Anadolu Üniversitesi Sosyal Bilimler Dergisi | AÜSBD | Anadolu University Journal of Social Sciences

Örgütlerde Bilgi Güvenliği Yönetimi, Kurumsal Entegrasyon Süreci ve Örnek Bir Uygulama

Information Security Management in Organizations, Enterprise Integration Process and A Case Study

Yrd. Doç. Dr. Yusuf Yalçın İleri

Başvuru Tarihi: 04.02.2016
Kabul Tarihi: 30.09.2016

Öz

Bu çalışmanın amacı, bir üniversite hastanesinde, planlama, uygulama ve iyileştirme aşamalarıyla toplamda üç yıl süren Bilgi Güvenliği Yönetim Sistemi kurulum süreci tecrübelerimizi ve ulaştığımız sonuçları, yöneticilere rehber olabilecek uygulamalı bir örnek olarak literatüre kazandırmaktır. Bu çalışmada; hastanede oluşturulan temel bilgi güvenliği yönetimi politika ve prosedürleri hakkında bilgi verilmekte, uygulanan yöntemler ile karşılaşılan teknik ve yönetimsel zorluklar ve bu zorlukların nasıl üstesinden gelinebileceği başarılı bir uygulama örneği üzerinden tartışılmakta, kurumsal bilgi güvenliği kültürü ve bilinci oluşturma aşamaları ile sistem kurulmadan önce ve sonra hastanenin bilgi güvenliği seviyesinin durumu karşılaştırmalı şekilde aktarılmaktadır.

Anahtar Kelimeler: *Bilgi Sistemleri Yönetimi, Bilgi Kaynakları Güvenliği, Bilgi Güvenliği Süreçleri, Yönetim Bilişim Sistemleri*

Abstract

The aim of this article is to represent planning, implementation and the improvement phases of Information Security Management System installation process which took three years at a university hospital and reflect our experiences, and the results as a practical example for the administrators and the literature. This study, gives information on basic policies and procedures of hospital information security management system, discusses applied methods, encountered technical and administrative difficulties and points how these challenges were managed through the example of a successful application and informs about establishing stages of institutional information security culture and awareness and compares the attitude of the hospital's information security before and after the establishment of the system.

Keywords: *Information Systems Management, Information Resources Security, Information Security Processes, IT Management*

Giriş

Günümüzde, kurumlar iş süreçlerinin birçoğunda elektronik iletişim sistemlerini ve bilgi kaynaklarını kullanmaktadırlar. Bilgi teknolojilerinin kullanılmasıyla iş süreçlerinin hızlandırılması, kalitenin artırılması ve denetimin kolaylaştırılması sağlanarak kurumun toplam etkinliğinin yükseltilmesi hedeflenmektedir. Ancak, iletişim altyapısında veya bilgi kaynaklarına erişimde meydana gelebilecek bir kesinti, iş süreçlerinin işleyememesine neden olacak, eğer bu iş süreci kritik sistemlerden birine ait ise, kurumsal güvenlik zafiyetleri meydana gelebilecek, çalışanların ve

Yrd. Doç. Dr. Yusuf Yalçın İleri, Necmettin Erbakan Üniversitesi Sağlık Bilimleri Fakültesi, **yusuf.ileri@gmail.com**

müşterilerin kuruma ve kurumun bilişim altyapısına güveni olumsuz yönde etkilenecektir. Bu noktada, kurumlarda bilgi güvenliği yönetiminin bir sistem olarak ele alınması ve kurumsal ve toplumsal seviyede bilgi güvenliği kültürünün oluşturulması büyük önem taşımaktadır.

Bilgi güvenliği yönetiminde amaç; olayları meydana gelmeden önce öngörebilmek ve önleyici tedbirler almak, önlenemeyen olaylar meydana geldiğinde ise, en az zararla en kısa zamanda normal çalışma şartlarına geçebilmektir. Bunun için, uygulanabilecek en etkili süreçlerin belirlenmesi ve kurumun bu süreçleri uygulayabilecek bilgi, kültür ve yetkinliğe sahip olması gerekmektedir. Ayrıca, kurumlarda işletilecek bilgi güvenliği yönetim sürecinin politika ve prosedürlerinin oluşturulması, düzeltici ve geliştirici faaliyetler ile sistemin sürekli iyileştirilmesi, yönetimsel süreçlerle ilgili tüm kayıtların tutularak kurumsal bilgi güvenliği hafızasının ve kültürünün oluşturulması sağlanmalıdır.

Kurumsal bilgi kaynaklarının güvenliğinin sağlanması ulusal siber güvenliğimizin sağlanmasına da öncülük edecek ve bireylerden başlayarak tüm topluma kadar yayılan bilgi güvenliği farkındalığının oluşturulmasına fayda sağlayacaktır. Toplumda ve kurumlarımızda artan bilgi güvenliği farkındalığı ise, ürettiğimiz bilginin ve ticari sırların gizliliğini ve güvenliğini garanti altına alacak, bilgi kayıplarının oluşturduğu iş, zaman, para ve moral kayıplarını azaltacak, ülkemizin teknolojik bilgi birikimi sürecini hızlandıracak, zamanla bir sinerji ve bilinç oluşturarak, özellikle genç nesilleri katma değer yaratan ileri teknolojiye dayalı ürün ve hizmetleri geliştirmeye sevk edebilecek ve ülkemizin kalkınmasına yardımcı olacaktır.

Bilgi Güvenliği Yönetimi

Bilgi güvenliği yönetimi, kurumsal bilgi kaynaklarının farkına varma, bu kaynaklara her türlü denetimsiz erişimi engelleme, risk analizleri yaparak bilginin gizliliğinin ve bütünlüğünün korunması için gerekli idari ve teknik önlemleri alma ve tüm iş süreçlerini bilgi güvenliği politikaları doğrultusunda düzenleyerek yönetme işlevidir.

Bir kurum veya kuruluşun kar etmek, katma değer sağlamak, rekabet oluşturmak ve kurumsal sürdürülebilirliğini sağlamak amacıyla sahip olduğu ürün, pazar, teknoloji ve organizasyona ait bilgilerin tümü bilgi varlıkları olarak kabul edilebilir (Baykara vd., 2013, s. 232). Bilgi güvenliği yönetimi, bu bilgilerin, güvenli bir bilgi işleme platformu oluşturulmasıyla saklanması ve taşınması esnasında bütünlüğünün ve doğruluğunun bozulmadığından emin olmak (Canbek ve Sağıroğlu, 2006, s.168), yetki verilen kişilerin bu bilgilere her an kesintisiz ulaşabilmesini sağlamak (iso27001bilgiguvenligi.com, 2015), bilgi kaynaklarına karşı risk analizi ve derecelendirmesi yapmak, varlık, açıklık ve tehdit temelli düzeltici ve iyileştirici faaliyetlerde bulunmak (bilgiguvenligi.gov.tr, 2015), yaşanan bilgi güvenliği olaylarından ders çıkarmak ve yeniden oluşmasını önlemek (He vd., 2014, s. 525) gibi işlemlerin kurum bilgi yöneticisi liderliğinde (Sağsan, 2007, s. 107) belli bir sistem dahilinde yürütülmesidir.

Alınabilecek teknik güvenlik önlemlerinin seviyesindeki gelişmelere rağmen bilgi kaynaklarına karşı yapılan saldırıların bilgi sistemleri üzerinde yüksek derecede etki yapan hasarlara neden olması, teknik yöntemlerin tek başına bilgi güvenliğinin sağlanmasında yetersiz olduğunu göstermektedir. Bu durum, bilgi güvenliğinin, insan faktörünü de gözönüne alan karmaşık idari çözüm ve önlemleri gerektiren ve yönetilmesi zorunlu bir süreç halinde ele alınması gerekliliğini ortaya koymaktadır (Tekerek, 2008, s. 132; Cavalli vd., 2004, s. 298).

Kurumsal bilgi kaynaklarını zafiyete uğratmak, kurumlara doğrudan veya dolaylı olarak zarar vermek, sistemlere izinsiz girerek işleyişlerini aksattırmak, durdurmak, çökertmek gibi kötü niyetle yapılan tüm saldırı girişimleri (Canbek ve Sağıroğlu, 2006, s. 169) ile ticari sırların çalınması (Eminağaoğlu ve Gökşen, 2009, s. 2), finansal kayıplar, itibar kayıpları (Tekerek, 2008, s. 132), hizmetlerin sunulamaması veya aksaması (Vural ve Sağıroğlu, 2007, s. 192) gibi tehlikelere karşı yöneticilerin en güçlü silahları bilgi güvenliği yönetim sistemlerini tüm iş süreçlerine entegre etmek ve kurumsal bilgi güvenliği kültürünün oluşmasını sağlamak olacaktır.

Kurumlarda elektronik sistemlerin kullanılması, kağıt üzerinden yapılan işlemlere göre erişim yetkilerinin ve olaylarının çok daha kolay yönetilmesini sağlamaktadır (Bartlett vd., 2008, s. 66; NEHTA, 2007). Elektronik sistemlere geçilmesiyle birlikte,

kullanıcılar tam ve güvenilir bilgiye zamanında, hızlı ve kesintisiz (Şahin, 2008, s. 158) şekilde erişebilmeyi talep etmektedirler. Bu noktada devreye giren bilgi güvenliği yönetim sistemlerinin temel amacı, bilgi kaynaklarında gizlilik, bütünlük ve yetki bazında erişimi sağlamaktır (Cavalli vd., 2004, s. 298).

