Bilgi Güvenliği Yönetim Sistemi Kapsamında Risk Yönetimi Modeli

Risk Management Model Within İnformation Security Management System

Faruk Çalıkuşu, Bilge Karamehmet, Arş.Gör.Dr.Ömer Mert Denizci
Marmara Üniversitesi, Bilişim Bölümü, İstanbul, Marmara Üniversitesi, Reklamcılık ve Tanıtım Bölümü, İstanbul, Marmara Üniversitesi, Gazetecilik Bölümü,İstanbul

ÖZET
Bilgi varlıklarının korunabilmesi, kurumların karşılaşabileceği risklerin en aza indirgenmesi ve iş sürekliliğinin sağlanması, Bilgi Güvenliği Yönetim Sistemlerinin kurumlarda üst yönetim desteğiyle hayata geçirilmesiyle mümkün olmaktadır.

Bu çalışmada, Bilgi Güvenliği' nin sağlanmasında önemli olan unsurlar gözden geçirilmiştir. Yüksek seviyede Bilgi Güvenliği' nin sağlanabilmesi için bilgi güvenliği standartlarının bilinmesi ve uygulanmasının yanında güncel tehditlerin bilinmesi önemlidir

Yüksek seviyede bir Bilgi Güvenliği sağlanabilmesi için teknoloji-insan-eğitim üçgeninde yönetilen bir yaklaşımın dikkate alınması gerektiği tespit edilmiştir. Kurumsal bilgi güvenliğinin yüksek seviyede sağlanması ve ülkemizde kurumsal bilgi güvenliği bilincinin geliştirilmesi için kurumlar ve bireylerin bilgilendirilmesi amaçlanmıştır. Bu çalışmanın, kurumsal bilgi güvenliğinin yüksek seviyede sağlanmasına yönelik farkındalık oluşturması, mevcut ve yeni standartlar hakkında daha fazla bilgi içermesi, literatür özetini sunması ve yüksek seviyede güvenliğin sağlanmasına katkılar sağlayacağı düşünülmektedir.

ABSTRACT
Securing and protecting information assets, minimising the risks encountered by organizations and sustainability of businesses are only possible through Information Security Management Systems supported by top management.

In this work, factors that are important to Information Security are examined. In order to guarantee a high standard of Information Security, the information security standards should be known and practiced as well as acknowledging the threats that are currently common.

In order to obtain a high level of information security, a management style to embrace technology-human-education triangle should be adopted. It is our objective in this work that corporate information security is guaranteed; corporations and people are well informed in order to raise the awareness of information security issues and current and new standards are discussed in detail in order to assure a high level of information security.

1 GİRİŞ

Günümüzde kurumlar ve bireylerin sahip olduğu en değerli varlıkları olan bilginin; gizlilik, bütünlük ve erişilebilirlik nitelikleri bakımından sürekli korunması gerekmektedir. Koruma bir takım fiziksel ve sistemsel önlemlerin yanında bireylerin bilgi güvenliğine ilişkin tehdit ve risklerden, kurum bilgi güvenlik politika ya da kurallarından haberdar olması, bu tehditlere nasıl karşı koyabileceği, olası riskleri mümkün olabilecek en düşük risk düzeyinde nasıl tutabileceği konusunda bilgilenmesiyle mümkün olabilir.

Bilgi güvenliği; iş devamlılığı, kaçınılmaz felaket durumlarında kaybın en aza indirilmesi, firmaların yapı taşları sayılan kaynakların her koşulda gizliliğinin,

ulaşılabilirliğinin ve bütünlüğünün korunması amaçlarını taşır.

BGYS, günümüz iş dünyasında vazgeçilmez hale gelen bilgi güvenliği konusunda tüm dünya tarafından kabul görmüş standartlara uygun bir yapı sunmaktadır. BGYS kavramının ve bağlı olduğu standartların doğru anlaşılması bu yapının sağlayacağı faydayı önemli ölçüde arttıracaktır. BGYS kurulumunu fazladan bir iş yükü ve gereksiz zaman kaybı olarak görmenin baştan kaybetmek anlamına geleceği bilinmelidir.

