HUKUK BÜROLARINDA BİLGİ GÜVENLİĞİNİN ARTTIRILMASINDA MODEL ÖNERİLERİ

MODEL SUGGESTIONS FOR INCREASING INFORMATION SECURITY IN LAW OFFICES

Berker KILIÇ*
Nursel YALÇIN**
Esra KILIÇ***

Özet: Bu çalışmada hukuk bürolarında İnsan Kaynakları, Bilişim Teknolojileri ve İletişim özellikleri ile ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri (BGYS) kontrolleri arasındaki ilişkilerin incelenmesi sonucunda, Hukuk Bürolarında Bilgi Güvenliği düzeyleri, 0-100 arasında Bilgi Güvenliği Yönetim Sistemi Puanı (BGYSP) adı verilen bir değerlendirme puanına dönüştürülmüştür.

Elde edilen verilere dayalı olarak hukuk büroları için Güçlendirici Model ve Tamamlayıcı Model ismi verilen iki model önerisi geliştirilmiştir.

Güçlendirici Model, hukuk bürolarının ISO/IEC 27001 BGYS amaçları içerisinde yeterli oldukları alanlarda, Tamamlayıcı Model ise yetersiz oldukları alanlarda alınacak aksiyonlarla hukuk bürosunun BGYSP puanlarının arttırılmasını önceliklemektedir.

Anahtar Kelimeler: Bilgi Güvenliği, Hukuk Bürosu, ISO 27001

Abstract: In this study, as a result of examining the relationship between Human Resources, Information Technologies and Communication features and ISO/IEC 27001 Information Security Management Systems (ISMS) controls in law offices, Information Security levels in Law Offices are called Information Security Management System Points (ISMSP). It has been converted to evaluation score.

Based on the data obtained, two model proposals, namely Empowering Model and Complementary Model, were developed for law offices.

The Empowering Model prioritizes the increase of the ISMSP scores of the law firm with the actions to be taken in areas where the law offices are sufficient for the purposes of ISO/IEC 27001 ISMS, and the Complementary Model in the areas where they are insufficient.

Keywords: Information Security, Law Office, ISO 27001

* Adli Bilişim Uzmanı, berker.kilic@gmail.com, ORCID: 0000-0001-8751-8192

** Yrd. Doç. Dr., Gazi Üniversitesi Gazi Eğitim Fakültesi, nyalcin@gazi.edu.tr, ORCID: 0000-0002-0393-6408

*** Bilişim Teknolojileri Öğretmeni, esracaya_5281@hotmail.com, ORCID: 0000-0003-3009-9462, Makalenin Gönderim Tarihi: 13.07.2020, Kabul Tarihi: 13.07.2020

1. GİRİŞ

Bilgi güvenliği, bilgi alanındaki nesnenin (bilginin kendisi ve bulunabileceği tüm ortamlar) korunması, toplanması, oluşturulması, işlenmesi, bilginin dağıtılması ve kullanılması ve ayrıca ortaya çıkan sosyal ilişkilerin düzenlenmesine ilişkin geniş çaplı tehditlere karşı korunması olarak anlaşılır.

Günümüzde ticari işletmeler, kamu kurumları, her türde organizasyon kısaca kişisel verilerle çalışan bütün kuruluşlar, kritik bilgilerinin manipülasyonu ve çalınması gibi çeşitli iç ve dış güvenlik tehditlerine maruz kalmaktadır. Olası bir iç veya dış müdahaleye ek olarak, doğal felaketler veya bilgisayar kullanıcılarının kasıtsız hataları da sonuçları itibariyle birer tehdit olarak ele alınmaktadır.

Kuruluşlar, bilgi varlıklarını korumak ve büyük para kayıplarını önlemek için bilgi güvenliğine giderek daha fazla yatırım yapmaktadırlar.[1] Ancak güvenlik ihlallerinin de sayısı artmaya devam etmektedir.[2] Çoğu kuruluş, teknik bilgi güvenliği önlemleri olarak sadece saldırı ve izinsiz giriş tespit sistemleri kullanmaktadır.[3] Ancak bazı kuruluşlar da, veri alışverişi yaparak, bilgiyi paylaşarak ya da dış kaynak kullanımı ile diğer sistemlerle, insanlarla ve kuruluşlarla etkileşime girdikleri bir sistem içerisinde çalışıyor olabilirler.[4] Bu gibi durumlarda da, bilgilerin gereğinden fazla miktarda detay içerecek şekilde paylaşılması durumu ortaya çıkarak, bilgilerin gizliliği ve özel verilerin bütünlüğünü bozabilir veya paylaşım güvenilmeyen üçüncü taraflarla yapılmış olabilir.