Bilgi güvenliği yönetimi sürecinde yapılan planlamalar kurumsal ve sektörel dinamikleri göz önüne almalıdır. Örneğin, sağlık sektöründe yapılan çalışmalar, sağlık çalışanlarının; değişime karşı korku (Sultan vd., 2014, s. 182), inanç, kuşku, motivasyon, kişisel gelişim isteği (Holden, 2011, s. 193-203; Yucel vd., 2011, s. 1212; Fernando ve Dawson, 2009, s. 821; Wakefield vd., 2007, s. 885-890), değişimi gerektiren nedenleri tam olarak anlayabilme (Pagliari, 2005, s. 98-103), sistemlerin erişim ve kullanım kolaylığı (Chen and Hsiao, 2012, s. 810) gibi nedenlerle yeni kurulmaya çalışılan sistemlere karşı direnç gösterdiklerini (Khalifa, 2013, s. 336) belirtmektedir. Bununla birlikte, sağlık sektöründe bilgi güvenliğine yönelik çalışmalar, hastanelerde sağlık personelinin otomasyon sistemleri erişim şifrelerini sıklıkla diğer çalışanlarla paylaştığını, bunun ise, işlemlerin aslında kim tarafından yapıldığının bulunmasını zorlaştırdığını ortaya koymaktadır (Fernando ve Dawson, 2009, s. 823; Medlin ve Caizer, 2007, s. 40-45; Timmons, 2003, s. 257-260; Williams, 2008, s. 211-214). Dolayısıyla, bilgi güvenliği yönetim sisteminin çalışanlar tarafından sahiplenilmesi ve bilgi güvenliği kültürünün kuruma yerleştirilebilmesi için yöneticiler, sistemin temel gerekliliklerini yerine getirirken sektörel ve organizasyonel değişkenlere de gerekli önemi vermelidirler.

Türkiye'de ve Dünyada Bilgi Güvenliği

Çağımızda, ülkelerin sıklıkla karşılaştıkları siber bilgi hırsızlığı olaylarına karşı güvende olabilmeleri ve ulusal bilgi güvenliklerinin sağlanması, bilgi güvenliği yönetim sistemlerinin öncelikle kurum ve kuruluşlara uygulanması ile mümkün olabilecektir.

Ülkemizde, özel sektör veya kamuda hizmet veren kuruluşların ürettikleri bilgiyi koruyamamaları, üretilen yeni teknoloji, süreç ve yöntemlerin siber casusluk taktikleriyle yabancı kaynakların eline geçmesine neden olmaktadır. Bilgi kaynaklarına erişimde güvenli erişim seçeneklerinin tercih edilmemesi, hesap sahiplerinin genellikle zayıf parolalar kullanmaları veya parolalarını başka kişilerle paylaşıyor olmaları, birçok kurumumuzda görevi değişen veya işten ayrılan personellerin kapatılmamış hesapları ile işlem yapabilmeye devam edebilmeleri ve bilgi kaynaklarına karşı saldırılarda sorumluların ve olayların detaylarının tespit edilememesi gibi durumlarla sıklıkla karşılaşılmasının yanı sıra kamu kurumlarınca yayınlanan bazı listelerde kişilere özel ayrıntılı bilgiler bulunması ve birtakım bilgilerin uygun olan zamandan önce açıklanması vb. ülkemizde yaşanan bilgi güvenliği olaylarından bazılarıdır. Ayrıca, birçok kurumda özellikle bilgi kaynaklarına erişim ve yetkilendirme konularında büyük bir bilgi eksikliği göze çarpmakta, bilgi kaynaklarına yönelik tehditlerde sorumluların tespitinde yaşanan zorluk ve zafiyetler bilgi kaynaklarının güvenliğinin yeterli ölçüde izlenemediğini ve erişimlerin standartlara uygun şekilde kayıt altına alınamadığını göstermektedir.

Yukarıda verilen örnekler, kurumlarımızda bilgi kaynaklarının güvenliğine önem verilmediğine, halkımızın bilgi güvenliği konusunda yeterli bilgi sahibi olmadığına dolayısıyla ülke olarak kurumlar ve vatandaşlarıyla beraber siber tehditlere karşı hazırlıksız olduğumuza dair önemli ipuçlarıdır.

Kurumlarda bilgi sistemlerinin güvenliğinin sağlanamaması sonucu sıklıkla yaşanan sistem kesintilerinin iş süreçlerini olumsuz yönde etkilediği, veri kayıplarının ve bilgi hırsızlıklarının ciddi ekonomik kayıplara neden olduğu aşağıdaki tabloda da açıkça görülmektedir (PWC, 2015, s. 8).

Kurumlarına bilgi güvenliği yönetim sistemlerini entegre etmek isteyen orta kademe yöneticilerin %56'sı en çok güçlük çektikleri konunun bilgi güvenliği noktasında kurumsal kültürün değiştirilmesi, %18'i ise üst yönetimin desteğinin sağlanması olduğunu bildirmişlerdir (CE, 2008, s. 8). Kurumsal bilgi güvenliği kültürünün oluşturulmasının yönetimsel desteğin yanında belli bir zaman, eğitim ve özümseme gerektirdiği açıktır ancak üst yöneticilerin desteğinin bu noktada henüz yeterli seviyede olmaması konunun öneminin tam olarak anlaşılamadığını göstermektedir.

Tablo 1. Dünyada, Bilgi Kaynaklarına Yönelik Güvenlik Olayları Sonucu Kurumların Tahmini Yıllık Ortalama Ekonomik Kayıpları

Kurum Büyüklükleri	2013	2014
Küçük Kurumlar (Yıllık geliri 100 milyon $ ve daha az)	0.65 milyon $	0.41 milyon $
Orta Büyüklükte Kurumlar (Yıllık geliri 100-999 milyon $ arası)	1.0 milyon $	1.3 milyon $
Büyük Kurumlar (Yıllık geliri 1 milyar $ ve üstü)	3.9 milyon $	5.9 milyon $

Kaynak: PWC, 2015, s. 8.

Aşağıdaki tablo, Avrupa ülkeleri arasında ülkemizin bilgi güvenliği yönetim sistemi noktasında bulunduğu yeri göstermesi açısından önem taşımaktadır. Ülkemiz, 2014 yılı başı itibariyle, 51 Avrupa ülkesi arasından bilgi güvenliği sertifikasına sahip en çok kurumu olan 11. ülke konumundadır. Bununla birlikte, Avrupa'da, bilgi güvenliği yönetim sistemine sahip en çok kurumu olan ülke konumundaki İngiltere'nin oldukça gerisinde olduğumuz anlaşılmaktadır. Yine, 2014 yılı istatistiklerine bakarak, Dünyada en büyük 13. ekonomi olan İspanya ile en büyük 18. ekonomi olan Hollanda'nın kurumlarının sahip olduğu bilgi güvenliği sertifikası sayıları, 16. en büyük ekonomiye sahip olan ülkemizden (IMF, 2014) oldukça fazla olduğu göze çarpmaktadır.

Tablo 2. Avrupa'da BGYS Sertifikasına Sahip Olan Ülkeler ve Sertifika Sayıları

Sıra	Ülkeler	2007	2008	2009	2010	2011	2012	2013
1	İngiltere	519	738	946	1157	1464	1701	1923
2	İtalya	148	233	297	374	425	495	901
3	Romanya	16	44	303	350	575	866	840
4	İspanya	93	203	483	711	642	805	799
5	Almanya	135	239	253	357	424	488	581
6	Çek Cumh.	77	88	264	529	301	264	397
7	Hollanda	41	56	76	97	125	190	316
11	Türkiye	27	33	86	117	100	132	181

Kaynak: ISO, 2013

Tablo 3. İş Süreçlerine BGYS Entegrasyonu Yapan Kurumların Sayısında Yıllık Artış Oranları

Yıllar	2010	2011	2012	2013
Dünya	%21	%12	%13	%14
Avrupa	%35	%10	%21	%25
Türkiye	%36	- %15	%32	%37

Tablo 3'de görüldüğü gibi, ülkemizde, bilgi güvenliği yönetim sistemini iş süreçlerine entegre eden kurumların sayısındaki yıllık yüzdesel artış, son dört yılın üçünde Dünya ve Avrupa'daki ortalama artışların üzerinde gerçekleşmiştir. Ancak, listede daha üst sıralara çıkabilmek için bu büyüme oranlarının yeterli olmadığı anlaşılmaktadır.

Ülkemizin bilgi güvenliği noktasında arzu edilen seviyelere ulaşabilmesi, dünyadaki teknolojik değişime ayak uydurabilmesi, siber ataklara ve hatta siber savaşlara hazırlıklı olabilmesi öncelikle kurumlarının bilgi güvenliği sistemlerini iş süreçlerine entegre etmeleri ve bilgi güvenliği noktasında kurumsal kültürlerin yerleştirilmesi ile mümkün olacaktır. Bilgi güvenliği yönetim sistemlerini uygulayan kurumlarımızın ise, beklenmeyen durumlara hazırlıklı olabilmeleri ve çevik hareket edebilmeleri için sistemlerini bağımsız kuruşların düzenli denetiminden geçirmeleri, önleyici ve geliştirici faaliyetlerini hazırlanan raporlara göre sürekli güncellemeleri büyük önem taşımaktadır.

Bilgi Güvenliği Yönetim Sisteminin Sağlık Sektörü Örneğinde Kurulum Süreçleri

Bilgi güvenliği yönetim sistemlerinin bir kuruma entegre edilmesi ciddi bir çalışma, araştırma ve zaman gerektirmektedir. Bu çalışmadaki amacımız, üç yıllık yoğun bir kurumsal çalışma ile bilgi güvenliği yönetim sistemini kurduğumuz Tıp Fakültesi Hastanesi'nde yaşadığımız tecrübelerin, sistemin kurulma ve geliştirme aşamalarının, karşılaşılan zorlukların, kurumsal bilgi güvenliği kültürünün oluşturulması için geliştirilen süreçlerin ve elde dilen sonuçların sunulmasıdır. Böylelikle, bilgi güvenliği yönetim sistemlerini iş süreçlerine entegre etmek isteyen kurum yöneticilerine yol gösterebilecek ve ülkemizin bilgi güvenliği noktasında gelişimine katkı yapabilecek bu çalışmanın literatürümüze kazandırılması hedeflenmektedir.

Bilgi güvenliği yönetim sistemi entegre edilen hastane 1200 yataklı tam teşekkülü bir üniversite hastanesi olup tam elektronik otomasyon sistemine sahiptir. Hastane otomasyon sisteminde aynı anda yaklaşık 2000 kullanıcı işlem yapabilmektedir ve hastanedeki tüm tıbbi ve idari süreçler otomasyon sistemleri yardımıyla işlemektedir. RBS (Radyoloji Bilgi Sistemleri), LBS (Laboratuvar Bilgi Sitemleri), dijital arşiv gibi tüm birimleri hastane otomasyon sistemiyle entegre çalışmaktadır. Tüm radyolojik cihazlardan alınan dijital görüntüler hastane sunucularında saklanmakta ve hastaların tedavi öncesi randevu almalarını sağlayan elektronik randevu sisteminden taburcu oldukları ana kadarki tüm medikal süreçler elektronik bilgi ortamı üzerinden yürütülmektedir.

Sağlık sektöründe faaliyet gösteren kurumlar, 7 gün 24 saat kesintisiz hizmet verirlerken, bu kurumların veritabanlarında biriken bilgi miktarı çok hızlı bir şekilde artmaktadır. Bununla birlikte, tutulan veriler değerini hiçbir zaman kaybetmemekte, sağlık hizmetlerinin yapısı gereği, bir hastanın tedavi süreci geçmiş tıbbi işlemlerinden etkilendiğinden uzun yıllar önceki bilgilere bile her an ulaşılabilme isteği ve gereği doğabilmektedir. Hastanelerde, otomasyon sistemlerinde kayıt altında tutulan on binlerce hastanın medikal verileri ile yüzlerce idari sürecin her türlü çıktısının yanında, ofis otomasyon sistemleri, kullanılan tüm tıbbi cihazlar ve diğer tüm elektronik aletler ile otomasyon sistemlerine doğrudan kaydedilemeyen ve fiziksel ortamlarda tutulan her türlü veri hastanelerin bilgi kaynaklarını oluşturmaktadır

ve bu çalışmada ilgili hastanede kurulmuş olan bilgi güvenliği yönetim sistemleri, bilgi kaynakları ile tıbbi ve idari süreçlerin tamamının gizliliğinin korunmasından sorumludur.

Kurumda BGYS Kapsamında Oluşturulan Politika ve Prosedürler

Hastane bünyesinde kurulan bilgi güvenliği yönetim sisteminin çerçevesi; gizlilik, bütünlük, kullanılabilirlik, erişim denetimi ve kontrol süreçlerini kapsayan 5 temel politika ve bu politikaları yürüten 22 prosedür ile belirlenmiştir.

Bilgi güvenliği politikaları, kurumsal bilgi güvenliği amaç ve hedeflerini içeren, çalısanların görev ve sorumlulukları ile gerekli yönetimsel denetim mekanizmalarını belirleyen, kurumun yapısına ve kültürüne uygun kurallar bütünü şeklinde hazırlanmıştır. *Eş zamanlı olarak,* hastane bilgi kaynakları belirlenerek önem derecelerine göre sınıflandırılmıştır. Her bilgi kaynağına yönelik; tehlike oluşturabilecek açıklıkların ortaya çıkma ihtimali, açıktan faydalanması mümkün olan olgular, bilgi kaynağının kurum için önem derecesi, açığın ortaya çıkması için oluşması gereken koşullar ile tehlikeye karşı o anda cevap verebilecek ve sonrasında raporlayacak takımların kimlerden oluştuğu gibi bilgileri içeren analizler yapılmıştır.

Analizleri takiben bilgi güvenliği yönetim süreçlerini detaylandıran toplam 22 prosedür oluşturulmuştur. Hastane içerisindeki bilgi kaynaklarını ilgilendiren her türlü işlem, ürün veya hizmetin, üretilmesi veya satın alınıp kurulması ve faaliyete geçirilmesinden, çıktıların elde edilmesi, saklanması ve yedeklenmesine kadar tüm hastane süreçlerinin bilgi güvenliği gözetilerek yapılmasını sağlayan bu prosedürlerin listesi ve kısa açıklamaları aşağıdaki tabloda verilmiştir.

Tablo 4. Hastanede BGYS'nin Çerçevesini Oluşturan Prosedürler ve Etki Alanları

Prosedürler	Etki ve Kontrol Alanı Tanımı
Erişim Denetimi Prosedürü	Hastane çalışanlarının hastane bilgi kaynaklarına erişimlerinde yetkilendirme ilkelerini düzenler. Çalışılan birim, meslek grubu, idari göreve sahip olup olmama gibi temellerde her bilgi kaynağına erişimin ayrı ayrı yetkilendirme işlemlerini tanımlar ve süreçleri yönetir.
Veri Kontrolü Prosedürü	Hastane otomasyon sistemi ile RBS, LBS ve dijital arşiv birimlerinden gelerek veritabanında saklanan verilerin günlük, haftalık, aylık kontrol ve bakım kurallarını düzenler ve ilgili süreçleri ayrıntılı biçimde açıklar.
Satınalma Prosedürü	Hastanenin bilgi kaynaklarını ilgilendirebilecek malzeme, hizmet ve demirbaş taleplerinin satın alma öncesi ön değerlendirmelerinin kontrollü şekilde yapılabilmesi için kurulan Ön Değerlendirme Komisyonu'nun işleyişini tanımlar.
Tedarikçi Değerlendirme Prosedürü	Hastane bilgi kaynaklarını ilgilendirebilecek mal ve hizmetleri sağlayan firmaların hastane şartlarını karşılayan ürün sağlama yeteneği temelinde değerlendirme ve seçme sistemi ile ilgili süreçleri düzenler.
Harici Hizmet Alımı Prosedürü	Bilgi güvenliği sistemi kapsamına giren harici hizmet alımlarında yönetimsel süreç ve aşamaları belirler.

Tablo 4. Hastanede BGYS'nin Çerçevesini Oluşturan Prosedürler ve Etki Alanları (Devamı)

Uygun Olmayan Hizmet Prosedürü	Bilgi güvenliği yönetim sistemi şartlarını sağlamayan hizmetlerin tanımlanması, hakkında karar verilmesi gibi işlemlerin yapılmasında yetki ve sorumluluklar ile yönetim ilkelerini ve süreçleri tanımlar.
İç Tetkik Prosedürü	Hastanede işletilen bilgi güvenliği yönetim sisteminin planlara ve standartlara uygunluğunun ve etkinliğinin periyodik olarak doğrulanması, uygunsuzluklar için düzeltici faaliyetlerin belirlenmesi ve iyileştirme alanlarının tespit edilmesini sağlayan kontrol süreçlerini tanımlar.
Düzeltici Faaliyet Prosedürü	Bilgi güvenliği yönetim sisteminde; mevcut uygunsuzlukların sebeplerinin ortadan kaldırılması amacıyla düzeltici faaliyetlerin planlanması, uygulanması, sonuçların izlenmesi ve tekrarlarının önlenmesi için esasları belirler.
Önleyici Faaliyet Prosedürü	Bilgi güvenliği açıkları ve tehditlerine karşı alınabilecek önleyici uygulamaların planlanması, uygulanması ve sonuçlarının izlenmesi için esasları belirler.
Yönetimin Gözden Geçirme Prosedürü	Bilgi Güvenliği Yönetim Sisteminin belirlenmiş politika ve hedefler doğrultusunda varlığını sürdürebilmesi için sistemin periyodik olarak (yılda 4 kez) üst yönetim tarafından incelenme ve değerlendirme esaslarını belirler.
Temel Bakım ve Onarım Prosedürü	Hastanedeki tüm bilgi kaynaklarına ait makine ve teçhizatın işletimsel sorunları, arıza, periyodik bakım ve yazılımlarının güncellenmesi ile ilgili faaliyetleri düzenler, yetki ve sorumlulukları belirler.
Eğitim Prosedürü	Bilgi güvenliği yönetimi kapsamında çalışanların eğitim ihtiyaçlarının belirlenmesi, planlanması ve etkinlik ölçümü için esasları belirler. Yeni işe başlayan personelin beş günlük temel oryantasyon eğitimlerini düzenler.
Teknik Uyum Prosedürü	Hastaneye alınan donanım, yazılım, network ürün ve hizmetlerinin, hastane ihtiyaçlarına ve güvenlik politikalarına uygunluğunu ve mevcut sistemle teknik anlamda uyumlu çalışıp çalışmadığının kontrol süreçlerini belirler.
Network, Donanım ve Fiziki Güvenlik Prosedürü	BGYS kapsamında kullanılan ve hastane ağına erişen tüm cihazlar ile diğer teçhizatların yazılımsal, donanımsal ve fiziksel anlamda güvenliğinin sağlanması, periyodik denetimlerin yapılması, yetkisiz her türlü erişimin engellenmesi ile ilgili uygulanması gereken süreçleri açıklar.
Yedekleme Prosedürü	Tüm sistem verilerinin yedeklerinin alınması, saklanması ve olağanüstü durumlarda sistemin yedeklenmiş veriler vasıtasıyla sürekliliğinin sağlaması ve işleyişin durmaması için gerekli süreçleri tanımlar. (İlk yılın sonunda donanım ve personel yedekliliğini de sağlayacak şekilde geliştirilmiştir)

Tablo 4. Hastanede BGYS'nin Çerçevesini Oluşturan Prosedürler ve Etki Alanları (Devamı)

Değişim Yönetimi Prosedürü	Sistemde faaliyete geçirilen yeni yazılım ve donanımların bilgi güvenliği yönetim sistemi üzerinde oluşturabileceği yeni tehdit ve açıklıkların belirlenmesi ve kullanıcıların değişime uyumunu izleme süreçlerini içerir.
Sistem İzleme ve Planlama Prosedürü	Sistem arızalarının en az seviyeye indirilmesi için kapasite ve kaynakların yeterliliklerinin belirlenmesi ve kapasite paylaşımı ile sistemin aşırı yüklenmesini önleyici faaliyetleri kapsar.
Kötü Niyetli Yazılımlara Karşı Koruma Prosedürü	Hastane içerisinde ineternete ve hastane ağ sistemine erişim kabiliyeti olan tüm cihazların virüs, trojen, key logger gibi kötü niyetli yazılımlardan korunması, kullanıcıların cihazlara erişim yetkileri, cihazların ağ ve internete erişim yetkileri ile merkezden yönetilen antivirus yazılımlarının kurulum ve yönetim ilkelerini kapsar.
Risk Yönetimi ve Değerlendirilmesi Prosedürü	Hastane bilgi güvenliği yönetim sistemi kapsamına giren yazılı veya elektronik ortamdaki tüm bilgi kaynaklarına karşı oluşabilecek risklerin belirlenmesi, oluşma ihtimali, önem derecesi ve yönetimi ile ilgili süreçleri kapsar. Gerekli karşı önlemlerin alınma süreçleri ile ilgili kişi ve birimlerin görev ve sorumluluklarını açıklar.
Bilgi İmha Prosedürü	Kurumda, hassas bilgi içeren bilgi ortamlarında bulunan bilgilere gereksinim kalktığında, bilgilerin yok edilmesi aşamasında kopyalanma, yetkisiz kişilerin eline geçme veya kaybolma gibi durumlara karşı alınacak önlemleri açıklar ve bu bilgi ortamlarının emniyetli ve geri dönüşümsüz şekilde imha edilmesini düzenleyen süreçleri içerir.
Bilgi Etiketleme Prosedürü	Bilgi güvenliği yönetimi kapsamında, hastane bilgi kaynaklarının uygun koruma seviyesine göre sınıflandırılmasını ve etiketlenmesini düzenler.
Olay Raporlama Prosedürü	Hastanedeki bilgi varlıklarına ve kaynaklarına etki eden olayların raporlanması sırasında takip edilecek süreçleri açıklar, bu olaylara karşı önlem alırken hangi prosedürlerin seçilmesi gerektiğini ve sorumlulukları tanımlar.