1.1 Bilgi Güvenliği Yönetim Sisteminin Tarihsel Gelişimi

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. Bilgi güvenliği yönetimi konusunda en 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.

Her iki standardın Türkçe hali TSE tarafından sırasıyla TS ISO/IEC 17799:2005 ve TS ISO/IEC 27001:2005 isimleri ile yayınlanmıştır. Söz konusu standardın belgelendirmesi konusunda TSE tarafından TS 13268-1 BGYS Belgelendirmesi İçin Gereksinimler ve Hazırlık Kılavuzu standardı yayınlanmıştır.

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.

1.2 Bilgi Güvenliği Nedir ?

Bilgi, insanın etrafında olup bitenleri tam ve doğru olarak kavramasını sağlayan kişiselleştirilmiş enformasyondur. Bilgi, kendini düşünceler, öngörüler, sezgiler, fikirler, alınan dersler, uygulamalar ve yaşanan deneyimler şeklinde gösterir.

Bilgi, kurumdaki diğer varlıklar gibi, kurum için önem taşıyan ve bu nedenle de en iyi şekilde korunması gereken bir varlıktır.

Bilgi güvenliği; kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin geniş çağlı tehditlerden korunmasını sağlar. Bilgi birçok biçimde bulunabilir. Bilgi, kağıt üzerinde yazılı olabilir, elektronik olarak saklanıyor olabilir, posta yada elektronik posta yoluyla bir yerden bir yere iletilebilir ya da kişiler arası sözlü olarak ifade edilebilir. Bilgi hangi formda olursa olsun, mutlaka uygun bir şekilde korunmalıdır.

İş (aktiviteler), organizasyon (yönetimsel birimler), işin mekânı, varlıklar ve teknoloji

karakteristikleri belirtilerek ve kapsam dışında kalacak olan her ayrıntının sebepleri açıklanarak BGYS'nin sınırları ve kapsamı tanımlanır. Hangi yönetimsel birimlerin ve aktivitelerin bilgi güvenliği yönetim kapsamı içerisinde yer alacağı belirtilmelidir.

Bilgi Güvenliği Yönetim Sistemi kapsam dokümanının çok sık değişime uğraması gerekmese de "yaşayan" bir dokümandır. Gerektiğinde kapsamın içeriği değiştirilebilir. Fakat kapsamın ilk aşamada belirlenirken yönetilebilir boyutta tutulması önemlidir. Bu yüzden organizasyonun fiziksel yapısı ve süreçleri göz önüne alınmalıdır. Örneğin; az görülmesine rağmen yönetilebilirlik adına çok büyük bazı organizasyonlarda Finans bölümü ve Yazılım geliştirme bölümü için iki ayrı BGYS oluşturulduğu gibi örnekler mevcuttur.

Bilgi güvenliği politikaları, bir kurumun değerli bilgilerinin yönetimini, korunmasını, dağıtımını ve önemli işlevlerinin korunmasını düzenleyen kurallar ve uygulamalar bütünüdür.

Her seviyedeki politikanın tek bir dokümanda bulunması yerine, en üst seviyede temel ilkeleri barındıran bir Bilgi Güvenliği Politikası'nın oluşturulması ve bu dokümanla diğer ayrıntılı politikaların ilişkilendirilmesi tavsiye edilmektedir.

CBK (Common Body of Knowledge-Ortak Bilgi Kitlesi) bilgi havuzu denen sektörün en uzman sayılan profesyonellerinin, CISSP (Certified Information Security Systems Professional –Profesyonel Sertifikalı Bilgi Güvenliği Sistemleri) girdi yaptığı en iyi uygulamalar kütüphanesinden oluşan veritabanı kullanılır. Buna göre bilgi güvenliği konularını incelerken üç kavram bakış açısından ele alınır. Bu üç kavrama başka kurumlar iki kavram bakış açısı daha eklemektedirler. Bu beş kavram, CBK dâhilindeki üçü olan gizlilik, bütünlük ve erişilebilirlik ile bu üçü kadar sık dile getirilmeyen diğer iki öğe olan hesap verebilirlik ve yetkilendirmedir.