Kişilerin kimliğini belirleyen kişisel verilerine ek olarak, kritik bilgilerinden birisi de kişilerin suç ve suça ilişkin hukuki bilgileridir. Hukuk alanında kişiyi vekaleten temsil eden avukatlar, kişinin bu kapsamdaki her türlü bilgisine sahiptirler. Bu temsil ile avukatın, kişinin

---

1 HM Goverment, 2015 Information Security Breaches Survey, HM Raporu, Londra, İngiltere, 2015.

2 PWC, Turnaround and Transformation in Cybersecurity, PWC Raporu, Londra, İngiltere, 2016.

3 Ernst&Young, Into the Cloud, Out of the Fog: Ernst & Young' s 2011 Global Information Security Survey, Ernst&Young Raporu, Londra, İngiltere, 2011.

4 Elda Paja, Fabiano Dalpiaz ve Paolo Giorgini, "Modelling and Reasoning About Security Requirements in Socio-Technical Systems", 24th International Conference on Advanced Information Systems Engineering (CAiSE), 2015, 855(1).

suçuna yahut mağduriyetine ilişkin sahip olduğu kişisel bilgilerini koruması önemlidir. Kişisel Verilerin Korunması Kanunu (KVKK), Avukatlık Kanunu ve ilgili diğer kanunlarının bu doğrultuda maddeleri mevcuttur. KVKK açısından avukat, müvekkilinin kişisel bilgilerini koruma yükümlülüğü bakımından veri sorumlusudur.

ISO/IEC 27002, ISO/IEC tarafından yayımlanan bir standarttır. ISO/IEC 27002, ISO/IEC 27K paketinin bir parçasıdır ve bilgi güvenliği gereksinimlerini içeren standarttır, ISO/IEC 27002 ise standardın uygulanmasına rehberlik eden uygulama kodudur.[5]

Bu çalışmada, "ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Açısından Türkiye' de Hukuk Bürolarında Bilgi Güvenliği Yönetimi" başlıklı yüksek lisans tezi[6] için hazırlanan ISO/IEC 27001 BGYS öz değerlendirme anketi kullanılmıştır. Öz değerlendirme anketi ile elde edilen bilgilerden hukuk bürolarının, İnsan Kaynakları, Bilişim Teknolojileri Ekipman (BTE) ve Bilişim Teknolojileri İletişim (BTİ) özellikleri ile ISO/IEC 27001 BGYS alt amaçları arasında bir ilişki olup olmadığı araştırılmış ve öz değerlendirme sonucu hukuk bürolarına özel bilgi güvenliği yeterliliklerine bağlı bir bilgi güvenliği modelinin optimum gereksinimleri ölçülmüştür.

Ankette ISO/IEC 27001 BGYS içerisinde yer alan 14 Amaç, 35 Alt Amaç ve 113 kontrol için 294 anket maddesi hazırlanmıştır.

Bilgi günümüzde değeri olan bir nesneye yani metaya dönüşmüştür. Bu nedenle, bilginin artık bir veri bütününden ziyade, alınabilir, satılabilir bir nesneye dönüşmüş olması bilgi güvenliği gereksinimini de artırmıştır.

Hukuk büroları açısından bakıldığında, müvekkillerine ait soruşturma yahut kovuşturmaya dahil olan bilgiler yani bir dosya bütünü hem fiziksel hem de elektronik ortamda bir değerdir. Bu değer müvekkil açısından imaj ve itibar olarak değerlendirilebileceği gibi, avukat

---

5 Malik Motii ve Elalami Semma, "Towards a New Approach to Pooling COBIT 5 and ITIL V3 with ISO IEC 27002 for Better Use of ITG in the Morrocan Parliament", *IJCSI International Journal of Computer Science Issues*, 2017, 14(3), 49-58.

6 Berker Kılıç, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Açısından Türkiye' de Hukuk Bürolarında Bilgi Güvenliği Yönetimi, Yüksek Lisans Tezi, Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim Anabilim Dalı, Ankara, Türkiye, Aralık-2019.

açısından da işlediği ve geliştirdiği ekonomik değeri olan anlamlı bir veri bütünüdür. Yani nesnel bir değeri vardır.

