgi güvenliği kavramları içinde olan Gizlilik kavramının Telekomünikasyon kurumunun yayınladığı yönetmelik kullanılarak kurum için önemi vurgulanmıştır. Bilgi Güvenliği kavramının açıklanmasının ardından bilgi güvenliğini etkileyen faktörler incelenmiş, bu faktörlerin çalışanlar üzerine etkilerinin anlaşılabilmesi için anket çalışması yapılmıştır. Bilgi Güvenliğini etkileyen faktörler İnsan, Süreç, Teknik, Telekomünikasyon sektöründe Bilgi Güvenliği Yönetimi ve Denetimi için Standartlar, Yasalar ve Düzenlemeler, Yaptırımlar ve Cezalar ile Sosyal Baskı ana başlıkları altında incelenmiştir. Birinci faktör olarak belirlenen İnsan faktörü detaylı olarak incelenmiş ve öncelikle İnsan faktörünün yönetiminin kurum içinde bilgi güvenliğinin sağlanabilmesi için önemi bu başlık altında anlatılmıştır. Ayrıca İnsan faktörü başlığı altında Üst Yönetim, Bilgi ve Ağ Güvenliği Yöneticisi, Bölüm ve Takım Yöneticileri, İç Denetim Ekibi, Bilgi ve Ağ Güvenliği Bölümü, Son Kullanıcı Güvenlik Bilinci, Son Kullanıcı Bilgi Güvenliği Eğitimleri, Bireysel İçgüdü ve Farkındalık alt faktörleri ve bu faktörlerin Bilgi Güvenliğine etkileri incelenmiştir. Süreç faktörü altında ise özelikle kurum içinde bilgi güvenliği süreçlerinin tanımlanması ve regülasyonlar açısından çok önemli olan Bilgi Güvenliği Yönetim Sistemi-BGYS kavramı incelenmiştir. Ek olarak bu başlık altında BGYS süreçlerinin

kurum içinde gerekliliği, kuruluşu, gerçekleştirilmesi, işletilmesi, izlenmesi gözden geçirilmesi, sürekliliğinin sağlanması ve iyileştirilmesi konuları açıklanmıştır. Yine kurum için çok önemli olan ve belirlenmiş süreçler ile uygulanması gereken Risk Yönetimi konusu da Süreç faktörü altında incelenerek ve bu faktörün bilgi güvenliğine etkisi incelenmiştir. Telekomünikasyon sektöründe Bilgi Güvenliği Yönetimi ve Denetimi için Standartlar, Yasalar ve Düzenlemeler faktörü altında ise ISO 27001, ISO 27002, PCI, 5651 ve SOX konuları açıklanmış ve bu konuların bilgi güvenliğine etkisi incelenmiştir.

Üçüncü bölümde Telekomünikasyon Sektöründe Bilgi Güvenliğini Etkileyen Faktörler ve Bu Faktörlerin Çalışanlar Üzerine Etkilerini belirlemek amacıyla yapılan uygulama aşaması yer almaktadır. Bu aşamada anket yöntemi kullanılarak Telekomünikasyon sektörü çalışanları ile anket çalışması yapılmıştır. Bu çalışma sonucunda elde edilen veriler faktör analizi, regresyon ve korelasyon analizleri kullanılarak değerlendirilmiştir. Son bölümde ise sonuçlar değerlendirilmiştir.

2. BİLGİ KAVRAMI VE BİLGİ YÖNETİMİ

2.1. Temel Kavramlar

Bilgi yönetimi alanında bilgi için verilen, kabul edilen tanımların ortaya konmasından önce bilgi yönetimi kavramı içinde açıklayıcı olacak veri ve enformasyon kavramlarının incelenmesinde fayda vardır. Bilgi yönetiminde bilgi, veri ve enformasyondan farklı olarak değerlendirilmektedir.

2.1.1. Veri ve Enformasyon Kavramları

Veri, ham sonuçlar, toplu sonuçlar ve sayılar, olaylar hakkındaki birbirinden ayrı, nesnel gerçekler şeklinde tanımlanabilir. Bir başka tanım ise, yapılan işlemlerin belli biçimlerde tutulmuş kayıtlarıdır. Verilerin, tek başlarına başka olaylara ilişkileri kurulamaz ve kendi içlerinde bir amaçları yoktur (Ağır, 2008, 4).

Veri, olaylara ilişkin nesnel gerçekler olup birbirleriyle ilişkilendirilmemiştir. Veri kurumsal amaçlara bağlı olarak işlemlerin yapılandırılmamış bir biçimde kaydedilmesidir. Modern kurumlarda veri, teknolojik sistemlerde saklanır. Veri, özümlenmemiş ve yorumlanmamış gözlemler, işlenmemiş gerçekler olarak tanımlanabilir. Çoğu kez bir anlamı içeriği yoktur. Örneğin, 710 x 370 A41 bir datadır ancak birçok kişi için hiçbir şey ifade etmez (Barutçugil, 2002, 57). Günümüzde veri, bir çok organizasyonda sıklıkla kullanır. Bazı organizasyonlar için ise veri diğerlerine göre çok daha fazla önemlidir. Örneğin, bankalar, sigorta şirketleri gibi (Ağır, 2008, 4).

Veri içinde değerlendirme, yorum yoktur ve karar verme açısından güvenilecek salt bir temel oluşturamazlar. Kendisinin önemi yada işe yarayıp yaramayacağı hakkında bir fikir vermezler (Davenport and Prusak, 1998, 23).

Bir diğer kavram enformasyon ise düzenlenmiş, biçimlendirilmiş veridir ve literatürdeki yaygın tanımı, belli bir bağlam içinde veriye bir anlam oluşturmaktır.

Düzenleme başkaları tarafından yapılmıştır. Yalnızca ilgili kişi için bir anlam taşımaktadır. Örneğin, "9.15 -9.45 Paris- London AF201 18E" ifadesi, uçakla seyehat etmekte olan bir kişi için bir çok şey anlatabilir. Enformasyon, fark yaratan anlamlı, ilişkilere ve amaca sahip bir mesaj olarak da tanımlanmaktadır. Kısaca anlamlı biçimde derlenen ve birleştirilen veridir, bu anlamıyla bir kaynaktan iletilen mesajın içeriğidir (Ağır, 2008, 5; Barutçugil, 2002, 57).

Her mesajda olduğu gibi burada da bir gönderici, bir de alıcı vardır. Enformasyonun amacı alıcının bir konudaki düşüncelerini değiştirmek, değerlendirmesi ya da davranışı üzerinde bir etki yaratmaktır. Enformasyon alıcısını biçimlendirmek zorundadır; bakış açısında ya da anlayışında bir fark yaratır Alınan mesajın gerçek bir enformasyon niteliği taşıyıp taşımadığına, yani alıcıyı yeniden biçimlendirip biçimlendirmeyeceğine karar verecek olan alıcıdır. Birbiriyle ilgisiz dağınık ifadelerden oluşan bir kayıt onu kaleme alan tarafından 'enformasyon' gibi görülebilir ama alıcı için bir değeri yoktur (Davenport and Prusak, 1998, 24; Ağır, 2008, 4).

Bilgi kolayca ya da doğrudan tanımlanabilecek bir kavram değildir ve bilgiyi tanımlayabilmek için çeşitli disiplinlerden birçok girişim mevcuttur. Bell'e göre bilgi, sistematik formdaki çeşitli iletişim araçları yoluyla başkalarına iletilen akli bir yargı yada deneysel bir sonuç sunan fikir yada gerçeklerin düzenli ifadeler bütünüdür (Ağır, 2008, 8).

Verilerin önemli bir özelliği kendi baslarına bir anlam taşımamalarıdır. Veri sadece olup bitenlerin bir bölümünü açıklar. İçinde değerlendirme, yorum yoktur ve karar vermek açısından tek basına güvenilecek bir temel oluşturmaz, fakat karar vermeyi kolaylaştırabilir. Bütün bunlara rağmen veriler kuruluşların vazgeçilmez bir kaynağıdır. Tüm kurum ve kuruluşların verilere ihtiyacı olmakla birlikte bazı endüstriler özellikle verilere fazlasıyla bağımlı çalışmaktadırlar. Bankalar, sigorta şirketleri, kamu hizmeti veren kuruluşlar, sosyal güvenlik kurumları gibi. İşletmeler müşteriyle olan ilişkilerini geliştirmek için amaçlarına uygun veri kültürü oluşturmaktadırlar. Veri kültürünün temelinde müşterilere ait çeşitli verilerin belirli kayıtlar altında tutulması esası vardır. Karar vericiler, verileri enformasyon

oluşturmak veya geliştirmek için bir hammadde olarak ele alıp değerlendirmektedirler. Diğer taraftan yöneticiler, verilere dayalı olarak gerçeğe ulaşmayı hedeflemektedirler. Veri, herhangi bir problemin çözümünde ve herhangi konuda alınacak kararlarda anahtar rol oynar. Fakat problemin çözümünde ve kararların alınmasında sebep sonuç ilişkisi kurmamıza yardımcı olmaz. Verilerden hareketle elde edilecek sonuçları yorumlamak ve bu sonuçlara belli bir şeyler katmak tamamen bireylere aittir. Bu bağlamda sadece verileri olduğu gibi almak ve bunlar üzerinden hareket etmek istenilen sonucu vermez. Ancak verilerin, enformasyon ve bilgi için de temel olduğu unutulmamalıdır (Durna, 2008, 4).

2.1.2. Bilgi Kavramı

Kişisel anlamda düzenlenmiş enformasyondur. Özümlenmiştir. Öğrenme ve deneyim yoluyla kazanılmış olan önceki bilgilerle bütünleşmiştir. Kararlara ve davranışlara yol gösterir. Bilgi, insanların beynindedir ve tüm yaşam boyunca öğrendiklerinin ve deneyim yoluyla kazandıklarının toplamıdır. İnançlarımıza ve değerlerimize dayanmaktadır. İnsanlar arasında iletişim yoluyla enformasyon akışı bilginin yaratılmasını sağlar. Eğer, alınan enformasyon bir değer taşıyorsa onu alan kişinin var olan bilgi birikimi ile bütünleştirilir ve bilgi deposuna eklenir. Eğer bir değer taşımıyorsa reddedilir ve silinir (Barutçugil, 2002, 58).

Bilgi, veri ve enformasyondan daha karışık bir kavramdır ve "deneyim ve değerlere ilişkin enformasyonun akışkan bir karması" şeklinde bir tanımı yapılmaktadır. Diğer bir tanıma göre ise bilgi, enformasyon parçaları arasında kurulan yararlı ilişkidir. Bilgi, sadece kayıtlarda ve bilgi bankalarında değil kurumsal rutinlerde, süreçlerde, uygulama ve normlarda da içerilmiştir. Bazen sezgiseldir, sözlere dökülmesi her zaman mümkün olmayabilir. Enformasyon nasıl verilerden türetiliyorsa, bilgi de enformasyondan türetilir. Bu dönüşümde yaşanılan düşünce süreçleri şunlardır (Barutçugil, 2002, 58);

- **Karşılaştırma:** Herhangi bir duruma ilişkin enformasyon bildiğimiz başka durumlarla karşılaştırıldığında bu bize neyi gösteriyor?
- **Varılan sonuçlar:** Enformasyonun karar verme ve eyleme geçme konusunda bizi getirmiş olduğu son nokta nedir?

- **İlişkilendirmeler:** Bu bilgi kümesi diğer bilgi kümeleriyle nasıl ilişkilendirilir?
- **Sohbet:** Başkaları bu bilgiye ilişkin ne düşünmektedir?

Bu süreçlerin sentezi bizi bilgiye ulaştırır. Bilginin değerli olma nedeni veri ve enformasyondan farklı olarak eyleme daha yakın olmasıdır. Sahip olduğumuz bilginin sonucunda bir karar verebilmekte ve onu eyleme geçirebilmekteyiz.

Bilginin elde edilmesi çok uzun bir süreçtir. Veri ile başlar öğrenmenin en üst ve son ürünü olan akı ile biter. Enformasyon amacı olan veri olarak tanımlandığından, çalışanlar çok fazla enformasyona sahip olabilirler. Ancak, bu enformasyonları yaptıkları işe değer katarak, katma değer sağlayacak şekilde kullanabildikleri zaman, bilgi elde edildiği söylenebilir. Aksi halde çalışanların bilgili olduğu söylenmez. Yani bilgi enformasyonla uygulamanın birleşimidir. Veri'den bilgiye ve hatta bilginin bilgeliğe dönüşmesi yalnızca bir toplama işleminden ibaret değildir. Veriden enformasyona geçerken önemli olan veriler arasındaki ilişkilerin anlaşılmasıdır. Aralarından bir ilişki olmayan veriler enformasyon oluşturmazlar. Enformasyon, veriler arasındaki ilişkilerin ortaya çıkarılması olduğu için bu ilişkilerin arasında bir model vardır. Bu model, veriler arasındaki ilişkilerin birbiri ile ilişkilendirilmesi ve bir ilişki yumağı oluşturulması olarak görülebilir. Enformasyonun bilgiye geçiş süreci, aradaki bu modellerin anlaşılmasıdır. Model anlaşılıp, içeriği açıklandığında artık bilgi yapısı kazanır. Bilgi, yüksek derecede güven, inanılırlık ve tamlık içerir (Başaran, 2003, 6)

2.2. Bilgi Yönetimi

Yazının keşfi ile bilgi kayıtlara geçirilmiş, kitaplar yazılmış ve kütüphaneler oluşturulmuştur. M.Ö. 4000 yıllarında Sümer ve Akad saraylarında devletin, var olan ticaretin ve uygarlığın kayıtları tutulmuştur. M.Ö. 3. yy'da Mısır'daki Alexandria kütüphanesinde 500.000 den fazla el yazması kitap bulunmaktaydı. Bilginin sözlü ve yazılı olarak kaydedilmesi, saklanması, dağıtılması çalışmaları geleneksel bilgi yönetimi olarak görülebilir (Ağır, 2008, 2).

Yaklaşık 250 yıl önce bilginin anlamında bir değişim başlamış, zamanla bilgi artık aletlere, süreçlere ve ürünlere uygulanmaya başlamıştır (Drucker, 1994). 20. yy'ın ikinci yarısında yaşanan teknolojik gelişmeler öncelikle veri ve enformasyonun işlenmesine ve yayılmasına daha sonra da bilginin işlenmesine ve yayılmasına önemli katkılarda bulunmuşlardır.

Literatürde Bilgi Yönetimi'nin çok sayıda tanımı vardır. Tanımların çokluğu bilgi yönetimi alanında çalışanların yönetim, işletme, fen bilimleri, sosyoloji, strateji, üretim mühendisliği, psikoloji, gibi farklı alanlardan gelmelerinden kaynaklanmaktadır. Wiig bilgi yönetimini geniş anlamda şöyle tanımlamaktadır: Bilgi yönetimi, şirketin bilgi varlıklarıyla ilgilenme, yaratma ve onlardan faydalanmak için gereksinim duyulan tüm faaliyetler ve bakış açılarını, bunların şirketin iş ve işleme konularını desteklemedeki özel konumunu kapsamaktadır (Ağır, 2008, 7).

Von Krogh bilgi yönetimini bir organizasyonda rekabet için kolektif bilginin saptanması ve desteklenmesi olarak görmektedir. Tüm çalışanların rekabet için birlikte olmasını gerektiğini düşünmektedir (Von Krogh, 1998, 2).

Barutçugil, Bilgi Yönetimi kavramını bilgiyi yaratmak, elde tutmak, paylaşmak ve geliştirmek için kullanılacak yeni radikal yol olarak olarak tanımlamakta buna ek olarak bilgi yönetimini, örgütsel amaçların daha iyi bir şekilde elde edilebilmesi için bireylere, takımlara ve bütün organizasyona bilginin kollektif ve sistematik olarak yaratılması, paylaşılması ve uygulanması için olanak sağlayan yeni bir disiplin olarak değerlendirmektedir (Barutçugil, 2002, 59).

Bilgi Yönetimi Amerikan Üretkenlik ve Kalite Merkezi (APQC), Bilgi Yönetimini 'rekabetin geliştirilmesi için bilginin belirlenmesi, edinilmesi ve etin kılınması çabaları şeklinde tanımlamaktadır (McCampbeil et al, 1999). Daha geniş bir tanımlama ile Bilgi Yönetimi, organizasyonun; bilginin elde edilmesi, kişisel bilginin kurumsal bilgiye dönüştürülmesi, kişilerin kişilerle, kişilerin bilgiyle ve bilginin bilgiyle ilişkilendirilmesi, kaynakların yönetilmesi konusunda bilginin katkısının ölçülmesi konusunda gösterdiği çabaların toplamıdır (Başaran, 2003, 10)

Bilginin elde edilmesi sürecinin başlangıcı olarak, işletme öncelikle kendi içinde bilgi kavramının tanımını yapmak durumundadır. Genellikle, işletmeler edinmek istedikleri bilgilere geçmiş tecrübeleri ve yazılı dökümanları ile sahiptirler. Şirket arşivlerinde işlenmeyi ve kazanılmayı bekleyen büyük ölçüde bilgi kaynağı bulunmaktadır. Önemli olan, sahip oldukları bu bilgilerin ortaya çıkarılıp, kullanılabilir ve ulaşılabilir duruma getirilmesidir. İşletmeler bu bilgilerin kazanılması ve edinilmesi için Firma Çaplı Sistemleri (ERP : Enterprise Resource Planning) kullanabilmektedirler. (Başaran B. 2003, 10) Kişisel bilginin kurumsallaştırılması, örgüt içinde etkin bir bilginin paylaşılması kültürünün geliştirilmesi ile mümkün olmaktadır. Örgüt içi iletişim sistemleri, bilginin akışını sağlayarak, bilgiyi kurumsal olarak kullanılabilecek bir formata sokar.

Bilginin edinilmesi ve organize edilmesi aşamasını, bu bilginin doğru kişilere nasıl ulaştırılacağı sorusu takip eder. Bu aşama şu şekilde bir risk içermektedir. Bilginin, doğru kişilere ulaştırılabilmesi son derece önemlidir. Ancak, bilginin yanlış, kişilere ulaştırılması da buna ters olarak risk içermektedir. Bu şekilde değerli bilginin yanlış ve amacının dışında kullanılması gündeme gelebilir. Bu nedenle, bilginin kişilerle ilişkilendirilmesi dendiğinde, doğru bilginin, doğru zamanda, doğru kişilere ulaştırılması söz konusu edilmektedir (Başaran B. 2003, 11).

Çapar, bilgi yönetimi için organizasyonlarda amaçların gerçekleştirilmesini dikkate alan bir tanım yapmaktadır. Bu amaçları şu şekilde sıralamaktadır (Çapar, 2003, 4);

- Örgüt içerisinde yeni bilginin üretilmesi.
- Dış kaynaklardaki değerli bilginin örgüte kazandırılması.
- Örgütsel kararlarda ulaşılabilir bilginin kullanılması.
- Bilginin dokümanlar, veri tabanları ve yazılımlar aracılığı ile (yani mevcut örgütsel bilgi varlıkları ile) sunulması.
- Toplumsal kültür ve özendiricileri ile bilginin büyümesini kolaylaştırması (daha makro düzeyde).

- Örgütün birimleri içerisinde oluşan bilginin veya başka örgütlerdeki benzer birimlerin, birimler arası transferinin gerçekleştirilmesi.
- Örgütsel bilginin kıymetlendirilerek entelektüel sermayeye çevrilmesi ve bilgi yönetimi sayesinde ölçülmesi.

Veri, enformasyon ve bilgi, organizasyonlarını içinde ve dışında farklı yerlerde birikir. Bilgi yönetimi, organizasyonun bu bilgi varlıklarının yerini ve niteliğini belirleyerek elde edilmesi, geliştirilmesi ve kullanılması için yapılacak çalışmaları ifade eder. Bu, bir anlamda, organizasyonun sahip olduğu bilgi alanlarının kapsamını genişletmek ve bu alanlar arasındaki ilişkileri yoğunlaştırmaktır (Barutçugil, 2002, 59).

Bilgi, üretilen, yapılan, satılan ve satın alınan şeylerin asıl bileşeni haline gelmiş bulunmaktadır. Bilgi sanayi ve hizmetler sektöründe daha fazla kullanılmakta ve üretimde işgücü ve sermayeden daha önemli bir unsur haline gelmektedir. Bunun sonucu olarak bilgiyi yönetmek bireylerin, örgütlerin ve ülkelerin en önemli ekonomik görevi haline gelmektedir (Ağır, 2008, 10). Unutulmamalıdır ki, bilgi yönetimi; bilginin verimli bir şekilde teknolojik süreçlere uygulanmasının bir modele dönüşmesini ve örgüt amaçları doğrultusunda bilginin kullanılması için yapılması gereken hareket planıdır.

3. BİLGİ GÜVENLİĞİ VE BİLGİ GÜVENLİĞİNİ ETKİLEYEN FAKTÖRLER

3.1. Bilgi Güvenliği Tanımı

Bilgi güvenliği, bilgileri izinsiz erişimlerden, kullanımından, ifşa edilmesinden, yok edilmesinden, değiştirilmesinden veya hasar verilmesinden koruma işlemidir (http://tr.wikipedia.org). Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunması. Ek olarak, doğruluk, açıklanabilirlik, inkâr edememe ve güvenilirlik gibi diğer özellikleri de kapsar (ISO/IEC 27001, 2006, 8). ISO/IEC 27001 dökümanı Bilgi Güvenliği Olayını ise; "Olası bir bilgi güvenliği politikası açığı, koruyucuların başarısızlığı ya da güvenlikle ilgili olabilecek önceden bilinmeyen bir durumu belirten bir sistem, hizmet ya da ağ durumunun tanımlanan bir ortaya çıkışı" olarak tanımlamaktadır.

Bilgi güvenliği, kurumların bilgi envanterindeki varlıklarının gizliliğini, bütünlüğünü, erişilebilirliğini tehdit eden risklerin tanımlanıp, bu konuda risk yönetimi gereklerinin yapılmasıdır. Risk yönetimi kapsamında bilgilerin maruz kalabileceği tehditler bilgilerin önemine, tehlikenin olabilirliğine ve gerçekleştiğinde etkisine göre şu seçeneklerden biri tercih edilir (Yıldız, 2007, 4);

- Riskin azaltılması,
- Riskin kabul edilmesi,
- Tamamen üçüncü bir tarafa devredilmesi (sigorta etmek gibi)
- Risk kaynağının yok edilmesi seçeneklerinden biri tercih edilir.

Bilgi güvenliği, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür (Gürol ve Sağıroğlu, 2006, 168). Bilgi Güvenliğinin sağlanması için, uygun güvenlik politikası belirlenmeli ve mutlaka bu politika başarılı bir şekilde uygulanmalıdır. Politika oluşturma ilkeleri ilerideki bölümlerde daha derin anlatılacaktır fakat genel olarak

faaliyetlerin sorgulanması, erişimlerin izlenmesi, değişikliklerin kayıtlarının tutulup değerlendirilmesi, silme işlemlerinin sınırlandırılması gibi bazı temel güvenlik problemleri ile ilgili çözümleri içermelidir. Bilgi güvenliği daha genel anlamda, güvenlik konularını detaylı olarak ele alan "güvenlik mühendisliği'nin" bir alt alanı olarak görülmektedir.

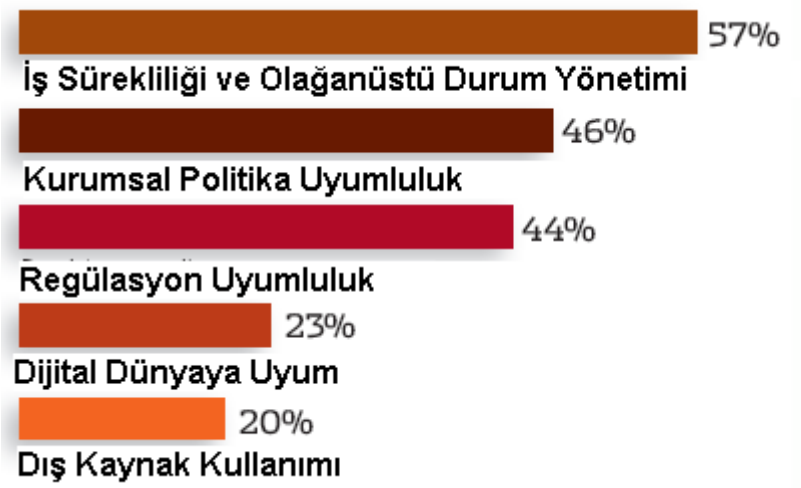
Günümüzde ticari şirketler ve devlet kurumları işlerini sürdürebilmek için yoğun bir şekilde bilgi kullanımına yönelmişlerdir. Zaman geçtikçe bilginin önemi artmış, sadece güvenli bir şekilde saklanması ve depolanması gelişen ihtiyaçlara cevap verememiş aynı zamanda büyüyen organizasyonlar ve duyulan ihtiyacın artması nedeniyle bilginin, bir yerden bir yere nakil edilmesi de kaçınılmaz bir ihtiyaç haline gelmiştir. Bilgiye olan bu bağımlılık bilginin içeriği bozulmadan korunması ve gerekli durumlarda ihtiyaç duyulan kadarının yetkili kullanıcılar tarafından kullanılması ihtiyacını gündeme getirmiştir. Bu anlamda bilgi, kurumun sahip olduğu varlıklar arasında çok önemli bir yere sahiptir. Bilgiye yönelik olası saldırılar, tahrip edilmesi, silinmesi, bütünlüğünün ve/veya gizliliğinin zarar görmesi, bilgi altyapısının bozulmasına ve bu da beraberinde işlerin ve bilgi akışının aksamasına neden olmaktadır. Bu nedenlerle; bilgi, kurumdaki diğer varlıklar gibi, kurum için önem taşıyan ve bu nedenle de en iyi şekilde korunması gereken en önemli varlıktır. Bilgi güvenliği de; kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin geniş çaplı tehditlerden korunmasını sağlar.

Bilgi birçok biçimde bulunabilir. Bilgi, kâğıt üzerinde yazılı olabilir, elektronik olarak saklanıyor olabilir, posta ya da elektronik posta yoluyla bir yerden bir yere iletilebilir ya da kişiler arasında sözlü olarak ifade edilebilir. Bilgi hangi formda olursa olsun, mutlaka uygun bir şekilde korunmalıdır. Bilgi güvenliğinin sağlanabilmesi, bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin yeterli düzeylerde sağlanabilmesi ile mümkündür (Önel ve Dinçkan, 2007, 6).