- Gizlilik
- Bütünlük
- Kullanılabilirlilik
- Hesap verebilirlilik
- Yetkilendirme

1.2.1 Gizlilik

Gizlilik, Uluslararası Standartlar Örgütü (ISO) tarafından "Bilgiye sadece yetkilendirilmiş kişilerce ulaşılabilmesi" (http://en.wikipedia.org) olarak nitelenir. Bugün Şifreleme altyapılarının olmasının sebebi temel olarak gizlilik, ve bütünlüktür. Bilgi güvenliğinin her kavramı her kurum için eşit önemde olmayabilir. Gizlilik özellikle kamu kurumları ve bankalar gibi kuruluşlar için önemlidir.

Gizlilik, özellikle bir yasa ya da sözleşme dolayısıyla 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.

1.2.2 Bütünlük

National Information Assurance'nin tanımına göre bütünlük (veri bütünlüğü) dar güvenlik anlamında verinin yahut bilginin yetkisiz kişilerce değiştirilmesine veya yok edilmesine karşı korunmasıdır. 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 aşağıdaki üç kıstası sağlamalıdır.

- Kesinlik
- Doğruluk
- Geçerlilik

1.2.3 Kullanabilirlik

Matematiksel olarak ifade edilirse, erişilebilirlik herhangi bir sistemin yapılış amaçlarına göre işlev gördüğü zamanın, işlev gördüğü ve görmediği toplam zamana oranıdır. Daha yalın bir anlatımla, doğru yetkilendirilmiş bir kişinin ihtiyacı olduğu anda ihtiyacı olan hizmetin orada olma oranına 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.

1.2.4 Hesap Verebilirlik

Hesap verebilirlik kişisel sorumluluğun bir ölçütüdür. Hesap verebilirliğin en kısa tanımı, kişilerin yaptıkları hareketlerden ve görevi olduğu halde yapmadıklarından sorumlu olmalarıdır. Hesap verebilirliğin alt kavramları olan sorumluluk, suçlanabilirlik, cevap verebilirlik gibi konular büyük tartışmaların merkez noktaları olduğundan hesap verebilirlik diğer üç kavramın yanında değil, biraz uzağında değerlendirmeye tabi tutulur. Kamu kurumlarında hesap verebilirliğin en önemli yansıması şeffaflıktır. Kamu kaynaklarını kullanmakla görevli yetkililerden eylemlerini ve planlarını anlaşılabilir bir halde kamuoyu denetimine açmaları beklenmektedir.

1.2.5 Yetkilendirme

Bilgi güvenliği bakış açısından yetkilendirme kimlik doğrulama sistemidir. Bilgiye erişim sürecinde yetkilendirme, bilgiye doğru kişinin ulaşıp ulaşmadığını kontrol eden alt sistemdir. Gündelik işlerimizde hemen her bilgisayar ağ kaynağına eriştiğimizde yetkilendirme çözümlerini kullanmaktayız. Microsoft Windows işletim sistemine her şifre girildiğinde, şifre alan kontrolcüsünün Kerberos sisteminde kontrol edilip, cevap geriye yollanır. Bu aşamadan sonra kişi her ağ kaynağı kullanmak istediğinde, bağlanılan sistem kişinin kimliğini gene "alan sunucusundan" teyit eder.

Yetkilendirme konusunda dikkat edilmesi gereken, bilgi sistemlerinde geçerli olan "en az bilgi" kuralıdır. Başlangıçta askeri olan bu kural, kişilerin işlerini yapmaları için gereken en az bilgiyi bilmeleri gerektiği prensibini kurumlara benimsetmektedir.

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.

Sadece teknik önlemlerle (güvenlik duvarları, atak tespit sistemleri, antivirüs yazılımları, anticasus yazılımlar, şifreleme, vb.) bilgi güvenliğinin sağlanması mümkün değildir. BGYS; insanları, süreçleri ve bilgi sistemlerini içine alan ve üst yönetim tarafından desteklenen bir yönetim sistemidir. Kurumlar açısından önemli bilgilerin ve bilgi sistemlerinin korunabilmesi, risklerin en aza indirilmesi ve sürekliliğinin sağlanması, BGYS'nin kurumlarda hayata geçirilmesiyle mümkün olmaktadır. BGYS'nin kurulmasıyla; olası risk ve tehditlerin tespit edilmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun yöntemlerin geliştirilmesi, örgütsel yapılar kurulması ve yazılım/donanım fonksiyonlarının sağlanması gibi bir dizi denetimin birbirini tamamlayacak şekilde gerçekleştirilmesi anlamına gelmektedir.

1.3 Bilgi Güvenliği Yönetim Sistemi Neden Gereklidir?

Bir kuruluşun sadece teknik önlemlerle bilgi güvenliğini ve is sürekliliğini korumasının mümkün olmadığı, bunun yanı sıra BGYS gibi bir takım önlem ve denetimlerin sağlanması gerektiği konusu tüm dünyada kabul edilmiş bir yaklaşımdır. BGYS çerçevesinde oluşturulacak güvenlik politikalarına üst yönetim ve tüm çalışanların destek vermesi ve tavizsiz bir şekilde uygulaması gerekmektedir. Ayrıca işbirliğinde bulunulan tüm kişi ve kuruluşların da bu politikalara uygun davranması güvenliği artırıcı bir faktördür.

Aşağıda bir kuruluşa BGYS'nin sağlayacağı faydalar ana hatlarıyla belirtilmektedir:

- Tehdit ve risklerin belirlenerek etkin bir risk yönetiminin sağlanması.
- Kurumsal prestijin korunması ve artısı
- İş sürekliliğinin sağlanması.
- Bilgi kaynaklarına erişimin denetlenmesi
- Personelin, yüklenicilerin ve alt yüklenicilerin güvenlik konusunda farkındalık düzeyinin yükseltilmesi ve önemli güvenlik konularında bilgilendirilmesi.

- Otomatik ve elle yönetilen sistemlerde, duyarlı bilgilerin uygun bir şekilde kullanıldığının garanti altına alınması amacıyla gerçekçi bir kontrol sistemi kurulması.
- Bilgi varlıklarının bütünlüğünün ve doğruluğunun sağlanması.
- Personelin, müşterilerin ve yüklenicilerin görevlerini yerine getirirken, bilgi sistemleri kaynaklarını kotu amaçlı olarak kullanma ve/veya kaynakları suiistimal etmelerinin engellenmesi.
- Bilgi varlıklarının gizliliğinin korunması
- Personelin, başkaları tarafından yapılabilecek olan suiistimal ve tacizlere karşı zan altında kalmasının engellenmesi.
- Duyarlı bilgilerin uygun bir şekilde üçüncü taraflara ve denetmenlere acık olmasının sağlanması.

1.4 Bilgi Güvenliği Yönetim Sisteminin Yararları Nelerdir?

Bilgi güvenliği yönetim sisteminin kurumlara sağlayacağı yararları şöyle sıralamak gerekirse;

- Müşterileriniz, onların bilgilerini güvende tutacağınız konusundaki taahhüdünüzden dolayı güven hissederler.
- İş devamlılığını sağlamak, meydana gelebilecek zararı en aza indirebilmek, kazancın ve iş fırsatlarının artırılması amacıyla bilginin birçok tehlikeye karşı korunmasını sağlar.
- Kuruluşun kurumsal değerlerini, yatırımlarını ve hedeflerini sürdürebilip, koruyabilmesi için ortaya konması gereken kontrollerin firma içinde yerleştirilmesi ve uygulanması yolunda temel teşkil eder.
- Rakiplerinizin bir adım önüne geçmenizi sağlar.
- Uluslararası ihalelere katılımda şart olan ISO/IEC 27001:2005 gereklerinin sağlanmış olur.
- Tek bir bilgi güvenlik ihlalinin çıkaracağı masraf çok büyük olabilir. Belgelendirme işlemi maruz kalacağınız bu tür masrafları azaltır ve bu da iş dalınızdaki yatırımcılar ve müşteriler için önemlidir.
- Bilgi güvenliğiniz ile ilgili sigorta primlerinizde düşüş sağlar.
- İlgili geçerli tüm kanun ve tüzüklere uygunluğunuzu yetkili makamlara kanıtlamanıza yardımcı olur.
- Organizasyonun tüm aşamalarında taahhüt/bağlılığın sağlanması ve kanıtlanmasında yardımcı olur.
- Kuruluş genelinde, bilgi sistemleri ve zayıflıklarının nasıl korunacağı konusundaki farkındalık artar.
- Donanım ve veriye daha güvenilir erişim sağlanır.
- Çalışanların kuruluş içerisindeki sorumlulukları ve bilgi güvenliği konularındaki bilinçlerinin artmasını sağlar.
- Düzenli olarak gerçekleştirilen denetimler sisteminizin etkinliğini izlemenize ve iyileştirmenize yardımcı olur.
- Gizlilik sağlanır.
- Bilginin sadece yetkili kişiler tarafından erişilebilir olması sağlanır.
- Bütünlük sağlanır.
- Bilginin ve işlem metotlarının doğruluğunun ve bütünlüğünün korunması, içeriğinin değişmemesi sağlanır.
- Bilgiye ulaşılabilirlik, elde edilebilirliği sağlanır.
- Başarılı bir e-ticaretin gerekli olan işlevsellik, güvenlik, güvenilirlik ve veri koruması konusunda gereklilikleri sağlar.

2 BİLGİ GÜVENLİĞİ'NDE RİSK YÖNETİMİ

2.1 Bilgi Güvenliği'nde Risk'in Yeri Ve Önemi

Risk, Fransızca *risque* olarak dilimize geçmiş olup sözlük anlamı "Riziko, zarara uğrama tehlikesi" şeklindedir. **Risk** (**riziko**), bir olayın gerçekleşme olasılığı ve olaydan

etkilenme olanağı olarak tanımlanmaktadır. Genellikle risk olumsuz bir durum yani tehlike olarak değerlendirilir. Bu nedenle risklerin olumsuz etkilerinden zarar görmemek için olasılıklar söz önüne alınarak, önlemler almaya yönelik, çalışma ve planlama faaliyetlerini içeren ve risk yönetimi olarak anılan bir disiplin ortaya çıkmıştır.

Risk, gelecekte oluşabilecek potansiyel problemlere, tehdit ve tehlikelere işaret eden, belirli bir zaman aralığında, hedeflenen bir sonuca ulaşamama, kayba ya da zarara uğrama olasılığı olarak da tanımlanabilir. Risk Yönetimi ise bir kurumun ya da kuruluşun çalışabilirliği, ticari kuruluşlar içinse öncelikle kârlılığını olumsuz yönde etkileyebilecek risk faktörlerinin belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecidir. Risk yönetiminde, riskin tamamıyla ortadan kaldırılması mümkün değildir. Sorunlara sistematik ve dikkatli bir şekilde yaklaşılması ve almaya karar verilen risklerin dikkatli yönetimi yoluyla gereksiz kayıpların engellenmesi amaçlanmaktadır. Başarılı bir risk yönetimi için, kuruluşların bilgi varlıklarına ve hedeflerine yönelik risklerin belirlenerek, analiz edilmesi, tanımlanan risklerin denetim altında tutularak izlenmesi gereklidir. Riski yönetmenin en doğru yolu, gerçekleşme olasılığı ve gerçekleştiğinde vereceği zarar en yüksek olan riskleri azaltacak bilgi teknolojisi risk yönetim sürecinin oluşturulmasıdır.