Hukuk bürolarının bilgi güvenliği gereksinimi, her ne kadar az sayıda çalışan ve ekipmana sahip yapılar olması nedeni ile kapsamlı ve maliyetli bir şekilde değerlendirmeye uygun olmasa da işlenen verilerin kritik önemi, iş sürekliliği gereksinimi ve iş kapasitesine bağlı iş verimliliği gereksinimleri açısından değerlendirildiğinde, yönetilmesi gereken bir seviyededir.

2. KAVRAMSAL ÇERÇEVE

Bilginin kullanımı ve paylaşılması, bilgiye sahip insanlar arasında iletişimi gerektirir. Günümüzde bilgi paylaşımını destekleyecek çok sayıda teknik araç vardır. Bunlar arasında, coğrafi olarak birbirlerinden ayrı olan insanlar arasındaki yüz yüze iletişimi taklit etmek için tasarlanmış farklı bilgi sistemleri ve sosyal medya araçları vardır. Ayrıca bilgi, tekrar kullanılabilmek ve paylaşılabilmek için bir taraftan da depolanmaktadır. Bilgiye bağlı riskleri tanımlamanın ve yönetmenin sistematik bir yolu, bilginin birleşik bir korunma düzeyi oluşturulmasına yardımcı olacaktır. Ancak araştırmalar bunun en azından yaygın olarak bulunmadığını göstermektedir.[7]

Bilginin aşağıdaki gibi birçok tanımı vardır:[8]

- Bilgi birisi hakkındadır veya bir şey onlar hakkında gerçeklerden oluşur.
- Girdi verilerinin bir programla işlenmesi yoluyla bir bilgisayardan çıktı olarak önemli veya faydalı bilgiler elde edilebilir.
- Bilgi, bir kuruluş için değerli olan ve dolayısıyla uygun şekilde korunması gereken diğer önemli ticari varlıklar gibi bir varlıktır.
- Bilgi birçok biçimde olabilir. Kâğıda basılabilir veya yazılabilir, elektronik olarak saklanabilir, posta yoluyla iletilebilir veya elekt-

---

7 Atif Ahmad, Rachelle Bosua ve Rens Scheepers, "Protecting Organizational Competitive Advantage: A Knowledge Leakage Perspective", Computers & Security, 2014, 42(1), 27-39.

8 Firkhan Ali Bin Hamid Ali ve Mohd Zalisham Jali, "Human-Technology Centric In Cyber Security Maintenance for Digital Transformation ERA", 1st International Conference on Big Data and Cloud Computing (ICoBiC), 2017.

ronik araçlar kullanılarak, filmlerde gösterilir veya görüşme sırasında konuşulabilir.

- Kişisel verinin tanımlanmış veya tanımlanabilir bir birey hakkında herhangi bir bilgi olduğu kabul edilir.[9] Tanımlanabilirlik kimliği doğrudan veya dolaylı olarak belirlenebilen herhangi bir kişi anlamına gelmektedir.
- El ile veya otomatik olarak kişisel verilerin toplanması, depolanması ve işlenmesi izni, sahiplerinin mahremiyet alanına girer ve bu nede nlebu işlemlerden sorumlu kuruluşların, onları korumak için yasalarca zorunlu tutulması gerekir.[10]

Bu hali ile kişisel veri belirli bir kişiyi gösterebilmesi ve nesnel ve işlenebilir olması nedeni ile meta bir bilgi olarak adlandırılabilmektedir.

3. BİLGİ GÜVENLİĞİ YAPISI

Kurumsal bir bilgi güvenliği yapısı kurmak için aşağıdaki adımlar izlenebilir.[11] Bu adımlar hukuk büroları gibi, küçük bir işletme olarak görülebilecek yapılar için de geçerlidir.

Hazırlık: İlgili iş ortakları da gözetilerek, veriler hazırlanır ve tespit edilen sorunlar da bu aşamaya dahil edilir.

Veri toplama ve analizi: Mevcut yapılar, kaynaklar, ilgili çalışanlar ve tesislerin bir envanterini içerir. Toplanan veriler, potansiyel zayıflıkları bulmak için uygun bir risk değerlendirme ile analiz edilir.