Bilgi güvenliği genel yanılgının aksine gerçekte teknolojik bir konu değildir; bilgi güvenliği bir iş sürecidir. Bilgi güvenliği, politikalar, uygulamalar, yöntemler, örgütsel yapılar ve yazılım fonksiyonları gibi bir dizi uygun denetimi gerçekleştirme

aracılığıyla sağlanır. Bu denetimler, kurumun belirli güvenlik hedeflerinin karşılandığını garanti altına almak için kurulmalıdır. Bu denetimler hem kurumun iç kaynakları yani İç Denetim bölümleri tarafından yapılabilir hem de kurum Dış Denetim firmaları tarafından bu prosedürlere uyumluluğu denetlenebilir. Denetim kurumları, yapıları ve uyumluluk süreçleri "Telekomünikasyon Sektöründe Bilgi Güvenliği Yönetimi ve Denetimi için Standartlar, Yasalar ve Düzenlemeler" bölümünde detaylı olarak incelenecektir.

PricewaterhouseCoopers şirketinin 2008 yılında 7000 den fazla güvenlik uzamanı ile yaptığı araştırmada kurumların Bilgi Güvenliğine neden önem verdiklerini içeren sonuç Şekil 3.1 de görülmektedir. Sonuçtan da görülebileceği gibi Regülasyonların ve kurumsal Politikaların yani Bilgi Güvenliği Yönetim Sisteminin kurum çalışanları üzerine etkisi çok büyüktür (PricewaterhouseCoopers, 2008, 2).



3-1 Bilgi Güvenliği Neden Önemlidir? (PWC, 2008, 2)

3.2. Bilgi Güvenliği Kavramları

Bilgi; kullanılabilirliği, gizliliği ve bütünlüğü boyutlarında zarar görmediği sürece güvenlidir. Bilgi güvenliği bu üç vektörün bileşkesinde oluşan kavramdır. Temel olarak bilişim dünyasında güvenliğin artırılabilmesi için tüm varlıklarda gizliliğin, devamlılığın ve bütünlüğün sağlanması gerekmektedir. Bunun

sağlanabilmesi için teknoloji ve insan tarafından ortaya çıkan güvenlik zayıflıklarının giderilmesi gerekmektedir.

Teknolojik çözümler bulunurken güvenlik göz ardı edilmektedir. Güvenliği düşünülmemiş bir ortam elbet bir gün bilgi hırsızlığına uğramaya mahkumdur. Sonradan sağlanmaya çalışan bilgi güvenliği hem daha maliyetli hem de verimsiz olmaktadır. Güvenliği zayıf bir sistemin güvenli hale getirilmesi için bütün yapı yeniden tasarlanmalıdır. Bu nedenle oluşturulacak süreçler ile güvenlik baştan kurumunun tüm yapısına dahil edilmelidir.

3.2.1. Gizlilik

Gizlilik Uluslararası Standartlar Örgütü (ISO) tarafımdan "Bilgiye sadece yetkilendirilmiş kişilerce ulaşılabilmesi" (http://en.wikipedia.org) olarak nitelenir. Günümüzde birçok Bilişim ve Telekomünikasyon firmasında şifreleme alt yapılarının kullanılmasının sebebi temel olarak bilginin gizliğinin sağlanılmasının gerekliliğidir. Gizlilik genel bir tanım olarak ise; "Bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir" (Önel ve Dinçkan, 2007, 6).

Gizlilik, özellikle bir yasa, kanun veya standart dolayısıyla kurum için bir zorunluluk ise önemlidir. Örneğin avukat - müvekkil ilişkisi ya da doktor hasta ilişkisi gibi mesleki bilgiler kanun ile koruma altına alınmıştır. Bazı durumlarda ise taraflar birtakım bilgileri sözleşme ile birbirlerine verirlerken gizlilik anlaşmaları yaparlar. Her iki durumda da gizlilik büyük önem taşımaktadır (Yıldız, 2007, 25)

Telekomünikasyon sektörü içinde gizlilik; bilgi güvenliği kavramları arasında en önemli kavram olarak nitelenmektedir. Bu nedenle Bilgi Teknolojileri ve İletişim Kurumu tarafından 2004 yılında 25365 Sayılı Resmi Gazete ile "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik" yayınlanmıştır. Bu yönetmelikte Telekomünikasyon Sektöründe Gizliliğin önemi Madde 8 ile açıkça belirtilmiştir. Madde 1 ile de ilgili yönetmeliğin kapsamı belirlenmiştir (http://www.tk.gov.tr).

Madde 1 — Bu Yönetmeliğin amacı, Telekomünikasyon sektöründe kişisel bilgilerin işlenmesi ve gizliliğinin korunmasının güvence altına alınmasına ilişkin usul ve esasları düzenlemektir. Bu Yönetmelik, Telekomünikasyon sektöründe hizmet veren ve alan gerçek ve tüzel kişileri kapsar (http://www.tk.gov.tr).

Madde 8 — Yasaların ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının izni olmaksızın, telekomünikasyonun üçüncü şahıs tarafından dinlenmesi, kaydedilmesi, saklanması, kesilmesi veya gözetimi yasaktır. İlgili trafik verilerinin ise işletmeci tarafından hizmet amaçları dışında kaydedilmesi, saklanması ve gözetimi yasaktır (http://www.tk.gov.tr).

Bu yönetmelik sonrası birçok Telekomünikasyon kurumu kurum için Erişim Politikaları hazırlayarak yönetmeliğe uyum sağlamışlardır. Erişim Politikaları; şifre üretim ve dağıtım, yetkilendirme, uzaktan erişim, bilgi paylaşım prosedürlerini içermektedir.

3.2.2. Bütünlük

National Information Assurance'nin tanımına göre veri bütünlüğü güvenlik anlamında verinin yahut bilginin yetkisiz kişilerce değiştirilmesine veya yok edilmesine karşı korunmasıdır (Yıldız, 2007, 26). Bütünlük, bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır. Bütünlük için kısaca kazara veya kasıtlı olarak bilginin bozulmaması diyebiliriz (Önel ve Dinçkan, 2007, 6).

Verinin bozulması kasten yahut kaza ile olabilir ve bu bütünlüğün bozulmuş olduğu gerçeğini değiştirmez. Güvenlik önlemi alanların iki tür riske karşı da tedbir almaları gerekmektedir. Bilginin bütünlüğü için "Kesinlik, Doğruluk ve Geçerlilik" kıstasları sağlamalıdır. (Yıldız, 2007, 26).

3.2.3. Kullanılabilirlik

Matematiksel olarak ifade edilirse, kullanılabilirlik herhangi bir sistemin yapılış amaçlarına göre işlev gördüğü zaman, işlev gördüğü ve görmediği toplam zamana oranıdır. Daha yalın bir anlatımla, doğru yetkilendirilmiş bir kişinin ihtiyacı olduğu anda ihtiyacı olan hizmetin orada olma oranına kullanılabilirlik, diğer bir deyişle ise erişilebilirlik denir. Verilen hizmetin ne kadar güvenilir olduğunun bir ölçütüdür. Kurumlar hizmetin ne kadar önemli olduğunun ölçümünü yapıp sistemleri ve verileri bu ihtiyaca göre yedekli hale getirirler (Yıldız, 2007, 27)

Kullanılabilirliği anlatan bir diğer tanım ise bilginin her ihtiyaç duyulduğunda kullanıma hazır olmasıdır. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim kullanıcının hakları çerçevesinde olmalıdır (Önel ve Dinçkan, 2007, 6). Kullanılabilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir. Bu nedenle özellikle kurumun güvenlik kurallarının verinin erişilebilirliğini engellemesi gerektiği unutulmamalıdır.

3.3. Bilgi Güvenliğini Etkileyen Faktörler

PricewaterhouseCoopers şirketinin 2008 yılında 7000 den fazla güvenlik uzamanı ile yaptığı araştırmada kurumların güvenlik vakalarını nasıl öğrendikleri ile ilgili bir araştırma yapılmıştır ve sonucunda %39'unun Firewall ve Sunucu loglarından, %37'sinin IDS- Atak Önleme Sistemi ile, %36'sının ise Çalışanlardan öğrenildiği tespit edilmiştir (PricewaterhouseCoopers, 2008, 2). Bu da kurum içi vakaların sadece %36'sının teknik altyapı ile önlenebildiğini, geri kalan %64 lük kısmın çalışanların dikkati ve birbirilerine olan etkileri ile tespit edilebildiği görülmektedir.

Bilgiye çok hassas derecede önem veren organizasyonlarda bilgi sistemlerinin güvenli yönetimi kritik derecede önemlidir. Çoğu organizasyon güvenlik teknolojilerini uzun zamandır kullanmasına karşın teknoloji çözümlerinin tek

başlarına yetersiz oldukları yaygın şekilde bilinmektedir. Dolayısıyla organizasyonlarda son kullanıcıların güvenlik ile ilgili alışkanlıkları giderek önem kazanmaya başlamıştır. Bilgi güvenliğinde son kullanıcıların davranışlarının ortaya koymak zorlu bir süreçtir. Bunun ötesinde son yapılan çalışmalar göstermektedir ki son kullanıcılar farklı sınıflarda değerlendirilebilecek güvenlik anlayışlarına sahiptirler (Tejaswini and Rao, 2009, 1).

Kuruluşlar bilgiye verdikleri önem doğrultusunda aktif olarak güvenlik teknolojilerini kullanmaktadırlar. Bu zamana kadar Bilgi Güvenliği üzerine yapılmış mevcut araştırmalar teknolojinin kullanımına ve kullanım biçimine odaklanmıştır. Son zamanlarda akademisyenler ve uygulamacılar bilgi güvenliğinin sadece teknolojik araçlarla hayata geçirilemeyeceğini ve verimli organizasyonel bilgi güvenliğinin insanlar, süreçler ve teknolojiden oluşan üçlü temele dayandığını fark etmeye başlamışlardır. Bununla beraber son kullanıcıların güvenlik davranışları ve bunları etkileyen etmenler üzerine yapılan ampirik araştırmalar hala başlangıç aşamasındadır (Tejaswini and Rao, 2009, 2).

Literatür çalışmaları sırasında bilgi sistemlerinin güvenliğinin sağlanması için gerekli teknik kontrollerle ilgili araştırmaların çokça olduğunu fakat güvenlik literatüründe politika uyumluluğu ve uyumluğu sağlama üzerinde az durulduğunu görülmüştür. Buna karşın, davranışsal bilgi güvenliği üzerine çalışan sınırlı sayıda uygulamacı ve akademisyenin güvenlik yönetiminin şekillendirdiği son kullanıcı alışkanlıklarına dikkat çekmeye çalıştığı görülmüştür.

Bu çalışma Tejaswini ve Rao nun yaptığı tanımı baz almış ve Bilgi Güvenliği'ni Etkileyen Faktörleri 6 ana başlık altında toplanmıştır. Süreç, Teknoloji ve İnsan önemli 3 faktörü oluşturmaktadır. Bunların yanında diğer araştırmalarda da önemi sıklıkla bahsedilen Sosyal Baskı ile Yaptırımlar ve Cezalar konuları da ayrı birer başlık olarak ele alınmıştır. Ayrıca Telekomünikasyon Sektöründe Standartlar, Yasalar ve Düzenlemelerin öneminin fazlalığı nedeniyle bu konuda ayrı bir başlık olarak incelenmiştir.

3.3.1. İnsan Faktörü

İster büyük ister küçük çaplı olsun tüm kurumlar kendilerini; günümüzde sürekli artan tehditlere karşı güçlü, kurumsal güvenlik kuralları ve prosedürleri ile koruyabilirler. Kurallar ve prosedürler kurum içinde kullanılan güvelik teknolojileri desteklerler. Bu kurallar ve prosedürler datanın gizlilik, bütünlük ve erişilebilirliğinin nasıl korunacağı ile ilgili yol gösterirler. Her ne kadar teknoloji ve süreç kurumsal bilgi güvenliğinin temelini oluştursalar da, 3. bir bileşen olarak "İnsan" ile ancak kurumsal bilgi güvenliği resmi tamamlanabilir (Egan, 2005, 1).

Tablo 3.1; PricewaterhouseCoopers şirketinin 2007 ve 2008 yılının sonuçlarını açıkladığı ve 7000 den fazla güvenlik uzamanı ile yaptığı araştırmanın Bilgi Güvenliğinin en büyük tehditlerini açıkladığı bölümünde; mevcut ve eski çalışanların en büyük tehlikeyi oluşturduğu açıklanmıştır. Güvenlik vakalarının neredeyse yarısının kaynağının ise belli olmadığı iletilmiştir (PWC, 2008, 12)

Tablo 3-1Kurum İçi Vakaların Kaynakları (PWC, 2008, 12)

Vaka kaynağı	**2007**	**2008**
Belirsiz	*	%42
Çalışanlar	%48	%34
Hackerlar	%41	%28
Eski Çalışanlar	%21	%16
İş Ortakları	%19	%15
Müşteriler	%9	%8
Diğer	%20	%8
Terörist/Yabancı Devletler	%6	%4

İnsan faktörünün önemi; kurulan tüm teknolojilere rağmen insan faktörünün tamamen kontrol edilememesinden kaynaklanmaktadır. Kurulan birçok teknolojik yapıda insana ait faaliyetler kontrol edilemez, yönetilemez, ölçülemez olmaktadır. Bu durum ise süreçlerin sağlıklı işlememesine ve kullanıcılar tarafından yapılan

hataların yol açtığı sorunların anlaşılamamasına, giderilememesine neden olmaktadır. Dolayısıyla güvenliğe ait geliştirilen çözümlerin operasyonel işleyiş açısından hızlı ve kullanılabilir olması kadar, güvenlik açısından kontrol edilebilir, ölçülebilir ve yönetilebilir çözümler olmasına özen gösterilmelidir (Lacey, 2009, 3)

İnsanlar sadece güvenlik teknolojinin yürütülmesini sağlamazlar aynı zamanda kritik güvenlik kurallarının, prosedürlerinin ve süreçlerinin yaratılmasını ve sürdürülmesini sağlarlar. Süreçler ile doğru kişiye doğru yetkinin verilmesini sağlarlar. Bu nedenler insanlar, bilgi güvenliği döngüsünün hem en güçlü hem de en zayıf bağlantısı olabilirler (Egan, 2005, 1).

Bilginin erişilebilirliği güvenli bir şekilde sağlanmalıdır. Bilgiyi korumak diğer teknoloji konularına nazaran kurum açısından daha önemlidir. Bilginin korunması içinde üst yönetim, bilgi ve ağ güvenliği yöneticisi ve güvenlik operasyonu yapan çalışanların desteği çok önemlidir. Bilgi güvenliği programı üst yönetim kadrosu tarafından mutlaka desteklenmeli ve özellikle bilgi ve ağ güvenliği yöneticisi tarafından üst yönetimin ilgisi bilgi güvenliğine çekilebilmelidir. Bilgi güvenliği projeleri finansman ve kaynaklar ile desteklenmelidir. Bilgi güvenliği kuralları kurum içinde tüm süreçleri ve tüm kurumsal donanım ve yazılımları ilgilendirmektedir. Ayrıca bilgi güvenliğinin müşteri memnuniyeti ve kurumsal marka oluşumuna doğrudan etkisi bunmaktadır (Egan, 2005, 1).

Son kullanıcıların yani kurum çalışanlarının uyması gereken Bilgi Güvenliği kurallarının algılanmasını değerlendiren son zamanlarda yapılmış çalışmalar, çalışanların bilgi güvenliği kurallarına uyum ile performansının ters orantılı olduğunu göstermektedir. Yani çalışanların güvenlik standartlarına uyumluluklarının artması, iş performansını düşürdüğünü ortaya koymaktadır. Böyle bir algılama çalışanların günlük rutin çalışmalarının verimliliğini sağlamak adına güvenlik politikalarını reddetmelerine neden olabilir (Lacey, 2009, 3).

Başarılı ve etkin işleyen bir bilgi güvenliği bilinçlendirme süreci oluşturulabilmesi ve kurumların sahip oldukları bilginin gizliğini, bütünlüğünü ve kullanılabilirliğini koruyabilmeleri için BT kullanan ve yöneten kurum çalışanlarının

ve kurumun bazı özelliklere sahip olması gerekmektedir (Örnek, 2003, 6; Önel, 2008, 5);

- Kurumun misyonu doğrultusunda görev ve sorumluluklarını açık ve net bir biçimde belirlenmesi ve ilgili çalışanlara anlatılması gerekmektedir. Çünkü olgunlaşmış bir bilinçlendirme süreci, bu görev ve sorumlulukların sahipleri tarafından doğru anlaşılması, bilinmesi ve uygulanması ile mümkündür.

- Kurumun bilgi güvenliği politika, prosedür ve uygulamalarının hazırlanması, sürekliliğinin sağlanması ve çalışanlara anlatılması gerekmektedir.

- Çalışanların sorumlu oldukları bilgi (bilişim) kaynaklarını korumaya yönelik yönetimsel, operasyonel ve teknik açıdan gerekli asgari bilgi seviyesine sahip olmaları gerekmektedir.

Bilgi güvenliği bilinçlendirme süreci kurum içinde en üst seviyeden en alt seviyeye kadar çalışanların katılımını gerektirmektedir. İnsan faktörü uygun ve yeterli seviyede güvenliğin sağlanmasında anahtar role sahiptir. Bu sebeplerden ötürü bir kurum varlığı olarak insan üzerinde daha büyük bir dikkatle durulması gerekmektedir. Bu bağlamda, Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamında her seviyedeki kurum çalışanın bilgi güvenliği konusundaki sorumluluklarını kavramasını sağlayacak bir bilinçlendirme sürecinin oluşturulması zaruridir (Önel, 2008, 5).

3.3.1.1. Bilgi Güvenliğinde İnsan Faktörü

Bilginin korunmasını sağlayan teknolojik araçlar yıllardır kullanılmaktadır. Bilgi Güvenliğini sağlamaya yönelik bu teknolojilere rağmen hala ciddi veri kayıpları, büyük ölçekli kimlik hırsızlıkları ve ulusal veritabanlarının ele geçirilmesi gibi sorunlar görülmektedir. Kurumsal bilgi sistemleri ve verileri; tasarım kusurları, zayıf şifreler, sosyal mühendislik ve daha birçok kötü örnek ile zayıflatılmaktadır. Ayrıca bilgi güvenliğini tehdit eden bu riskler teknolojinin karmaşıklığının ve zorluğunun artmasıyla beraber hızla büyümektedir Bu durum açıkça bilgi güvenliğinin sadece bir teknoloji problemi olmadığını göstermektedir. Son dönem

birçok güvenlik sunumunda “Bilgisayarlar suç işleyemezler, insanlar işlerler” ibaresi yer almaktadır (Lacey, 2009, 3).

İnsanlar bilgi güvenliğinin omurgasını oluşturmaktadır. İnsanlar bilgi güvenliğini tasarlar, uygular ve yürütürler. Bunun yanında kurumsal sistem ve bilgilere fiziksel ve mantıksal erişimi yönetirler ve bu sırada hatalar yapabilir, vakalar oluşturabilir ve sistemlerde büyük açıklıklar oluşturabilirler. Bu yüzden güvenlik yönetimi konulu çalışmalarda insan faktörünün önemi her geçen gün daha fazla önemsenmeye başlamaktadır (Lacey, 2009, 3).

Güvenlik; diğer kurumların varlıklarını sömürmeye çalışan “kötü çocuklar” ve bu varlıkları korumaya çalışan “iyi çocuklar” arasındaki oyun gibidir. Bu yüzden sistemlere ve verilere erişimi kendi kullanıcılarımız için ne kadar kolaylaştırırsak, aynı zamanda hackerlar içinde sistemlerimize izinsiz erişimi aynı derecede kolaylaştırmış oluruz. Bu nedenle kurum içinde hangi kullanıcının, hangi veriye, hangi hak ile erişmesine izin verilmesi gerektiği doğru tespit edilmelidir (Lacey, 2009, 3).

Güvenlik teknolojilerindeki gelişmelerle; yama yönetimi, anti virüs güncellemeleri gibi birçok bilgisayar süreçleri son kullanıcıların üzerindeki ilgili süreç bilgilerini ve zaman yükünü azaltacak şekilde otomatize hale getirmiştir. Buna karşın bilgisayar ve ağ kaynaklarının uygun kullanımı, uygun parola kulanım alışkanlıkları gibi davranışlar organizasyonel bilgisayar güvenliği politikaları ile yönetilen güvenlik teknolojilerince adreslenemezler. Son dönemlerde yaşanan güvenlik sızması olayları ile bilgi güvenliği uyumlulukları dışına çıkılmasının ve çalışanların ilgisizliklerinin organizasyonların milyonlarca dolar kaybetmelerine neden olduğu görülmüştür. Misra ve Dillon bu yanlışlıkları son kullanıcı uyumsuzluklarını güvenlik sızmalarını en aza indirmek veya önlemek amacıyla yaygın standartlara ve uyumluluklara politikalarında yer vermeyen bilgi sistemleri güvenliği yönetişim programlarının başarısızlıklarına kanıt olarak otaya koymaktadır (Tejaswini and Rao, 2009, 2).

Bilgi Güvenliğinde "İnsan" faktörünün hangi konular için önemli olduğunu bazı temel maddeler ile anlatılabilir (Lacey, 2009, 20);

- Kurum üst yönetimleri öngörülü, cesaretlendirici ve destekleyici olmalıdır.
- Yöneticiler riskleri tanımlamalı ve yönetebilmelidir.
- Proje ekipleri yeni sistemler için güvenlik gereklerini ortaya koymalıdır.
- Programcılar güvenli kod yazımını temel almalıdır.
- Operasyon personelleri güvenli süreçler ve altyapılar oluşturmalı ve işletmelidir.
- Kullanıcılar, personel ve müşteriler güvenli çalışmaya uyum sağlamalıdır.
- Güvenlik ekibi tüm bunların hayata geçtiğini takip etmeli ve olası güvenlik istisnalarını etkinlik veya yaygınlık kazanmadan öngörmelidir.
- Güvenlik ekibi için düşmanları erken fark edebilme yeteneği ve potansiyel düşmanları risk değerlendirme sürecinin bir parçası olarak görmesi önemlidir

3.3.1.2. Bilgi Güvenliğinde İnsan Faktörünün Yönetimi

Organizasyonlar farklı yapılara sahiptirler. Her bir organizasyon kendi özgün kültürler harmanına, risk profiline ve yönetim süreçlerine sahiptir. Tarz, karar verme, risk algısı, ülkeler ve topluluklara göre değişmektedir. pazarlama anlayışları ülkeden ülkeye değişmektedir. Fakat büyük ölçekli bir değişim programına uygulanabilecek evrensel prensipler vardır.

Geçmişte, güvenlik problemleri kurum içindeki herhangi bir Enformasyon Teknolojileri(IT) elemanı tarafından çözülebilmekteydi. Tehtitler bu zamana göre nispeten yavaşça yayılırlardı ve nedeninin bulunması, yok edilmesi ve kontrol altına alınması kolay olurdu. Fakat artık bilgi güvenliği sorunları böyle kolay bir şekilde çözülememekte. Son yıllarda bilgisayar kullanıcıların bilgi seviyelerinin artması ile beraber internet tehtitlerinin karmaşıklığı da çok üst seviyelere çıkmaya başlamıştır. Özellikle yazılım açıkları giderek yaygınlaşmakta ve IT çalışanları tarafından hızlıca geçerli yama çalışmalarının yapılabilmesi için daha az kaynak bulunabilmektedir. Bu yüzden kurum içinde bugünün ve yarının açıklıklarını sürekli olarak takip eden kalıcı bir bilgi ve ağ güvenliği ekibi oluşturulmalıdır. Kurum içinde her 1000 çalışan

için hızlıca güvenliği ve kurumsal bilginin erişilebilirliğini sağlayabilecek en az tecrübeli bir bilgi güvenliği çalışanı bulunmalıdır. Bilgi ve Ağ Güvenliği ekibine Yönetim kuruluna direk bağı çalışan bir yönetici atanmalıdır (Egan, 2005, 2).

Bilgi Güvenliği kuralları ve prosedürler belirli aralıklar ile bilgi güvenliği yönetim grubu tarafından gözden geçirilmelidir. Bu grup teknik detayda bir değişiklik yapamayacağı için özellik teknik detaylara ve güncel açıklıklara hakim olan Bilgi/Ağ Güvenliği ekibi bilgi güvenliği yönetim grubuna düzenli aralıklar ile bilgilendirme yapmalıdır. İç kontrol mekanizması için gerekli olan bir diğer kipte Bilgi Güvenliği Denetimcilerinden oluşan İç Denetim ekibidir. Bu ekip özellikle regülasyonlar, yasalar ve uyumluluk süreçlerine hakim olmalıdır ve bu süreçler doğrultusunda gerekli kontrolleri yapmalıdır. Bu grubun üyelerinin CISA- Certified Information Systems Auditors sertifikasına sahip olması tercih edilmelidir. Bağımsız denetim firmaları tarafından kurumlara yapılan denetimlerde bilgi güvenliği kurallarının kurum içindeki etkililiğini arttırmasına yardımcı olmaktadır. Ek olarak dış denetim firmalarının birçok kurum ile çalışması dolayısıyla oluşmuş tecrübeleri doğrultusunda problemleri daha rahat tespit edebilirler ve kontrollerin sıkılaştırılması için güvenilir tavsiyelerde bulunabilirler (Egan, 2005, 2).

3.3.1.3. Yönetimin Sorumlulukları ve Desteği

Bilişim güvenliğinin yönetilebilmesi, yaygınlaştırılabilmesi, kuralların güncelliğinin sağlanabilmesi için olmazsa olmaz koşul üst yönetim desteğidir. Üst yönetim, güvenlik politikalarını bizzat belirleyerek, komitelere katılarak, gerek parasal gerekse de insan kaynağı anlamında bilişim güvenliğini ve denetimini destekliyor olmalıdır (Örnek, 2003, 4)

Başarılı kurumsal yönetim tüm başarılı ve karlı kurumların kalite işaretidir. Başarılı yönetim, kurumun doğru bir yön ve hedef seçmesini ve kurumun bu doğrultuda ilerlemesini sağlar. Bilgi güvenliğinin başarılı olabilmesi için kurumsal yönetim tarafından yol gösterilmesine ihtiyaç duyar. Bilgi güvenliği tüm kurumu etkiler, bu yüzden bilgi güvenliği yönetim grubu işletme birimleri ve fonksiyonel

departmanlardan liderleri de içermelidir. Bilgi güvenliği yönetimi içinde söz sahibi olacak bu departmanlar hukuk, insan kaynakları ve IT olmalıdır. Hatta kurumsal yönetim grubu kurumun yönetilmesinden soruluyken, bilgi güvenliği yönetim grubu kurumun bilgi güvenliği programından sorumludur (Egan, 2005, 3).

Bilgi güvenliği yasa ve regülasyon kontrollerinin artmasıyla beraber kurumun günlük operasyonlarının içinde yer almaya başlamıştır. Bundan dolayı, bilgi güvenliği ancak bilgi güvenliği uzmanları ile yönetimin birlikte çalışması ile kurum içinde etkin hale getirilebilir (Lacey, 2009, 29).

Bilgi Güvenliğinin kurum için önemini Bilgi Güvenliği başlığı altında açıklamıştık. Buradaki nedenlerden dolayı bilgi güvenliği kurallarının titizlikle kurum içinde uygulanmasının sağlanması gerekmektedir. Organizasyon içinde Bilgi Güvenliği konusunda en temel ve genel hata sistemler ile ilgili yeterli kontroller yapılmadan sistemin güvenli olduğu ve şirketin bu konuda bir sorun yaşamayacağı düşüncesidir. Bu hata bilişim güvenliği bilincinin hem kurum, çalışanlar ve yönetim tarafından yeterince anlaşılamamasından hem de üst yönetimin kurum içinde bilişim güvenlik konusunu yeterince desteklememesinden kaynaklanır. Bilişim güvenliği bilinci kurum çapında, yöneticiden en son kullanıcıya kadar yaygınlaştırılmalı, kullanıcılar eğitimler ile bilinçlendirilmeli, güvenlikten herkesin bundan sorumlu olduğu anlatılmalı ve güvenlik kurumca sahiplenilmelidir (Örnek, 2003, 7)

3.3.1.3.1. Üst yönetim

Bir organizasyonun yönetim kurulu şirket değerlerinin korunmasından en yüksek seviyede sorumlu gruptur. Risk yönetim süreçleri uygulanan organizasyonun doğru yönetilmesini sağlamalı, risk yönetimini destekleyici iç kontrollerle de efektif bir sistem oluşturmalıdır. Kurulun ve üyelerinin sorumlu olduğu birçok yasal zorunluluk vardır ve yasal anlaşmalara uyulmaması durumunda sert yaptırımlar uygulanmaktadır. Şirket yönetimi bu hedefleri gayretle, kesintiye uğratmadan, suistimal etmeden, yasal kurallara uyarak yerine getirmelidir (Humphreys, 2008, 248)

Bilgi güvenliği açısından şirket değerleri ve bu değerlerin korunması söz konusu olduğunda risklerin bilinebilir ve yönetilebilir olmaları konusuna özen gösterilmelidir. Bu, iş ve bilgi güvenliği risklerini tanımlama ve değerlendirmesini aynı zamanda etkin kontrol sistemlerin uygulanmasını, takibini ve kontrollerin etkinliğinin devamlılığını, değil ise geliştirilmesini içerir. Bir başka deyişle organizasyonun bilgi varlıklarını koruyacak bir bilgi güvenliği yönetim süreci olmalıdır (Humphreys, 2008, 248).

Üst yönetim özellikle yasal zorunluluklar nedeniyle bilgi güvenliği bilinçlendirme sürecinden nihai olarak sorumlu olan taraftır. Kurum üst yönetimi etkin bir bilinçlendirme süreci oluşturulmasına yönelik bilgi ve ağ güvenliği ekibini uyarmalıdır. Bilinçlendirme sürecinin başarıya ulaşmasında üst yönetimin tutum ve yaklaşımı son derece önemlidir.

Bu alanda üst yönetime düşen bazı görev ve sorumluluklar vardır (Önel, 2008, 7);

- Kurum içinde bir Bilgi ve Ağ Güvenliği Yöneticisi atanması
- Kurum çapında işleyen bir bilgi güvenliği bilinçlendirme sürecinin oluşturulması.
- Yeterli kaynak ve bütçe ile bu süreçlerin desteklenmesi.
- Kurumun bilgi varlıklarının korunmasını sağlayabilecek seviyede bilinçli ve eğitimli bir personel kadrosunun bulunması

ISO 27001 kurumun; risk yönetimi ve risk işleme planlarını, görev ve sorumlulukları, iş devamlılığı planlarını, acil durum olay yönetimi prosedürleri hazırlamasını ve uygulamada bunların kayıtlarını tutmasını gerektirir. Kurum tüm bu faaliyetlerin de içinde yer aldığı bir bilgi güvenliği politikası yayınlamalı ve personelini bilgi güvenliği ve tehditler hakkında bilinçlendirmelidir. Seçilen kontrol hedeflerinin ölçülmesi ve kontrollerin amacına uygunluğunun ve performansının sürekli takip edildiği yaşayan bir süreç olarak bilgi güvenliği yönetimi ancak yönetimin aktif desteği ve personelin katılımcılığıyla başarılabilir. Üst yönetimin BGYS'nin gerekliliğine ve faydasına inanması BYGS 'nin sürekliliği ve uyumu için birincil şarttır.

3.3.1.3.2. Bilgi ve Ağ Güvenliği Yöneticisi

Bilgi ve Ağ Güvenliği Yöneticisi kurum üst yönetimi tarafından bilgi güvenliği bilinçlendirme sürecinin oluşturmasını yönetmekle görevlendirilen kişidir. Etkin bir bilinçlendirme süreci için Bilgi ve Ağ Güvenliği Yöneticisinin, Bilgi Sistemleri Yöneticisi (BT Yöneticisi veya direktörü CIO- Chief Information Officer) ile birlikte çalışması gerekmektedir. Bilgi ve Ağ Güvenliği Yöneticisinin görevleri tespit edilmiş, atanmış ve yetkili olmalıdır. Bilgi ve Ağ Güvenliği Yöneticisinin görev alanı ve kontrol mekanizmaları net olarak mutlaka tespit edilmiş olmalıdır (Carlson, 2001, 7; Önel, 2008, 8).

Bilgi ve Ağ Güvenliği Yöneticisinin görev ve sorumlulukları şu şekilde sıralanabilir (Carlson, 2001, 7; Önel, 2008, 8);

- Bilgi güvenliği bilinçlendirme süreci için genel stratejinin belirlenmesi.
- Güvenlik Grubuna liderlik yapılması.
- Vaka tespit ve yönetim takımına liderlik yapılması ve vakaların çözümlenerek gerekli yaptırımların belirlenmesi.
- Kurum içinde bir bilgi güvenliği bilinçlendirme süreci yürütücüsü atanması.
- Üst yönetimin, bölüm yöneticilerinin, diğer seviyedeki yöneticilerin, çalışanların ve diğer personelin bilinçlendirme sürecinin temel kavramlarını ve hedeflerini anlamalarını sağlamak, onları sürecin gelişimi ve ilerlemesi konusunda bilgilendirmek.
- Bilinçlendirme sürecinin yeterli seviyede finanse edilmesini sağlamak.
- Kurum personeline bilgi güvenliği sorumluluklarının eğitimler ile öğretilmesi.
- Kurumun bilgi kaynaklarına erişen tüm kullanıcıların bilgi güvenliği sorumluluklarını bildiklerinden emin olunması.
- Regülasyon süreçleri için mevcut güvenlik standartlarının güncel tutulması.
- Bilgi güvenliği bilinçlendirme sürecinin takip edilmesi ve uygunsuzlukları tespit edecek mekanizmaların devreye alınmış olması.

3.3.1.3.3. Bölüm ve Takım Yöneticileri

Yöneticiler bilgi güvenliği bilinçlendirme ve eğitimi sürecinin gereklerine personelinin uymasını sağlamakla sorumludurlar. Bilgi Güvenliğinin sağlanması konusunda diğer görev ve sorumlukları ise şu şekilde sıralanabilir (Önel, 2008, 7);

- Bilgi güvenliği bilinçlendirme süreci kapsamında ortak sorumlulukları yerine getirmek amacıyla Bilgi ve Ağ Güvenliği Yöneticisi ve Bilgi Güvenliği Bilinçlendirme Süreci Yürütücüsü ile birlikte çalışmak.
- Bilgi güvenliği alanında görev ve sorumluluğa sahip personelinin mesleki anlamda bireysel gelişimine katkıda bulunmak.
- Yarı zamanlı personel, stajyer çalışan ve yüklenici firma personeli dahil olmak üzere tüm kullanıcıların erişimde bulunmadan önce bilgi güvenliği sorumluluklarını yerine getirebilmeleri için uygun eğitimleri almalarını sağlamak.
- Yarı zamanlı personel, stajyer çalışan ve yüklenici firma personeli dahil olmak üzere tüm kullanıcıların kullandıkları sistem ve uygulamanın, ilgili politika veya prosedürle belirtilen kurallarını bilmelerini ve anlamalarını sağlamak
- Eğitim ve bilinçlendirme eksikliği sebebiyle kullanıcıların yaptıkları hata veya ihmallerden kaynaklanabilecek, bilgi varlıklarındaki her türlü kayıp ve zararı azaltmaya çalışmak.

3.3.1.3.4. İç Denetim Ekibi

Sistemler yaşayan insanlar gibi sürekli gelişir, değişir. Dolayısıyla güvenlik ihtiyaçları ve güvenlik açıkları da gelişir, değişir. Bilişim dünyası için yılda bir kez yapılan denetim yeterli değildir. Güvenlik sürekli bir ihtiyaçtır, dolayısıyla güvenliğin denetimi de sürekli bir ihtiyaçtır (Örnek, 2003, 5). Bu ihtiyaç dolayısıyla kurum içinde Bilgi Güvenliği kuralları ile regülasyon süreçlerinin kontrollerini düzenli aralıklar ile yaparak bu kontrol sonuçlarını üst yönetime raporlayan İç Denetim ekiplerinin varlığı çok önemlidir.

Bilişim güvenliği denetiminin devamlılığı için belirli aralıklar ile çalışmalar yapılmalıdır. Bu çalışmalar için verilebilecek örnekler şu şekildedir (Örnek, 2003, 5);

- Önceden içerikleri belirlenmiş yazılı raporların otomatik olarak üst yönetime, yöneticilere gelmesi sağlanmalıdır. Yani düzenli olarak açıklıklar ve riskler yönetime raporlanmalıdır.
- Yetki kontrolleri yapılmalı ve ihlalleri düzenli olarak raporlanmalıdır.
- Güvenlik parametreleri değişiklikleri düzenli olarak raporlanmalıdır.
- Yüksek yetkilere sahip kullanıcıların yaptıkları işlemler düzenli olarak raporlanmalıdır.
- Çok kritik kaynaklara erişimler düzenli olarak raporlanmalıdır.
- Kurumda çalışan Bilişim teknolojileri müfettişleri ile özellikle kritik bilgisayar sistemlerini yılda en az 2 kez bilişim güvenliği denetiminden geçirilmelidir.
- Sistemleri denetleyen, temel güvenlik açıklarını bulan programlarla en az ayda 1 kez sistemleri kontrol edilmelidir.
- İkili kontrol mekanizmaları oluşturularak, kritik uygulamaların en az 2 kişi tarafından yürütülmesi ve görevler ayrılığı prensiplerine göre düzenlemeler yapılmalıdır.

Denetim ekibi çalışanları risk yönetimini doğru yapabilmesi için şirket süreçleri çok iyi bilmelidir. Denetimlerde en iyi müfettiş, sistem mühendisinden en çok bilgiyi alabilendir. Bu yöntemle ancak süreçlerin iyileştirilmesi sağlanabilir. Bilişim denetimi bir metodolojiye bağlı kalınarak yapılmalıdır. Kurum bilişim güvenliğini ilk defa kontrol ediyorsa öncelikle bilişim güvenliği yönetimini kontrol etmelidir. Bilişim güvenliği yönetiminin kontrolü BS 7799 belirtilen ilkelerin varlığının kontrolü ile yapılabilir. Eğer kurum bu metodolojilerde yazılı kuralları tam olarak yerine getirdiğine düşünüyorsa farklı metrik metotlarla da denetim yapılabilir (Örnek, 2003, 5).

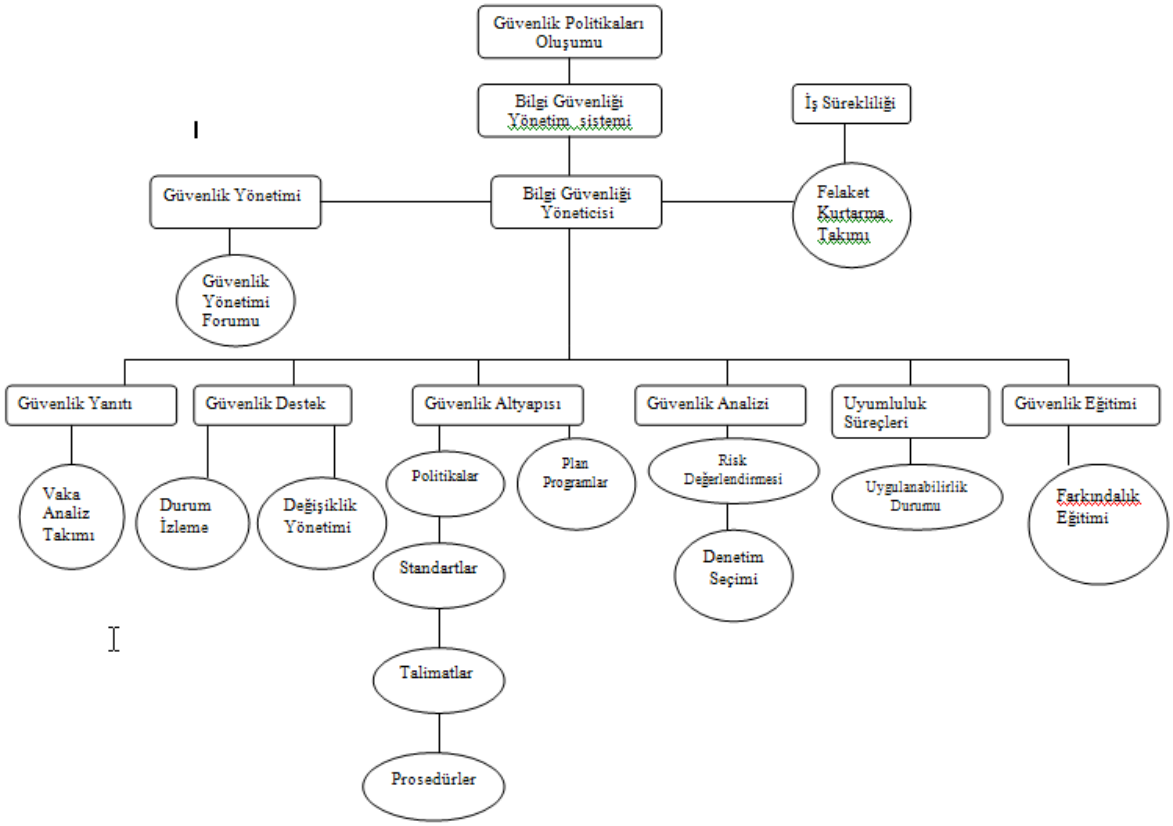
3.3.1.3.5. Bilgi ve Ağ Güvenliği Bölümü

Kurum içerisinde Bilgi Güvenliği ile ilgili çalışmaları yürütecek güvenlik ve denetim takımının ve yöneticisinin bilgi güvenliği yönetimi konusunda iyi eğitimli olmaları gerekmektedir. Risk yönetimi, politika oluşturma, güvenlik prosedürlerinin hazırlanması ve uygun kontrollerin seçilerek uygulanması aşamalarında uzman desteği ve danışmanlık almaları faydalı olacaktır. Bilgisayarlar ağınıza saldırganların nasıl sızabileceğini söylemezler. Size toplam bilgi güvenliği ve "yaşayan bir süreç olarak" bilgi güvenliğinin nasıl "yönetileceğini" tanımlar.

Kurumsal Bilgi ve Ağ Güvenliği takımı güvenlik altyapılarının yönetimi ve güncel açıklıkların kapatılması konularına odaklanarak çalışlar. Bilgi ve Ağ Güvenliği takım lideri ise, bilgi güvenliği konularında yapılan çalışmaları değerlendirerek son kararı vermektedir. Ayrıca takımın çalışma konuları olarak şunlar verilebilir (Carlson, 2001, 7);

- **Bilgi Güvenliği Yönetimi:** Kurumsal Bilgi Güvenliği açıklıklarını takip eder ve bilgi güvenliği komitesine düzenli olarak raporlarlar.
- **Bilgi Güvenliği Sorumlulukları**: Bağımsız bilgi güvenliği sorumlulukları açıkça belirlenmiş ve bireylerin iş tanımlarında detaylıca açıklanmalıdır.
- **Yetkilendirme Süreci**: Çalışanlara gerekli yetkinin gerekli ölçüde verilmesi ve bu yetkilendirme konusunun belirlenmiş bir bilgi güvenliği sürecine dönüştürülmesi.
- **Kurumsal İşbirliği**: Bilgi paylaşılan diğer firmalar ve kurumsal yasa yürürlüğe koyma yetkilileri arasında işbirliği sağlar.
- **Bağımsız Gözlem**: Güvenlik grubunun etkililiğinin bağımsız olarak gözlemlenebileceği yapılar kurar.
- **Üçüncü Parti erişimler**: İş ihtiyaçları doğrultusunda 3. Parti firmaların kuruma hangi koşullarda bağlanabileceği konusunda kuralları belirler.
- **Dış Kaynak Kullanımı:** Kurumsal dış kaynak kullanımı net ve açık güvenlik süreçleri ile yapılmalıdır.

Şekil 3.2 de açıklanan Carlson'ın kurumlar için önerdiği Güvenlik Organizasyon Yapısı şekildeki gibidir. Bu yapı ile özellikle Bilgi Güvenliği Yöneticisinin tüm güvenlik alt yapısına hakim olması sağlanmaktadır. Bunun dışında güvenlik birimleri için çok önemli olan Vaka Analiz ekibi, Güvenlik Alt yapı yönetim ekibi ve güvenlik analiz ekiplerinin görevleri birbirinden ayrılmaktadır. Ayrıca kurum içi bilgi güvenliği bilincinin arttırılması için çalışan güvenlik eğitim ekibi ile Uyumluluk süreçleri için çalışan ekiplerde organizasyon şemasında ayrıca yer almaktadır (Carlson, 2001, 24).



3-2 Güvenlik Organizasyon Yapısı (Carlson, 2001, 24)

Bilgi güvenliği başta Yönetim Kurulu ve CEO olmak üzere tüm yönetim birimlerinden genel personele kadar herkesin sorumluluğunda olmak zorundadır. Üst yönetim tüm şirket politikaları ve bilgi güvenliği yönetiminden sorumludur ve bilgi güvenliğini uygulamak için yeterli kaynakların sağlanabilirliğinden emin olmalıdır. Kıdemli yöneticiler ise üst yönetimin direktiflerini uygulamada ilave destek sağlamalıdır. Tüm iş birimleri de, bilgi güvenliği ile günlük çalışmalarının ve iş

tanımlarının bir parçası gibi meşgul olmalıdır. Ancak bu şekilde en tepeden en alt seviyeye kadar etkin bir şekilde uygulanabilir. Ne yazık ki güvenlik vakaları, yönetim yapısındaki kural zinciri yönetim ve uygulamadaki çatlaklar ve zayıflıklar yüzünden gerçekleşmektedir. Bu tür problemlerin çözümü için denenmiş, test edilmiş ve kanıtlanmış birçok yöntem olduğu için bu mazur gösterilebilir bir konu değildir. Organizasyonlar yıllardır bilgi güvenliği yönetimi konusuna aşinadır ve günümüzde ISO/IEC 27001, ISO/IEC 27002 gibi bir çok uluslararası standart geliştirmiştir (Humphreys, 2008, 248)

3.3.1.3.6. Son Kullanıcı Güvenlik Bilinci

Şirket çalışanları bilgi güvenliği bilinçlendirme sürecindeki en büyük ve önemli hedef kitledir. Kurum içindeki işler yürütülürken istemeden yapılan hataları ve bilgi sisteminde oluşabilecek açıklıkları en aza indirmek çalışanların elindedir. Kurum çalışanları, yüklenici firma personeli, yarı zamanlı personel, stajyerler, diğer kurum çalışanları, ziyaretçiler, iş ortaklarının çalışanları, destek alınan firmaların personeli, kısaca kurumun bilgi varlıklarına erişim gereksinimi olan herkes kullanıcı kategorisine girmektedir.

Son kullanıcıların bilgi güvenliği konusunda eğitilmeleri çalışanlar üzerinde yapılacak Sosyal Mühendislik saldırılarının engellenmesi için çok önemlidir. Sosyal mühendislik; insanları manipule ederek bazı eylemler gerçekleştirmelerini sağlamak ve gizli olması gereken bilgileri açığa çıkarma sanatıdır. Bir şirket paranın alabileceği en iyi güvenlik teknolojilerini satın almış; çalışanlarını, akşam eve giderken her şeylerini kilit altına alacak şekilde son derece iyi eğitmiş ve bina güvenlik görevlilerini sektörün en iyi güvenlik şirketinden kiralamış olabilir. Bu şirket yinede tamamen savunmasızdır. Bireyler, uzmanların önerdiği en iyi güvenlik uygulamalarını çalıştırıyor, önerilen her güvenlik ürününü bilgisayarına yüküyor olabilirler ve uygun sistem yapılandırmasını ve güvenlik yamalarını kullanmak konularında son derece dikkatli davranabilirler ama yinede hala bu bireyler İnsan Faktörü nedeniyle savunmasızdır çünkü İnsan unsuru aslında güvenliğin en zayıf halkasıdır (Mitnick, 2002, 1)

Kullanıcıların sorumlulukları şu şekilde sıralanabilir (Dinçer Ö. ,2008);

- Güvenlik politika ve prosedürlerini anlamak, gereklerine uymak.
- Erişim hakkının bulunduğu bilgi varlıklarının kullanım ve güvenlik kurallarını öğreten eğitimleri almak.
- Bilinçlendirme ve eğitim ihtiyaçlarının giderilmesi için yönetimle birlikte çalışmak.
- Kullandıkları yazılım ve uygulamaların güvenlik yamalarının güncel tutulmasını sağlamak.
- Güçlü parola kullanımı, antivirüs yazılımı kullanılması, şüpheli olay ve ihlal durumlarının rapor edilmesi, veri yedeklemesi, sosyal mühendislik saldırılarına karşı koyulan kurallara uyulması vb. gibi kurum bilgisini daha iyi korumaya yönelik uygulama ve faaliyetlerin farkında ve bilincinde olmak.

3.3.1.4. Son Kullanıcı Bilgi Güvenliği Eğitimleri

Kurumun, herkese açık olmayan bilgilerin kötüye kullanılmasından doğabilecek ciddi sorunlara karşı çalışanlarını bilgilendirme sorumluluğu vardır. Üzerinde düşünülmüş bir bilgi güvenliği politikası, düzgün bir bilgilendirme ve eğitimle birleşince şirket bilgilerinin doğru kullanımıyla ilgili çalışan bilinci görünür şekilde artacaktır. Bir veri sınıflandırma politikası, bilgi vermeye yönelik uygun denetimler getirilmesine yardımcı olacaktır. Veri sınıflandırma politikası olmadan, tüm şirket içi bilgilerin aksi belirtilmediği sürece gizli olarak değerlendirilmesi gerekecektir (Mitnick, 2002, 27). Bilgi varlıklarını korumaya ilişkin şirket kuralarıyla ilgili güvenlik eğitimleri, yalnızca şirketin Bilgi Teknolojileri varlıklarına elektronik ya da maddi erişimi olan çalışanlara değil, şirketteki herkese yönelik olmalıdır (Mitnick, 2002, 32).

Bilgi ve ağ güvenliği grubu ve yöneticisi bilinçlendirme kuralların belirlenmesinde ve uygulama seviyesinde bilinçlendirme sürecinin hayata geçirilmesinden sorumlu olan kişidir. Bu roldeki kişinin görev ve sorumlukları şu şekilde sıralanabilir (Örnek, 2003, 8);

- Her seviyedeki personel için uygun bilinçlendirme ve eğitim materyalinin zamanında geliştirilmiş olmasını sağlamak

- Her seviyedeki personel için uygun bilinçlendirme ve eğitim materyalinin planlanan kişilere etkin bir şekilde dağıtılmasını sağlamak
- Bilinçlendirme ve eğitim materyalleri ile bunların sunumları hakkında personel ve yöneticilerin görüşlerini iletebilmelerine imkan veren uygun bir geri besleme yönteminin sağlanması
- Bilinçlendirme ve eğitim materyallerinin periyodik olarak gözden geçirilmesini ve gereksinim halinde güncellenmesini sağlamak
- Bilgi güvenliği bilinçlendirme sürecinin takip edilmesi ve uygunsuzlukların rapor edilmesinde Bilgi Güvenliği Yöneticisine yardımcı olmak

Bilgi Güvenliği Farkındalık Programlarına katılacak çalışanların, kurumsal bilgi güvenliğinin temelinde kendilerinin olduğunu bilmeleri gerekmektedir. Ayrıca Bilgi Güvenliği eğitim programı mutlaka işe yeni başlayan çalışanlar için ayrı bir içerik ile hazırlanmalı ve oryantasyon sürecinde aktarılmalıdır. Bilgi Güvenliği Farkındalık Programlarının odak konuları aşağıdaki gibi belirlenebilir (Carlson, 2001, 21);

- Güvenliğin neden önemli olduğuna ve kontrollerin neden gerektiğini net ve açık bir şekilde anlatabilmelidir.
- Çalışan Güvenlik sorumluluklarını net bir şekilde anlatmalıdır.
- Güvenlik sorunlarının tartışılması için eğitim sonunda mutlaka ek toplantılar yapılmalı ve uygulamaların etkili olabilmesi için fikir alış verişleri sağlanmalıdır.

BGYS kurallarının kuruma adapte edebilmenin önemi, önerilen sistemin kurulabilmesi ve sürdürülebilmesi için bir sürecin gerekliliğinden kaynaklanmaktadır. Eğitim ve bilinçlendirme süreçleri uzmanlıklar ve sorumluluklar kurum içinde değişik seviyelerde belirlenir ve çalışanların bu sürece katımı sağlanabilirse etkili olur. Hem sınıf için eğitimler hem de internet üzerinden verilebilecek online eğitimler BGYS süreç gelişimi ve devamlılığı için önerilebilir. Bu eğitim kurumsal güvenlik ve farkındalık eğitim programının bir parçası olmalıdır. BGYS eğitimi BGYS ve Bilgi Güvenliğinin yayarları ve BGYS'nin operasyonel işlemlere sağladığı fayda ve kurumun iş hedefleri üzerine odaklanmalıdır. Ayrıca

BGYS eğitimi BGYS konusunda başarılı olabilmenin çalışanların bireysel olarak kurallara ve sürece verdiği önemi vurgulamalıdır (Broderick, J., 2006, 30).

3.3.1.5. Bireysel İçgüdü ve Farkındalık

Bilgi Güvenliğini inceleyen bir çok makale bilgi güvenliğini etkileyen faktörler için özellikle dış faktörlere değinmiştir fakat Tejaswini ve Rao yaptıkları çalışmada bireylerin kişisel özellikleri ile farkındalık seviyelerinin de çalışanın bilgi güvenliği kurallarına uymasında önemli olduğunu ortaya koymuştur.

Geçmiş yıllarda ekonomi uzmanları içsel değerlerin yani bireysel içgüdünün rolünü incelemiş ve araştırmacılar "hiç bir yapay teşvik içsel motivasyonun gücü kadar etkili olamaz" önerisini kanıtlamışlardır. Benabou ve Tirole ekonomik ve psikolojik görüşlerin bağdaştırıldığı formal bir analiz sonucu, içsel motivasyon olgusunun oynadığı merkezi rolün sosyal ve ekonomik etkileşimlerde çok daha mantıklı olduğunu göstermiştir (Benabou and Tirole, 2003, 5).

Davis, kıdemce alt seviyede bulunan çalışanların iş hedeflerini gerçekleştirdiklerinde olduğu gibi içsel manevi ödüllerle desteklendiğinde çalışmaya daha çok motive olduğunu, dolayısıyla çalışan performansının olumlu yönde etkilendiğini belirtmiştir. Wasko, Faraj ve Ardichvili, çalışanların organizasyonda alınacak iyi sonuçları sadece kendileri için değil diğer çalışanlar ve tüm organizasyon için istediklerini deneysel olarak belirlemişlerdir. Çoğu sosyal değişim "kısıtlı kişisel ilgiler" nedeniyle değil ahlaki zorunluluklar ve toplumun görüşleri yüzünden gerçekleşmektedir. Çalışanlar gerçekten de organizasyonun menfaatinde olan aktivitelere olumlu bakmaktadır çünkü organizasyona bağlılık hissetmekte ve bu hareketlerin organizasyonel sonuçları geliştireceğini düşünmektedirler (Tejaswini and Rao, 2009, 5).

Güvenlik davranış bağlamında bazı araştırmacılar buna benzer bir görüşü baz almıştır. Culnan araştırmasında ev bilgisayarları kullanımında kullanıcı bilgi güvenliği davranışlarında "algılanan kullanıcı etkisini" göz önünde bulundurmuştur.

Bu yaklaşım Anderson tarafından da ev bilgisayarı ortamındaki güvenlik davranışları ile ilgili çalışmasında kullanılmıştır. Bu çalışmalarda "algılanan kullanıcı etkisi"; kullanıcının yaptığı bireysel hareketlerin internet güvenliği açısından bir fark yaratacağı inancını temsil etmektedir. Bu algı ile kullanıcılar yararlı güvenlik davranışlarını üstlenmektedir. Benzer olarak organizasyonlarda güvenlik politika kuralları bağlamında, eğer çalışanlar bu konudaki davranışlarının bir fark yaratacağını ve organizasyonun bilgi güvenliği hedeflerine bir katkıları olacağına inanırlarsa, güvenlik davranışlarını benimsemede daha istekli olacaklardır (Tejaswini and Rao, 2009, 5).

Özellikle kullanıcı hatalarıyla mücadele eden ekiplerde, güvenlik kültürü gelişiminin temelini oluşturan konu; kurum politikaları ve bireylerin farkındalık seviyeleridir. Farkındalık, güvenlik politikasının ortaya çıkması, onun benimsenmesi ve anlaşılmasıdır. Bir güvenlik kültürünün yapılandırılabilmesi için, güvenlik kuralları, kullanıcının tehditleri anlayışı, etkili caydırıcılar ve cezalar arasında denge kurmak zorundadır. Çalışanlara düzenli olarak verilecek güvenlik politikası eğitimi farkındalığı ve güvenlik kültürünü oluşturmada şarttır. Bu, bilgi güvenliğine olan geniş bir yönetim yaklaşımı ihtiyacını gösterir. İnsanlar, teknoloji ve organizasyon yapısı arasındaki karşılıklı etkileşim, kültürün karmaşık yapısını ve onu etkileyen faktörleri şekillendirir. Bu açıdan, özellikle organizasyonel faktörlerin güçlü olduğu yerlerde, yaptığı iş dolayısıyla daha fazla güvenilir olan organizasyonel kültür, daha emniyetsiz olabilir (Williams, 2008, 210).

3.3.2. Süreç

Mitnick Aldatma Sanatı kitabında "Güvenlik bir ürün değil, bir Süreçtir" tanımını yapmıştır. Bilgi Güvenliği altyapısındaki tüm düzenlemeler ve standartları da dâhil ederek baktığımızda, gereksinimlerin hepsini sağlayabilmek için ortak süreç kullanılmasının yararları ve bunu uygulama işlemleri güvenlik yönetimi faydaları açıkça görülebilir. Organizasyon gereksinimlerin tek bir sürece ilave edilmesindeki en zor taraf ifade edilmiş değişik dilleri ve gereksinimleri rasyonelleştirmektir. En basit yöntem, en zor gereksinimi sağlamak ve sonra bunun diğer tüm zorlu

gereksinimlerin adresleriyle derlenerek geçerli bir tanım oluşturulmasıdır. Bu yaklaşımla süreçlerdeki karmaşık bir dile olan ihtiyaç hangi varlık sınıfının dikkate alındığına göre değişir ve elenebilir (Broderick, 2006, 27).

Güvenlik çatısının kullanımını kontrol eden bir organizasyon tüm ilgili gereksinimleri belirlemelidir. Bu güvenlik çatısı, denetim tablolarının ortak kurulumunu tanımlar ve kullanır, organizasyonlarının diğer ihtiyaçlarına uygulanabilir ve derleme ile birlikte işlemi denetleyebilir. Bu fikirler kritik BGYS alanının kapsamında adreslenir. Bir organizasyonun adreslenmesi gereken en önemli faktör BYGS süreç kapsamıdır (Broderick, 2006, 27). Kapsam çok genişse BGYS'nin gelişimi ve işletimi masrafı fazla olabilir. Kapsam sınırlıysa BGYS, organizasyonun bilgi varlığını korumada etkisiz olabilir.

3.3.2.1. Bilgi Güvenliği Yönetim Sistemi

Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası (ISO/IEC 27001, 2006).

1990'lı yıllarda İngiliz standardı BS-7799' un gelişimi ile Bilgi güvenliği yönetim sistemi (BGYS- ISMS) kavramı resmi olarak ortaya çıktı. Bundan önceki BS-5750 ve ISO-9000 gibi nitelikli standartlar, bazı organizasyonlar tarafından işlerini daha tahmin edilebilir kılmak için benimsenmiş ve bazı bilgi güvenliği programlarına dahil edilmiştir. BS-7799 standardı, bilgi güvenliği dünyasında ilk ve en yaygın olarak geliştirilmiş standarttır. BS-7799 öncesinde birçok organizasyon bilgi güvenliği konusunda kendine has bir kurallar zinciri oluşturmuştur. 2000 kadar organizasyon (bilgi güvenliği yönetim sistemi uluslararası kullanıcı grubu) kendi seçtikleri BGYS çatısına uyumlu sertifikasyonu başarmışlardır (Broderick, 2006, 26).

Tablo 3.1'de BS-7799 sonrası oluşan BGYS standartları ve karşılaştırmaları bulunmaktadır. Tablonun belirttiği gibi, en son güvenlik standartı, ISO- 27001:2005, doğrudan BS-7799 ile ilişkilidir. ISO- 27001:2005 içeriğinde orijinal standardın ana

terimleri korunmuş olmasına karşın gerçekleştirme ve yönetim gereksinimleri mevcut güvenlik gereksinimlerine göre değiştirilmiştir. BS-7799 ‘de 127 olan kontrol sayısı ISO-27001:2005 ile 133 e çıkmıştır (Broderick, 2006, 26);

Tablo 3-2 BS-7799’dan sonraki gelişim (Broderick, 2006, 27)

ISO-27001:2005	**ISO/IEC-17799:2005**	**BS-7799-2:2002**	**ISO/IEC-17799:2000**
Güvenlik Politikası Bilgi güvenliğinin düzenlenmesi	Güvenlik Politikası Bilgi güvenliğinin düzenlenmesi	Bilgi güvenliği Politikaları Organizasyonel güvenlik	Güvenlik Politikası Organizasyonel güvenlik
Varlık yönetimi İnsan kaynakları güvenliği	Varlık yönetimi İnsan kaynakları güvenliği	Varlık sınıflandırma ve kontrol Çalışan güvenliği	Varlık sınıflandırma ve kontrol Çalışan güvenliği
Fiziksel ve çevresel güvenlik	Fiziksel ve çevresel güvenlik	Fiziksel ve çevresel güvenlik	Fiziksel ve çevresel güvenlik
İletişim ve İşlemlerin yönetimi	İletişim ve İşlemlerin yönetimi	İletişim ve İşlemlerin yönetimi	İletişim ve İşlemlerin yönetimi
Erişim Denetimi Bilgi sistemlerinin oluşturulması, geliştirilmesi ve bakımı	Erişim Denetimi Bilgi sistemlerinin oluşturulması, geliştirilmesi ve bakımı	Erişim Denetimi Sistemlerin geliştirilmesi ve bakımı	Erişim Denetimi Sistemlerin geliştirilmesi ve bakımı
Bilgi güvenliği vaka yönetimi	Bilgi güvenliği vaka yönetimi	Herhangi bir bölüm dahil edilmemiştir	Herhangi bir bölüm dahil edilmemiştir
İş sürekliliği	İş sürekliliği yönetimi	İş sürekliliği yönetimi	İş sürekliliği yönetimi
Uyumluluk	Uyumluluk	Uyumluluk	Uyumluluk

IT yönetim enstitüsü ve Bilgi teknolojileri Sistemleri denetleme ve kontrol birliği'nin modeli olan COBIT sadece bilgi güvenliği değil adresleme için de tasarlanmıştır, örneğin COBIT IT yönetimi ve altyapı denetimi, güvenlik ve diğer riskleri kapsar (Broderick, 2006, 28).

Bilgi Güvenliği Yönetimi, akademik dünya, kamu kurumları ve özel sektör tarafından ilgiyle takip edilen bir kavramdır. Kurumlardaki bilgi güvenliği sorumluluğunun, kurumun en üst düzey yöneticisinde olması ve üst düzey yöneticinin bilgi güvenliği ile ilgili kararları alması ve bu kararların uygulandığını takip etmesi şeklinde özetlenebilecek bir kavramdır. Bilgi güvenliği yönetimi gelişmiş ülkelerde yasalar tarafından desteklenmektedir. 2002'de Amerika Birleşik Devletleri'nin yürürlüğe koyduğu Federal Information Security Management (FISMA) yasası ya da Türkiye'de Amerikan Serbest Piyasa Kurulu'na (SEC) kayıtlı olan şirketlerinde uymak zorunda olduğu Sarbanes-Oxley (SOX) yasası örnek olarak verilebilir. Ayrıca, uluslararası organizasyonlar tarafından bilgi güvenliği yönetişimi konusunda raporlar ve kılavuzlar üretilmektedir. OECD'nin(Organization for Economic Cooperation and Development) bilgi sistemleri ve ağlarda güvenliğin sağlanması ile ilgili kılavuzu buna örnek olarak verilebilir. Bilgi güvenliği yönetimi konusunda yapılmış akademik çalışmalar da mevcuttur. Ayrıca, enstitüler, kar amacı gütmeyen kurumlar ve kamu kurumlarının hazırlamış olduğu yurtdışı kaynaklı bilgi güvenliği yönetişimi çalışmaları bulunmaktadır (Karabacak, 2008, 1).

3.3.2.1.1. Kavram Olarak BGYS

Bilgi Güvenliği Yönetim Sistemi(ISMS- Information Security Management System) kurumun risk yönetim stratejisidir. BGYS güvenlik kuralları ile belirlenmiş ve Bilgi Güvenliği yöneticisi tarafından yönetilen bir süreçtir. BYGS içinde güvenlik çemberi belirlenmiş, kontrol alanları tanımlanmış ve her bir kontrol alanı için bir risk yönetim stratejisi belirlenmiştir. BGYS kuruma özel bir bilgi güvenliği yol haritasıdır (Carlson, 2001, 7).

BGYS dökümantasyonunun içeriği kuruma özgü olarak değişebilir ama ana başlıkları belirlidir (Carlson, 2001, 7);

- Güvenlik Altyapı Organizasyon Şeması,
- Risk Yönetim Stratejisi
- Bilgi Güvenliği Grubu ve Takım Yöneticisi iş tanımı
- BGYS Dökümanı kontrol ve Süreklilik Planı
- Güvenlik Risk Yönetim Planı
- Uygulanabilirlik Beyannamesi
- Müşteri Yönetim Kodu
- Tüm kabul edilen dökümantasyonu içeren BGYS dökümantasyon matrisi

Bilgi güvenliği yönetim sistemi ile işletmelerdeki örgütsel bilgi öğrenme sürecinde ve örgütsel bilgi akışında üretilen ve paylaşılan bilgilerin gizliliğine, bütünlüğüne ve erişilebilirliğine riskler yönetilebilir hale gelir. Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası olarak tanımlanır (Carlson, 2001, 8).

Entelektüel sermaye tanım olarak "bir işletmenin bilgi ilişkileri birikiminin ekonomik değerini ifade etmektedir. Bilgi güvenliği üzerine artan ve yoğunlaşan çalışmalar artık her şeyin bir "rekabet" unsuru olduğu çağımızda ekonomik değer haline gelen entelektüel sermayenin korunması ihtiyacından kaynaklı ortaya çıkmıştır. Organizasyonların bilgi güvenliği yönetim sistemlerini kurmalarının ve diğer denetim mekanizmalarına dahil olmalarının altında yatan kök neden, çağımızın asıl değeri haline gelen, şirketlerin insan sermayelerinin, yapısal sermayelerinin ve müşteri sermayelerinin karşılıklı etkileşimi ile ortaya çıkan entelektüel sermayelerinin korunması gerekliliğidir.

Bilgi Güvenliği Yönetim Sistemi BGYS, kurumun hassas bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşımdır. Bu sistemin temel amacı hassas bilginin korunmasıdır. Bu sistem çalışanları, iş süreçlerini ve bilgi teknolojileri (BT) sistemlerini kapsar. Bilgi Güvenliği Yönetim Sistemi deyimi ilk kez 1998 yılında BSI (British Standards Institute) tarafından yayınlanan BS 7799-2 standardında kullanılmıştır. Daha sonra bu standart Uluslararası Standartlar Kurumu

ISO tarafından kabul edilmiş ve ISO/IEC 27001:2005 olarak yayınlanmıştır. BSI tarafından yayınlanan bir diğer standart BS 7799-1 ise bilgi güvenliğinin sağlanmasında kullanılacak kontrollerden bahsetmektedir. Bu da yine ISO tarafından kabul edilmiş ve ISO/IEC 27002:2005 olarak yayınlanmıştır. ISO/IEC 27002:2005 bu standardın Temmuz 2007'den itibaren kullanılan ismidir, bu tarihe kadar standart ISO/IEC 17799:2005 olarak adlandırılıyordu (Dinçer ve Dinçkan, 2007, 7).

Bilgi güvenliği yönetimi konusunda yaygın olarak kullanılan standart, "ISO/IEC 27002:2005 "Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri" standardıdır. Bu standart, işletmeler içerisinde bilgi güvenliği yönetimini başlatmak, gerçekleştirmek, sürdürmek ve iyileştirmek için genel prensipleri ve yönlendirici bilgileri ortaya koyar. ISO/IEC 27002:2005 rehber edinilerek kurulan BGYS'nin belgelendirmesi için "ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler" standardı kullanılmaktadır. Bu standart, dokümante edilmiş bir BGYS'ni kurumun tüm iş riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsamaktadır. İş risklerini karşılamak amacıyla ISO/IEC 27002:2005'te ortaya konan kontrol hedeflerinin kurum içerisinde nasıl uygulanacağı ve denetleneceği ISO/IEC 27001:2005'te belirlenmektedir (Dinçer ve Dinçkan, 2007, 7).

ISO/IEC 27001 ve ISO/IEC 27002 standartları BGYS konusunda en temel başvuru kaynaklarıdır. Bu iki standart da doğrudan bilgi güvenliği konusunu ele alırlar. Teknik ve teknoloji bağımlı standartlar değildirler. Belli bir ürün veya bilgi teknolojisi ile ilgilenmezler. Hatta bilgi teknolojileri güvenliği dahi bu standartların içerisinde yer almaz. Tek ilgi alanı vardır, o da bilgi güvenliğidir.

Bilgi güvenliği yönetim sistemi, kurum içinde var olan tüm bilgi varlıklarının değerlendirilmesi ve bu varlıkların sahip oldukları zayıflıkları ve karşı karşıya oldukları tehditleri göz önüne alan bir risk analizi yapılmasını gerektirir. Kurum kendine bir risk yönetimi metodu seçmeli ve risk işleme için bir plan hazırlamalıdır. Risk işleme için standartta öngörülen kontrol hedefleri ve kontrollerden seçimler yapılmalı ve uygulanmalıdır. PUKÖ çevrimi uyarınca risk yönetim faaliyetlerini yürütmeli ve varlığın risk seviyesi kabul edilebilir bir seviyeye geriletilene kadar

çalışmayı sürdürmelidir. Bunun yanında BGYS'nin her kurumun özelliklerine bağlı olarak özelleştirilmesi gerektiği unutulmamalıdır.

3.3.2.1.2. PUKÖ (Planla – Uygula – Kontrol et – Önlem al) Modeli

Kuruluş, dokümante edilmiş bir BGYS'yi, kuruluşun tüm ticari faaliyetleri ve karşılaştığı riskleri bağlamında, kurmalı, gerçekleştirmeli, işletmeli, izlemeli, gözden geçirmeli, sürdürmeli ve geliştirmelidir. Bu standardın bir gereği olarak, kullanılan proses, Şekil 3.2'de gösterilen PUKÖ modeline dayanır (ISO/IEC 27001, 2006).

PUKÖ (Planla – Uygula –Kontrol et – Önlem al) modeli, BGYS standartları kapsamında BGYS'in kurulumu, gerçeklenmesi, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve tekrar gözden geçirilmesi çalışmaları için kullanılmaktadır. PUKÖ modelinde yer alan temel maddelerin karşılıkları aşağıdaki gibidir. (ISO/IEC 27001, 2006; Dinçer ve Dinçkan, 2007, 9)

1. **Planla:** İş gereklerine ve yasalara göre BGYS'ye girdi olan ihtiyaçlar belirlenir. Bu ihtiyaçlara uygun risk değerleme yaklaşımı belirlenir ve BGYS'nin ayrıntıları tasarlanır. BGYS' nin kurulum adımı olarak ta tanımlanmaktadır.

2. **Uygula:** Risk analizinde elde edilen sonuçlara göre standardın ön gördüğü kontrol maddeleri uygulanır. Yani BGYS'nn gerçekleştirilmesi ve işletilmesi adımıdır.

3. **Kontrol Et:** BGYS süreçleri gözden geçirilerek kontrollerin gerçekleşme oranları tespit edilir. BGYS'nin izlenmesi ve gözden geçirilmesi adımıdır.

4. **Önlem Al:** Tespit edilen önleyici etkinlikler için gerekirse yeniden planlama yapma yoluna gidilir. BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi adımıdır.

PUKÖ modelini görsel olarak anlatan Şekil 3.3; bir Bilgi Güvenliği Yönetim Sistemi'nin bilgi güvenliği gereksinimlerini ve ilgili tarafların beklentilerini girdi olarak nasıl aldığını ve gerekli eylem ve prosesler aracılığıyla, bu gereksinimleri ve beklentileri karşılayacak bilgi güvenliği sonuçlarını nasıl ürettiğini gösterir (Dinçer ve Dinçkan, 2007, 9).

PUKÖ modeli özet olarak kurum içinde Bilgi Güvenliği ve sürekliliği konusunda ne yapılacağına karar verilmesi, kararların gerçekleştirilmesi, çalıştığının kontrol edilmesi hedefine uygun çalışmayan kontroller için önlemlerin alınmasıdır.

3-3 PUKÖ Döngüsü

Bilgi güvenliği yönetimi, başlangıç, bitiş tarihleri ile bir kontrol süreci ve süreç güncelleme dökümantasyonu olan bir proje gibi görülmemelidir. Bu proje ek olarak sürekli devam eden bir gelişim süreci olarak düşünülmelidir. PUKÖ modelinde gösterildiği gibi BGYS konusunda kurum faaliyetleri, kontrolleri ve güncellemeleri bir döngü içinde durmaksızın devam etmelidir. Bundan sonraki BYGS ile ilgili bölümler ISO/IEC 27001 dökümanı baz alınarak değerlendirilmiştir.

3.3.2.1.3. BGYS'nin Kurum için Önemi

Kurum için Bilgi Güvenliği Yönetim Sistemi kurulumu, kurulum adımları, Kurulum Adımları, Gerçekleştirilmesi ve İşletilmesi, İzlenmesi ve Gözden Geçirilmesi, Sürekliliğinin Sağlanması ve İyileştirilmesi adımları ISO/IEC 27001 dökümantasyonunda detaylı olarak aktarılmaktadır.

ISO 27001 Bilgi Güvenliği Yönetim Sistemi kurmanın yararları şu şekilde sıralanabilir;

- Bilgi varlıklarının farkına varma: Kuruluş hangi bilgi varlıklarının olduğunu, değerinin farkına varır.
- Sahip olduğu varlıkları koruyabilme: Kuracağı kontroller ile koruma metotlarını belirler ve uygulayarak korur.
- İş sürekliliği: Uzun yıllar boyunca işini garanti eder. Ayrıca bir felaket halinde, işe devam etme yeterliliğine sahip olur.
- İlgili taraflar ile barış halinde olma: Başta tedarikçileri olmak üzere, bilgileri korunacağından ilgili tarafların güvenini kazanır.
- Bilgiyi bir sistem sayesinde korur, tesadüfe bırakmaz.
- Müşterileri değerlendirirse, rakiplerine göre daha iyi değerlendirilir.
- Çalışanların motivasyonunu arttırır.
- Yasal takipleri önler ya da takip durumunda gerekli verilerin düzenli sağlanması.

3.3.2.2. Risk Yönetimi

Bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler (ISO/IEC 27001, 2006). Bilgi, bir kurumun en kritik iş kaynağıdır. Bunun bir sonucu olarak, kurumlar işlerinin standart uygulamaları gibi, bilginin güvenilirliğini de yönetebilmeliler. Kurumların, bilgi güvenliği yönetimi uygulamalarında aşırıya kaçmaları, risk yönetimine çok fazla kaynak harcanmasına, bu da işlerin yürütülebilmesi ya da risklerin azaltılması için yeterli kaynağın kalmamasına sebebiyet verebilir (Broderick, 2001, 1).

Glenn Weakdock, "Exploding the Computer Myth- Bilgisayar Efsanesinin Doğuşu" isimli kitabında; bilgisayarlar da insanlar gibi düşünebilseydi, birçok bilgisayar sisteminin aşağıdaki özelliklere sahip olabileceğini konu almıştır (Broderick, 2001, 2);

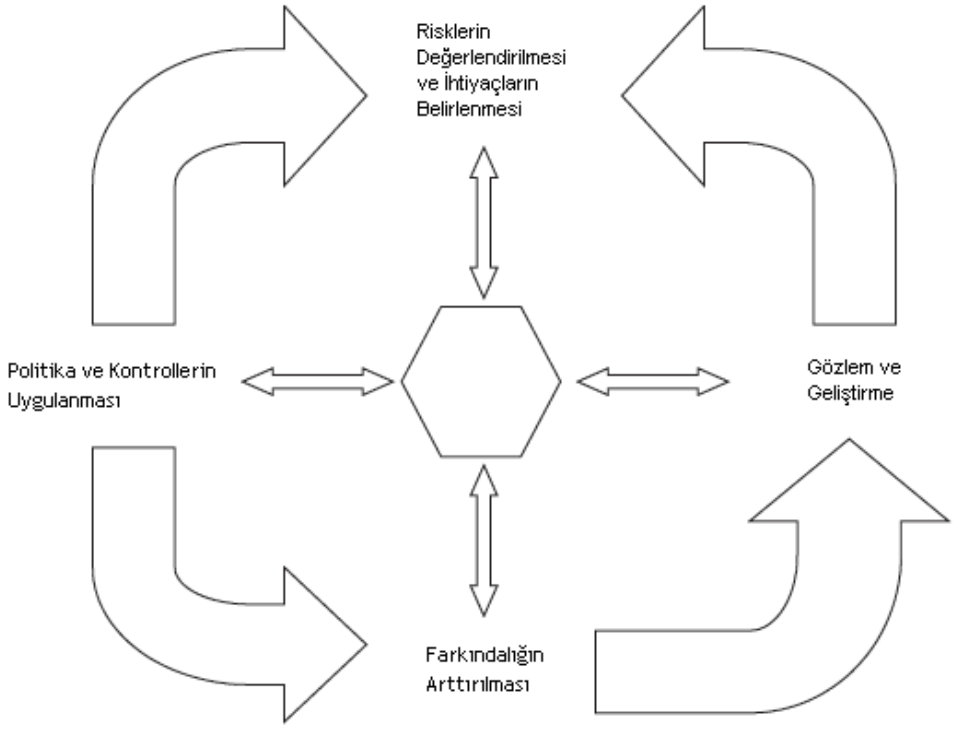
- Yüksek ücretlendirme, eksik çalışma, vaktin boşa harcanması.
- Maliyet: Bir işin yaşam döngüsü düşünüldüğünde; eğitim, dokümantasyon, devamlılığın sağlanması, sorun giderme, onarma ve teknik destek gibi giderin maliyetinin yüksek olması
- Eğitim ve İletişim Güçlükleri: Çok az seviyede dil bilgisine sahip olma, belki başlangıç seviyesinde bir İngilizce ve duyma-konuşma yetileri ile iletişim kuramama
- İnisiyatif ya da yaratıcı düşünceye sahip olamama, yeni ve orijinal fikirler oluşturamama
- Değişen çevre şartlarına uyum sağlamak için davranış biçimini değiştirememe
- Sadece çok iyi detaylandırılmış komutları birebir yerine getirme: Yıkıcı bir etkiye sahip olabilecek komutları dahi sorgulamadan yerine getirme, yargı yetisine sahip olmama
- Elverişli kullanım için eğitilmiş insan desteğine ihtiyaç duyma

Bu maddeler göz önüne alındığında; bilgiyi oluşturmak, saklamak ya da işlemek için bilgisayar sistemleri kullanan her şirket, çeşitli riskler ile karşılaşacaktır. Karşılaştığı bu riskleri anlamak ve risk yönetiminde uygulayacağı politikaya; kabullenmek, azaltmak ya da ret etmek gibi, karar vermek zorundadır.

Şirketler bazen çok ender durumlarda olsa bile bilgi güvenliği için risk yönetimi yapamayabilir. Bu durumlar; bilgiye, açıklanması gereken bilgiye, kaybetmemesi gereke bilgiye, kaybolması ya da ulaşılamaması durumunda, iş yaşam döngüsünü negatif yönde etkileyen bilgiye sahip olunması durumlarıdır. Bir kurum sahip olduğu bilgiyi korumak zorunda olmaması, bilginin yaratılması, işlenmesi, depolanması ve yok edilmesi işlemleri sırasında karşılaşılabilecek risklerin

yönetiminin gerekliliğini de ortadan kaldırır. Diğer bütün durumlar için, kurum Bilgi Güvenlik Riskleri yönetiminden sorumludur (Broderick, 2001, 2).

Bilgi ve sahip olunan bilginin korunması şirketler için kritik bir gereklilik olduğundan, Bilgi Güvenlik Yönetimi, birçok kurum için, kurumların Kalite Güvencesi programlarının bir parçası olarak düşünülmektedir. Bilgi Güvenlik Riskleri Yönetiminin, her yönüyle bilginin yaratılması, işlenmesi, depolanması ve yok edilmesi işlemleri için uygulanma gerekliliği olmakla beraber çalışmalar, bilgisayar sistemleri ile yönetilen bilgi ile sınırlandırılmıştır. Şekil 3.3'de gösterilen Risk Yönetim Devri, 1998 yılında Amerika İdari Muhasebe Ofisi tarafından hazırlanan Bilgi Güvenliği Yönetim raporu kapsamında yayınlanmıştır. Bu diyagramda da açıklandığı gibi, Risk Yönetimi süreklilik gerektiren, aynı temellere bağlı kalınarak tekrarlanması gereken bir uygulamadır. Diyagramda, Risk Yönetiminin 4 temel prensibinin odaksal merkez noktası etrafındaki birliktelikleri, yani risk yönetimi prensiplerinin etkileşimlerini gösterilmektedir. Odaksal merkez noktası; yönetimin, risk değerlendirme işleminden haberdar olduğunu ve cevap vermeye hazır olduğunu garanti eder (Broderick, 2001, 3).



3-4 Risk Yönetim Devri (Broderick, 2001, 3)

Bilgi Güvenliği Risk Yönetimi birçok yönü ile Bilgi Güvenliğine benzemektedir. İkisinin de yaşam döngüsü 4 ana madde ile değerlendirilebilir. Bu maddeler İş Süreci, Bilginin Hassasiyeti, Bilginin Kritikliği ve Bilginin Değeridir. Bu maddeleri daha detaylı olarak açıklayabiliriz; (Bojanc and Jerman, 2008, 3)

- **İş Süreci:** Bu terim, kurumların iş yaşam döngüsü içindeki pozisyonlarını göstermektedir. Kurumun başlangıç veya başlangıç öncesi evreleri, kurumun beş ile yüz yıl arasındaki dönemi ile kıyaslandığında Bilgi Riski konusunda tamamen farklı bir perspektife sahiptir. Temel farklar; bilgi rezervi miktarı, sahip olunan bilgilerin değeri ve bilgiye erişimin engellenmesi, gecikmesi, bilginin silinmesi, kopyalanması ya da değiştirilmesi durumunun kurum üzerindeki etkisi olarak söylenebilir. Kurumlar yaşam döngülerinin başlangıç evrelerinde, sonraki dönemlere göre genelde daha az ancak müşteri ya da araştırma bilgileri gibi yüksek değerli bilgilere sahiptirler.

- **Bilginin Hassasiyeti:** Bilginin hassasiyeti genelde ilgili bilginin değeri ile ilişkilidir. Bilginin hassasiyetini etkileyen faktörler; bilginin yaratılma ya da elde edilme maliyeti ile sahip olduğu bilgiye göre değerlendirildiğinde kurumun değeri olarak belirtilebilir. Maaş detayları, çalışan kayıtları, finansal kayıtlar gibi kurum çalışanlarına ya da kuruma ortak kişilere ait bilgiler genelde hassas bilgi kapsamına girmektedir. Kurumlar hassas bilgiye yetkisiz erişimi, değiştirmeyi, silmeyi ve yayınlamayı engellemek için çeşitli koruma mekanizmaları araştırmaktadırlar.

- **Bilginin Kritikliği:** Bir faaliyet veya kurumun başarısının devamı için gerekli olan bilgi doğası gereği bu kapsamda yer alır. Hassas bilginin korunması gibi kritik bilgi de çok iyi bir şekilde korunmalıdır.

- **Bilginin Değeri:** Birçok kurum, sahip olduğu bilgiye değer biçememekte veya bilginin çok az bir değere sahip olduğunu öne sürmektedirler. Ancak bu iki yaklaşımda doğru değildir. Her bilginin bir değeri vardır, çünkü her bilginin yaratma, devamlılık ve kullanım ile ilişkilendirilmiş bir maliyeti

bulunmaktadır. Güncelliğinin veya uygunluğunun devamı sağlanmayan ya da kullanılmayan bilgi kurum için bir değere sahip değildir ve silinmesi gerekir. Aksi halde bilgilerin depolanması ve yönetimi kurum için gereksiz bir masraf olacaktır. Bilginin yaratılması, bilgi ister orijinal olsun ister başka bir bilgiden türetilsin her zaman değeri ile ilişkilendirilmiş bir maliyete sahiptir.

Riskin önemi, onun kurum faaliyetleri üzerindeki etkisine bağlıdır. Bu yüzden güvenlik riski, bilginin yaratılması, depolanması, yönetilmesi, işlenmesi veya dağıtılması işlemlerinin uygun bir şekilde yönetilmesi ile doğrudan ilişkilidir. Risk yönetimine çok fazla odaklanmak kurumu zayıflatabilirken, gereğinden az önem vermek ise kurumu gereksiz risklerle karşılaştırabilir.

3.3.3. Teknik

Bilgisayar ve iletişim endüstrilerindeki hızlı gelişme, programcı, sistem analisti, bilgisayar mühendisi, web tasarımcısı gibi mesleklere büyük ve giderek daha da büyüyen bir talep yaratmıştır. E-ticaret ve e-öğrenme alanlarındaki gelişmeler de çok sayıda insanın geleneksel iş alanlarında yeni bilgi ve beceriler kazanarak enformasyon teknolojisi ile ilgili iş alanlarına geçmesine olanak sağlamaktadır (Barutçugil, 2002, 34). Bu iş alanlarındaki artış ile beraber internet kullanımı yayınlaşmakta ve internet üzerinden yapılan bilgi paylaşımları hızla artmaktadır. Bilgi paylaşımı sonucunda uzaman kişiler tarafından tespit edilen sistem açıklıkları artmaya başlamış ve dolayısıyla bu açıklıkların nasıl kullanılabileceğine dair bilgiye erişimde artmaktadır. Bu açıklıkları kullanarak sistemlere ve kurumlara her gün binlerce saldırı gerçekleşmektedir. Şirket içi Tehdit kavramı da bu noktada büyük önem kazanmaktadır. Şirket içi tehdit kavramı içinde baz alınan tanım ise işçiler, personel, yönetim veya şirkette bulunan yüklenici firma elemanlarının sistemin, süreçlerin ve uygulamaların açıklarını kullanarak hile ve sahtekarlık ile kişisel kazanç ve kar elde etmesi veya şirkette operasyon veya IT seviyesinde farkında olmadan zarar ya da kötü niyet ile sabotaj gerçekleştirmesidir (Humphreys, 2008, 247).

Şirket içi tehdit kimi zaman direktör seviyesinden, üst düzey yönetim kademesinden hatta CEO'dan bile gelebilir. Aynı şekilde yönetim kademesinde olmayan herhangi bir işçi tarafından da gerçekleşebilir. Teknik uzmanlar, sistem yöneticisi veya teknik olamayan bir çalışan için de geçerlidir. Organizasyonun içinde olmak veya çalışmak hakkına sahip olan her kişi potansiyel adaydır. Kin tutan, adil bulmadığı bir yaklaşımla karşılaştığını düşünen herhangi biri olabilir. Bu durumdaki bir çalışan IT sistemini sabote etme, şirket dosyalarına zarar vererek bilgi kayıplarına neden olma, bilgi çalma veya bu durumu eşitleyebileceğini düşündüğü başka davranışlar içine girebilir. Organizasyonlar için probleme neden olacak bu tür bir çok davranış gözlemlenebilir, aynı zamanda bu davranışların organizasyon dışında da ciddi etkileri gözlemlenebilir. Örneğin, kin tutan bir çalışan şirket dosyalarına zarar verirken iş ortakları, müşteriler ve tedarikçilere ait bilgilere de zarar vermiş olabilir (Humphreys, 2008, 247).

Elbette ki bu, bilgiye ulaşan ayrıcalıklı haklara sahip olan bir çalışan ya da bu bilgiyi yetkisiz, kural dışı olarak iş fonksiyonu dışında herhangi bir yöntemle kullanarak kazanç elde etmek isteyen bir çalışan da olabilir. Sahtekarlık/ dolandırıcılık bu tarz tehditlere örnektir. Amerika ve İngiltere'de yapılan araştırmalar organizasyonlarda gerçekleşen güvenlik vakalarının %35'ine şirket içi tehditlerin neden olduğunu göstermiştir ve bu tür vakalar gün geçtikçe artmaktadır. Çoğu çalışma göstermiştir ki en sık karşılaşılan iç tehdit türleri bilgi hırsızlığı, dolandırıcılık ve şirket varlıklarını sabote eden davranışlardır.

İç tehditlerin şirketler için büyüyen bir problem olduğu gözlemlenilse de en az bu konu kadar önemli başka bir problem de şirket içi zayıflıklardır. Bu açıklar/zayıflıklar organizasyonun bilgi varlığı güvenliğini tehdit edebilir. Örneğin veri işlerken yapılacak insan hataları, teknik sistemlerin yetersizliği ya da güncel olmaması veya bilgi güvenliği sistemlerini yöneten teknik personelin eğitim yetersizliği; bilgi varlığı bütünlüğünü tehdit edecek zayıflıklara örnek oluşturabilir. Ayrıca ters sosyal mühendislik tekniğinin tehlikesinin farkında olmamak masum bir bilgi güvenliği teknik personel ekibindeki bir çalışanın şirkete ait gizli bilgilerini açığa çıkarmasına neden olabilir. Ayrıca yine sosyal mühendislik saldırıları ile

güvenlik bölümü çalışanlarından alınacak kullanılan güvenlik ürünlerinin bilgileri kurum için çok büyük tehdit oluşturacaktır (Humphreys, 2008, 247).

PricewaterhouseCoopers şirketinin 2007 ve 2008 yıllarına göre bazı güvenlik araçları kullanımının dağılımı ile ilgili sonuçlar tablo 3.3'de gösterilmiştir. Bilgi güvenliği projelerinin birincil kaynağı IT grupları ile teknoloji birçok güvenlik sorularının cevabı haline geldi. Birçokları geniş kapsamlı IT şirketi altyapı güvenliği için çeşitli güvenlik araçları kullanmaktadır. Aşağıdaki tablo 2007- 2008 yıllarına göre bazı güvenlik araçları kullanımının dağılımı vermektedir.

Tablo 3-3 Güvenlik Araçları kullanımı (PricewaterhouseCoopers, 2008, 11)

Teknoloji	**2007**	**2008**
Şüpheli Kod Tespit Araçları	%80	%84
Uygulama Seviyesi Güvenlik Duvarları/Firewalllar	%62	%67
Atak Tespit	%59	%63
Atak Engelleme	%52	%62
Şifreleme		
Veritabanı	%45	%55
Dizüstü Bilgisayar	%40	%50
Yedekleme- kartuş	%37	%47
Otomatik Parola Sıfırlama	%40	%45
Elde Taşınabilen Cihaz Güvenliği	%33	%42

Bilgi ve bilgisayar güvenliğinde, karşı taraf, kötü niyetli olarak nitelendirilen kişiler (korsanlar veya saldırganlar) ve yaptıkları saldırılardır. Var olan bilgi ve bilgisayar güvenliği sistemini aşmak veya atlatmak, zafiyete uğratmak, kişileri doğrudan veya dolaylı olarak zarara uğratmak, sistemlere zarar vermek, sistemlerin işleyişini aksattırmak, durdurmak, çökertmek veya yıkmak gibi kötü amaçlarla bilgisayar sistemleri ile ilgili yapılan girişimler saldırı veya atak olarak adlandırılmaktadır. Saldırganlar, amaçlarına ulaşmak için çok farklı teknikler içeren saldırılar gerçekleştirmektedirler. Saldırı türlerinin bilinmesi, doğru bir şekilde analiz edilmesi

ve gereken önlemlerin belirlenmesi, bilgi güvenliği için büyük bir önem arz etmektedir (Canberk G. ve Sağıroğlu Ş., 2006)

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 önleme olarak" tanımlanır. Bilgisayar teknolojilerinde güvenliğin amacı ise "kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin yapılarak gerekli önlemlerin önceden alınmasıdır" (Canberk G. ve Sağıroğlu Ş., 2006)

Güvenlik açıklarını kurum içinde en aza indirmek ve yetkisiz kişilerin kurum için bilgilere erişimlerini engelleyebilmek amacıyla bazı altyapılar kullanılmakta ve bu alt yapılar belirli politikalar, prosedürler, planlar ve standartlar yardımıyla yönetilmektedirler.

Standartlar; bilgi güvenliği kurallarının kurum içinde uygulanmasını sağlarlar. Kurum içi bilgi güvenliği teknik standartları şu konuları kapsamalıdır (Carlson, 2001, 16);

- Kişisel Güvenlik
- Çalışan Yönetimi
- Veri Sınıflandırma
- Veri Kullanma
- Veri İletimi
- Veri şifreleme
- VPNs- Sanal Özel Ağlar Virtual Private Network
- Veri Kurtarma
- Veri Yönlendirme(routing)
- Erişim Kontrol
- Firewall Standart
- Ağ Güvenliği
- Ağ Uygulamaları
- Log Üretimi ve Yönetimi

- Varlık Yönetimi
- Alarm Yönetimi
- Fiziksel Güvenlik

Politikalar; Bilgi güvenliğinin en iyi uygulanma biçimini resmileştirerek kurum içinde uygulanmasını sağlarlar. Kurum içi bilgi güvenliği teknik politikaları şu konuları kapsamalıdır (Carlson, 2001, 17);

- Erişim Kontrol
- Veri Güvenliği
- Router Konfigürasyonu ve Yönetimi
- Organizasyonel Güvenlik

Prosedürler; Detaylı Bilgi güvenliği kurulumunu uygun standart ve kurallar ile kurum içinde uygulanmasını sağlarlar. Kurum içi bilgi güvenliği teknik prosedürleri şu konuları kapsamalıdır (Carlson, 2001, 17);

- Risk Yönetimi
- Yedekleme ve Geri Yükleme (Backup/Restore)
- Sistem kullanıcı ekleme, silme ve değiştirme
- Altyapı Bakım
- Altyapı Kontrol
- Güvenlik Bakım
- Şifre Yönetimi
- Firewall Kurulumu
- Vaka Yönetimi

Plan/Programlar; Bilgi güvenliği hedeflerine uyuma teşvik ederler.. Kurum içi bilgi güvenliği teknik plan ve programları şu konuları kapsamalıdır (Carlson, 2001, 17);

- Bilgi Güvenliği Farkındalık
- Değişim Yönetimi
- Vaka Yönetimi

- Atak Tespit
- İş Sürekliliği

Kurumun güvenliği, organizasyonu koruyan teknolojilerden kaynaklanan ek tehditlere açık olabilir. Bu gibi durumlar, uygun teknik çözümlerin bilinmemesi ve teknoloji yönetimindeki yetersizlikler nedeniyle ortaya çıkar. Daha açık söylemek gerekirse, yanlış ve etkisiz bir konfigurasyon veya teknoloji çözümleri yönetiminin uygunsuz olması teknolojinin bilmeden ve yanlış kullanılmasına sebep olmaktadır. Kurum içi tehditler incelendiğinde tehdidi oluşturan kişinin potansiyel olarak kurum içindeki koruyucu sistemlere giriş bilgisine ve genişletilmiş erişim kontrollerine sahip olduğu görülmüştür. Bütün bunlar saldırıyı etkiler ve tespit edilmeyi zorlaştırır (Williams, 2008, 210). Bu nedenle Bilgi Güvenliği Ekibinin yetkinlik seviyesi teknik açıklıkların kapatılmasında ve vakaların önlenmesi açısından çok önemlidir.

3.3.4. Telekomünikasyon Sektöründe Bilgi Güvenliği Yönetimi ve Denetim İçin Standartlar, Yasalar ve Düzenlemeler

3.3.4.1. Standartlar

Bilgi güvenliği yönetimi, IT güvenliğinin tersine ancak günümüzde olgunlaşmış bir alandır. Yıllar boyu odaklanan nokta IT güvenliğiydi ve bu güvenliğin uygulanması ve kontrolü IT departmanları ve teknik uzmanlar tarafından yürütülmekteydi. 90'ların başında bu durum, güvenliğin IT kadar insana, süreçlere ve bilgiye bağlı olduğu noktasına odaklanan BS 7799 bilgi güvenliği yönetimi standardının ilk taslağıyla değişmeye başladı. 90'lardan bugüne bilgi güvenliğini bu seviyeye getiren ise taslak durumundaki bu güvenlik standartlarının birçok yenilenme ve gelişim ile ISO/IEC tarafından yayınlanan uluslararası standartlara dönüşmesidir. Bu standartlar günümüzde dünya çapında binlerce organizasyon tarafından kullanılmaktadır (Humphreys, 2008, 249).

3.3.4.1.1. TS ISO/IEC 27001

Bu standart, ISO tarafından kabul edilen, ISO/IEC 27001 (2005) standardı esas alınarak, TSE Bilgi Teknolojileri ve İletişim İhtisas Grubu'nca hazırlanmış ve TSE Teknik Kurulu'nun 02 Mart 2006 tarihli toplantısında Türk Standardı olarak kabul edilerek yayımına karar verilmiştir (ISO/IEC 27001, 2006).

Bu standart, Bilgi Güvenliği Yönetim Sistemi'ni -BGYS (Information Security Management System - ISMS) kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model sağlamak üzere hazırlanmıştır. Bir kuruluş için BGYS'nin benimsenmesi stratejik bir karar olmalıdır. Bir kuruluşun BGYS tasarımı ve gerçekleştirmesi, ihtiyaçları ve amaçları, güvenlik gereksinimleri, kullanılan prosesler ve kuruluşun büyüklüğü ve yapısından etkilenir. Bunların ve destekleyici sistemlerinin zaman içinde değişmesi beklenir. Bir BGYS gerçekleştirmesinin kuruluşun ihtiyaçlarına göre ölçeklenmesi beklenir (örneğin, basit durumlar basit BGYS çözümleri gerektirir) (ISO/IEC 27001, 2006).

ISO/IEC 27001, uyumluluğu değerlendirmek için ilgili iç ve dış taraflarca kullanılabilir. 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardı, tüm kuruluş türlerini (örneğin, ticari kuruluşlar, kamu kurumları, kar amaçlı olmayan kuruluşlar) kapsar. Bu standart, dökümante bir BGYS'yi kuruluşun tüm ticari riskleri bağlamında kurmak, gerçekleştirmek, izlemek gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsar. Bağımsız kuruluşların ya da tarafların ihtiyaçlarına göre özelleştirilmiş güvenlik kontrollerinin gerçekleştirilmesi için gereksinimleri belirtir. BGYS, bilgi varlıklarını koruyan ve ilgili taraflara güven veren yeterli ve orantılı güvenlik kontrollerini sağlamak için tasarlanmıştır.

Bilgi güvenliği standardı BS 7799-2'nin revize edilip 2005'in sonlarında ISO 27001:2005 olarak değiştirilmesiyle yürürlüğe giren bu standart kurumların bilgi güvenliği yönetim sistemi kurmaları için gereklilikleri tanımlamaktadır. Bu bölümde temel olarak ISO 27001 standart oluşumu ve içeriğine değinilmiştir. Standartın içeriği ile ilgili maddeler ve diğer detaylar Bilgi Güvenliği Yönetim Sistemi kurulumu ile ilgili başlıklar altında aktarılmıştır.

3.3.4.1.2. TS ISO/IEC 27002

ISO 17799:2002 numaralı standart ISO 17799:2005 "bilgi teknolojileri güvenlik teknikleri en iyi uygulamalar rehberi" olarak revize edilip yayınlanmıştır ve ISO 27001'e göre kurulacak bir BGYS'nin nasıl gerçekleştirilebileceğine dair açıklamaları içerir. ISO 17799:2005 ismi daha sonra ISO/IEC 27002:2005 olarak değiştirilmiştir.

3.3.4.2. Telekomünikasyon Sektörü için Yasalar ve Düzenlemeler

Kurumlara bilgi güvenliği yönetim altyapısını oluşturma zorunluluğu getirmenin en önemli ve kaçınılmaz yolu gerekli bilgi güvenliği yasalarını çıkarmaktan geçmektedir. BGYS kurulmasında itici güç olarak ülkedeki tüm kamu kurumlarının ve özel sektörün uyması gereken bilgi güvenliği kurallarının yer aldığı, teknoloji bağımsız bir bilgi güvenliği kanunu olması gerekmektedir. Türkiye'de gerek kamu kurumlarında gerekse özel sektörde bilgi güvenliği yönetimi tüm kuruluşların uymakla yükümlü olduğu bir yasa olmadığı için tam manasıyla algılanıp uygulanamamaktadır. Örneğin ABD'de kurumsal yönetişim ile ilgili ilkeleri ortaya koyan SOX ve bilgi güvenliği yönetişimi ile ilgili FISMA kanunları çıkartılmış ve uygulamaya konulmuştur. Türkiye'de ise bu konuda yasal bir düzenleme bulunmamaktadır (Karabacak, 2008, 1). Bu durumda, kurumlar için ISO/IEC 27001:2005 standardı çerçevesinde kurumsal çapta bir Bilgi Güvenliği Yönetim Sistemi oluşturmak ve işletmek oldukça zor olmaktadır.

Tele.com.tr dergisinin Ağustos Sayısında "Elektronik Haberleşme Kanunu Tasarısı ile telekomünikasyon sektöründeki bir çok düzenleme tek bir kanun altında toplanacak" ibaresi yer almaktadır.Bu kanunun amacı olarak TBMM'de ilgili komisyonlarda görüşülmeye başlanacak Kanun tasarısı, elektronik haberleşme hizmetlerinin yürütülmesi, elektronik haberleşme altyapı ve şebekesinin tesisi ve işletilmesi, geliştirilmesi, yeni elektronik haberleşme şebeke ve hizmetlerin teşvik

edilmesi konuları ile ilgili politika, hedef ve ilkelerin tespiti, kaynakların etkin ve verimli kullanılması belirtilmektedir(tele.com.tr, 2009, 54)

Türkiye de Telekomünikasyon sektöründe etkiliğini gösteren Yasa ve Düzenlemeler olarak 5651 yasası ve SOX kanunu gösterilebilir. Sarbanes-Oxley kanunu (SOX), Enron, Arthur-Anderson, Worldcom gibi uluslar arası firmalarda çıkan kurumsal ve muhasebesel skandallarla yitirilmiş olan yatırımcı güvenini arttırmak ve firmalardaki kurumsal yönetimi güçlendirmek amacıyla 2002 yılında Amerikalı Senatör Paul Serbanes ve Amerikalı Temsilci Michael Oxley tarafından çıkarılmıştır. Yasa, ABD Sermaye Piyasası Kurulu'na (Securities and Exchange Commission-SEC) kayıtlı şirketlerin, finansal raporlama üzerindeki iç kontrollerin etkinliğini değerlendirecek bir iç kontrol sistemi oluşturmalarını öngörmektedir. Dolayısıyla Türkiye'de SOX, Amerikan Serbest Piyasa Kurulu'na (SEC) kayıtlı olan şirketler üzerinde yaptırımlar içermektedir. SOX Yasası, Amarika Birleşik Devletleri borsasında kurumların alınıp satılmasının yasalaştırılmasını etkileyen en önemli parçalardan biridir.

SOX'un Telekomünikasyon sektöründeki kuruluşlara etkileri şu şekilde sıralanabilir (Gordon et al, 2006, 2);

- SEC'e kayıtlı şirketlerin her yıl bağımsız denetim firmaları tarafından SOX denetimi geçirmesi zorunlu hale gelmiştir. Denetlenen firmaların diğer ülkelerde bulunan bağlı ortaklıklarının %90 'ı da bu denetlemelerden geçmek zorundadır.
- Birçok firma iç denetim sistemlerini SOX ile uyumlu hale getirebilmek için iç denetim hizmeti veren danışmanlık firmaları ile çalışmaktadır. Bu firmalar PriceWaterHouseCoopers, KPMG ve Ernst&Young gibi dünyaca kabul görmüş danışmanlık firmalarıdır. Danışmanlık firmaları şirketlerin iç denetim departmanları ile ortak çalışarak firma genelinde danışmanlık hizmeti verir.
- Şirketlerde SOX sayesinde hemen hemen her iş prosedürlere bağlanmış, özellikle manuel işler minimum seviyeye indirilmiş ve kontroller için yeni raporlar hazırlanmıştır.

Symantec firmasının web üzerindeki makalesi "Sarbanes-Oxley uyumluluğuna giden yol" 'a göre firmalar mutlaka Sarbanes-Oxley Yasası'nın 5 aşamalı aşağıdaki planlarına uymalıdır (Broderick, 2006, 28);

i. **Tanım:** İşlemdeki birinci basamak, değişikliklerin yapılması gerektiği alanın denetlenmesi işlemidir. Şirketin uygun durumda ve kontrollerde işlemler için uyumlu olması gereklidir. Garter raporlarına göre CIO'lar, uygun bir uyarlama biriminin üyesi gibi denetleme işlemlerinde büyük ölçüde yer almalıdır.

ii. **Değerlendirme:** Denetleme tamamlandığında firmalar şu soruyu sorabilecek durumda olmalılar: Sarbanes–Oxley yaklaşımı adımlarından hangisindeyiz? Bir GAP Analizi uyarlamaya ilişkin gerekleri gösteren yol olacaktır.

iii. **Düzenleme/Gerçekleştirme:** Sistem ve kanunlara uygun olmayan işlemlerin versiyon yükseltilmesinde mutlaka insiyatif kullanılmalıdır. Proje zaman çizelgesi kritiktir.

iv. **Ölçüm:** Uyum için istenen noktaya gelindiğinde tüm işlemler düzenli olarak zaman aşımı ve denetleme gereksinimlerine uyum açısından değerlendirilmelidir.

v. **Raporlama/Bildirim:** Son denetim test edildikten sonra sıra, uygun yönetim durumu ile iletişim kurmaktadır.

Aynı makalede Sarbanes–Oxley Yasasının gerekleri ise şu maddeler ile açıklanmıştır (Broderick, 2006, 28);

- Organizasyonun güvenliği için bir risk yönetimi yaklaşımı kullanın.
- Kuralara Uygun işlemlerin gereksinimlere uygun kayıtlarının yani loglarını tutun.
- İş sürekliliği yapısının kullanın ve servis seviyesinde anlaşmaların, ilgili bilgi ve kayıtlarla uygun bir biçimde korunduğundan emin olun.
- Sistemlere, uygulamalara ve kritik bilgi değişikliklerine rutin denetimler yapın.
- Sitemlerinize diğer şirketlerinin erişimini kontrol altında tutun.

Bu regülasyon gereksinimleri, regülasyonun ve BGYS çatısının ne kadar benzer olduğunu gösterir. Gordon ve arkadaşlarının yaptığı çalışma SOX yasası çıkarıldıktan sonra, kurumsal bilgi güvenliği faaliyetlerine ilginin arttığı yönünde güçlü, dolaylı kanıtlar sağlamaktadır.

3.3.4.3. Telekomünikasyon Sektöründe Denetim Kurumları ve Kapsamları

Kurumlar genellikle yılda bir kez danışman firmalara sistemlerinin güvenlik denetimlerini yaptırmaktadır. Fakat Danışman firmalar yanında, sistemler muhakkak kurumda çalışan bilişim teknolojileri müfettişleri tarafından denetlenmelidir. Buda kurumlarda İç Denetim ekiplerinin oluşturulması ile sağlanabilir.

Denetlemeler iç veya dış denetçiler tarafından gerçekleştirilebilir. ISO/IEC 27001 standartı bu konuda BGYS süreçleri dahilinde kurum içinde iç denetim fonksiyonu bulunmasını ve organizasyonun bunu normal denetim fonksiyonu gibi gerçekleştirmesini beklemektedir. BGYS iç denetimine ek olarak organizasyon ISO/IEC 27001 uygunluğu konusunda dış sertifikasyon denetimi almaya karar verebilir ya da şirket hisse senetlerinin SEC de değerlendirilmeye başlaması ile mecburi olarak SOX denetimlerine tabi tutulmaya başlanabilir (Humphreys, 2008, 249).

Dışarıdan sağlanacak bir denetim seçme kararı tamamen organizasyona bağlıdır, iç denetim ise yönetim, risk yönetimi ve etkin bilgi güvenliğinin sağlanması, uygulanması, kontrolü ve yönetimi ve güncellenmesinin zorunlu bir parçasıdır. Humphreys'nin 2008 yılında yaptığı çalışmaya göre 4600 şirketin ISO/IEC 27001 sertifikasına sahip olduğu gözükmektedir.

3.3.5. Yaptırımlar ve Cezalar

Ahlaki gelişim, yaş, cinsiyet, eğitim, uyruk, din veya iş tecrübesi gibi kişisel özelliklerin ahlak kuralları üzerinde birçok güçlü etkileri vardır. Bu etkilerin

birçoğunu kontrol altında tutabilmek için kurallar ve prosedurler olmalıdır. Eğer çalışanın temel ahlaki değerleri zaten güçlüyse, güvenlik kurallarının varlığı küçük farklar yaratmaktadır. Fakat, etik davranışların daha az olduğu yerde, belli kural ve ana noktaların olması güvenlik durumlarındaki ethical responseların daha fazla olmasını kolaylaştırmıştır. Bu nedenle, bütün organizasyonlardaki etik ve uygun bilgisayar teknolojisi kullanımı politikası, güvenlik için minimum standart olarak gösterilmelidir. Fakat, sadece bu kuralların olması yeterli değildir, kuralların yanısıra ceza ve sonuçların olması zorunludur (Williams, 2008, 210).

Suç ve caydırmanın yolları yıllardır ekonomik bir bakış açısından araştırılmıştır. Son zamanlarda, en uygun ceza analizi, faaliyet teori bağlamında uygulanmıştır. Örneğin, Oliver cezaların rolünü ortak eylemler kapsamında düşünürken, Garoupa cezaları kolektif suç bağlamında biçimlendirir. Cezaların rolü birçok sosyal yanlısı hareketler içinde düşünülmüştür. Bu araştırma seli, çarpık bir davranış işlemeye karşı yaptırımların, olası suçluları sosyal karşıtı davranışlarda bulunmaktan alıkoyduğu izlenimi verir (Tejaswini and Rao, 2009, 8).

Ehrlich, suçlular, olası kurbanlar, ürün alıcıları ve davranışı mükemmelleştirme kurallarına bağlı olan yasa uygulama rollerini, olumlu ve olumsuz güdü değerlendirmesinde dikkate almıştır. Ehrlich'in deneysel bulguları, cezanın suçlular üzerinde caydırıcı kullandığını ileri sürer. Para cezası ya da kanuna itaatsizlik cezası olarak da adlandırılan cezalar,uyarma ,para cezasına çarptırma,işten kovma , hapis yatma ve diğer bazıları gibi mekanizmalar içerebilir (Tejaswini and Rao, 2009, 8).

Bu caydırma öğretisi, cezaların sezilen tehdidinin ceza kararlığı ve şiddeti dâhilinde davranışları etkileyeceğini öne sürer; mesela ceza kararlılığı ve ceza şiddeti arttıkça, yasadışı davranış seviyesi düşer. Caydırma teorisi aynı zamanda sosyal yanlısı çalışanların davranışlarını incelemek için de kullanılmıştır. Örgütsel ortamlarda caydırıcı ile ilişkili bilgi teknolojisini de içeren hayli ön araştırma vardır. Bilgi teknolojisi bağlamında, Stramb caydırıcı ölçülerin bilgisayar suiistimalini azaltmada faydalı öncelikli bir strateji olduğunun önemini vurgular (Tejaswini and Rao, 2009, 8).

Benzer mantık aynı zamanda çalışanların zararlı aktivitelerinin (mesela güvenlik politikalarına bağlı olmamak) cezaların uygulanarak caydırılabileceği bilgi güvenlik bağlamına da uygulanabilir. Örneğin, eğer çalışan örgütsel güvenlik politikasına karşı gelirken yakalanırsa organizasyon bir ceza uygulayarak yetkili cezalandırılabilir. Eğer bireyler itaatsizlikleri için iş kaybı, ağır para cezaları ya da diğer disiplinle ilgili hukuk davaları gibi yüksek düzeyde cezalar alırlarsa istenmeyen davranışları işleme kasıtları azalır (Tejaswini and Rao, 2009, 8).

4. BİLGİ GÜVENLİĞİNİ ETKİLEYEN FAKTÖRLERİN ÇALIŞANLARA ETKİLERİ ÜZERİNE BİR UYGULAMA

4.1. Araştırmanın Amacı

Bu çalışmanın amacı öncelikli olarak Bilgi güvenliği konusunu Telekomünikasyon sektörü için net bir şekilde tanımlayarak, bilgi güvenliğinin altyapısını oluşturan Gizlilik, Bütünlük ve Kullanılabilirlik kavramlarını literatür taraması ve çeşitli regülasyon süreçleri ile tanımlayabilmektir. Bilgi Güvenliği kavramının kurum için öneminin anlatılmasının ardından İnsan, Süreç, Teknik, Standartlar, Yasalar ve Düzenlemeler, Sosyal Baskı, Yaptırımlar ve Cezalar alt başlıkları ile Telekomünikasyon sektöründe Bilgi Güvenliğini etkileyen faktörler detaylı olarak incelenmiştir. Bu faktörlerin çalışanlar üzerine etkilerinin belirlenmesi için ise anket çalışması yapılmıştır.

Bilgi güvenliğini etkileyen faktörlerin çalışanlar üzerine etkilerini belirlemek için araştırma yapılmasının amacı ise, bilgi güvenliği kurallarının çalışanların performansına, örgüte bağlılığına ve işe bağlılığına olan etkilerini tespit edebilmektir. Bu çalışma ile özellikle Bilgi Güvenliğinden sadece teknik alt yapıları yöneten ekiplerinin görevi olmadığının, kurum içindeki her bir çalışanın sorumluluğu olduğu, bu nedenle de kuralların bilgi güvenliğini etkileyen faktörler doğrultusunda oluşturularak ve yaptırımların çalışanların performansını, örgüte ve işe bağlılıklarını olumsuz etkilemeyecek sıkılıkta ama bir yandan da etkililiğini çalışanlara hissettirebilecek şekilde oluşturulmasının ve çalışanların bu doğrultuda eğitilmesinin gerekliliğinin anlatılması amaçlanmıştır.

4.2. Araştırma Kısıtları

Bu araştırma Bilgi Güvenliğinin Telekomünikasyon sektöründeki etkilerin tespit edilmesini amaçladığı için anket çalışması Telekomünikasyon şirketlerinde çalışanlar ile sınırlandırılmıştır. Telekomünikasyon şirketleri genellikle büyük illerde konumlandırıldığından bölge sınırlaması da yapılmak zorunda kalınmıştır.

4.3. Araştırma Yöntemi

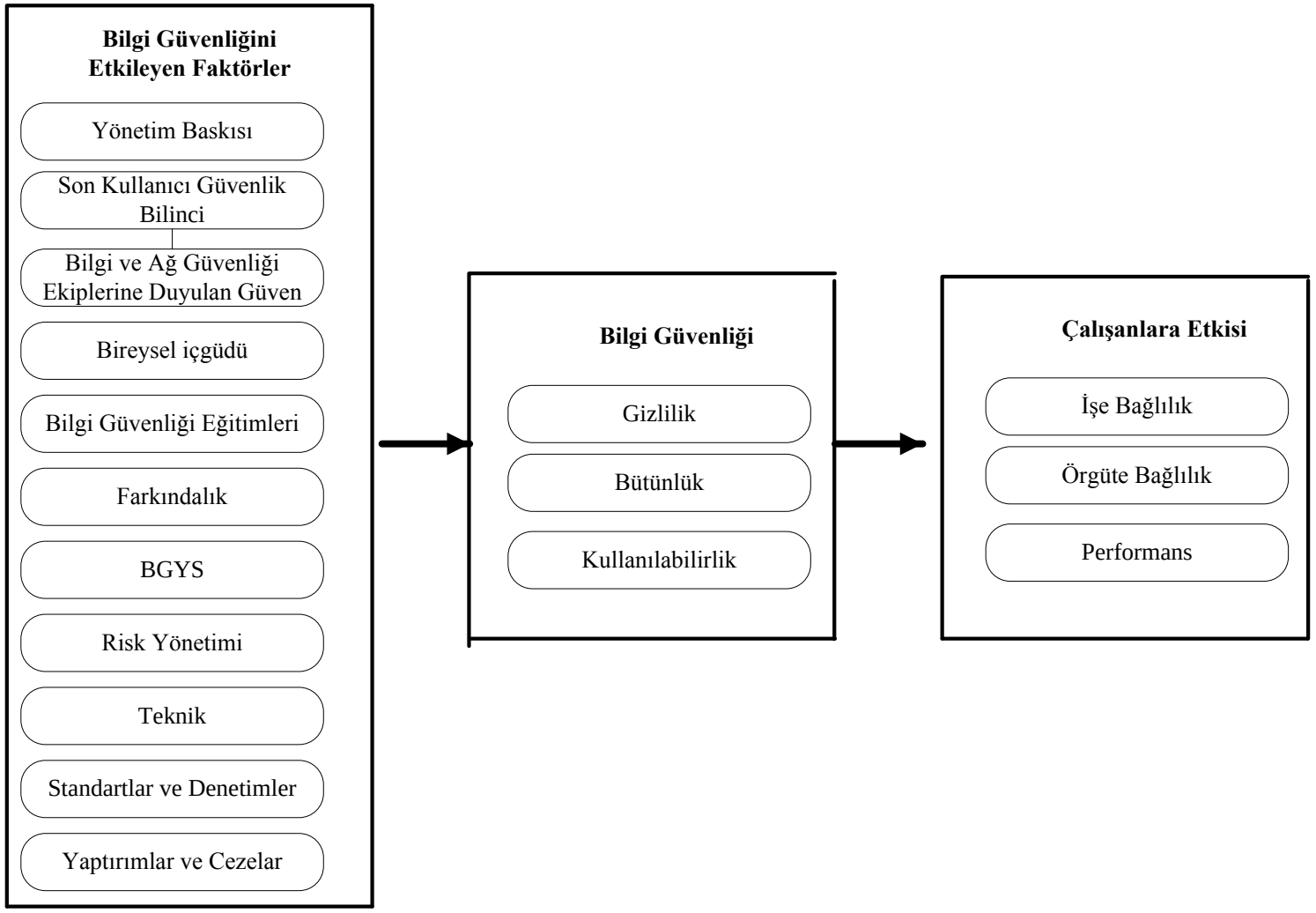
Bu anket çalışması toplamda 124 Telekomünikasyon Sektörü çalışanına uygulanmıştır. Telekomünikasyon Sektöründe Bilgi Güvenliğini Etkileyen Faktörlerin Çalışanlar Üzerine Etkilerini tespit edebilmek üzere anket yöntemi uygulanmıştır. Ankette 92 soru sorulmuş fakat soruların analizler ile değerlendirilme aşamasında anlamlı sonuçlar oluşabilmesi için 69 soru değerlendirilmiştir. Anket üç bölümden oluşmaktadır. Birinci bölümde çalışanların kişisel bilgileri, ikinci bölümde çalışanların firma bilgileri ve üçüncü bölümde bilgi güvenliğini etkileyen faktörlerin çalışanlar üzerine etkilerini ölçen sorular bulunmaktadır. Kullanılan anket, tez çalışması içinde bilgi güvenliğini etkileyen faktörler olarak belirlenen 6 ana başlık üzerine odaklanmıştır. Anket sorularının ikinci bölümü kurumda kullanılan bilgisayar sayısının çalışan sayısına oranı, bilgi/ağ güvenliği çalışan sayısının toplam çalışan sayısına oranı ile iç denetim ekibi çalışan sayınsın toplam çalışan sayısına oranının tespiti için hazırlanmıştır. Anket sorularının üçüncü bölümü için Tejaswini ve Rao nun yaptığı tanımı baz almış ve üçüncü bölümün başlangıcında Bilgi Güvenliği'ni Etkileyen Faktörleri 6 ana faktör ve alt faktörler ile ilgili sorular, devamında ise bilgi güvenliği kavramları ile ilgili sorular yer almaktadır. Bu sorular Tejaswini ve Rao'nun tezinde kullanmış olduğu anket sorularından, 2007 E-Crime Watch Survey sorularından ve Dlamini ve arkadaşlarının hazırladığı "Information security: The moving target" makalesinden faydalanılarak oluşturulmuştur. Üçüncü bölümün sonunda performans ile örgüte ve işe bağlılık konularındaki sorular ise Çağlar Bekiroğlu'nun İşletmelerde Örgütsel Bağlılık ve bir Uygulama Yüksek lisans tezi, Akyay Uygur'un Örgütsel Bağlılık ile İşgören Performansı İlişkisini İncelemeye Yönelik Alan Araştırması ve Doğan Başar'ın Çalışanların Şirket Politikası, Liderlik

Davranışları ve Etik İklimi Algılamaları ile İş Tatmini ve Örgütsel Bağlılık arasındaki İlişkiler yüksek lisans tezinden faydalanılarak oluşturulmuştur. Anket sorularının puanlaması Likert tipi 5'li derecelendire ile yapılmıştır. Anket uygulanmadan önce çeşitli Telekomünikasyon şirketlerinde çalışanlara dağıtılmış, gerekli düzenlemeler yapılıp, anlaşılır olmayan soru maddeleri düzenlenmiştir.

Araştırma örneklemini oluşturan Telekomünikasyon sektörü çalışanlarına yaklaşık 200 anket formu internet üzerinden mail aracılığıyla ve yüz yüze görüşmeler ile ulaştırılmıştır. Gönderilen anket formlarından 124 tanesi geri dönmüştür. Toplanan anket formları numaralandırılarak, verilen cevaplar kodlanmıştır. Verilerin analizinde SPSS 15.0 istatistiksel analiz paket programı kullanılmıştır.

Araştırmanın hipotezleri, bilgi güvenliği etkileyen 6 ana faktörün alt başlıklarıyla beraber bilgi güvenliğine etkisini, bilgi güvenliğinin ise çalışanların performans, işi bağlılık ve örgüte bağlılık düzeyinde etkilerini inceleyecek şekilde oluşturulmuştur. Araştırma hipotezleri doğrultusunda hazırlanan araştırma modeli Şekil 4.1'de gösterilmektedir.

H1: Yönetim Baskısı, Bilgi Güvenliğini pozitif yönde etkiler.
H2: Son Kullanıcı Güvenlik Bilinci, Bilgi Güvenliğini pozitif yönde etkiler.
H3: Bilgi ve Ağ Güvenliği Ekiplerine Duyulan Güven, Bilgi Güvenliğini pozitif yönde etkiler.
H4: Bireysel İçgüdü Bilgi Güvenliğini pozitif yönde etkiler.
H5: Bilgi Güvenliği Eğitimleri Bilgi Güvenliğini pozitif yönde etkiler.
H6: Farkındalık Seviyesi Bilgi Güvenliğini pozitif yönde etkiler.
H7: BGYS Bilgi Güvenliğini pozitif yönde etkiler.
H8: Risk Yönetimi Baskısının Bilgi Güvenliğini pozitif yönde etkiler.
H9: Teknik Bilgi Güvenliğini pozitif yönde etkiler.
H10: Standartlar ve Denetimler Bilgi Güvenliğini negatif yönde etkiler.
H11: Yaptırımlar ve Cezalar Bilgi Güvenliğini pozitif yönde etkiler.
H12: Bilgi Güvenliği Çalışanların İşe Bağlılığını pozitif yönde etkiler.
H13: Bilgi Güvenliği Çalışanların Örgüte Bağlılığını pozitif yönde etkiler.
H14:Bilgi Güvenliği Çalışanların Performansını pozitif yönde etkiler.



4-1 Araştırma Modeli

4.4. Araştırmanın Bulguları ve Değerlendirilmesi

Araştırmanın bu bölümünde; çeşitli Telekomünikasyon şirketlerinde çalışan ve uygulanan anket formu ile değerlendirilen 124 çalışana ait verilerin analizi sonucunda elde edilen bulgular yer almaktadır. Anket formunun Cronbach Alpha katsayısı ile güvenilirliği hesaplanmış α = ,70 ve üstü değerler bulunmuş, 0,70 ve üstü değerler güvenilir kabul edildiğinden; anket formu güvenilir kabul edilmiştir. İstatistiksel çözümlere geçmeden önce, araştırma grubunu oluşturan Telekomünikasyon sektörü çalışanlarının demografik özelliklerini gösteren frekans ve yüzde dağılımları çıkarılmıştır. Sonra ölçeğin aritmetik ortalama ve standart sapma değerleri hesaplanmıştır. Anket formundaki soruların ilişki durumlarını ölçmek için faktör analizi uygulanmıştır. Daha sonra değişkenler arasındaki birebir ilişkiyi bulmak için korelasyon analizi yapılmıştır. Birden fazla bağımsız değişken ile bir bağımlı değişken arasındaki ilişkiyi açıklamak için ise regresyon analizlerine ilişkin bulgulara ve yorumlara yer verilmiştir.

4.4.1. Demografik Özellikler

Demografi, dünyada veya bir ülkede bulunan nüfusun yapısını, durumunu, dinamik özelliklerini inceleyen bilim dalıdır. Nüfusun coğrafyası veya nüfusbilim olarak da tanımlanır. Mevcut nüfusun; yaş, cinsiyet, evlilik durumu, geçim durumu, öğrenim durumu gibi çeşitli sosyal ve ekonomik yönlerini inceleyen demografi; ülkelere ve bölgelere göre nüfus dağılımını ve doğum, ölüm, göç hareketi gibi gelişmeleri inceler (Öztürk, 2009, 64)

Bu bölümde katılımcıların cinsiyet ve yaş dağılımı, eğitim durumu, çalıştığı firmadaki ünvanı ile çalışılan firmada kullanılan bilgisayar sayısı, toplam çalışan sayısı, bilgi/ağ güvenliği ekiplerinde çalışan sayısı ve iç denetim ekibi çalışan sayınsının durumu gibi demografik özellikleri incelenecektir.

Tablo 4.1 araştırmaya katılan Telekomünikasyon sektörü çalışanlarının cinsiyet dağılımlarını göstermektedir. Tablodan görülebileceği gibi çalışanların % 32,2'si (40 kişi) kadın, %67,8'i (84 kişi) ise erkektir. Araştırma yapılan Telekomünikasyon şirketlerinde çalışanların büyük bir çoğunluğunun erkek olduğu görülmektedir.

Tablo 4-1 Cinsiyet Dağılımı

Cinsiyet	Katılan Sayısı	Yüzde %
Kadın	40	32,2
Erkek	84	67,8

Tablo 4.2 araştırmaya katılan Telekomünikasyon sektörü çalışanlarının yaş dağılımlarını göstermektedir. Tablodan görülebileceği gibi Telekomünikasyon sektörü çalışanlarının % 8'i (10 kişi) 18-24 yaş aralığında, %77,5'i (96 kişi) 25-34 yaş aralığında, %14,5'i (18 kişi) ise 35-50 yaş aralığındadır. Araştırma yapılan Telekomünikasyon şirketlerinde çalışanların büyük bir çoğunluğunun 25-34 yaş aralığında olduğu görülmektedir.

Tablo 4-2 Yaş Dağılımı

Yaş	Frekans	Yüzde %	Geçerli Yüzde %	Kümülatif Yiizde %
18 altı	0	0	0	0
18-24	10	8,0	8,0	8,0
25-34	96	77,5	77,5	85,5
35-50	18	14,5	14,5	100,0
50 yaş üstü	0	0	0	
Toplam	124	100,0	100,0	

Tablo 4.3 araştırmaya katılan Telekomünikasyon sektörü çalışanlarının eğitim durumu dağılımlarını göstermektedir. Tablodan görülebileceği gibi araştırmaya katılan Telekomünikasyon sektörü çalışanlarının % 2,4'ü (3 kişi) Ön Lisans mezunu, %64,5'i (80 kişi) Üniversite mezunu, %33,1'i (41 kişi) ise Yüksek Lisans-Doktora mezunudur. Araştırma yapılan Telekomünikasyon şirketlerinde çalışanların büyük bir çoğunluğunun üniversite mezunu olduğu görülmektedir.

Tablo 4-3 Eğitim Durumu Dağılımı

Ünvan	Frekans	Yüzde %	Geçerli Yüzde %	Kümülatif Yiizde %
Ön Lisans	3	2,4	2,4	2,4
Üniversite	80	64,5	64,5	66,9
Yüksek Lisans-Doktora	41	33,1	33,1	100,0
Toplam	124	100,0	100,0	100,0

Tablo 4.4 araştırmaya katılan Telekomünikasyon sektörü çalışanlarının ünvan dağılımlarını göstermektedir. Tablodan görülebileceği gibi Telekomünikasyon sektörü çalışanlarının % 0,8'i (1 kişi) kurum sahibi, %1,6'sı (2 kişi) kurumun genel müdürüdür. Çalışanların %8,1'i (10 kişi) kurumda bölüm/takım müdürü olarak, %56,4'ü (70 kişi) kurumda Mühendis/ Teknisyen olarak, %24,2'si (30 kişi) kurumda Kıdemli Mühendis olarak çalışmaktadır. Ankete katılan çalışanların %8,9'u (11 kişi) başka bir ünvan ile çalıştığını iletmiştir. Araştırma yapılan Telekomünikasyon şirketlerinde çalışanların büyük bir çoğunluğu kurum içinde Mühendis veya Tekniker olarak çalıştığı görülmektedir.

Tablo 4-4 Ünvan Durumu Dağılımı

Ünvan	Frekans	Yüzde %	Geçerli Yüzde %	Kümülatif Yiizde %
Başkan/Sahip	1	0,8	0,8	0,8
Genel Müdür	2	1,6	1,6	2,4
Bölüm/Takım Müdürü	10	8,1	8,1	10,5
Mühendis/ Teknisyen	70	56,4	56,4	66,9
Kıdemli Mühendis	30	24,2	24,2	91,1
Diğer	11	8,9	8,9	100,0
Toplam	124	100,0	100,0	

Tablolar ile aktarılan analizlerin ile beraber anketi dolduran kişilerden şirketlerindeki çalışan sayısı, kullanılan bilgisayar sayısı, bilgi ve ağ güvenliği ekiplerinde çalışan sayısı ile iç denetim ekibinde çalışan kişi sayısı sorulmuştur. Verilen cevaplardan kişi çalışan kişi başına düşen bilgisayar sayısının en çok 1,71 oranında en az ise 0,325 oranında olduğu görülmüştür. Bilgisayar sayısının çalışan

sayısına oranla az olduğu şirketlerde güvenlik konusunda çalışan ekiplerinde çok küçük yada hiç bulunmadığı analiz sonuçlarında gözlemlenmiştir. Bilgisayar sayısının çalışan sayısına oranının yüksek olduğu şirketlerde ise hem güvenlik hem de iç denetim ekiplerinin sayısının toplam çalışan sayısına oranının % 1 ile %7 arasında değiştiği gözlemlenmiştir.

4.4.2. Faktör Analizi

Faktör analizi, başlıca amacı aralarında ilişki bulunduğu düşünülen çok sayıdaki değişken arasındaki ilişkilerin anlaşılmasını ve yorumlanmasını kolaylaştırmak amacıyla daha az sayıdaki temel boyuta indirgemek veya özetlemek olan bir grup çok değişkenli analiz tekniğine verilen genel bir isimdir (Öztürk, 2009, 66). Anketi oluşturan soruların tümü faktör analizine tabi tutulduğundan bazı sorular beklenen faktör düzeyine girmediğinden analiz dışı bırakılmıştır. Tablo 4.6 'de görüldüğü gibi araştırma için sorulan sorular anket formu üzerinde belirtilen faktörlerin altına düşmektedir. Bu da soruların faktörlerle ilişkili olduğunu göstermektedir.

Anket çalışmasında faktörlere oturmamış soruların analiz dışı bırakılması sonucunda Bilgi Güvenliğini Etkileyen Faktörler ile ilgili 42, Bilgi güvenliğini oluşturan kavramlar ile ilgili 13, ve Bilgi Güvenliğinin Çalışanlar Üzerine Etkilerinin ölçümü için 14 soru solumuştur. Bu soruların güvenilirlik katsayısı olan α değerleri tablo 4.1 de verilmiştir. Analiz sonucu oluşan toplam varyans yüklenen faktörlerin ölçülmek istenen olguları ne kadar tanımladığını yüzde olarak göstermektedir. Tablo 4.5'de "BGEF"; Bilgi Güvenliğini Etkileyen Faktörler, "YB"; Yönetim Baskısı, "RY"; Risk Yönetimi, "SKGB"; Son Kullanıcı Güvenlik Bilinci, "BGBDG"; Bilgi/Ağ Güvenliği Bölümlerine Duyulan Güven, "Bİ"; Bireysel İçgüdü, "BGE"; Bilgi Güvenliği Eğitimleri, "F"; Farkındalık, "BGYS", Bilgi Güvenliği Yönetim Sistemi, "T"; Teknik, "SD", Standartlar ve Denetimler, " YC"; Yaptırımlar ve Cezalar, "BG"; Bilgi Güvenliği, "G"; Gizlilik, "B"; Bütünlük, "E"; Erişilebilirlik, "İB"; İşe Bağlılık, "ÖB"; Örgüte Bağlılık, "P"; Performans başlıklarını göstermektedir.

Tablo 4-5 Faktör Analiz Tablosu

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
BGEF																	
YB																	
C2	,817																
C3	,761																
C1	,667																
C5	,603																
C6	,557																
C4	,541																
RY																	
C11		,827															
C10		,804															
C9		,777															
C7		,671															
C8		,631															
SKGB																	
C13			,770														
C12			,752														
C14			,576														
C15			,572														
C16			,528														
BGBDG																	
C21				,795													
C19				,789													
C20				,738													
C22				,638													
C23				,616													
Bİ																	
C24					,904												
C25					,893												
BGE																	
C29						,859											
C28						,834											
C30						,676											
F																	
C32							,857										
C33							,808										
BGYS																	
C38								,813									
C37								,785									
C39								,743									
T																	
C40									,743								
C41									,583								
C42									,569								
S D																	
C50										,849							
C49										,823							
C47										,668							
C46										,614							
YC																	
C56											,714						
C55											,690						

C54											,601						
C53											,504						
BG																	
G																	
C59												,834					
C58												,822					
C57												,801					
C60												,753					
C61												,573					
B																	
C65													,814				
C63													,801				
C62													,786				
C64													,783				
E																	
C67														,777			
C66														,763			
C68														,736			
C69														,652			
ÇE																	
İB																	
C71.															,857		
C72															,835		
C70															,808		
C73															,620		
ÖB																	
C76																,808	
C75																,772	
C81																,760	
C79																,714	
C82																,698	
C78																,546	
P																	
C84																	,925
C85																	,873
C86																	,796
C83																	,679
Toplam Açıklanan Varyans : %77,01																	

Faktör analizi tablosunda, Bilgi Güvenliğini Etkileyen Faktörler on bir faktöre ayrılmıştır. Bu faktörler; Yönetim Baskısı, Risk Yönetimi, Son Kullanıcı Güvenlik Bilinci, Bilgi ve Ağ Güvenliği Bölümlerine Duyulan Güven, Bireysel İçgüdü, Bilgi Güvenliği Eğitimleri, Farkındalık, Bilgi Güvenliği Yönetim Sistemi, Teknik, Standartlar ve Denetimler ile Yaptırımlar ve Cezalar'dır. Bilgi güvenliğini oluşturan faktörler üç bölümde ele alınmıştır. Bu faktörler Gizlilik, Bütünlük ve Kullanılabilirliktir. Bilgi Güvenliğinin Çalışanlara Etkisi ise; İşe Bağlılık, Örgüte Bağlılık ve Performans bölümleri olarak belirlenmiştir. Bilgi Güvenliğini Etkileyen Faktörler için soru, Bilgi güvenliğini oluşturan faktörler için soru ve Bilgi Güvenliğinin Çalışanlara Etkisi için ise soru sorulmuştur.

4.4.3. Korelasyon ve Güvenilirlik Analizi

Korelasyon, olasılık kuramı ve istatistikte iki bağımsız değişken arasındaki doğrusal ilişkinin yönünü ve gücünü belirtir. Genel istatistiksel kullanımda korelasyon, bağımsızlık durumundan ne kadar uzaklaşıldığını gösterir. Korelasyon analizinde, bir ana kütleden seçilmiş en az iki veya daha fazla örnek grup alınarak, bu gruplar arasındaki etkileşime bir katsayı yardımıyla bakılır. Bu katsayı korelasyon katsayısıdır ve r ile gösterilir. Korelasyon analizinin yapılacağı değişkenler arasında etkileşime bakılırken, regresyon analizinde olduğu gibi bağımlı değişken veya bağımsız değişken olma şartı aranmaz (Öztürk, 2009, 72). Regresyon analizi, değişkenler arasındaki neden-sonuç ilişkisini bulmamıza imkan veren bir analiz yöntemidir. Örneğin "yemek yeme" ile "kilo alma" arasındaki ilişki regresyon analizi ile ölçülebilir. Korelasyon analizinde ise iki değişkene arasındaki ilişkinin yönü ve şiddeti hesaplanır. Fakat bu ilişki bir neden-sonuç ilişkisi olmak zorunda değildir (http://www.istatistikmerkezi.com)

Korelasyonuna bakılacak olan değişkenler ikiden fazla olsalar dahi ikili olarak ele alınırlar ve bu ikili değişkenlerin etkileşimi, katsayı yardımıyla yön ve kuvvet olarak tayin edilirler. Kullanılan anket ölçeğinin güvenirliğinin test edilmesinde Cronbach's Alpha katsayısı kullanılmıştır. Güvenirlik, korelasyon katsayısı (r) ile belirlenir ve sıfır ile bir arasında değişen değerler alır. Değer bir (l.00)'e yaklaştıkça güvenilirliğin yüksek olduğu kabul edilir. Alfa değerinin 0,70 ve üzerinde değer

alması güvenilir olduğunu ortaya koymaktadır. Ölçeğimizde alfa değerleri 0,7106 ile 0,8772 arasında değiştiğinden ölçeğimizi güvenilir kabul ediyoruz. Ölçeğin değişkenlere göre ayrı ayrı güvenilirlik için alfa(α) değerleri Korelasyon Analizi Tablosunda gösterilmiştir.

Tablo 4-6 Korelasyon Analiz Tablosu

	Ortalama	Standart Sapma	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
YB	3,7151	,67967	α = ,8669																
RY	3,6919	,77034	,421**	α = ,8807															
SKGB	3,5532	,70543	,539**	,543**	α = ,8510														
BGBDG	3,9516	,58733	,537**	,430**	,489**	α = ,8718													
Bİ	4,0484	,82002	,170	-,095	,069	,052	α = ,8574												
BGE	3,6882	1,0207	,542**	,316**	,385**	,342**	,216*	α = ,8772											
F	4,1532	,65076	- ,004**	,273	,094	,047	,180*	,177*	α = ,7190										
BGYS	3,5000	,83347	,422**	,426**	,330**	,359**	,083	,379**	,202*	α = ,8535									
Teknik	3,8441	,69250	,333**	,417**	,533**	,530**	,135	,195*	,120	,172	α = ,7138								
SD	2,5625	,72178	-,011	-,054	-,072	-,157	,067	,122	-,053	-,014	-,081	α = ,7530							
YC	3,4113	,74367	,490**	,390**	,538**	,481**	,069	,461**	,169	,474**	,393**	,038	α = ,8267						
Gizlilik	4,2887	,61488	,567**	,485**	,488**	,369**	,248**	,504**	,287**	,330**	,425**	-,128	,440**	α = ,8040					
Bütünlük	4,3387	,55874	,387	,431**	,383**	,361**	,141	,436**	,278**	,250**	,451**	-,166	,284**	,733**	α = ,8051				
K	4,0806	,53396	,487**	,520**	,546**	,410**	,242**	,541**	,219**	,434**	,412**	-,082	,457**	,624**	,538**	α = ,7106			
İB	3,7500	,69405	,386**	,186*	,270**	,253**	,270**	,510**	,110	,152	,251**	,043	,125	,424**	,457**	,363**	α = ,7928		
ÖB	3,3978	,66792	,313**	,244**	,238**	,366**	,248**	,533**	,088	,205**	,275**	,035	,258**	,396**	,438**	,474**	,680**	α = ,8078	
Performans	3,8938	,60517	,349**	,290**	,378**	,224*	,262**	,366**	,043	,094	,335**	-,009	,120	,426**	,458**	,555**	,604**	,578**	α = ,8307

* : p< 0,05 Korelasyon ilişkisi .05 düzeyinde geçerlidir.
** : p< 0,01 Korelasyon ilişkisi .01 düzeyinde geçerlidir.

Tablo 4.6'de gösterilen korelasyon analiz tablosu ile bilgi güvenliğini etkileyen faktörler (Yönetim Baskısı, Risk Yönetimi, Son Kullanıcı Güvenlik Bilinci, Bilgi ve Ağ Güvenliği Bölümlerine Duyulan Güven, Bireysel İçgüdü, Bilgi Güvenliği Eğitimleri, Farkındalık, Bilgi Güvenliği Yönetim Sistemi, Teknik, Standartlar ve Denetimler, Yaptırımlar ve Cezalar), Bilgi Güvenliği Kavramları (Gizlilik, Bütünlük, Kullanılabilirlik) ile Bilgi Güvenliğinin Çalışanlar Üzerine Etkileri (İşe Bağlılık, Örgüte Bağlılık ve Performans) arasındaki korelasyon ilişkisi, alfa değerleri, standart sapma ve aritmetik ortalama değerleri gösterilmektedir.

Korelasyon analizi 3 farklı ilişki ile incelenmiştir. Öncelikle Bilgi Güvenliğini Etkileyen Faktörler ile Bilgi Güvenliği Kavramları arasındaki korelasyon ilişkisi incelenirken değişkenlerin birebir ilişkisi incelenmiş ve bu ilişkinin anlamlılık düzeyi ile yönü tespit edilmeye çalışılmıştır. Ardından Bilgi Güvenliğini oluşturan Kavramların Çalışanlar Üzerine etki ilişkisi incelenmiştir. Son olarak ise Bilgi Güvenliğini Etkileyen Faktörlerin Çalışanlar Üzerine Etkilerinin birebir ilişkisi incelenmiştir.

Bilgi Güvenliğini Etkileyen Faktörlerden Yönetim Baskısı, Risk Yönetimi, Son Kullanıcı Güvenlik Bilinci, Bilgi ve Ağ Güvenliği Bölümlerine Duyulan Güven, Bilgi Güvenliği Eğitimleri, Bilgi Güvenliği Yönetim Sistemi, Teknik ve Yaptırımlar ve Cezalar faktörlerinin Bilgi Güveliğini oluşturan Gizlilik, Bütünlük ve Kullanılabilirlik kavramları arasında birebir ilişkide, pozitif yönlü, %1 seviyesinde, kuvvetli ve anlamlı bir ilişki vardır. Bilgi Güvenliğini Etkileyen Faktörlerden Bireysel İçgüdü faktörü ise Bilgi Güveliğini oluşturan kavramlardan Gizlilik ve Erişilebilirlik üzerinde birebir ilişkide, pozitif yönlü, %1 seviyesinde, kuvvetli ve anlamlı bir ilişkisi bulunduğu, Bütünlük kavramı üzerinde ise anlamlı bir ilişkisi bulunamamıştır. Bilgi Güvenliğini Etkileyen Faktörlerden Farkındalık faktörü ise Bilgi Güveliğini oluşturan kavramlardan Gizlilik ve Bütünlük üzerinde birebir ilişkide, pozitif yönlü, %1 seviyesinde, kuvvetli ve anlamlı bir ilişkisi Kullanılabilirlik kavramı üzerinde ise %5 seviyesinde ilişkisi bulunmuştur. Bilgi Güvenliğini Etkileyen Faktörlerden Standartlar ve Denetimler faktörü ise Bilgi Güveliğini oluşturan kavramların hepsi üzerinde birebir ilişkide anlamlı bir ilişki bulunamamıştır.

Korelasyon analizi tablosundan Bilgi Güvenliğini oluşturan Kavramların Çalışanlar Üzerine Etki ilişkisi incelendiğinde; Gizlilik, Bütünlük ve Kullanılabilirlik kavramlarının her birinin birebir ilişkide Çalışanın İşe Bağlılık, Örgüte Bağlılık ve Performansı üzerinde pozitif yönlü, %1 seviyesinde, kuvvetli ve anlamlı bir ilişkisi olduğu görülmektedir.

Korelasyon analizi tablosundan Bilgi Güvenliğini Etkileyen Faktörlerin Çalışanlar Üzerine Etki ilişkisi incelendiğinde ise; Bilgi Güvenliğini Etkileyen Faktörlerden Yönetim Baskısı, Son Kullanıcı Güvenlik Bilinci, Bireysel İçgüdü, Bilgi Güvenliği Eğitimleri ve Teknik faktörlerinin Çalışanın İşe Bağlılık, Örgüte Bağlılık ve Performansı üzerinde pozitif yönlü, %1 seviyesinde, kuvvetli ve anlamlı bir ilişkisi olduğu görülmektedir. Bilgi Güvenliğini Etkileyen Faktörlerden Risk Yönetimi faktörü ise Çalışanın; Örgüte Bağlılık ve Performansı üzerinde birebir ilişkide, pozitif yönlü, %1 seviyesinde, kuvvetli ve anlamlı bir ilişkisi bulunduğu, Çalışanın İşe Bağlılığı üzerinde ise %5 seviyesinde ilişkisi bulunmuştur. Bilgi Güvenliğini Etkileyen Faktörlerden Bilgi ve Ağ Güvenliği Bölümlerine Duyulan Güven faktörü ise Çalışanın; İşe ve Örgüte Bağlılığı üzerinde birebir ilişkide, pozitif yönlü, %1 seviyesinde, kuvvetli ve anlamlı bir ilişkisi bulunduğu, Çalışanın Performansı üzerinde ise %5 seviyesinde ilişkisi bulunmuştur. Bilgi Güvenliğini Etkileyen Faktörlerden BGYS'nin Çalışanın İşe Bağlılık ve Performansı üzerinde birebir ilişkide anlamlı bir ilişkisi bulunamamış fakat Çalışanın Örgüte Bağlılığında %5 seviyesinde ilişkisi bulunmuştur. Benzer bir durum Yaptırımlar ve Cezalar faktörü içinde geçerlidir. Bilgi Güvenliğini Etkileyen Faktörlerden Yaptırımlar ve Cezaların Çalışanın İşe Bağlılık ve Performansı üzerinde birebir ilişkide anlamlı bir ilişkisi bulunamamış fakat Çalışanın Örgüte Bağlılığında %5 seviyesinde ilişkisi bulunmuştur. Bilgi Güvenliğini Etkileyen Faktörlerden Farkındalık ve Standartlar ve Denetimler faktörlerinin Çalışanın İşe Bağlılık, Örgüte Bağlılık ve Performansı üzerinde birebir ilişkide anlamlı bir ilişkisi bulunamamıştır.

4.4.4. Regresyon Analizi

Regresyon, iki ya da daha çok değişken arasında doğrusal bir ilişki olup olmadığının bulunması ve bu doğrusal ilişkinin bir doğrusal denklemle nasıl ifade edildiğinin gösterilmesidir (http://tr.wikipedia.org). Regresyon analizinin temelinde; gözlenen bir olayın değerlendirilirken, hangi olayların etkisi içinde olduğunun araştırılması yatmaktadır. Bu olaylar bir veya birden çok olacağı gibi dolaylı veya direkt etkileniyor da olabilirler (Öztürk, 2009, 74).

Bu çalışama da Bilgi Güvenliğini Etkileyen Faktörlerin Bilgi Güvenliğine ve Bilgi Güvenliğinin, Çalışanlar üzerine etkilerinin anlaşılabilmesi için iki farklı regrasyon analizi kullanılmıştır. Tablo 4.7 'de Bilgi Güvenliğini Etkileyen Faktörlerin, Bilgi Güvenliği kavramları ile ilgili ilişkilerini gösteren regresyon analizi verilmiştir. Bu analizde Bilgi Güvenliğini Etkileyen Faktörler Bağımsız değişkenler olarak alınmış, Bilgi Güvenliği kavramları ise bağımlı değişkenler olarak ele alınmıştır. Tablo 4.8 'da ise bilgi güvenliğinin, çalışanlar üzerine etkilerini gösteren regresyon analizi verilmiştir.

Tablo 4-7 Bilgi Güvenliğini Etkileyen Faktörlerin, Bilgi Güvenliğine Etkisi Üzerine Regrasyon Analiz Tablosu

Bağımsız Değişkenler	Bağımlı Değişkenler					
	Gizlilik		Bütünlük		Kullanılabilirlik	
	β	Sig.	β	Sig.	β	Sig.
Yönetim Baskısı	,236*	,014	,006	,956	-,012	,901
Risk Yönetimi	,273*	,002	,257*	,008	,256*	,003
Son Kullanıcı Güvenlik Bilinci	,034	,715	-,013	,903	,183	,053
Bilgi ve Ağ Güvenliği Bölümlerine Duyulan Güven	-,112	,218	,016	,877	-,006	,944
Bireysel İçgüdü	,152*	,030	,041	,590	,161*	,021
Bilgi Güvenliği Eğitimleri	,227*	,007	,330**	,000	,291**	,001
Farkındalık	,127	,072	,194*	,014	,085	,227
Bilgi Güvenliği Yönetim Sistemi	-,050	,537	-,037	,678	,101	,211
Teknik	,157	,070	,277*	,004	,090	,293
Standartlar ve Denetimler	-,148*	,029	-,158*	,035	-,090	,179
Yaptırımlar ve Cezalar	,084	,345	-,093	,344	,028	,750
	R^2 = ,536 F = 11,769 Sig = ,000		R^2 = ,433 F = 7,791 Sig = ,000		R^2 = ,541 F = 11,999 Sig = ,000	

* : p< 0,05 Korelasyon ilişkisi .05 düzeyinde geçerlidir.
** : p< 0,01 Korelasyon ilişkisi .01 düzeyinde geçerlidir.

Tablo 4.7'de Bilgi Güvenliğini etkileyen bağımsız faktörlerin (Yönetim Baskısı, Risk Yönetimi, Son Kullanıcı Güvenlik Bilinci, Bilgi ve Ağ Güvenliği Bölümlerine Duyulan Güven, Bireysel İçgüdü, Bilgi Güvenliği Eğitimleri, Farkındalık, Bilgi Güvenliği Yönetim Sistemi, Teknik, Standartlar ve Denetimler, Yaptırımlar ve Cezalar) Bilgi Güvenliği kavramlarından ve bağımlı değişken olarak verilen Gizlilik kavramını hangi oranda açıkladığı görülmektedir. Bağımsız değişkenlerin bağımlı değişkeni açıklama oranı olan R^2 değeri; 0,536 olarak

bulunmuştur. Bilgi Güvenliğini etkileyen faktörler, Bilgi Güvenliği kavramlarından Gizlilik kavramını %53.6 oranında açıklamaktadır. Tablo 4.3'de Bilgi Güvenliğini etkileyen faktörlerin, Bilgi Güvenliği kavramlarından Gizlilik kavramını ile bütüncül ilişkisi incelendiğinde; Yönetim Baskısı, Risk Yönetimi, Bireysel İçgüdü, Bilgi Güvenliği Eğitimleri ile Standartlar ve Denetimler faktörlerinin %5 düzeyinde anlamlı bir ilişkisi olduğu, diğer faktörlerin anlamlı bir ilişkisi olmadığı bulunmuştur.

Tablo 4.7'de Bilgi Güvenliğini etkileyen bağımsız faktörlerin (Yönetim Baskısı, Risk Yönetimi, Son Kullanıcı Güvenlik Bilinci, Bilgi ve Ağ Güvenliği Bölümlerine Duyulan Güven, Bireysel İçgüdü, Bilgi Güvenliği Eğitimleri, Farkındalık, Bilgi Güvenliği Yönetim Sistemi, Teknik, Standartlar ve Denetimler, Yaptırımlar ve Cezalar) Bilgi Güvenliği kavramlarından ve bağımlı değişken olarak verilen Bütünlük kavramını hangi oranda açıkladığı görülmektedir. Bağımsız değişkenlerin bağımlı değişkeni açıklama oranı olan R^2 değeri; 0,433 olarak bulunmuştur. Bilgi Güvenliğini etkileyen faktörler, Bilgi Güvenliği kavramlarından Bütünlük kavramını %43.3 oranında açıklamaktadır. Tablo 4.8'de Bilgi Güvenliğini etkileyen faktörlerin, Bilgi Güvenliği kavramlarından Bütünlük kavramını ile bütüncül ilişkisi incelendiğinde; Risk Yönetimi, Farkındalık ve Teknik faktörlerinin %5 düzeyinde anlamlı bir ilişkisi, Bilgi Güvenliği Eğitimleri faktörünün ise %1 düzeyinde kuvvetli ve anlamlı bir ilişkisi olduğu görülmüştür. Bilgi Güvenliğini etkileyen faktörlerden Standartlar ve Denetimler ise Bütünlük ile %5 düzeyinde negatif yönlü bir ilişkisi olduğu görülmektedir. Diğer faktörlerin anlamlı bir ilişkisi olmadığı bulunmuştur.

Tablo 4.7'de Bilgi Güvenliğini etkileyen bağımsız faktörlerin (Yönetim Baskısı, Risk Yönetimi, Son Kullanıcı Güvenlik Bilinci, Bilgi ve Ağ Güvenliği Bölümlerine Duyulan Güven, Bireysel İçgüdü, Bilgi Güvenliği Eğitimleri, Farkındalık, Bilgi Güvenliği Yönetim Sistemi, Teknik, Standartlar ve Denetimler, Yaptırımlar ve Cezalar) Bilgi Güvenliği kavramlarından ve bağımlı değişken olarak verilen Kullanılabilirlik kavramını hangi oranda açıkladığı görülmektedir. Bağımsız değişkenlerin bağımlı değişkeni açıklama oranı olan R^2 değeri; 0,541 olarak bulunmuştur. Bilgi Güvenliğini etkileyen faktörler, Bilgi Güvenliği kavramlarından Kullanılabilirlik kavramını %54.1 oranında açıklamaktadır. Tablo 4.8'de Bilgi

Güvenliğini etkileyen faktörlerin, Bilgi Güvenliği kavramlarından kavramını ile bütüncül ilişkisi incelendiğinde; Risk Yönetimi ve Bireysel İçgüdü faktörlerinin %5 düzeyinde anlamlı, Bilgi Güvenliği Eğitimleri faktörünün ise Kullanılabilirlik üzerinde % 1 seviyesinde düzeyinde kuvvetli ve anlamlı bir ilişkisi olduğu görülmüştür. Diğer faktörlerin anlamlı bir ilişkisi olmadığı bulunmuştur.

Tablo 4-8 Bilgi Güvenliğinin, Çalışanlar Üzerine Etkilerini Gösteren Regrasyon Analiz Tablosu

Bağımsız Değişkenler	Bağımlı Değişkenler					
	İşe Bağlılık		Örgüte Bağlılık		Performans	
	β	Sig.	β	Sig.	β	Sig.
Gizlilik	,131	,310	-,005	,969	-,025	,832
Bütünlük	,296*	,014	,291*	,026	,239*	,032
Kullanılabilirlik	,123	,237	,336**	,001	,442**	,000
	R^2 = ,235 F = 12,296 Sig = ,000		R^2 = ,272 F = 14,923 Sig = ,000		R^2 = ,344 F = 21,003 Sig = ,000	

* : p< 0,05 Korelasyon ilişkisi .05 düzeyinde geçerlidir.
** : p< 0,01 Korelasyon ilişkisi .01 düzeyinde geçerlidir.

Tablo 4.8 'de Bağımsız değişkenler olarak gösterilen Bilgi Güvenliği kavramlarının (Gizlilik, Bütünlük ve Kullanılabilirlik) bağımlı değişkenler olarak gösterilen Çalışanların İşe Bağlılık, Örgüte Bağlılık ve Performans kavramlarını hangi oranda açıkladığı görülmektedir.

Bağımsız değişkenlerin (Gizlilik, Bütünlük ve Kullanılabilirlik) bağımlı değişken olarak verilen İşe Bağlılık kavramına etkisi öncelikle incelenecektir. Bağımsız değişkenlerin bağımlı değişkeni açıklama oranı olan R^2 değeri; 0,235 olarak bulunmuştur. Bilgi Güvenliği kavramlarının Çalışanın İşe Bağlılığını %23.5 oranında açıklamaktadır. Tablo 4.8'de Bilgi Güvenliği kavramlarının, Çalışanın İşe Bağılığı ile bütüncül ilişkisi incelendiğinde; Bütünlük kavramının %5 düzeyinde

anlamlı bir ilişkisi olduğu görülmüştür. Diğer faktörlerin anlamlı bir ilişkisi olmadığı bulunmuştur.

Bağımsız değişkenlerin (Gizlilik, Bütünlük ve Kullanılabilirlik) bağımlı değişken olarak verilen Örgüte Bağlılık kavramına etkisi incelendiğinde; bağımsız değişkenlerin bağımlı değişkeni açıklama oranı olan R^2 değeri; 0,272 olarak bulunmuştur. Bilgi Güvenliği kavramlarının Çalışanın Örgüte Bağlılığını %27.2 oranında açıklamaktadır. Tablo 4.8'de Bilgi Güvenliği kavramlarının, Çalışanın Örgüte Bağılığı ile bütüncül ilişkisi incelendiğinde; Bütünlük kavramının %5 düzeyinde anlamlı, Kullanılabilirlik kavramının ise % 1 seviyesinde kuvvetli ve anlamlı bir ilişkisi olduğu görülmüştür. Gizlilik faktörünün Örgüte Bağlılık ile anlamlı bir ilişkisi olmadığı bulunmuştur.

Bağımsız değişkenlerin (Gizlilik, Bütünlük ve Kullanılabilirlik) bağımlı değişken olarak verilen Çalışan Performansı kavramına etkisi incelendiğinde; bağımsız değişkenlerin bağımlı değişkeni açıklama oranı olan R^2 değeri; 0,344 olarak bulunmuştur. Bilgi Güvenliği kavramlarının Çalışanın Performansına %34.4 oranında açıklamaktadır. Tablo 4.8'de Bilgi Güvenliği kavramlarının, Çalışanın Performansı ile bütüncül ilişkisi incelendiğinde; Bütünlük kavramının %5 düzeyinde anlamlı, Kullanılabilirlik kavramının ise % 1 seviyesinde kuvvetli ve anlamlı bir ilişkisi olduğu görülmüştür. Gizlilik faktörünün Çalışan Performansı ile anlamlı bir ilişkisi olmadığı bulunmuştur.

5. SONUÇ VE ÖNERİLER

Günümüz IT sektöründe kurumların rekabet ortamında ayakta kalabilmesi, karlılığını ve verimliliğini devam ettirebilmesi, uyumluluk kontrolleri karşısında süreç haline dönüştürülmüş kurum standartları ve prosedürleri ile yaşamını sürdürebilmesi ancak kurumun en önemli hazinesi olan bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanabilmesi yani bilgi güvenliği ile sağlanabilmektedir.

Bu noktada özellikle oluşturulan bilgi güvenliği politikalarının sürdürülebilir süreçler ile kurum içinde yaşaması sağlamalıdır. Bu nedenle kurum içinde bilgi güvenliğini olumlu ve olumsuz yönde etkileyen faktörler öncelikle tespit edilmelidir. Bu faktörlerden en önemlisinin "İnsan" yani kurum çalışanları olduğu unutulmamalıdır. Bu nedenle sadece teknik ekiplere değil tüm çalışanlara bilgi güvenliği eğitim programları düzenlenmeli, dünyada son dönemlerde sıklaşan sosyal mühendislik saldırıları ve bu saldırıları erken fark etme yöntemleri anlatılmalıdır. Bilgi güvenliği eğitimlerinde ayrıca şirket varlıklarından ve öneminden bahsedilerek, uyumluk süreçleri, bu süreçler doğrultusunda oluşturulmuş kurumsal süreçler aktarılmalıdır. Kurumun, herkese açık olmayan bilgilerin kötüye kullanılmasından doğabilecek ciddi sorunlara karşı çalışanlarını bilgilendirme sorumluluğu vardır. İnsan unsurunun aslında güvenliğin en zayıf ve kontrol edilmesi en zor halkası olduğu unutulmamalıdır.