Risk yönetim süreci oluşturulduktan sonra yapılması gereken diğer bir is risk yönetimi sorumlusunun atanmasıdır. Sorumlunun kim olacağı veya isi nasıl yürüteceği, kurumun büyüklüğüne ve ihtiyaçlarına göre değişecektir. Büyük ölçekli kurum ve kuruluşlarda, risklerle ilgili önemli bilgileri toplayarak uygulanması gereken kararları verecek, risk yönetimi politikalarını ve kılavuzlarını oluşturacak özel amaçlı risk yönetim sistemlerinin devreye alınmasını sağlayacak ayrı bir birimin kurulması gereklidir. Risk yönetiminde tek bir birimin veya tek bir kişinin çalışmasının yanında kurum içi ortak bir çalışmaya da ihtiyaç duyulmaktadır. Risk yönetiminde kurum içi haberleşme kanallarının doğru yapılarak üst yönetimle iyi bir iletişim kurulması gereklidir. Risk yönetimi çalışmalarının başarısı, üst yönetimin desteğine ve kurumun is hedefleriyle uyumlu olmasına bağlıdır. Risk yönetimi ile ilgili üst yönetim ve kurum çalışanlarının desteği sağlandıktan sonra isleyiş yöntemlerinin oluşturulması gereklidir. Öncelikle kurulusun uzun dönemdeki hedefleri üzerinde çalışılmalı ve gelecekteki hedefleri tehlikeye atacak risklerin tanımlanarak denetimlerin oluşturulması gereklidir. Risk yönetim planları daima güncel tutulmalıdır.

Bilgi güvenliği risk yönetiminde, bilgi güvenliğini tehdit eden daha önceki bölümlerde açıklanan unsurların meydana gelmesinin engellenmesi hedeflenmektedir. Ancak riskler tamamen ortadan kaldırılamayacağından tedbirlere rağmen riskler oluştuğunda bilgi güvenliğinin bu risklerden en az etkilenmesi risk yönetimiyle sağlanacaktır. Risklerin oluşmasını en aza indirgemek için, önceden alınması gereken tedbirler ve denetimler tarif edilerek kurum çalışanları ve yöneticileri tarafından gerekli önlemler alınmalıdır. Risk oluştuğunda probleme müdahale, iş sürekliliğinin sağlanması ve olağanüstü durumdan kurtulma yöntemlerini içeren felaket yönetimiyle ilgili politikalar oluşturulmalı ve sorun oluştuğunda gecikmeksizin uygulanmalıdır. Burada önemle üzerinde durulması gereken, risklerin ortadan kaldırılması veya azaltılması için oluşturulacak denetimlerin dengesidir. Gereksiz veya iyi bir risk planlaması yapılmadan oluşturulan denetimler sonucunda iş yapılamaz duruma gelinmesi de kurumlar için önemli bir risk faktörüdür.

2.2 Risk Yönetiminde Farkındalık

Bir organizasyonda bu konuyla ilgili yapılabilecek çok çeşitli uygulamalar vardır. Yıllardır yöneticiler bu konuda “başlarını kuma gömme tekniği” kullanmışlardır.Yani bilgi güvenliği ile ilgili yeterince farkındalık sağlanamamıştır. Yöneticiler genellikle güvenlik konularında yeterli bilgi sahibi olamayabilirler veya bütçeleri bu konudaki

riskleri elimine etmeye olanak sağlamayabilir.

11 Eylül 2001'deki olaylar güvenlik konularındaki riskleri önemli oranda ortaya çıkarmıştır. O günkü trajedi havaalanlarındaki güvenliğin önemini tüm dünyaya duyurmuştur. Güvenlik konusu daha önce hiç olmadığı kadar farkındalık yaratmıştır. Sadece fiziksel yönlü teröristler tarafından gizliliği ihlal edilmiş güvenlik konuları değil, aynı zamanda her organizasyonda var olan bilgi güvenliği açıkları veya siber güvenlik gibi konular da herhangi bir teknoloji yada ticaret dergisinin hemen her sayısında işlenmiştir. Bu trajik günden önce güvenlik konusunda dikkat ve farkındalık yaratılmamıştır.

Riski yönetmek ve riskin üstesinden gelmek için en çok kullanılan yöntem riski azaltmaktır. Bu içerik insanlar ve süreçler (prosesler) gibi teknoloji ve güvenlik kontrollerini göz önüne alarak kapsamlı bir güvenlik programını ortaya koyar. Bu, şirket güvenliğine ilave katmanlar eklenmesi anlamına gelebilir. Risk yönetimiyle açıkların ortadan kaldırılması ve güvenlik politikası uygulamaya veya güvenlik farkındalığı konusunda kullanıcıların eğitilmesi anlamına da gelebilir.

2.3 Risk Faktörü Ve Risk Yönetim Modeli

Risk Faktörü	*Değer*	*Risk Yönetimi*	*Değer2*
Teknoloji Kapsamı	3	Güvenlik Harcamaları	2
Tehdide Maruz Kalma	2	Güvenlik Bilinci	2
Varlık Değeri	3	Güvenlik Kontrol kabulü (satın alınan)	1

Tablo 1. Risk faktörü ve Risk yönetim modeli

Basitleştirilmiş risk yönetimi modeli amaçları için, modelde kullanılan 3 bileşen vardır. Bunlar teknoloji kapsamı, tehdide maruz kalma ve varlık değeridir. Bu bileşenler risk faktörünü oluşturmaktadır. Risk faktörünün herhangi bir bileşeninin herhangi bir değerini düşürerek sonucumuzu(ve riskimizi) kolaylıkla iyileştirebiliriz. Varlık değeri bir grup faktörüdür ve bu sebeple diğer iki faktör üzerinden gidilmelidir. Modeldeki bir diğer grup ise risk yönetimidir. Güvenlik durumunu risk yönetim grubundaki herhangi bir bileşeni değiştirerek iyileştirebiliriz. Güvenlik harcamalarını arttırıp güvenlik bilinçlendirme programına ekleriz veya güvenlik kontrol kabulünü arttırırız.

Eğitilen kullanıcılar üzerinde daha iyi kontrol kabulleri için mevcut güvenlik bilinci programına odaklanırsak, 1 numaralı faktördeki artışla risk yönetimimizde anlamlı bir iyileşme sağlanacaktır.

Bunu yaparak finansman ve kaynakları daha verimli hale getirerek güvenlik yönetimine destek sağlanacağı beklenmektedir. Basitçe kullanıcıların iyileştirilmesi, risk yönetimini de iyileştirecektir. Varlık değerinde değişiklik yapılmasından ziyade organizasyon boyunca riski azaltan kullandığımız teknoloji kapsamına odaklanılmalıdır. Teknolojinin kurumda kullanım derecesini çok büyük değişiklikler yapmadan skoru 3 'ten 2'ye düşürerek risk faktörünü yaklaşık %25 azaltabiliriz.

Sonuç olarak bu yakınlaşmanın ve teknolojinin elverişliliğinin doğrudan riske karşılık geldiği görülmektedir. Riskin analizi, bir kuruluşun bilgi varlıklarının korunmasına etki eden iki denklemden oluşan faktörler üzerinde çalışılmasıdır.

Risk yönetimi için faktörler, kullanılan bütçeden, güvenlik bilincinden ve güvenlik kontrol kabulünden meydana gelmektedir. Güvenlik programında bu bileşenlerden herhangi birini değiştirebilmeniz mümkündür, fakat bunlar risk üzerindeki etkileri gösteren en iyi bileşenlerdir.

Bir organizasyonun güvenlik durumunu iyileştirmek için pek çok yöntem vardır.

Günümüz dünyasında teknoloji kullanımının yaygınlaşması ve teknolojinin dijital uçuruma maruz kalmadan kullanımı sayesinde bu gün risk olarak adlandırdığımız tehditler oryadan kalkacaktır.

SONUÇ VE DEĞERLENDİRME

ISO 27001 standardı BGYS kurmak isteyen kuruluşun risk analizi çalışmasının ardından çeşitli kontrolleri devreye sokarak mevcut riskleri tedavi etmesini ve kabul edilebilir risk seviyesinin altına indirmesini şart koşmaktadır.

Bilgi güvenliğinin yönetilmesi bilgi güvenliğinin sağlandığı anlamına gelmemektedir. BGYS'nin kurumsal bilgi güvenliğini taahhüt ettiği seviyede sağlayıp sağlamadığı, sağlamıyorsa eksikliklerinin neler olduğu, güvenlik denetimlerinin güvenli biçimde kurulup kurulmadığı, güvenlik denetimlerinin etkin ve politikalara uygun olarak uygulanıp uygulanmadığı, iyi bir belgelendirme yapılıp yapılmadığı gibi bilgi güvenliğinin sağlanması açısından kritik olan soruları cevaplamanın tek yolu BGYS kapsamında belirlenen bilgi varlıklarının güvenliğini test etmekten geçmektedir.

Risk oluştuğunda probleme müdahale, iş sürekliliğinin sağlanması ve olağanüstü durumdan kurtulma yöntemlerini içeren Risk yönetimiyle ilgili politikalar oluşturulmalı ve sorun oluştuğunda gecikmeksizin uygulanmalıdır. Önemle üzerinde durulması gereken konu, risklerin ortadan kaldırılması veya azaltılması için oluşturulacak denetimlerin dengesidir.

Güvenlik durumumuzu risk yönetim formülümüzdeki herhangi bir bileşeni değiştirerek iyileştirebiliriz: güvenlik harcamalarını arttırıp güvenlik bilinçlendirme programımıza ekleriz veya güvenlik kontrol kabulünü arttırırız.

Bilgi teknolojileri alanında yapılan yatırımlar sonucunda yazılımsal veya donanımsal açıklar üzerinden bilginin sömürülmesi, bilginin uygunsuz kullanımını zorlaştırmıştır. Bu açıklar yerine insan faktörünü kullanarak bilgiler üzerinde bir takım çıkarlar elde etme çabası yoğunlaşmış durumdadır. Tüm bu riskler göz önünde tutulduğunda riskleri gidermek ya da olası en düşük düzeyde tutmanın yolu bireyler üzerinde bir farkındalık oluşturmadan geçmektedir. Bunun en temel yolu ise özellikle kurumlarda yeni başlayan çalışan başta olmak üzere tüm çalışanlara, paydaşlara, tedarikçileri kısaca kurum bilgi güvenliği politikasında yer alan tüm bireylere gereksinimlere göre farklı kategorilerde eğitim programlarının hazırlanması ve bireyler üzerinde bir farkındalık bilincinin oluşturulması gerekmektedir.

3 KAYNAKLAR

Purser, S., 2004,"*A Practical Guide to: Managing Information Security*", Artech House, Boston, (27-28 s.)

F.Tipton, H., 2006,"*Information Security Management*" Handbook Sixth Edition, Auerbach Publications, New York(277-278 s.)

R.Saliba, 1998,"*Callio Secura 17799 - A tool for implementing the ISO 17799 / BS 7799*", pp. (12 –14 s)

T.Humphreys, "*ISMS Standarts The ISO 27000 Family and BS7799-2* ", ISMS International User Group Seminar, pp. (32-35. s.)

Yıldız, B.,2007, "*Bilgi Güvenliği ve E-devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetimi Standartlarının Uygulanması*", Yüksek Lisans Tezi, Gebze Yüksek Teknoloji Enstitüsü Sosyal Bilimler Enstitüsü,(25-27 s.)

Tübitak Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, 2007,"*Bilgi Güvenliği Yönetim Sistemi Kurulumu*", Tübitak-UEKAE-BGYS-001 Sürüm 1.00**,** Gebze, (7 s.)

Vural, Y., 2007,"*Kurumsal Bilgi Güvenliği ve Sızma Testleri*" Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, (81 s.)

Türkiye Bilisim Dernegi, 2005, "*E-Devlet Uygulamalarında Güvenlik ve Güvenilirlik Yaklasımları 4. Çalısma Grubu Sonuç Raporu*"**,** TBD Kamu-B_B IV, Ankara, (9 s.)

Barutçugil, İ., 2002, "*Bilgi Yönetimi*"**,** Kariyer Yayınları,(10. S.)

Tuğlular T.,2003, "*Üniversitelerde Bilgi Güvenliği Politikaları*", Ulaknet Sistem Yönetimi Konferansı – Güvenlik.

Barman S., 2001 "*Writing Information Security Policies*", New Riders Publishing

http://www.ewet.com.tr/ISO%2027001-2005.asp, Erişim,20.04.2009

http://tdkterim.gov.tr/bts/?kategori=veritbn&kelimesec=267075, Erişim: 20.04.2009

http://tr.wikipedia.org/wiki/Risk,Erişim:20.04.2009