İş süreci geliştirme: Analiz sonucu elde edilen girdilerle yeni süreçler yaratılır. Risklerin süreçlerle birlikte nasıl yönetilebileceği ve iş süreçlerinin mümkün olduğu kadar etkili ve uygulanabilir tutulması düşünülür.

---

9 European Union (EU), Directive 95/46/EC, General Data Protection Regulation, 2016.

10 Santiago Martín-Romo Romero ve Carmen De-Pablos-Heredero, "Data Protection by Design: Organizational Integration", Harvard Deusto Business Research, 2016, 7(2), 60-71.

11 Christine Große, Towards an Integrated Framework for Quality and Information Security Management in Small Companies, Yüksek Lisans Tezi, Lulea Teknoloji Üniversitesi, Bilgisayar Bilimi Bölümü, Elektrik ve Uzay Mühendisliği, Lulea, İsveç, 2016.

Anlayış ve planlama: Uygun bir anlayış tanımını ve yaklaşan faaliyetlerin planlanmasını içerir. Bilgi güvenliği önlemleriyle mevcut iş süreçlerinin bir araya getirilir.

Uygulama: Önemli olan, çalışanların bu konuda bilinçli ve eğitilmiş olmasıdır. Çalışanların riskten kaçınma ve riskin gerçekleşmesi durumunda uymaları gereken prosedürler kendilerine anlatılmış ve gerekli ise riskin sonuçları konusunda sorumlulukları belirlenmiş olmalıdır.

İzleme ve bakım: Sürecin uygulanması sırasında, yapılan ölçümlerle süreç sürekli izlenir ve karar verilen kalite ve bilgi güvenliği düzeyi korunur. Tekrarlanan riskler belirlenerek ek güvenlik tedbirlerinin alınması amacıyla ek eylemler gerçekleştirilebilir.

Harici sertifika: Zorunlu olmasa da kurumun güvenlik yönetim süreçlerini bir sertifikasyon aracılığı ile tescil edebilmesi mümkündür.

Bilgi güvenliği, kendisini bilimsel bir araştırmaya hazırlayan net bir şekilde ayrılmış akademik çalışma alanı değildir. Aksine, bilgi güvenliği, teknikten davranışsal ve kültüre kadar çok sayıda disiplini birleştirmektedir.[12] Teknolojiye ek olarak, bilgi güvenliği ayrıca insanların veriye ve işlemlere erişiminin olduğu anlamına da gelmektedir. Erişim yetkili veya yetkisiz olabilir. Tehditler ayrıca kuruluşların içinden, ayrıcalıklı kullanıcılardan veya son kullanıcılardan gelebilmektedir. Siber saldırganların temel amaçları manipüle, tahrip, bozma ve çalmaktır.[13]

Fayda-maliyet analizi ve bilgi güvenliği maliyet değerlendirmesinin yapılması, kuruluşların ne kadar etkili tedbirler alacağını ve kuruluşun, alınan tedbirlerin işe yaramaması durumunda kayıplarını nasıl azaltacağını belirlemede yardımcı olmaktadır. Fayda-maliyet analizinin amacı, bilgi güvenliği için harcanan maliyetlerin, sağlanması beklenen faydadan daha düşük olmasını sağlamaktır. Bilgi güvenliği, kuruluşların doğrudan kar etmesini sağlayan bir faaliyet değildir. Ancak, bilgi güvenliği maliyetinin göz ardı edilmesi durumunda orta-

12 European Union (EU), European Cybersecurity Centres of Expertise Map: Definition and Taxonomy, Publications Office of the European Union, Lüxemburg, 2018.

13 Petac Eugen ve Duma Petruţ, "Exploring the New Era of Cybersecurity Governance", Ovidius University Annals, Economic Sciences Series, 2018, 18(1), 358-363.

ya çıkabilecek potansiyel zarardan kaçınılmasının sağlayacağı fayda değerlendirmektedir.

Çoğu kuruluş kritik ve hassas bilgilere sahiptir. Kuruluşlar ne kadar düzenli çalışırlarsa çalışsınlar, operasyonlarını tehlikeye atan, hatta kesintiye uğramasına neden olan, önemli verilerinin kaybına veya çalınmasına neden olan olaylarla karşılaşmaları muhtemeldir. Çoğu durumda, bu olaylar kuruluşun maddi kayıplarına veya itibarlarının kaybına neden olabilmektedir. