# Türkiye'deki İşletmelerin Bilgi Güvenliği Yönetim Sistemi Alt Yapısının Değerlendirilmesi

Mehtap Çetinkaya Kılıç[1] Orhan Gökçöl[2]

[1]Yüksek Bilgisayar Mühendisi, Bilgi Güvenliği Danışmanı, İstanbul
[2]Mühendislik Fakültesi, Bahçeşehir Üniversitesi, İstanbul

[1]e-posta: mehtap.cetinkaya@lostar.com.tr [2] e-posta: gokcol@bahcesehir.edu.tr

## Özetçe

Bu çalışmada, Türkiye'deki çeşitli kurumların/şirketlerin bilgi güvenliği yönetimi konusundaki yaklaşımları ortaya çıkartılmış ve ISO/IEC 27001:2005'e göre bakıldığında hangi alanlarda eksikleri olduğu araştırılmıştır.

Çalışma sonucunda elde edilen bulgulara göre, ülkemizdeki kurum/şirketlerde genelde, "Uyum", İş Sürekliliği Yönetimi" ve "Bilgi Güvenliği İhlal Olayı Yönetimi" konularında uygulama eksiklikleri bulunduğu görülmektedir. Buna karşılık, "Haberleşme ve İşletim Yönetimi" ve "İşletim Kontrolü" konularının daha başarılılıkla ele alındığı söylenebilir.

***Anahtar Kelimeler:*** *Bilgi güvenliği, bilgi güvenliği yönetim sistemi, BGYS ISO/IEC 27001:2005*

## 1. Giriş

Günümüzde, pek çok farklı alanda bulunan bilgi, sadece çalışanlarıyla değil, müşterileri, iş ortakları ve tedarikçileri ile birlikte varlığını sürdüren kurumlarda, çok değerlidir ve bilginin korunması büyük önem taşımaktadır.
Bilgi güvenliği, bilgilerin izinsiz erişimlerden, kullanımından, ifşa edilmesinden, yok edilmesinden, değiştirilmesinden veya hasar verilmesinden korunmasıdır. Bilgi güvenliği "gizlilik", "bütünlük" ve "kullanılabilirlik" kavramları üzerine kuruludur. Gizlilik sadece bilgiye yetkili kişilerin erişmesini ifade ederken, bütünlük bilginin içeriğinin bozulmaması ya da değiştirilmemesi anlamına gelmektedir. Kullanılabilirlik ise bilgiye her ihtiyaç duyulduğunda, yetkisi olan kişilerin ulaşabilmesi anlamına gelir. Bilgi güvenliği yönetimi ise, bilginin korunması ile güvenli erişimi arasında kurulan bir denge hali olarak nitelendirilebilir. Bunu sağlamak için işletmeler üst yönetim tarafından desteklenen bir çerçeve dahilinde, çeşitli politikalarla sınırları çizilen bir güvenlik yönetimi yaparlar.

Bilgileri bu üç açıdan ele alan ve korunması yönünde çalışan bilgi güvenliği yönetim sistemleri, aynı zamanda felaket durumlarında kaybın en aza indirilmesi, firmaların yapı taşları sayılan kaynakların her koşulda gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanmasını amaçlar.

Bu amaçları uygulamaya yönelik, ISO 27001 standardı, ülkelere göre özel tanımlar içermeyen, genel tanımların bulunduğu uluslararası bir standarttır. İşin içinde sadece bilgisayar, bilişim güvenliği yoktur. Bunların yanında, kâğıt üzerindeki ya da sözlü olarak paylaşılan bilgiler gibi her tür sürecin güvenliğini de kapsar.
Kurumlarda bilginin açığa çıkması, zarara uğraması ya da değiştirilmesi gibi durumlar, kurumun işine devam etmesini engellemenin yanı sıra, pazar ve itibar kaybetmesine, müşteriler, iş ortakları ve hissedarları karşısında güven yitirmesine, yasal yaptırım uygulanmasına ve finansal kayba neden olabilmektedir. Bütün bunların geri kazanılmaya çalışılması, yitirilmemesi için alınacak önlemlerden her zaman daha pahalı ve zaman alıcıdır.

Ülkemizde, birçok kurum ve şirketin bilgi güvenliği konusunda çalışmalara başlamasıyla birlikte, bu kavramlar da yaygınlaşmaya başlamıştır. Önceden bilgi güvenliği adı altında yapılmayan birçok uygulama ve kontrol bu gözde değerlendirilerek iyileştirilmeye başlanmıştır. Böylece bilginin korunamaması durumunda oluşabilecek zararlar da engellemeye başlanmıştır.

Bildirinin birinci bölümünde, "Bilgi Güvenliği Yönetim Sistemi (BGYS)"nin ne olduğu anlatılmaktadır. İkinci bölümde, BGYS kurmak isteyen kurumlarda/şirketlerde çalışmalara başlamadan önce ve sonraki yapılması gerekenlere yer verilmiştir.

Üçüncü bölümde, "İşletmelerde Bilgi Güvenliği Altyapısının Değerlendirilmesi Test Aracı" isimli yüksek lisans tezi projesinde elde edilen verilere göre kurumlardaki bilgi güvenliği zayıflıklarından bahsedilmektedir. Çeşitli kurumlarda/şirketlerde bilgi güvenliği ile ilgili durumu ölçmek amacıyla yapılan bu çalışmada, hem ISO/IEC 27001 BGYS standardına uygun olarak çalışmalarını yürüten, hem de BGYS konusunda hiçbir çalışma yapmamış olan kurumlardaki/şirketlerde incelenmiştir.

Son bölümde ise bilgi güvenliğiyle ilgili zayıflıkları ortadan kaldırmaya yönelik neler yapılması ve nasıl bir yaklaşım izlenmesi gerektiği anlatılmaktadır.

## 2. Bilgi Güvenliği Yönetim Sistemi (BGYS)

ISO 27001 dünya üzerinde geçerliliği olan ve her geçen gün birçok alanda zorunlu hale getirilmeye başlanan bir standarttır. ISO27001, uygulanacak bir takım kontroller yardımıyla, kurumlara/şirketlere bilgi güvenliğini

yönetebilecekleri ve etkinliğini ölçebilecekleri standart bir yaklaşım sunmaktadır.

ISO27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardı, tüm kuruluş türlerini (örneğin, ticari kuruluşlar, kamu kurumları, kar amaçlı olmayan kuruluşlar gibi) kapsar. Özellikle, elektronik imza servis sağlayıcıları, bankalar, hastaneler, sigorta şirketleri, bilgi teknolojileri hizmet sağlayıcıları, e-ticaret ile uğraşan şirketlerde BGYS'nin uygulanması önemli bir ihtiyaçtır.

Bir kurum ya da şirketin BGYS standardını uygulaması ve sertifikayı alması, bilgilerinin korunmasında yüzde yüz bir güvenlik sağladığı anlamına gelmez. Bunun anlamı, şirketin bilgi güvenliğinin ne seviyede olduğunun, zayıflıklarının, risklerinin, risk sonuçlarının, risklerin kabul edilip, edilemeyeceğinin ve alınması gereken aksiyonların şirket yöneticileri tarafından bilindiği ve takip edildiğidir.

## 3. BGYS Kurmak

Bilgi Güvenliği Yönetim Sistemi'ni uygulamak isteyen bir kurumda yapılması gerekenler şunlardır:

- **Proje Ekibinin Kurulması:** BGYS Projesi çalışmalarını düzenleyecek, uygulayacak ve yönetebilecek bir takım oluşturulmalıdır.

- **Kapsamın Belirlenmesi:** Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmanın ilk aşaması, kapsamın belirlenmesidir. Bilgi varlıklarının belirlenmesi, sahiplerin atanması, güvenlik seviyelerinin sorgulanması, risklerin ve mevcut durumun ortaya konması kapsam tarafından yönlendirilir. Özellikle ISO 27001 sertifikasını amaçlayan bir yönetim sistemi kuruluyorsa, hangi süreçlerin, departmanların, şehirlerin kapsam içine alınıp, hangilerinin dışarıda bırakılacağı daha da büyük önem kazanır.