Hastane içerisindeki tüm birimlerin ve personelin görev tanımları, bilgi güvenliği noktasındaki yetki ve sorumlukları ile bilgi kaynaklarını ilgilendiren süreçlerde uyulması gereken kuralları detaylı şekilde açıklayan bu prosedürlerin kurumda çalışan tüm personel tarafından çok iyi bilinmesi ve özümsenmesi amacıyla, hastane otomasyon sisteminde BGYS modülü oluşturulmuş ve hastane personeline sorumlulukları çerçevesinde modüle erişim yetkisi verilerek gerektiği anda bu prosedürlere ve görev tanımlarına ulaşma imkanı sağlanmıştır.

Bilgi Güvenliği Yönetimi Kapsamında Eğitim Prosedürlerinin Uygulanması

Hastanede bilgi güvenliği yönetim sistemi kurulum sürecinde karşılaşılan en büyük zorluklar; bu sürecin sadece teknik birimlerin ve personelin işi olduğu kanısı, hastane çalışanlarının bir bölümünün bilgi sistemlerini kullanma güçlüğü yaşamaları, yeterli bilgi, yetenek veya eğitime sahip olmamaları gibi nedenlerle bilgi güvenliği sistemine gereken önemi vermemeleri ve bu konudaki kurumsal hedeflere katkı sağlamaktan ziyade direnç oluşturmaları olarak sıralanabilir.

Bilgi güvenliği yönetim sistemi kurulmadan önce birim yöneticileri ile düzenlenen toplantılar ve çalışanlarla yapılan anketler genel olarak kurum çalışanlarının bilgi sistemlerine olan yatkınlıklarını ortaya çıkarmıştır. Bilgi güvenliği ve bilgiyi koruma yolları ile denetimli erişim ve yetkilendirilmiş kullanım gibi konularda personelin çok kısıtlı bilgiye sahip olduğu hatta bazılarının yanlış bilgiler nedeniyle yanlış uygulamalara yöneldikleri belirlenmiştir. Bu noktada gözlemlenen ihtiyaca binaen hastane bünyesinde kurulan "Bilgi Sistemleri Eğitim Birimi", eğitim prosedürlerinde belirlenmiş hedeflere ulaşılıncaya kadar tüm hastane çalışanlarına yönelik yoğun eğitim programları düzenlemekle görevlendirilmiştir. Bu birim hastane yönetimini temsilen bir hastane müdür yardımcısı, iki bilgisayar mühendisi (kurum sistem sorumlusu ve kurum bilgi güvenliği sorumlusu), dört hastane bilgi sistemleri uzmanı ve hastanenin eğitim hemşirelerinden oluşturulmuştur.

Kurumun ve çalışanların bilgi güvenliğine gerekli önemi vermesi, bilginin her türlü süreçte korunabilmesi, kurumsal yeterliliğin ve kültürün oluşturulması gibi amaçlarla gerekli eğitimler düzenli olarak doktor, asistan, hemşire, tıbbi tekniker/teknisyen, büro çalışanları, sekreter, hastabakıcı ve hastane güvenlik personeli de dahil olmak üzere tüm meslek gruplarına verilmiştir.

Özellikle Bilgi İşlem Birimi personeli ve sistem yöneticilerinin bilgi güvenliği yönetimi ve bilginin korunması noktasında yeterli teknik bilgi birikimine sahip olmaları için bu konuda profesyonel destek veren kuruluşlardan teknik eğitim almaları sağlanmıştır. Ortaya çıkan problemlerin çözülme süreleri takip edilerek bilgi işlem personelinin etkinliği sürekli olarak kontrol altında tutulmuştur.

Kurumda, bilgi güvenliği yönetim sisteminin gerekliliklerinden olan (USGT, 2011, s. 23), biri sistem sorumlusu biri de bilgi güvenliği sorumlusu olmak üzere iki uzman personel arasında yetki ve sorumluluklar paylaştırılmış ve birbirlerinin yerlerine gerektiğinde vekalet edebilecekleri şekilde bir organizasyon yapısı oluşturulmuştur. Bilgi güvenliği uzmanlarının görev tanımlarında öncelikli ve ikincil yetki ve sorumluluklar detaylı şekilde belirlenmiştir. Başta bilgi güvenliği uzmanları olmak üzere, hastane bilgi güvenliği yönetimi noktasında birbirini yedekleyen personellerin eğitim planlarına özel önem verilmiş ve görev tanımlarında belirtilen birincil ve ikincil görevlerinin tamamını yerine getirebilmeleri için gerekli eğitimleri almaları sağlanmıştır.

Tablo 5'de hastane çalışanlarına BGYS kapsamında verilen yıllık eğitim süreleri gösterilmiştir. Her yıl bu konuda uzman 6 personelin verdiği eğitimler, 3 yılın sonunda her yıl ortalama 1217 hastane personeline yılda ortalama 23 saat seviyesinde gerçekleşmiştir. Sağlık kurumlarının ne kadar yoğun hizmet verdikleri ve sağlık çalışanlarının üzerlerindeki zaman baskısı göz önüne alındığında, hastane personelinin müsait oldukları zamanlarda eğitim takvimi oluşturmanın ve bu eğitimleri 3 yıl süreyle düzenli şekilde yürü-

Tablo 5. Hastanede Düzenlenen Bilgi Güvenliği Yönetim Sistemi Eğitim Detayları*

Yıllar	Bilgi Güvenliği Eğitimleri			
	Toplam Eğitim Süresi	Eğitmen Sayısı	Toplam Katılımcı Sayısı	Hedef Katılımcı Sayısı
1. Yıl	26 saat	6	1286 kişi	1400
2. Yıl	25 saat	6	1306 kişi	1400
3. Yıl	18 saat	6	1359 kişi	1400
Ortalama	23 saat	6	1317 kişi	1400

*Sadece kurum içinde düzenlenen eğitimleri kapsamaktadır

tebilmenin yönetimsel açıdan oluşturduğu zorluk daha iyi anlaşılmaktadır. Eğitimler eğer mümkünse öğle araları ve mesai harici saatlerde yapılmış, bunun mümkün olmadığı zamanlarda ise "Bilgi Sistemleri Eğitim Birimi" 'nden ilgili personelin bizzat sağlık çalışanlarının birimlerine gitmeleri suretiyle uygulamalı olarak verilmiştir.

Kurumdaki tüm birimlerde bir bilgi güvenliği sorumlusu belirlenmiştir. Örneğin, yataklı servislerin bilgi güvenliği sorumlusu servis başhemşireleridir. Tüm birimden sorumlu olmak farklı yetki, bilgi ve beceri gerektirdiğinden, birim sorumlularına bilgi güvenliği eğitimleri yanında kurum dışından uzmanların katılımıyla yönetimsel boyutta da eğitimler verilmiştir.

Bilgi güvenliği zincirinin en önemli halkasını oluşturan faktörün insan olduğu bilinciyle, hastane çalışanlarının eğitimler sonrasında da bilinç düzeylerini yüksek tutmak ve konunun gündemden hiçbir zaman düşmemesini sağlamak amacıyla kullanıcılara düzenli olarak uyarı e-postaları ve sistem mesajları gönderilmiştir. Ayrıca, kurum içerisinde belirli yerlere çeşitli bilgi güvenliği uyarıları yerleştirmek gibi bilgi güvenliğini hatırlatıcı yöntemler kullanılmıştır.

Hastalar ve refakatçilerin de bilgi güvenliğinin sağlanması noktasında destek alabilmek amacıyla bilgi güvenliğinin hastalar için önemini anlatan broşürler dağıtılmış ve hastanenin yoğun bölgelerine uyarı levhaları asılmıştır.

Hastaların geçmişte ellerinde taşımak zorunda kaldıkları rapor, film, tetkik sonuçları vb. belgeler tamamen dijital ortama dahil edildiğinden fiziksel olarak bu evrakların kaybından kaynaklanabilecek bilgi hırsızlığının önüne önemli ölçüde geçilebilmiştir. Özellikle genç ve orta yaştaki hastaların medikal ve kişisel bilgi içeren form, tetkik vb. çıktılarını almak veya hastaneden talep etmek yerine internet ortamını kullanarak bakmayı tercih ettikleri görülmüştür. İnternet üzerinden tetkik sonuçlarına ulaşmak isteyen hastalar, hastane tarafından kendilerine özel olarak üretilerek verilen ve her tetkikte değişen şifreler ile TC kimlik numarası veya doğum tarihi gibi bilgileri doğru şekilde girdikten sonra sonuçlarına ulaşabilmektedirler.