Bilgi Güvenliğinin sağlanabilmesi için Teknik ekipmanların ve teknik ekiplerin bilgi seviyelerinin yeterliliği de kurum içi bilgi güvenliğinin sağlanmasında önemli faktörlerdendir. Bu nedenle her sene kurum bütçesinden belirli bir oran güvenlik ekipmanlarına ayrılmalı, güvenlik ekiplerinin bilgi seviyelerinin üst düzeyde olması teknik eğitimler ile sağlanmalı ve teknik ekipmanlarda belirli aralıklar ile denetimlerden geçmelidir.

Özellikle son yıllarda yaşanan ekonomik krizlerde uluslararası firmalarda çıkan kurumsal ve muhasebesel skandalların ekonomiye çok büyük etkileri olmuş ve bu nedenle hem yitirilmiş olan yatırımcı güvenini arttırmak hem de firmalardaki

kurumsal finans yönetimini denetim altında tutmak amacıyla dünyada bazı yasalar ve kanunlar oluşturulmuştur. Amerika'da 2001 yılında yaşanan ve 20000 çalışanın işini kaybetmesi, şirket yöneticilerinin hapis edilmesi ve 3.2 milyar dolar zarara neden olan Enron skandalı sonrası SOX yasası yürürlüğe konulmuş ve Amerika borsasında değer gören tüm şirketlere bu yasaya uyum zorunluluğu getirilmiştir. Türkiye'de finansal kontroller üzerine yoğunlaşmış bu tip bir yasanın şu an için yürürlükte olmaması ileride bu tip skandallar neden olabilir. Türkiye'de mevcutta ISO 27001 ya da 5651 gibi daha süreç ve teknik kontroller odaklı standartlar bulunmaktadır. Telekomünikasyon sektöründe faaliyet gösteren firmaların birçoğu bu standartlara uymak zorundadır. BTK değişik aralıklarla bu standartlar ile ilgili denetimlerini yapmaktadır.

Kurumların oluşturdukları süreçlerin sürdürülebilirliğini sağlayabilmesi için İç Denetim ekiplerinin varlığı kurum için çok önemlidir. Bu ekiplerin belirli aralıklar ile yapacağı denetimler hem açıklıkların erken tespitini sağlamaktadır hem de çalışanlar üzerinde caydırıcı bir etki bırakmaktadır. Ayrıca bilgi güvenliğinin kurum içinde sağlanabilmesinin kurumun en üst seviyedeki yöneticisinden, tüm kurum çalışanlarına kadar herkesin görevi olduğu unutulmamalı ve bu doğrultuda bilgi güvenliği farkındalığının kurum içinde sağlanabilmesi için üst yönetimin desteği mutlaka gerekmektedir.

Şirket ve Bilgi Güvenliği bir denge konusudur. Yetersiz güvenlik, şirketinizi çok savunmasız bırakırken, güvenliğin üzerinde fazla durmak ise işle ilgilenilmesini engelleyerek, şirketin büyümesini ve kazancını kısıtlar. Ayrıca kurum öz kültürü göz önüne alınmadan hazırlanmış politikalar ve standartlar çalışanların işlerini yapmasını zorlaştırarak performansını düşüreceğinden, her kurumun dünyaca kabul edilen standartlar doğrultusunda kendine özgü bir bilgi güvenliği politikası oluşturması ve iç, dış denetimler ile bu politikaların sürdürülebilirliğini sağlaması önemli tavsiye edilmektedir. Asıl zor iş güvenlik ve üretkenlik arasındaki dengeyi kurmaktır. Güvenlik bir ürün değil, bir süreçtir. Dahası, güvenlik bir teknoloji sorunu değildir; bir insan ve yönetim sorunudur.

KAYNAKLAR

Ağır, A., "Bilgi Toplumuna Geçiş Sürecinde Bilgi Yönetimi Yaklaşımı", *İletişim Fakültesi Dergisi*, 30: 3-11, 2008

Barutçugil, İ., *Bilgi Yönetimi,* Kariyer Yayıncılık, İstanbul, 2002

Başaran, B., "*Bilgi Yönetimi*", Gebze Yüksek Teknoloji Enstitüsü - Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, 2003

Benabou, R. and Tirole, J., " Intrinsic and Extrinsic Motivation", *Review of Economic Studies*, 70: 5-6, 2003

Broderick, J., S. , "ISMS, Security Standards and Security Regulations", *Info rmationsecurity technical report*, 11 : 26-31, 2006

Broderick, J. S., and Lecturer, G., "Information Security Risk Management – When Should It be Managed?", *Information Security Technical Report*, 6 : 12- 18, 2001

Bojanc, R. and Jerman, B., "An Economic Modelling Approach to Information Security Risk Management", *International Journal of Information Management*, 28 : 413–422, 2008

Buchanan, S. and Gibb, F., "The information audit: Methodology selection", *Internal Journel of Information Management*, 28 : 3-11, 2008

Canberk, G., ve Sağıroğlu, Ş., "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", *Politeknik Dergisi*, 3 : 165-174, 2006

Carlson, T., "*Information Security Management: Understanding : ISO 17799*", Lucent Technologies Worldwide Services, 2001

Çapar, B., "Bilgi Yönetimi: Nasıl Bir İnsan Gücü?", *II. Ulusal Bilgi, Ekonomi ve Yönetim Kongresi,* 17-18 Mayıs, Derbent- Izmit, 2003

Dinçer, Ö., "Bilgi Güvenliği Bilinçlendirme Süreci Oluşturma Kılavuzu", *TÜBİTAK-UEKAE,* 2008

Dinçer, Ö. ve Dinçkan, A., "Bilgi Güvenliği Yönetim Sistemi Kurulumu", *TÜBİTAK-UEKAE,* 2008

Drucker, P., *Kapitalist Ötesi Toplum*, İnkilap Kitabevi, Anka, 6 Baskı, 1994

Durna, U., ve Demirel, Y., "Bilgi Yönetiminde Bilgiyi Anlamak", *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* 30 : 129-156, 2008

Egan, M., "Information Security and the Human Factor", *Information Systems Control Journal*, 3:1-2, 2005

Gansler, J. and Lucyshyn, W., "Improving the security of financial management systems:What are we to do?", *Journel of Accounting and Public Policy*, 24 : 1-9, 2005

Gonzalez, J. and Sawicka A., *A Framework for Human Factors in Information Security*, WSEAS International Conference on Information Security, Rio de Janeiro, 2002

Gordon, A. J., Loeb M. P. And Lucyshyn W., "The Impact of the Sarbanes-Oxley Act on the Corporate Disclosues of Information Security Activities", *Journal of Accounting and Public Policy*, 25 : 503-530, 2006

Humphreys, E., "Information security management standards: Compliance, governance and risk management", *Information Security Technical Report*, 13 : 247-255, 2008

Karabacak, B., "ISO/IEC 27001:2005 ve Bilgi Güvenliği Yönetişimi - Türkiye Analizi", *TÜBİTAK-UEKAE*, 2008
https://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/iso-iec-27001-2005-ve-bilgi-guvenligi-yonetisimi-turkiye-analizi.html
Krogh, V., "*Care in Knowledge Creation*", California Management Review, 3: 133-154, 1998

Lacey, D., *Managing the Human Factor in Information Security*, Wiley, Chichester, 2009

McCampbell, A. S., and Clare, L., "Knowledge management: the new challenge for the 21st century", *Knowledge management*, 3 : 172-179, 1999

Mitnick, D., *Aldatma Sanatı*, ODTÜ Yayıncılık, Ankara
Önal, S., ve Kök, D., 2002, *İşletmelerde Bilginin Stratejik Boyutu*, 10. Ulusal Yönetim ve Organizasyon Kongresi Bildiri Kitabı, 340- 343, Antalya, 2002

Örnek, K., "Bilişim Güvenliği Denetimlerinde Yapılan Hatalar", *Türkiye İç Denetim Enstitüsü E-DERGİ*, 8: 4-9, 2003

Öztürk, E., "*Teknolojik Yenilik Süreci ve Teknolojik Yenilik Yeterliliklerinin Firma Performansı Üzerine Etkisi Üzerine Uygulama*", Gebze Yüksek Teknoloji Enstitüsü - Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, 2006

Öztürk, S., "*Eğitim Yöneticisinin Karar Verme Sürecini Etkileyen Faktörler ve Eğitim Kurumlarında Bir Uygulama*", Beykent Üniversitesi - Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, 2009

PricewaterhouseCoopers, "*The Global State of Information Security Survey*", 2008

Prusak, L., and Thomas, D., *İş Dünyasında Bilgi Yönetimi*, Rota Yayınları, İstanbul, 2000

Soğukpınar İ., "Veri ve Ağ Güvenliği Ders Notları" GYTE Bilgisayar Mühendisliği Bölümü

Tele.com.tr dergisi Temmuz-Ağustos 2009 sayısı, sayı 57, sayfa 54, 2009

Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik, 06.02.2004 Tarih ve 25365 Sayılı Resmi Gazete, 2004
(http://www.tk.gov.tr/Duzenlemeler/Hukuki/yonetmelikler/Kisisel_Bil_Yon_06_02_04.pdf)

Tejaswini, H., and Rao, H., "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness", *Decision Support Systems* : 1-12, 2009

Thomson, K. and Rossouw, S, "Information security obedience: a definition" *Computers & Security*, 24 : 69-75, 2005

TS ISO/IEC 27001:2006 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler, 2006

Williams P. A., "In a 'trusting' environment, everyone is responsible for information security", *Information Security Technical Report*, 13 : 207- 215, 2008

Yıldız, B., "*Bilgi Güvenliği ve E-Devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetimi Standartlarının Uygulanması*", Gebze Yüksek Teknoloji Enstitüsü - Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, 2007

ÖZGEÇMİŞ

1983 yılında Bursa'da doğdu. İlk, orta ve lise öğrenimini Balıkesir Sırrı Yırcalı Anadolu Lisesi'nde tamamladıktan sonra 2001 yılında Kocaeli Üniversitesi Elektronik ve Haberleşme Mühendisliği bölümünde lisans eğitimine başladı ve 2005 yılında mezun oldu. Aynı yıl Gebze Yüksek Teknoloji Enstitüsü Bilim ve Teknoloji Stratejileri Yüksek Lisans programına girdi. 2006 - 2007 yılları arasında Tesaş Telekomünikasyon'da Teknik Destek Mühendisi olarak çalıştı. 2007 yılı Ocak ayında başladığı Turkcell İletişim Hizmetleri A.Ş. Network Güvenlik Mühendisliği görevine halen devam etmektedir.

EK-1 ANKET FORMU ÖRNEĞİ

GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ

Sayın İlgili,

Bu anket formu, Gebze Yüksek Teknoloji Enstitüsü İşletme Fakültesi tarafından yürütülmekte olan **"Telekomünikasyon Sektöründe Firma İçindeki Bilgi Güvenliğini Etkileyen Faktörler ve Bu Faktörlerin Çalışanlar Üzerine Etkileri"** konulu araştırmanın uygulama kısmı ile ilgilidir. Bu araştırma çalışması tamamen akademik bir çalışma olup, bilimsel bir amaca yönelik olarak kullanılacaktır. Gönderilecek cevaplarda firmalarla ilgili bilgiler kesinlikle gizli tutulacak olup, elde edilecek sonuçlar firma adı belirtilmeksizin genel ve ortalama değerler ile tez çalışmasında kullanılacaktır.

Anketi oluşturan soruları cevaplandırmak şüphesiz çok kıymetli zamanınızın bir kısmını alacaktır. Şimdiden teşekkür eder, çalışmalarınızda başarılar dileriz.

Saygılarımızla,

Doç.Dr. Salih Zeki İMAMOĞLU
GYTE İşletme Fakültesi, Strateji Bilimi Bölümü

Çiğdem YILDIZ
GYTE İşletme Fakültesi, Strateji Bilimi Bölümü Öğrencisi

A. Kişisel Özellikler

Cinsiyetiniz: Kadın ( ) Erkek ( )
Yaşınız: 18 altı ( ) 18-24 ( ) 25-34 ( ) 35-50 ( ) 50-65 ( ) 65 ve üstü ( )
Mesleğiniz: ……..
Eğitim Durumunuz: İlkokul ( ) Ortaokul-Lise ( ) Ön Lisans ( ) Üniversite ( ) Yüksek Lisans-Doktora ( )

Çalıştığınız firmadaki ünvanınız? (lütfen birini seçiniz)
____ 1 Başkan/Sahip ____ 2 Genel Müdür ____ 3 Bölüm/Takım Müdürü ____ 4 Mühendis/ Teknisyen 5____ Kıdemli Mühendis ____ 6 Diğer:

B. Firma Bilgileri

Firmanızda Toplam Çalışan Sayısı:
Firmanızda kullanılan PC/Laptop Sayısı:
Firmanızda Bilgi Güvenliği/ Network Güvenliği bölümlerinde toplam çalışan sayısı :
Firmanızda İç Denetim ekibinde çalışan sayısı:

C. Aşağıda cevaplayacağınız bölümde her soru için 1-5 arasında sadece bir rakam işaretlenecektir. Rakamların anlamları aşağıdaki kutuların içinde belirtilmiştir.

1 Kesinlikle katılmıyorum	2 Katılmıyorum	3 Kararsızım	4 Katılıyorum	5 Kesinlikle katılıyorum				
Yönetim Baskısı								
1. Takım/Birim liderleri Bilgi Güvenliği kurallarına hakimdir.				1	2	3	4	5
2. Takım/Birim liderleri Bilgi Güvenliği kuralları hakkında gerekli bilgilendirmeyi yapmaktadır.				1	2	3	4	5
3. Takım/Birim liderleri Bilgi Güvenliği yaptırımları ile ilgili gerekli bilgilendirmeyi yapmaktadır.				1	2	3	4	5
4. Üst Yönetim organizasyonun Bilgi Güvenliği Politikalarına uyma zorunluluğunu çalışanlara hissettirebilmektedir.				1	2	3	4	5
5. Bilgi/Ağ Güvenliği ekibi organizasyonun Bilgi Güvenliği Politikalarına uyma zorunluluğunu hissettirebilmektedir.				1	2	3	4	5
6. Üst Yönetimin, çalışanın Bilgi Güvenliği kurallarına uyumunu ölçebilecek mekanizmaları vardır.				1	2	3	4	5
Risk Yönetimi								
7. Şirketin "Risk Yönetimi Süreç" dökümanı bulunmaktadır.				1	2	3	4	5
8. Şirkette varlıkların, tehtitlerin ve açıklıkların belirlenmesini sağlayan donanımlar mevcuttur.				1	2	3	4	5
9. Şirkette belirli zaman aralıkları ile Risk Değerlendirme çalışmaları yapılmaktadır.				1	2	3	4	5
10. Şirkette belirli zaman aralıkları ile yapılan Risk Değerlendirme çalışmaları üst yönetime rapor olarak yayınlanmaktadır.				1	2	3	4	5

11. Şirkette Risk yönetim döngüsünün sürekli olarak işletilmesi ve değişiklikler sonucu oluşan yeni risklerin yönetim tarafından farkına varılmasını ve ele alınmasını sağlanmaktadır.	1	2	3	4	5
Son Kullanıcı Güvenlik Bilinci					
12. Son kullanıcılar Şirketin Güvenlik Politikası kurallarını bilmektedir.	1	2	3	4	5
13. Son kullanıcılar Şirketin Güvenlik Politikası yaptırımlarını bilmektedir.	1	2	3	4	5
14. Son kullanıcılar Şirketin Güvenlik Politikası Yaptırımlarını yeterli bulmaktadır.	1	2	3	4	5
15. Şirketin Bilgi Güvenliği Politikası çalışanların yanlış adım atmasını engellemektedir.	1	2	3	4	5
16. Şirketin Bilgi Güvenliği Politikalarına uymaktayım.	1	2	3	4	5
17. Şirketin Bilgi Güvenliği Politikası iş süreçlerini kolaylaştırmaktadır.	1	2	3	4	5
18. Şirketin Bilgi Güvenliği kurallarının sıkılığı ve çokluğu günlük rutin çalışmaları olumsuz etkilemektedir.	1	2	3	4	5
Bilgi/Ağ Güvenliği Bölümlerine Duyulan Güven					
19. Bilgi/Ağ Güvenliği Ekipleri yeterli bilgi seviyesine sahiptir.	1	2	3	4	5
20. Bilgi/Ağ Güvenliği Ekipleri oluşturduğu kurallara uyulması gerekmektedir.	1	2	3	4	5
21. Bilgi/Ağ Güvenliği Ekiplerinin farkındalık seviyesi yeterlidir.	1	2	3	4	5
22. Bilgi/Ağ Güvenliği Ekipleri Bilgi Güvenliği kural ihlallerini yakalayabilmektedir.	1	2	3	4	5
23. Bilgi/Ağ Güvenliği Ekiplerinin oluşturduğu Bilgi Güvenliği kuralları yeterlidir.	1	2	3	4	5
Bireysel İçgüdü					
24. Şirkete duyulan bireysel inanç bilgi güvenliği kurallarına uyumu etkiler.	1	2	3	4	5
25. Şirkete duyulan bireysel bağlılık bilgi güvenliği kurallarına uyumu etkiler.	1	2	3	4	5
26. Şirketin bilgi güvenliği politikası şirketin çalışan profiline göre oluşturulmaktadır.	1	2	3	4	5
27. Çalışanların şirketin Bilgi Güvenliği Politikalarına uymaları gerekmektedir.	1	2	3	4	5

Bilgi Güvenliği Eğitimleri					
28. İşe alımda Bilgi Güvenliği kurallarını içeren dokümanlar iletilmektedir.	1	2	3	4	5

29. Oryantasyon programında Bilgi Güvenliği kurallarını içeren dokümanlar iletilmektedir.	1	2	3	4	5
30. Şirket son kullanıcı Bilgi Güvenliği eğitimi programları düzenlemektedir.	1	2	3	4	5
31. Şirkette düzenlenen son kullanıcı Bilgi Güvenliği eğitim programlarını günlük çalışmaları olumlu yönde etkilemektedir.	1	2	3	4	5
Farkındalık					
32. Şirket Bilgi Güvenliği ancak tüm çalışanların kurallara uyması ile sağlanabilir.	1	2	3	4	5
33. Şirketin Bilgi Güvenliği Politikalarına uyarsam, şirketimin güvenliği için fark yaratacağımı düşünüyorum.	1	2	3	4	5
34. Çalışanlar Şirketi etkileyecek bir Bilgi Güvenliği vakası ile karşılaştığında ilgili gruplara bilgi vermektedir.	1	2	3	4	5
35. Şirketin tüm çalışanların Bilgi Güvenliği Politikalarına uymasının şirketin Bilgi Güvenliği Politikalarının devamlılığı için gerekmektedir.	1	2	3	4	5
Bilgi Güvenliği Yönetim Sistemi(BGYS)					
36. Şirketin BGYS Politikası mevcuttur.	1	2	3	4	5
37. Bilgi Güvenliği Yönetim Sistemi kurumun özellikleri ve ihtiyaçları baz alınarak oluşturulmuştur.	1	2	3	4	5
38. Şirkette Bilgi Güvenliği Komisyonu bulunmaktadır.	1	2	3	4	5
39. Şirketin ihtiyaçları doğrultusunda Bilgi Güvenliği Yönetim Süreci Komisyon tarafından belirli aralıklarla güncellenmektedir.	1	2	3	4	5
Teknik					
40. Şirket son kullanıcı bilgisayarları, bilgi güvenliği ihlallerine karşı izlenmektedir.	1	2	3	4	5
41. Şirket, ağ güvenliği konusunda yeterli teknik donanıma sahip bulunmaktadır.	1	2	3	4	5
42. Şirket, bilgi çalmaya yönelik yapılan teknik saldırılara karşı gerekli önlemleri almış bulunmaktadır.	1	2	3	4	5
43. Şirket bilgi güvenliği için İç ve Dış Testler(PT testler) belirli zaman aralıkları ile yapılmaktadır.	1	2	3	4	5
44. Ağ Güvenliği konusundaki teknik gelişmeleri şirket zamanında uygulamaktadır.	1	2	3	4	5
45. Şirketin bilgi güvenliği donanımlarında yapılacak geliştirmeler için şirket bütçesinden her yıl belirli bir oran ayrılmaktadır.	1	2	3	4	5
Standartlar ve Denetimler					
46. Şirketin bilgi güvenliği nedeniyle kullandığı Anti-virus, Firewall gibi yazılımlar günlük rutin çalışmaları olumsuz etkilemektedir.	1	2	3	4	5
47. Şirketin bilgi güvenliği konusundaki teknik politikaları(şifre, IP politikaları..vb.) günlük rutin çalışmaları olumsuz etkilemektedir.	1	2	3	4	5
48. Çalışanlar şirketin uymakla yükümlü olduğu standartları bilmektedir.	1	2	3	4	5

49. Şirketin uymakla yükümlü olduğu Standartlar(PCI, 27001..vb.) şirketteki günlük rutin çalışmaları olumsuz yönde etkilemektedir.	1	2	3	4	5
50. Şirketin uymakla yükümlü olduğu Yasalar(5651, SOX..) şirketteki günlük rutin çalışmaları olumsuz yönde etkilemektedir.	1	2	3	4	5
51. Şirket belirli aralıklarla İç Denetim ekibi tarafından uymakla yükümlü olduğu Standartlar ve Yasalar ile ilgili denetimden geçmektedir.	1	2	3	4	5
52. Şirket belirli aralıklarla Bağımsız Dış Denetim firmaları tarafından uymakla yükümlü olduğu Standartlar ve Yasalar ile ilgili denetimden geçmektedir.	1	2	3	4	5
Yaptırımlar ve Cezalar					
53. Çalışanlar Bilgi Güvenliği kuralarının yaptırımlarını net olarak bilmektedir.	1	2	3	4	5
54. Şirket yaptırımları ihlal edilen kuralın etkinlik derecesine göre belirlenmiştir.	1	2	3	4	5
55. Şirket, Bilgi Güvenliği kurallarını ihlal eden çalışanlara gerekli yaptırımları uygulamaktadır.	1	2	3	4	5
56. Şirket, Bilgi Güvenliği kurallarını bir kereden fazla ihlal eden çalışanların işlerine son vermektedir.	1	2	3	4	5

Gizlilik					
57. Bilgi, kurumdaki diğer varlıklar gibi, kurum için önem taşıyan ve bu nedenle de en iyi şekilde korunması gereken bir varlıktır.	1	2	3	4	5
58. Bilgi hangi formda(elektronik posta, kağıt… vb.) olursa olsun, mutlaka uygun bir şekilde korunmalıdır.	1	2	3	4	5
59. Kritik Bilgilerin erişim izinleri için şirket süreçleri mevcuttur.	1	2	3	4	5
60. Kritik Bilgilerin erişim izinleri belirli aralıklarla kontrol edilerek, tekrar düzenlenmektedir.					
61. Şirket birlikte çalıştığı diğer firmalar ile Gizlik Sözleşmeleri imzalamaktadır.	1	2	3	4	5
Bütünlük					
62. Bilgi hangi formda(elektronik posta, kağıt… vb.) olursa olsun, mutlaka uygun bir şekilde bütünlüğü sağlanmalıdır.	1	2	3	4	5
63. Bilginin Kesinlik, Doğluluk ve Geçerliliğinin sağlanmaktadır.	1	2	3	4	5
64. Bilginin bütünlüğün bozulması durumları için kritik bilgiler düzenli olarak yedeklenmektedir.	1	2	3	4	5
65. Şirket için önemli olan bilgilerin yetkisiz kişiler tarafından değiştirilmesine veya yok edilmesi karşı gerekli önlemler alınmaktadır.	1	2	3	4	5
Erişilebilirlik					
66. Şirket içinde çeşitli yetkilendirme süreçleri mevcuttur.	1	2	3	4	5
67. Şirket yetkilendirme süreçleri belirli aralıklarla kontrol edilerek, tekrar düzenlenmektedir.	1	2	3	4	5

68. Şirket içinde doğru yetkilendirilmiş bir kişinin ihtiyacı olduğu anda doğru bilgiye erişmesi sağlanmaktadır.	1	2	3	4	5
69. Felaket durumları için gerekli bilgiler yedeklenmekte ve erişilebilirlikleri düzenli olarak kontrol edilmektedir.	1	2	3	4	5
İşe Bağlılık					
70. Kariyerimin geri kalan bölümünü bu işi yaparak geçirmek beni mutlu eder.	1	2	3	4	5
71. İşime duygusal olarak bağlandığımı hissediyorum.	1	2	3	4	5
72. Organizasyonumda kendimi "ailenin bir parçası" gibi hissediyorum.	1	2	3	4	5
73. Sorumluluğumda bulunan işlerin şirket genelinde önemini yüksek buluyorum.	1	2	3	4	5
74. Aynı iş türü odluğu sürece, değişik bir kuruluşta çalışabilirim.	1	2	3	4	5
Örgüte Bağlılık					
75. Arkadaşlarıma bu şirket, çalışması çok zevkli bir iş yeri olarak söz ediyorum.	1	2	3	4	5
76. Şirketimin bir parçası olduğumu başkalarına anlatmaktan gurur duyuyorum.	1	2	3	4	5
77. Şirketime karşı çok az bir bağlılık hissi taşıyorum.	1	2	3	4	5
78. Bu şirkette çalışmayı sürdürmek için hemen her türlü görevi kabul ederim.	1	2	3	4	5
79. Şirketimin problemlerini sanki kendi problemlerimmiş gibi hissederim.	1	2	3	4	5
80. Şimdiki şartlarımda bu kuruluştan ayrılmam için az bir değişiklik yeter.	1	2	3	4	5
81. Bu şirketin geleceği ile gerçekten ilgileniyorum.	1	2	3	4	5
82. Benim için bu şirket tüm çalışılacak olasılıkların arasında çalışılması en iyi yer.	1	2	3	4	5
Performans					
83. Şirketimin başarılı olması için normalde beklenilenin çok üstünde çaba göstermeye hazırım.	1	2	3	4	5
84. Performansımın yüksek olduğunu düşünüyorum.	1	2	3	4	5
85. Verimliliğimin yüksek olduğunu düşünüyorum.	1	2	3	4	5
86. İşimin şirkete katkısının yüksek olduğunu düşünüyorum.	1	2	3	4	5

Değerli zamanınızı ayırdığınız ve bilimsel çalışmamıza katkılarınız için teşekkürlerimizi sunarız.