Kapsam seçerken, kurum için kritik bir bilgi/bilgi grubu seçilebileceği gibi, bir ya da birden fazla iş süreci ya da bir departmandaki tüm süreçler kullanılabilir. BGYS kurulması genellikle süreçler üzerinden devam ettiğinden, kapsamın süreçlere bağlı olarak seçilmesi çok daha yararlıdır. Kurumun BGYS kapsamının, bilgi güvenliği açısından en gelişmiş süreçlerinden/departmanlarından başlaması da bir başka avantajdır. Böylece BGYS kurma çalışmaları sırasında güvenlik seviyesinden çok, sistem kurmaya ağırlık vermek mümkün olacaktır [2, 6].

- **Proje ve İletişim Planının Hazırlanması:** Kurum ön proje hazırlıklarını tamamlayıp, proje takımını, kapsamını, stratejisini, danışmanlarını belirledikten sonra artık projede ilerleyeceği adımlar için bir proje planı hazırlamalıdır. Nelerin, ne zaman, kimlerle uygulanacağı proje planında yer alarak çalışmalara başlanır. Yapılan tüm çalışmalar, toplantılar çeşitli rapor ve tutanaklarla kayıt altında tutulurken yine kurum tarafından belirlenen aralıklarda (haftalık, aylık) yönetimle bilgilendirme yapılır.

- **Bilgi Güvenliği Politikası:** Bilgi Güvenliği Politikaları, tüm kurum çalışanlarının görev ve sorumluluklarını tanımlamaktadırlar. Hedef; bilgi güvenliği konusunda yönetimin bakış açısını, onayını ve desteğini çalışanlara uygun araç ve denetim mekanizmaları eşliğinde iletmektir.

- **Varlıkların Belirlenmesi:** Kapsam dahilinde ve kapsama destek veren birimlere yönelik varlıklarla ilgili dokümanlar hazırlanır. İlgili varlıklar, varlık sahipleri tarafından belirtilerek, kayıt altına alınır. Varlıklar, sınıflandırılıp, gizlilik, bütünlük ve kullanılabilirlik kriterlerine göre değerlendirilir ve böylece her varlığa ait bir değer ortaya çıkar.

- **Risk Yönetimi:** Bilgi güvenliği yönetim sistemi, 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 Yönetimi'nde, tehditler, zayıf noktalar ve bunlara karşılık gelen riskler belirlenir. Risklerin sıralanmasının ardından, öncelikli riskler belirlenir ve alınması gereken önlemlere karar verilir. Amaç, risklerin tanımlanması, gerekli tedbirlerin alınmasını ön plana çıkaran bir risk değerlendirme sürecini başlatmaktır.
- **Değişimlerin Yönetilmesi:** Bilgi işleme olanakları ve sistemlerinde olan değişiklikler kontrol edilmeli, değişimle ilgili prosedür ve diğer dokümanlar hazırlanmalıdır. Böylece, değişimlerin nasıl ele alınacağı, uygulama adımları ve değişim sonucunun başarı olamaması durumunda geri dönüş planları yapılır.

- **Bilgi Güvenliği İhlal Olayları**: Bilginin gizlilik, bütünlük ve kullanılabilirlik açısından zarar görmemesi için bu tür olayların nasıl yönetileceğine yönetili bir süreç tanımlanmalıdır. Bilgi güvenliği olaylarını anında saptayabilme ve güvenlik ihlal olaylarına hemen yanıt verebilmek için olay yönetimine yönelik planlar, prosedür ve diğer dokümanlar hazırlanmalıdır. Bilgi güvenliği olaylarında kimin haberdar edilmesi gerektiği gibi rol ve sorumluluklar da belirlenmelidir.

- **Döküman ve Kayıt Yönetimi:** Belirtilen politikalara bağlı olarak tüm şirket standart, kural ve prosedürleri gözden geçirilir ve bunun şirket içi işleyişe nasıl yansıyacağı belirlenir. Hizmet, güvenlik ile ilgili prosedürlerin geliştirilmesi ve dokümante edilmesi ile tamamlanır. Politika, prosedür, talimatlar ve ilgili formlar hazırlanır.

- **Dokümantasyon:** Standarta belirtilmiş olan ve özelliklede Bilgi Sistemleri tarafındaki süreçlerde yapılan işlerin dokümante edilmelidir.

- **Uygulanabilirlik Bildirgesi (SoA):** Standarttaki seçilen kontrol amaçları ve kontroller ve bunların seçilme nedenleri, mevcut gerçekleştirilmiş kontrol amaçları ve kontroller ile standart Ek A'da ki kontrol amaçları ve kontrollerden herhangi birinin dışarıda bırakılması ve bunların dışarıda bırakılmasının açıklaması, uygulanabilirlik bildirgesinde ele alınır.

- **Eğitim ve Farkındalık Çalışmaları:** BGYS çalışmaları sırasında ve sonrasında tüm çalışanların bilgi güvenliğinni artırmaya ve bilgilendirmeye yönelik farkındalık çalışmaları ve eğitimler verilir.

- **İş Sürekliliği:** İş süreklilik yönetimi süreci, koruyucu ve önleyici tedbirlerin bir arada kullanılmasıyla bilgi varlıkları kayıplarını makul seviyelere çekerek kayıpların kuruluş üzerindeki tesirini en aza indirmek ve kayıpları (doğal bir felaketin, kazanın, donanım arızasının veya kasten yapılan davranışların bir sonucu olarak ortaya çıkabilen) ortadan kaldırmak için uygulanmalıdır. Bu süreç, önemli iş süreçlerini tanımlamalı ve işletim, yönetim, malzeme, ulaşım ve tesisler gibi konularla ilişkili olan diğer süreklilik gereksinimleri ile iş sürekliliğinin bilgi güvenliği yönetim gereksinimlerini birleştirmelidir.

Doğal felaketlerin, güvenlik eksikliklerinin, hizmet verilememesinin ve hizmete elverişliliğin sonuçları iş tesir analizine bağlı olmalıdır. İş süreklilik planları gerekli işlemlerin zamanında sürdürülmesini temin etmek amacıyla geliştirilmeli ve gerçekleştirilmelidir.

İş süreklilik yönetimi genel risk belirleme sürecine ilave olarak riskleri tanımlamak ve azaltmak için denetimler içermeli, hasara neden olan olayların sonuçları sınırlandırılmalı ve iş süreçleri için gerekli olan bilginin kullanıma hazır olmasını sağlamalıdır. Kurum işini herhangi bir felaket ya da kesinti durumunda nasıl devam ettireceğini önceden planlamalı, yazılı hale getirmeli ve test etmelidir [2,3].

- **Denetim:** Kurum, BGYS kontrol amaçlarının, kontrollerinin, proseslerinin ve prosedürlerinin standarta göre gerçekleştirip gerçekleştirmediğini belirlemek için planlanan aralıklarda iç denetimleri ve bağımsız denetimler gerçekleştirmelidir. Tüm iş faaliyetlerinde olduğu gibi, kuruluşun bilgi güvenliğine ve bilgi güvenliğinin gerçekleştirilmesine olan yaklaşımı, her şeyin yolunda gittiğinden emin olmak için zaman zaman gözden geçirilmelidir. Söz konusu bu gözden geçirmelerin sonuçları yönetime rapor edilmelidir. Gözden geçirme işlemi kuruluşun BGYS uygulamalarının hâlâ yeterli ve etkin olduğunu üst yönetime göstermek amacıyla bağımsız bir kuruluş tarafından (kuruluş içinden ya da kuruluş dışından) yapılmalıdır.

Bağımsız kuruluş ya da kişilerce yapılan gözden geçirme faaliyetleri iyileştirme yapılabilecek alanları tanımlarsa yapılan düzeltici eylemler kadar gözden geçirme faaliyetinin tüm sonuçları da kayıt altına alınmalıdır [3].

- **Düzenleyici Önleyici Faaliyetler (DÖFİ):** Uygunsuzlukların nedenlerini gidermek üzere alınacak önlemler belirlenir. Gerçekleştirilen düzeltici, önleyici faaliyetler, olası sorunların yapacağı etkiye uygun olmalıdır.

- **Belgelendirme:** Belgelendirme denetimi seçilen belgelendirme kurumu tarafından yapılacaktır. Bu noktada, belgelendirme kurumu kurulan BGYS'yi gözden geçirecek ve belgelenme için önerilip önerilemeyeceğinizi tespit edecektir.

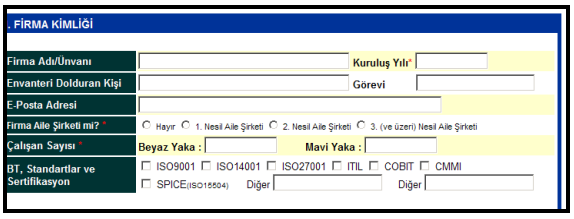
# 4. Türkiye'de Bilgi Güvenliği

## 4.1 Bilgi Güvenliği Test Aracı

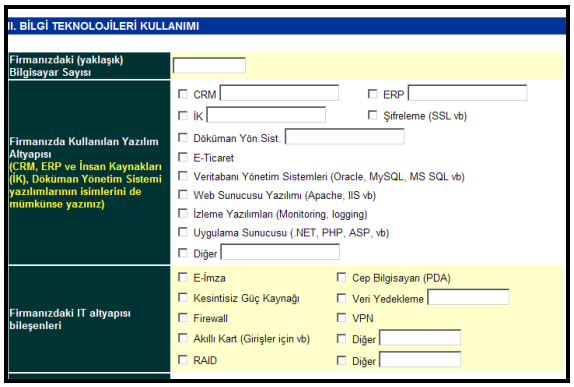
Türkiye'de çeşitli sektörlerde bilgi güvenliği'nin nasıl sağlandığını anlamaya ve ülkemizdelerdeki durumu ölçmeye yönelik "İşletmelerde Bilgi Güvenliği Altyapısının Değerlendirilmesi Test Aracı" adında bir uygulama hazırlanmıştır [1]. Bu araç web tabanlı bir uygulamadır ve çeşitli yöntemlerle(e-posta, forum gibi) iletişim kurulan şirketlerde uygulanması sağlanmıştır. Böylece farklı sektörlerdeki şirketlerin mevcut durumları hakkında bilgi alınmış ve bilgi güvenliği gözüyle durum incelenmiştir.


**Şekil 1** İşletmelerde Bilgi Güvenliği Altyapısının Değerlendirilmesi Test Aracı

Envanter soruları, ISO27001 ana başlıklarıyla uyumlu bir şekilde hazırlanmıştır ve bu haliyle, işletmenin bilgi güvenliği yönetim sistemi altyapısının ideal bir durumdan ne kadar farklı olduğunu belirlemede kullanılabilir. Envanterde, ISO27001 BGYS'nin dikkate aldığı 11 alana ait toplam 33 soru bulunmaktadır. Sorulara, işletmeler 1-5 likerd skalasında değişen cevaplar vermişlerdir. Verilen cevaplara göre, her bir ISO27001 alanına ait bir "uyum skoru" hesaplanmıştır. Bu değer, her bir alan için 0-15 arası değişmektedir. Toplam uyum skoru ise, 11 alan için en fazla 165 olabilmektedir.




**Şekil 2** Test Aracı Firma Bilgileri Ekranı




**Şekil 3** Test Aracı Firma Bilgileri Ekranı

Uygulama, toplanan bilgileri ISO/IEC 27001 ölçütleri çerçevesinde değerlendirerek, envanteri dolduran kurumun/şirketin (hem kurumsal, hem de her bir çalışanı bazında bireysel) bilgi güvenliği altyapısı ile ilgili çıkarımlarda da bulunmaktadır.


**Şekil 4** Test Aracı Envanter Soruları

Çalışma kapsamında, Haziran 2008-Eylül 2008 arasında çeşitli sektörlerde faaliyet gösteren 23 işletme (telekominikasyon:5, bilgi teknolojileri:9, eğitim:5, diğer:4) envanteri cevaplamıştır. İşletmeler envanteri web üzerinden doldurmuşlardır. Verdikleri cevapların doğru olduğu ve işletmelerindeki durumu doğru yansıttığı kabul edilmiştir.

Envanteri yanıtlayan işletmelerden bazıları Bilgi Güvenliği konusunda önemli çalışmalar yapıp, sertifika sahibi iken bir kısmı da bu konuda hiçbir çalışma yapmamış ancak kendi bünyesinde güvenliği sağlamaya çalışan şirketlerdir.

İşletmeler bu test aracı ile halihazırdaki durumlarını Bilgi Güvenliği Yönetim Sistemi altyapılarını ISO27001 normlarına değerlendirirken, elde edilen bulgularla Türkiye'de işletmelerin bilgi güvenliğine ve yönetimine bakış açıları ve kuvvetli/zayıf yanları da bulunmaya çalışılmıştır.

İşletmeler bu test aracını kullanarak kendi bilgi güvenliği yönetim sistemi altyapılarını hızlı bir şekilde değerlendirip hangi alanlarda eksiklikleri olduğunu görmüşlerdir. Bilgi güvenliği projelerinde mevcut durumun ne olduğunu anlamaya yönelik yapılan "Fark Çözümlemesi (GAP Analizi)", bu uygulama aracılığıyla çalışmaya katılan şirketlere yapılmıştır. Böylece şirketler hangi alanlarda güçlü hangilerinde zayıf kaldıklarını görmüşlerdir.

Envanter sorularının ve yorumların değiştirilebilir nitelikte olması, kurum/şirketlerden alınan veriler doğrultusunda içeriği daha da genişletilebilir olmasını sağlamıştır.

### 4.2 Değerlendirme Sonuçları

Alınan cevaplar doğrultusunda ISO 27001 standardının ana ve alt başlıkları (EK A) ile ilgili şartlara yönelik değerlendirmeler yapılmıştır. Bu değerlendirmelerde, BGYS altyapısı olan bazı firmalara uygulama yapıldığında %100 uyum olduğu ortaya çıkmıştır ve uyumluluk skoru tam değer olarak (165) bulunmuştur. Bu sonuçlardan, aynı zamanda uygulamanın başarılı bir şekilde çalıştığı sonucuna da varılmıştır.

Envanteri dolduran firmaların ortalama uyum skorlarının dağılımına bakıldığında (Şekil 5), ülkemizdeki kurum/şirketlerde genelde aşağıdaki bilgi güvenliği alanlarında uygulama eksikliği bulunduğundan söz edilebilir:

- Uyum
- İş Sürekliliği Yönetimi
- Bilgi Güvenliği İhlal Olayı Yönetimi

| ISO27001 Ana Başlıkları | Uyumluluk Skoru | % Uyumluluk |
|---|---|---|
| **A.5**. Güvenlik Politikası | 9.51 | 63.4 |
| **A.6**. Bilgi Güvenliği Organizasyonu | 10.51 | 70.1 |
| **A.7**. Varlık Yönetimi | 9.61 | 64.1 |
| **A.8**. İnsan Kaynakları Güvenliği | 9.76 | 65.1 |
| **A.9**. Fiziksel ve Çevresel Güvenlik | 10.11 | 67.4 |
| **A.10**. Haberleşme ve İşletim Yönetimi | 10.77 | 71.8 |
| **A.11**. Erişim Kontrolü | 10.3 | 68.7 |
| **A.12**. Bilgi Sistemleri Edinim, Geliştirme ve Bakımı | 11.01 | 73.4 |
| **A.13**. Bilgi Güvenliği İhlal Olayı Yönetimi | 9.04 | 60.3 |
| **A.14**. İş Sürekliliği Yönetimi | 8.64 | 57.6 |
| **A.15**. Uyum | 5.93 | 39.5 |
| ***TOPLAM*** | ***105.19*** | ***63.8*** |