Çalışanların Yetkilendirilmesi ve Erişim Denetimi

Hastane personelinin Hastane Bilgi Yönetim Sistemi'nde (HBYS) kullanmaya yetkili oldukları modüller ve erişim hakları, hastane BGYS yürütücüsü ve hastane üst yönetimiyle birlikte çalışanların; hangi meslek grubuna mensup oldukları, hangi birimde çalıştıkları, idari görevlerinin olup olmadığı gibi kriterler göz önüne alınarak belirlenmiştir. Hastane içerisindeki tüm bilgi kaynaklarına erişimlerin düzenlenmesi "Erişim Denetimi Prosedürü" temelinde yönetilmiştir.

Her bilgi kaynağına erişim yetkilendirmesi için farklı süreçler işletilmekle beraber, örneğin, hastane çalışanlarının HBYS erişimi için yetkilendirme işlemleri aşağıdaki aşamaların tamamlanmasından sonra yapılmaktadır (Erişim Denetimi Prosedürü 'ne göre; yeni işe başlayan personeller için 1. maddeden itibaren, birim değiştiren personeller *için* ise 2. maddeden itibaren uygulanmıştır).

1. İşe başlayan personel öncelikle; hastane ve hastane birimleri hakkında bilgilendirme alır. Hastane otomasyon sistemi ve önemi, temel iş süreçleri ve ilgili kurallar ile kişinin mesleğine özgü eğitimleri içeren bir haftalık "işe başlama oryantasyon eğitimi' ne katılır.

2. Çalışana, Bilgi İşlem Merkezi tarafından, işini yaparken ihtiyaç duyacağı HBYS modülleri ile ilgili detaylı eğitim verilir ve gözetmen eşliğinde temel işlemleri yapması istenir.

3. Çalışana bilgi güvenliğinin sağlanmasının önemi ve sıklıkla yapılan kullanıcı hataları bildirildikten sonra BGYS politikaları doğrultusunda hazırlanmış bilgi güvenliği ve gizliliği belgesini okuması ve imzalaması istenir.

4. Her çalışan, imzaladığı belgeyi bir de çalıştığı birimin sorumlusuna imzalatır.

5. Bilgi işlem personeli kişinin mesleği ve birimine göre önceden belirlenmiş yetkilere sahip kullanıcı adı ve şifrelerini çalışana iletir.

6. Çalışan HBYS' ne ilk girişinde parolasını değiştirmek zorundadır aksi hale işlem yapamaz. Çalışanlar, benzer şekilde, üç ayda bir şifrelerini değiştirmeleri için sistemden zorunlu uyarı alırlar.

Yukarıda kısaca anlatılan işlemler biraz bürokratik ve zaman alıcı süreçler gibi görünseler de yaşanılan tecrübeler göstermiştir ki; ortaya çıkan bir bilgi güvenliği zafiyetini düzeltmek ve iş ve süreçlerinin etkilenmeden devam etmesini sağlamak çok daha fazla emek ve zaman gerektirmektedir. Bu işlemlerden sonra kullanıcı adı ve şifresini alan çalışanlar bilgi güvenliğinin önemini ve hastane tarafından konuya verilen değeri anlamış olmaktadırlar. İlerleyen zamanlarda çalışanlara verilen bilgi güvenliği yönetimi ile ilgili eğitimler, temel bilgi güvenliği zafiyetini gidermek, konunun kurumsal kültür boyutunu oluşturmak ve gündemden düşmesini önlemek için düzenlenmiştir.

Hastanenin BGYS politikasına göre; bir hastane çalışanının mevcut erişim yetkilerinden daha fazla yetki talep etmesi durumunda, ilgili birim yöneticisinin başvurusu, sistem yöneticilerinin olumlu yönde görüşü ve üst yönetimin oluru gibi aşamalar sırayla takip edilmektedir.

Hastaneden ayrılan veya hastane içerisinde farklı bir birimde görevlendirilen personelin erişim haklarının kaldırılması veya güncellenmesi işlemleri de bilgiye erişim denetimi politikasının önemli bileşenlerindendir. Hastaneden ayrılacak olan personeller işlemlerini tamamlamak için bilgi işlem sorumlusu ve sistem yöneticisinin ıslak imzalarını aldıkları formu insan kaynaklarına iletmeden işlemlerini tamamlayamamaktadırlar. Ayrılan personelin HBYS sistemindeki kullanıcı adı ve şifreleri iptal edilir, bilgisayarlarına bilgi işlem merkezinde ilgili prosedür gereği veri temizleme işlemi uygulanır, hastaneye ve hastane içi birimlere giriş-çıkış yaparken kullandıkları akıllı kartları geri alınır. Hastanenin BGYS politikası gereği, üç ayda bir bilgi sisteminde aktif durumdaki erişim hakları gözden geçirilmektedir.

Kurum Ağ ve Sisteminin Bilgi Güvenliği Yönetimi Sürecine Entegrasyonu

Hastanede hizmete alınacak tüm sistem ve süreçlerde, güvenlik bir temel tasarım aracı olarak kullanılmış ve bilgi güvenliği yönetimi politika ve hedeflerine uygun olduğu ilgili prosedürlerle belirlendikten sonra yeni sistemlere işlerlik kazandırılmıştır. Mevcut bilgi kaynakları ve işleyen süreçler ise bilgi güvenliği yönetim sistemi amaçlarına uygun şekilde güncellenmiş ve yeni yatırımlarla desteklenmiştir.

Kurumsal bilgi kaynaklarının istenmeyen, zararlı ve casus yazılımlara karşı korunabilmesi için hastane ağına bağlanabilen ve veri alış-verişinde bulunabilen tüm cihazlara güncel bir antivirüs programı kurulmuştur. Merkezden yönetilen antivirüs sunucu yazılımı sayesinde, hastanede hangi cihazlarda güncelleme yapılmadığı, hangilerine virüs bulaştığı ve temizlendiği, virüslerin bulaşma yolları gibi olgular kolaylıkla izlenerek hastane ağı sürekli denetim altında tutulmuştur. Kullanıcıların cihazlara taktıkları taşınabilir donanımlar vasıtasıyla hastane dışı kaynaklı virüslerin bulaşma ihtimaline karşı, cihazların veri alışverişinde bulanabileceği her türlü taşınabilir donanımın erişilebilir duruma ancak virüs taraması yapıldıktan sonra geçebilmesi sağlanmıştır.

Hastane bilgi kaynaklarına karşı saldırıları tespit sistemlerine büyük önem verilmiş ve hastane ağı içerisine giren ve çıkan elektronik trafiğin tümü firewall cihazları ile sürekli izlenmiş ve kontrol altında tutulmuştur. Saldırı tespit sistemlerine ait uygulamaların ürettiği kayıtlar, ilgili prosedür gereği düzenli olarak kaydedilmiş ve incelenmiştir. Böylelikle, kurumsal bilgi kaynaklarına yönelik saldırıların tespiti ve güvenlik açıklarının belirlenmesi kolaylaşmış ve bu saldırı ve açıklıklara karşı alınan önlemlerin daha isabetli ve etkin olması sağlanmıştır. Tüm bu işlemler, birbirlerini destekleyen geri bildirim ve denetim süreçleri içerdiğinden sistem güvenliği noktasında otomatik kontrol sağlanabilmiştir.

Hastanenin bilgi güvenliği yönetim sistemi politikalarından biri olan "erişilebilirlik" hedefi doğrultusunda, kullanıcılara bilgiye istedikleri zaman istedikleri yerden erişebilme imkanı vermek amacıyla, fiziki olarak çok geniş alanlara yayılmış bir sağlık kurumu olmasına rağmen, hastane bir yandan kablosuz iletişim sağlayabilen cihazlarla donatılmış, bir yandan da kablosuz ağlar üzerinden yetkisiz erişimlerin önlenmesi için 802.1x protokolleri gibi gelişmiş kablosuz ağ güvenlik uygulamaları hayata geçirilmiştir. Dışarıdan herhangi bir cihazın hastane ağına yerleştirilmesi veya hastane içerisindeki mevcut cihazlara fiziksel olarak erişilerek konfigürasyonlarının değiştirilememesi için fiziksel ve mantıksal güvenlik önlemleri alınmıştır. Hastane içerisinde kurulmuş olan tüm ağ anahtarları ve kablosuz ağ cihazları kilitli kutulara yerleştirilerek fiziksel güvenlikleri sağlanmaya çalışılmıştır. Bu cihazların mantıksal güvenlik sorunları ise, entegrasyon aşamasında merkezden yönetim

protokollerine göre kurulmalarının verdiği avantaj da kullanılarak, özel güvenlik yazılımlarıyla sürekli izlenerek ve en küçük bir güvenlik sorununda bile bilgi işlem merkezi içerisindeki ekranlardan ilgili yöneticilere uyarı gönderebilen sistemler kullanılarak çözülmüştür.

Hastane içerisinde belirlenen kritik birimler ile sistem, kamera odası vb. yerlere giriş ve çıkışların özel yetkilendirilmiş kartlarla yapılması sağlanmıştır. Buralara giriş-çıkış yetkili personel sayısı kısıtlı olmasına rağmen, her giriş yapan kişinin giriş çıkış saatleri detaylı olarak tutulmakta ve kameralar ile kayıt altına alınmaktadır. Kritik birimler içerisindeki güç kaynakları herhangi bir elektrik kesintisinde otomatik olarak devreye girmekte ve kurum jeneratörlerinin hizmet veremediği durumlarda bile sistemin birkaç saat daha çalışmasına olanak sağlamaktadırlar. Hastane bilgi kaynakları açısından kritik cihazların bulunduğu mekanlar içerisinde sıcaklık ve nemin belirlenen sınırların dışında seyretmesi, elektrik kesintisi veya dalgalanması, su baskını vb. her türlü olayda sistem otomatik olarak önceden belirlenen kişilere kısa mesaj yoluyla bilgilendirme yapmaktadır, böylelikle normal mesai saatleri haricinde de kısa bir sürede sisteme insan eliyle müdahale edilebilmesi garanti altına alınmıştır.

Bakım ve Onarım Prosedürleri

Hastanedeki bilgi kaynaklarına dahil olan tüm yazılım, donanım ve tıbbi cihazlar etiketlenerek gruplanmış ve grup bazında hangi birimlerin bakım, onarım, güncelleme vb. işlemlerden sorumlu oldukları belirlenmiştir. Hastane kaynaklarıyla çözülemeyen problemlerde, dışarıdan hizmet alımına gidilmiş ve ilgili süreçlerde "Satın Alma" ve "Harici Hizmet Alımı" prosedürlerine uyulmuştur. Hastane bilgi kaynaklarına doğrudan erişim sağlanması gereken veya tıbbi cihaz ve donanımların dışarıda bakımının gerektiği durumlarda ise "Tedarikçi Değerlendirme Prosedürü" ilgili süreçleri belirlemektedir. Hastane bilgi kaynaklarına ürün veya hizmet alımı sonucunda kısıtlı da olsa erişim yetkisi verilen tüm kurum ve firmalarla gizlilik anlaşmaları imzalanmıştır.

Özellikle ürün ve hizmet satın alımı ile tedarikçi değerlendirme işlem ve süreçleri sektörlere göre çok farklılık gösterebildiğinden, kurum yönetimi ve BGYS yürütücüsü sektörel parametreleri de göz önünde bulundurarak ilgili prosedür süreçlerini en uygun şekilde oluşturmalıdırlar.

Hastanenin acil servis, ameliyathane ve yoğun bakımları gibi kritik birimlerinde iş süreçlerinin aksamamasını garanti altına alabilmek için, her yıl istatistiki olarak yoğunluğun en az olduğu bir gün ve saat seçilerek, bu birimlerdeki personele de önceden bilgi verilmek suretiyle, Hastane Bilgi Yönetim Sistemi'nin (HBYS) durduğu bir durum prova edilmiş ve görevli personelin acil durum sorumluluklarını yerine getirip getiremedikleri, acil durum plan ve prosedürlerinin işleyip işlemediği ve sistemin kaç dakika içerisinde tekrar işler duruma getirilebildiği ölçülmüştür. Böyle bir durumda veri kaybı yaşanıp yaşanmadığı, hastaların ve personelin olaydan etkilenme durumu ile kurumun kesintiden kaynaklanabilecek ekonomik kayıpları incelenmiştir. Elde edilen bulgular tartışmaya açılmış ve "Yönetimin Gözden Geçirme Prosedürü" kapsamında gerekli görülen iyileştirme ve güncellemeler yapılarak eldeki imkanlarla mümkün olan en iyi seviyeye ulaşılmaya çalışılmıştır.

Kurumsal Bilgi Güvenliği Hafızasının Oluşturulması

Hastane bilgi kaynaklarından herhangi birinde yaşanan bilgi güvenliği olayı çözüme kavuşturulduktan sonra elde edilen bilginin kurumsal bilgi birikimine dönüştürülebilmesi amacıyla; bilgi güvenliği olaylarının türlerinin, hangi bilgi kaynaklarını etkilediğinin, yaşanma sıklığının ve neden olduğu hasarın ölçülüp izlenmesini sağlayan "Olay Raporlama Prosedürü", ilgili birimlerin bilgi güvenliği sorumlusu tarafından hastane BGYS yöneticisi gözetiminde işletilmiştir. Böylelikle, hastanede, bilgi güvenliği zafiyetlerinin kayıt altına alınabileceği bir sistem kurularak bilgi-beceri havuzu oluşturulmuştur.

Hastanede yaşanan bilgi güvenliği olaylarından oluşan bu tecrübe birikiminin kuruma üç önemli faydası olmuştur. Birincisi, aynı zafiyet farklı bir sistemde de raporlandığında buradaki bilgi ve tecrübeler kullanılarak hızlı ve etkin şekilde faaliyete geçilebilmiştir. İkincisi, bilgi işlem çalışanları, sistem sorumluları veya hastane BGYS yöneticilerinin kurumdan ayrılmaları durumunda yeni göreve başlayan personeller kurumsal bilgi güvenliği hafızasına kayıpsız şekilde

erişebilme imkanı bulmuşlardır. Üçüncüsü, bilgi güvenliği olaylarına dair kurumsal belleğin bulunması çalışanların risk farkındalığının sürekli yüksek tutulabilmesini sağlamış ve olayların ve zararların tekrarlamasını büyük ölçüde engellemiştir. Hastanedeki bilgi kaynaklarına yönelik güvenlik açığı takip listesini kendi kendine oluşturan bu bilgi güvenliği olayları havuzu, bulguların bir plan dahilinde ve kontrollü şekilde giderilmesini sağlamış ve risk yönetimi noktasında kuruma öngörülebilirlik avantajı sağlamıştır.

Bilgi Kaynaklarına Karşı Risklerin Yönetimi

Kurumda oluşturulan bilgi-beceri havuzu "Risk Yönetimi ve Değerlendirilmesi" prosedürünün önemli bileşenlerinden bir tanesidir. Havuzdaki bulguların risk seviyelerini değerlendirirken ilgili bilgi kaynağının önem derecesi de göz önüne alınmış ve iyileştirme planları yüksek, orta ve düşük seviyeli bulgulara göre sınıflandırma yapılarak oluşturulmuştur. Hastanenin bilgi güvenliği politikasına göre; yüksek seviyeli bulguların 5 gün içerisinde, orta seviyeli bulguların 15 gün içerisinde, düşük seviyeli olanların ise en fazla 60 gün içerisinde giderilmesi gerekmektedir.

Sistem dahilinde oluşturulan bilgi güvenliği politika ve prosedürlerinin işletilmesine, risk ve tehditlerin önceden belirlenme çabalarına, alınan önleyici faaliyetlere ve iyileştirme çalışmalarına rağmen, herhangi bir bilgi kaynağına yönelik aktif tehdit veya sistem kesintisi olma ihtimaline karşı, hastane çalışanlarının acil durum sorumlulukları ve görevleri açıkça belirlenmiştir. Özellikle sağlık hizmetlerini etkileyebileceği ve süreçlerde kesintiye sebep olabileceği öngörülebilen tüm durumlar için, bilgi işlem merkezi personelinin de dahil olduğu, birim ve bilgi kaynağı temelinde "acil durumlarda yapılacaklar listesi" hazırlanmış ve eğitimlerde bu konuya özellikle vurgu yapılmıştır.

BGYS Denetimleri

Hastanede kurulan bilgi yönetim sisteminin hedeflenen standartlarda çalışıp çalışmadığının tespiti için yapılan anlaşmalarla sistem, her yıl, en az biri üniversite olmak üzere iki bağımsız kurumun denetimine açılmıştır. Özellikle, hastane personelinin bilgi güvenliği noktasındaki bilinç seviyesi ve politika ve süreçlerin bilinip bilinmediği, hastane ağının ve elektronik sistemlerinin içeriden ve dışarıdan gelebilecek saldırı ve tehditlere karşı ne kadar güvende olduğu, tehdit algılama ve önleme sistemlerinin etkinliği, bilgi kaynaklarının risk analizleriyle uyumlu şekilde korunup korunmadığı, bilgi erişimi, güncellenmesi ve imhası noktasında prosedürlere uyulup uyulmadığı gibi bilgiyi ve bilgi kaynaklarını ilgilendiren her konuda hastanenin bilgi yönetim sistemi denetlenmiş ve sunulan raporlar ışığında; tespit edilen açıklar kapatılmaya, ilgili prosedür süreçleri iyileştirilmeye, gerekli durumlarda ise ek güvenlik yatırımlarıyla sistemin etkinliği yükseltilmeye çalışılmıştır.

Hastaneye bilgi güvenliği yönetim sistemi entegre edilmeye başlandığı yıl bağımsız kuruluşlara yaptırılan bilgi güvenliği testlerinde birçoğu port güvenliği zafiyeti olmak üzere çok sayıda güvenlik açığı tespit edilmiştir. Bu açıklıklar kapatılmasına rağmen, sonraki yıllarda yapılan denetimlerde, toplam güvenlik açığı sayısı azalmakla beraber, hastanenin firewall, ağ anahtarı veya sunucularında yeni açıklıklar tespit edilmiştir. Bu durum, bilgi güvenliği yönetiminin dinamik ve sürekli devam etmesi gereken bir süreç olması gerektiğini göstermektedir. Bu noktada dikkat çeken iki önemli husus bulunmaktadır. İlk olarak, insanoğlunun doğası gereği kendi kurduğu sistemdeki açıklıkları ve eksiklikleri tespit etmesi dışarıdan bakan bir kişiye göre çok daha zor olmaktadır ki; sistemin dışarıdan profesyonellerce düzenli olarak test edilmesi, fark edilemeyen eksiklikleri ve zayıflıkları ortaya çıkartması bakımından büyük önem taşımaktadır. İkinci olarak, her yıl yapılan güvenlik testlerinde sistemin farklı yerlerinde farklı açıkların tespiti teknolojinin ve bilimin hızlı ilerleyişi karşısında sistemlerin güncel, etkin ve güvenli tutulmasının ne kadar zor olduğunu ortaya koymaktadır ki; şu anda en güvenilen sistemler bile kısa zaman sonra, önceden hiç bilinmeyen güvenlik riskleri ile karşı karşıya kalabilmektedirler.

Yasal Mevzuata Uyum

Ülkemizde *t*emel bilgi güvenliği esasları, 23 Mayıs 2007 tarihli resmi gazetede yayımlanan "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ile yasal olarak ilk defa uygulamaya girmiştir (Resmi Gazete, 2007). Günümüzdeki mevcut düzenlemeyi yapan 28363 sayılı "Elektronik

Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik" 'e göre; kurumlar sakladıkları verilerin, istem dışı, yetki dışı ya da yasa dışı, erişim, tahrip, kayıp, değişiklik, depolama, işleme ve ifşasına karşı uygun teknik ve idari tedbirlerin alınmasından sorumludurlar. İlgili yönetmeliğe göre kurumlar ayrıca; verilerin sadece özel yetkilendirilmiş kişiler tarafından erişilebilir olmasının sağlanması için uygun teknik ve idari tedbirlerin alınması, işlenen ve saklanan verinin, saklama süresinin bitiminden itibaren en geç bir ay içinde imha edilmesini veya anonim hale getirilmesini ve bu işlemlerin tutanakla veya sistemsel olarak kayıt altına alınmasını sağlamak zorundadırlar (Resmi Gazete, 2012).

Yönetmelik, eğer kurum internet vb. hizmetlerin sağlayıcılığını da yapmış oluyorsa tüm erişim kayıtlarının en az bir yıl süreyle saklanmasını gerekli kılmaktadır. Birçok kurumu yasal mesuliyet altına alan bu yönetmelik doğrultusunda, hastane bilişim ve güvenlik altyapısı, özellikle internet ve dış ağ erişim kayıtlarını en az bir yıl süreyle tutabilecek biçimde şekillendirilmiş ve ilgili bilgi güvenliği prosedürleri kanun ve yönetmeliklerdeki değişimlere göre sürekli güncellenmiştir.

Yasal mevzuatta bilişim suçu olarak tanınan fiillerin tespit edilerek ilgili mercilere bildirilmesi için kurum avukatlarıyla ile temas halinde olunmuştur. Ayrıca ilgili kanun gereği bilgi güvenliğinin sağlanması ve internet erişimi gibi noktalarda kurumun üzerine düşen yasal sorumluluklar hukuk danışmanlarının yönlendirmeleri ile belirlenmiş ve kurumun bilgi güvenliği politikalarına yerleştirilmiştir. Hastane bilgi güvenliği yönetim sistemi kapsamına giren ürün ve hizmetleri sağlayan tedarikçilerle yapılan gizlilik anlaşmaları, hastaneyi denetleyen kurumlar ile ilgili hukuksal ilişkiler ve çalışanlarla imzalanan bilgi güvenliği sözleşmeleri hastane hukuk danışmanlarının da dahil olduğu bir ekip tarafından hazırlanmıştır.

Bilgi Güvenliği Yönetimi Sürecinde Erişim Esnekliğinin Oluşturulması ve Kısıtlılıkların Azaltılması

Hastanede bilgi güvenliğini yönetmek amacıyla kurulan sistemin personelin desteğini alabilmesi ve pozitif bir bilgi güvenliği kültürü oluşturulabilmesi için; çalışanların bilgiye ve teknolojiye ulaşmalarını zorlaştırabilecek engeller ve kısıtlılıklar mümkün olduğunca azaltılmaya ve güvenlik ile kullanılabilirlik arasındaki hassas denge korunmaya çalışılmıştır.

Kurum çalışanlarının gerektiği zaman hastane içerisindeki tüm servislerde bulunan tüm bilgisayarları kullanabilmelerini sağlamak amacıyla "aktif erişim desteği" adı verilen ve her çalışanın kendisine özel kullanıcı adı ve şifresiyle bilgisayarlarda oturum açmasına olanak veren sistem kurulmuştur. Hangi bilgisayarda oturum açtıkları fark etmeksizin, kullanıcılar kendilerine tanınan yetkilendirme bazında işlem yapabilmektedirler. Benzer süreç ve yetkilendirme Hastane Bilgi Yönetim Sistemi (HBYS) ve diğer bilgi kaynaklarına erişim için de geçerlidir.

Hastane bilgi kaynaklarının güvenliği sağlanırken, çalışanlara erişim özgürlüğü sağlanmaya çalışılmış, bilgiye erişim özgürlükleri hiçbir şekilde kısıtlanmadan, teknolojiden mümkün olan en fazla katkının alınabileceği, kullanıcı dostu, esnek ve çevik sistemler tercih edilmiştir. Bu noktada örnek olarak; bir doktorun, tablet veya akıllı telefonunu kullanarak, poliklinik veya serviste iken, hastane bahçesinde dinlenirken veya yemekhanedeyken hastanenin neredeyse tamamına döşenmiş kablosuz ağ cihazlarından kendisine en yakın noktada olanına otomatik olarak bağlanarak HBYS' ne ulaşıp, istediği medikal veriye veya radyoloji görüntülerine erişebilme, istem yapabilme, rapor yazabilme, okuyabilme veya internete güvenli bir şekilde girebilme olanağına sahip olması verilebilir. Diğer bir örnek ise; özellikle mesai dışı saatlerde ve bilhassa acil servislerde radyoloji uzmanlarına oluşan ani ihtiyaç göz önüne alınarak, belli protokoller çerçevesinde radyoloji uzmanlarına evlerinden HBYS'ne bağlanarak radyolojik tetkikleri değerlendirme ve raporlarını HBYS üzerinden yazma olanağı sağlanmasıdır.

Hastane yönetimi, bir taraftan çalışanlara dijital erişim özgürlüğü tanırken diğer taraftan da bilgi kaynaklarına erişim yetkilerini düzenleyerek, bilginin bütünlüğünü ve doğruluğunu sürekli koruyarak ve hastane içerisinde kullanılan tüm sistemlerin kesintisiz ve hızlı şekilde hizmet vermesini sağlayarak bilhassa çok yoğun iş yükleri olduğunu ve zaman baskısı altında kaldıklarını belirterek elektronik sistemleri kullanmayan, eski usül sistemleri kullanırken de bilginin doğruluğundan, güncelliğinden ve güvenliğinden emin olamayan doktor, asistan ve hemşirelerin tüm medikal ve idari bilgiye elektronik sistemleri kullanarak ulaşmasını sağlayabilmiştir.

Sonuç ve Tartışma

Aşağıdaki tablo, hastanenin elektronik bilgi kaynaklarına yönelik oluşan yıllık tehdit sayılarını, tehditlerin oluşumundaki süreci başlatan hatanın temelde nereden kaynaklandığını ve tehditlerin sitemlerin çalışmasını ne ölçüde kesintiye uğrattığını göstermektedir. Tabloda görülen majör tehdit, bilgi kaynaklarına yönelik beklenmeyen, ciddi sonuçlar doğurabilecek ve genellikle sistemleri ve süreçleri kesintiye uğratan tehditlerdir. Minör tehditler ise, risk planlamasına dahil edilmiş, dolayısıyla öngörülebilen ancak yine de oluşması engellenememiş, bununla birlikte, bilgi kaynaklarına ve süreçlerine çok fazla zarar vermesi beklenmeyen tehditlerdir.

Tablo 6. Bilgi Güvenliği Yönetim Sistemi Kurulmadan Önce ve Sonra Bilgi Kaynaklarına Yönelik Yıllık Ortalama Tehdit Sayıları, Hata Kaynakları ve Sistemlerin Kesintisiz Çalışma Oranları

Olgu	Majör Tehdit	Minör Tehdit	Ortaya Çıkma Nedeni		Bilgi Sistemlerinde Yıllık Ortalama Kesintisiz Çalışma Oranı
			İnsan Hatası	Sistem Hatası	
BGS kurulumu öncesi	13	87	%72	%28	%94
BGS kurulumu sonrası (1. Yıl)	6	35	%54	%46	%97
BGS kurulumu sonrası (2. Yıl)	2	18	%40	%60	%99
BGS kurulumu sonrası (3. Yıl)	-	5	%40	%60	%99,9

Hastaneye bilgi güvenliği yönetim sistemi entegre edilmeden önceki son yıl, bilgi kaynaklarına karşı belirlenebilen 13 majör tehdit, elektronik bilgi sistemlerini yıllık %6 gibi bir oranda kesintiye uğratmıştır. Bu rakamın, yoğun çalışmayı gerektiren ve kaybedilen her dakikanın çok önemli olduğu sağlık hizmetleri açısından kabul edilemez olduğu görülmektedir. Hastane bilgi sistemlerinde yıl içinde bu seviyede bir kesinti, çalışanların ve hastaların kuruma olan güvenlerini zedeleyebilecek, sağlık hizmetlerinde aksamaya sebep olabilecek, iş ve süreçlerde düzensizlik ve veri kaybı oluşturabilecek bir potansiyele sahiptir.

Hastanede, sistem kurulumu öncesi oluşan tehditlerin %72'sinin insan kaynaklı olduğu tespit edilmiştir ki; çalışanların bilgi güvenliğine dair henüz eğitim almadıkları, yeterli bilgiye sahip olmadıkları ve kurumsal bilgi güvenliği kültürünün henüz oluşmadığı gözönüne alındığında beklenen bir oran olduğu söylenebilir. Üç yıl süren düzenli bilgi güvenliği eğitimlerinden sonra, hastane bilgi kaynaklarına yönelik toplam tehdit sayısı büyük oranda (%95) azalmış ve insan hatası kaynaklı tehditlerin oranı %40 seviyesine düşmüştür.

Hastanede bilgi güvenliği yönetim sisteminin kurulumunu takip eden iki yıl içerisinde elektronik bilgi sistemlerindeki kesinti oranı %1'e gerilemiş ve üçüncü yılın sonu itibariyle hastane bilgi kaynaklarına yönelik hiçbir majör tehdit tespit edilmemiştir. Kullanıcı kaynaklı hataların oranının ve sayısının her yıl azalması ve elektronik bilgi sistemlerdeki %99,9'luk kesintisiz çalışma oranına ulaşılabilmiş olması; kurulan hastane bilgi güvenliği yönetim sisteminin bilgi kaynaklarına yönelik tehditleri oluşmadan engelleme hedefine büyük ölçüde ulaştığını, çalışanlara yönelik eğitimlerin sonuç verdiğini ve kurum çalışanlarının bilgi güvenliği bilinci ve kültürü noktasında ilerleme kaydettiğini göstermektedir.

Telefon ve elektronik posta gibi iletişim araçlarıyla, hastane web sayfası şikayet formu üzerinden ve hasta hakları birimi vasıtasıyla Bilgi İşlem Merkezi'ne iletilen hasta şikayetleri nicelik olarak incelendiğinde, bilgi güvenliği sisteminin kurulmasını takiben; sistem kesintileri, randevu sistemlerinin etkinliği, işlemlerin bitirilme süreleri, toplam bekleme süreleri vb. şikayet oranlarında %18'lik bir azalma olduğu, üç yılın sonunda ise toplamda %86'lık bir düşüş olduğu belirlenmiştir.