**Şekil 5** Envanter dolduran firmalara ait ortalama uyum skorları

Bilgi Güvenliği standardında yer alan ve uygulaması kurum/şirketin faaliyetlerinin devamlılığı açısından oldukça önemli olan "Uyum", "İş Sürekliliği" ve "Bilgi Güvenliği İhlal Olayı Yönetimi" konularında yapılan çalışma sonucunda eksiklikler olduğu gözlenmiştir. Diğer alanlarda, özellikle de bilgi güvenliği konusunda çalışmalar yapan şirketlerde oldukça iyi sonuçlarla karşılaşılmıştır.

Ayrıca, envanter sonucunda elde edilen bilgiler ve sektördeki bilgi güvenliğine yönelik çalışmalarda gözlemleneler doğrultusunda ülkemizdeki bilgi güvenliği ile ilgili aşağıdaki yorumlar yapılabilir:

• Ülkemizde, bazı şirketler bilgi güvenliği'nin iş gücü azalımı, gelir ve zaman kaybı yarattığını düşünmektedirler. Oysaki, herhangi bir felaket durumunda (yangın, sel, deprem vb.) uğranılabilecek kayıplar karşısında bilgi güvenliğine ayrılacak zaman, emek ve para çok daha az öneme sahiptir.

Bilgi güvenliğinin doğru şekilde anlaşılması ve uygulanması kurum/şirketlerin kendilerini güvende hissetmelerini, olabilecek tehlikelerden önceden haberdar olup B planlarını oluşturmalarını sağlayacaktır. Böylece, kurum/şirketler ciddi zaman ve emeklerle oluşturdukları şirket itibarlarını da koruyabileceklerdir.

- Türkiye'de bilgi güvenliği ile ilgili çalışmalar daha çok büyük firmalarda yapılmaktadır. Ancak, bilginin değerinin anlaşılması ile birlikte zamanla orta ve küçük ölçekli şirketlerde de bu çalışmalar yaygınlaşacaktır. Geçmişte karşılıklı güven ilkesiyle çalışan şirketler değişen koşullar ve farklı kültürdeki rakipleri karşısında bilgilerini korumaları gerektiğinin farkına varmaya başlamışlardır.

Türkiye'de bilgi güvenliğini bilinirliği arttıkça bu yöndeki yatırımlarda artmaktadır. Elinde tuttuğu bilgisinin değerini anlayan şirketler güvenlik konusundaki yatırımlarına da ağırlık vermektedirler. Olabilecek bir güvenlik açığının ne kadar büyük tehditler yaratabileceğini fark etmektedirler.

- Türkiye'de bilgi güvenliği kavramıyla tanışmayan firmalar da bile güvenliği sağlamaya yönelik alınmış pek çok önlem olduğunu gösterirken bunların yazılı ve dokümante edilmemiş olduğunu ve bir sistematiğe oturmasına ihtiyaç olduğunu göstermektedir. Bu firmalar tarafından alınmış olan önlemler ayrıca yapılacak bir çalışma ile ayrı bir istatistik olarak değerlendirilebilir.

- Çalışmaya katılan firmalarda genelde standardın büyük bir kısmı bilgi sistemleri alt yapısını içerdiğinden bu konudaki çalışanlar tarafından doldurulmaya çalışılmıştır. Bu da şirketlerin çoğunun bilgi güvenliği'ni sadece 'teknoloji' sorunu olarak gördükleri yönündedir. Oysaki bilgi güvenliği sadece teknoloji değil her alanı kapsamaktadır. Bu alanlar içinde insan kaynakları, hukuk, halkla ilişkiler gibi bölümlerde önemli yer almaktadır.

## 5. Sonuçlar

Bilgi güvenliği, kağıt üzerinde bir zorunluluk ya da bir sertifika almak demek değildir. Güvenlik sadece teknoloji problemi olarak değil aynı zamanda insan ve yönetim problemi olarak değerlendirilmelidir.

Kurumun stratejik hedeflerini belirleyen en üst seviyedeki yönetim kademelerinin kurumsal bilgi güvenliğinin sağlanması için verecekleri destek ve kurum/şirket içinde oluşacak "Bilgi Güvenliği" konusundaki farkındalık çok önemlidir.

Bilgi güvenliği ile ilgili farkındalık çalışmaları arttıkça ve kurum/şirketler bilgilerinin değerini anladıkça bilgi güvenliği ile ilgili çalışmalarda hız kazanacaktır. Bilgi güvenliği ve BGYS uyulması gereken kurallar zinciri olarak düşünülmeyip, kurum kültürünün bir parçası olacaktır.

Bu çalışma sonucunda Envanteri dolduran firmaların ortalama uyum skorlarının dağılımına bakıldığında, yapılan bu çalışmanın en net ve ispatlanmış sonucu olarak; ülkemizdeki kurum/şirketlerde genelde, "Uyum", İş Sürekliliği Yönetimi" ve "Bilgi Güvenliği İhlal Olayı Yönetimi" konularında uygulama eksiklikleri bulunduğu görülmektedir.

Bu çalışmada sonuçlarının bir kısmı kullanılan Bilgi güvenliği Test Aracı ise gelecekte yapılabilecek çalışmalar açısından oldukça önemlidir. Tüm kurum/şirketler ve envanter bilgilerinin merkezi bir veritabanında tutulması sebebiyle, yeterli veri toplandığında, ülke çapında genel ve sektörel bazda analizler yapmak da mümkün olacaktır. Böylece ülkemizdeki sektörlerin karşılaştırılması ve dünyadaki diğer sektörlerle de kıyaslanması mümkün olacaktır. Ayrıca test aracı, farklı standartlarla ilgili sorularında eklenmesi ile diğer standartlara yönelik değerlendirmeler yapılması da mümkündür. Daha da ileri çalışmalarda farklı standartların değerlendirilmesi ile aynı konuları içeren standartlar içinde ortak değerlendirmelere gidilebilir.

Ayrıca, buradaki yapılan çalışmaya ek anketler eklenerek daha geniş çalışmalar yapılabilir, farklı bakış açıları ve değerlendirmelerde yararlanılarak şirketler bilgi güvenliği konusunda yapmaları gerekenler konusunda daha detaylı bilgiler elde edebilirler.

## 6. Kısaltmalar

BGYS: Bilgi Güvenliği Yönetim Sistemi
TSE:Türk Standartları Enstitüsü
IEC:Uluslar arası Elektroteknik Komisyonu
ISO: Uluslararası Standard Organizasyonu (International Organization for Standardization)

## 7. Kaynakça


[1] Mehtap Çetinkaya, "İşletmelerde Bilgi Güvenliği Altyapısının Değerlendirilmesi Test Aracı", Yüksek Lisans Tezi, İstanbul Kültür Üniversitesi – Bilgisayar Mühendisliği, İstanbul, 2008

[2] TS ISO/IEC 27001, "Bilgi teknolojisi – Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri – Gereksinimler", Türk Standartları Enstitüsü, Ankara, 2006

[3] TS GUIDE 13268-2, "TS ISO/IEC 27001'e Göre Bilgi Güvenliği Yönetim Sistemi (BGYS) Gerçekleştirmeler", Türk Standartları Enstitüsü, Ankara, 2007

[4] http://www.tse.gov.tr/, Türk Standartları Enstitüsü

[5] http://www.sans.org/, SANS is the most trusted & by far the largest source for information security training, certification & research in the world

[6] http://www.lostar.com.tr/, Lostar Bilgi Güvenliği A.Ş.