Hastane bilgi sistemlerinin güvenli, kesintisiz, işleri kolaylaştıran ve süreçleri hızlandıran bir yapı içerisinde hizmet vermesi ve bilgiye tam, doğru ve zamanında erişim kabiliyetinin getirdiği avantajların zamanla anlaşılması, sistemin tüm çalışanların desteğini almasını sağlamıştır. Kesintiler nedeniyle daha önce sıklıkla sisteme girilemeyen ve fatura edilemeyen kayıp-kaçak işlem sayılarındaki azalmanın da katkısıyla, kurumun yıllık toplam gelirleri, bilgi güvenliğinin hastane süreçlerine entegre edildiği yıl, bir önceki yıla göre %37, üç yıllık sürecin sonunda ise %67 artış göstermiştir.

Üç yıl süren bilgi güvenliği yönetim sistemi entegrasyon süreçleri ve elde edilen sonuçlardan görüldüğü gibi, kurumların bilgi güvenliğinin sağlanmasının yolu; yöneticilerin tam desteğini alan bir süreç başlatarak kurumsal bilgi güvenliği politikalarını oluşturmak, hedefleri belirlemek, hedefler ve politikalar doğrultusunda ilgili prosedür süreçlerini detaylandırmak ve amaçlara ulaşıncaya kadar izleme, iyileştirme, güncelleme ve denetleme çalışmalarını aynı kararlılıkla devam ettirmekten geçmektedir. Zincirleme süreçlerin geri besleme yoluyla otomatik kontrol yapabilmesi ve sistemin kurum çalışanlarını ve hatta müşterilerini de içine alması kritik önem taşımaktadır. Çalışanlara bilgi güvenliği yönetiminin teknik bir iş olmadığı, kurumun tüm birimlerinin ve çalışanlarının sorumluluk yüklenmesi gerektiği en etkili şekilde anlatılmalıdır. Kurumsal iş yoğunluğu ne seviyede olursa olsun, kurumsal bilgi güvenliği hedefleri yakalanıncaya kadar tüm personele bilgi güvenliği yönetimi noktasında gerekli eğitimler tekrar tekrar verilmeli ve kurumsal bilgi güvenliği kültürünün oluştuğundan emin olunmalıdır. Oluşan bu kültür, bilgi kaynaklarını ilgilendiren her süreç ve işlemde devreye girecek ve çalışanların öz denetim yapmalarını sağlayacaktır.

Kurumlarda bilgi kaynaklarına karşı oluşan tehditlerden meydana gelen maddi kayıpların ne kadar büyük olduğu gözönüne alındığında, bilgi güvenliğinin sağlanması için yapılan yatırımların boşa giden harcamalar şeklinde görülmemesi, aksine kurumun sırlarını ve önemli ticari verilerini koruyan, iş süreçlerinin kesintisiz devam edebilmesini garanti altına alan, yedekli çalışmayı sağlayarak yangın, deprem, diğer doğal afetler ve fiziksel ve mantıksal hırsızlıklar gibi tehditlere karşı bir sigorta yatırımı gibi algılanması, kurumsal bilgi güvenliği yönetimine bir başlangıç yapabilmek için önem arz etmektedir.

Çalışmamızın başında da belirttiğimiz gibi, ulusal bilgi güvenliğimizin sağlanması öncelikle örgütlerimizin kurumsal bilgi güvenliklerini sağlamaları ve vatandaşlarımızın bilinçlendirilmesi ile mümkündür. Bu noktada örgüt yöneticilerine büyük görev ve sorumluluklar düşmektedir. Yöneticilerin, faaliyetlerini devam ettirebilmek için kurumlarının finansal yapısına, üretim kapasitelerine ve rekabet güçlerine verdikleri önemi kurumsal bilgi güvenliklerine de vermeleri günümüzde bir zorunluluk haline gelmiştir ve ülkemizde de, yöneticilerin liderliğinde, bu yönde bir bilinçlenme ve bilinçlendirme atılımı yapılması ve mevcut çalışmalara ivme kazandırılması gerekmektedir.

Ülkemizde, 27730 sayılı "Elektronik Haberleşme Güvenliği Kapsamında TS ISO/IEC 27001 Standardı Uygulanmasına İlişkin Tebliğ" ile birlikte, hizmet özelliklerine göre bazı kurumlara bu bilgi güvenliği standartlarına uygunluk sağlama yükümlüğü bir kısmına ise uygunluk belgesi alma zorunluluğu olmaksızın standarda uygunluk sağlama yükümlülüğü getirilmiştir (Resmi Gazete, 2010). Ülkemizde, sağlık sektörü de dahil pek çok sektör henüz bu tebliğ kapsamına girmemekle birlikte, yakın gelecekte bilgi güvenliği yönetimi standartlarına uymanın kurumlar için yasal zorunluluk haline gelebileceği görülmektedir.

Kaynakça

Bartlett, C., Boehncke, K. & Haikerwal, M. (2008). E-health: Enabler for Australia's Health Reform. www.health.gov.au/nhhrc/publishing (18.02.2015).

Baykara, M., Daş, R. & Karadoğan, İ. (2013). Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi. 1st International Symposium on Digital Forensics and Security (ISDFS'13) Proceedings, http://isdfsweb.firat.edu.tr/Upload/ISDFS2013_Proceeding_Book.pdf

Canbek, G. & Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi, 9*(3), 165-174.

Cavalli, E., Mattasoglio, A., Pinciroli, F. vd. (2004). Information Security Concepts and Practices: The Case of a Provincial Multi-Specialty Hospital. *International Journal of Medical Informatics, 73*(3), 297-303.

CE (Certification Europe), (2008). ISO 27001 Global Survey: The Facts and The Figures Underlying The Growth of ISO 27001 World-Wide. http://www.d10736251.blacknight.com/format/ISO27001GlobalSurvey.pdf (08.02.2015).

Chen, R. & Hsiao, J. (2012). An Investigation On Physicians' Acceptance Of Hospital Information Systems: A Case Study. *International Journal of Medical Informatics, 8* (12), 810–820.

Eminağaoğlu, M. & Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir, Türkiye' de Bilgi Güvenliği Sorunları ve Çözüm Önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11*(4), 1-15.

Fernando, J. I. & Dawson, L. L. (2009). The Health Information System Security Threat Lifecycle: An Informatics Theory. *International Journal of Medical Informatics, 78*(12), 815–826.

He, Y., Johnson, C., Lu, Y. vd. (2014). Improving the Information Security Management: An Industrial Study in the Privacy of Electronic Patient Records. IEEE 27th International Symposium on Computer-Based Medical Systems, http://ieeexplore.ieee.org/Xplore/home.jsp (20.01.2015)

Holden, R. J. (2011). What Stands in the Way of Technology-Mediated Patient Safety Improvements? A Study of Facilitators and Barriers to Physicians' Use of Electronic Health Records. *Journal of Patient Safety, 7*(4), 193-203.

http://www.iso27001bilgiguvenligi.com/53-iso_27001_bilgi_guvenligi (Erişim: 02.02.2015).

https://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari (Erişim: 25.02.2015).

IMF (International Monetary Fund) (2014). International Financial Statistics (IFS). http://www.imf.org, (24.05.2015).

ISO (International Organization for Standardization) (2013). The ISO Survey of Management System Standard Certifications. http://www.iso.org/iso/iso-survey (19.01.2015).

Khalifa, M. (2013). Barriers to Health Information Systems and Electronic Medical Records Implementation. Procedia Computer Science, 21, 35 – 342.

Medlin, D. B. & Cazier, J. A. (2007). An Empirical Investigation: Healthcare Employee Passwords And Their Crack Times In Relationship To HIPAA Security Standards. *International Journal of Health Care Informatics, 2*(3), 39–48.

NEHTA (National E-Health Transition Authority) (2007). Privacy Blueprint on Unique Healthcare Identifiers. www.nehta.gov.au (08.05.2015).

Pagliari, C., Donnan, P., Morrison, J. vd. (2005). Adoption And Perception Of Electronic Clinical Communications In Scotland. I*nformatics in Primary Care, 13* (2), 97-104.

PWC (2015). Managing Cyber Risks In An Interconnected World: Key findings from The Global State of Information Security Survey. http://www.pwc.com/gx/en/consulting-services/information-security-survey (07.04.2015).

Resmi Gazete (2007). İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Sayı 26530.

Resmi Gazete (2010). Elektronik Haberleşme Güvenliği Kapsaminda TS ISO/IEC 27001 Standardı Uygulanmasına İlişkin Tebliğ, Sayı 27730.

Resmi Gazete (2012). Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik, Sayı 28363.

Sağsan, M. (2007). Uygulamadan Disipline Bilgi Yönetimi Ve Bir Alan Çalışması. Amme İdaresi Dergisi, 40 (4), 103-131.

Şahin, A. (2008). Kamu kurumlarında bilgi Teknolojilerinin Kullanımında Yaşanan Sorunlar: Konya Kaymakamlıkları Örneği. *Amme İdaresi Dergisi, 41*(1), 149-171.

Sultan, F., Aziz, M. T., Khokhar, I. vd. (2014). Development Of An In-House Hospital Information System In A Hospital In Pakistan. *International Journal of Medical Informatics, 83*(3), 180–188.

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. *KSÜ Fen ve Mühendislik Dergisi, 11*(1), 132-137.

Timmons, S. (2003). Nurses Resisting Information Technology. *Nursing Inquiry, 10*(4), 257–269.

USGT (Ulusal Siber Güvenlik Tatbikatı Sonuç Raporu), 2011. Bilgi Teknolojileri Kurumu ve TÜBİTAK.

Vural, Y. & Sağıroğlu, Ş. (2007). Kurumsal Bilgi Güvenliği: Güncel Gelişmeler. ISO Turkey, Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı, 13-14 Aralık, Ankara, Türkiye.

Wakefield, D. S., Halbesleben, J. R., Ward, Marcia M. vd. (2007). Development Of A Measure Of Clinical Information Systems Expectations And Experiences. *Medical Care, 45*(9), 884–890.

Williams, P. (2008). When Trust Defies Commons Sense. *Health Informatics Journal, 14*(3), 211–221.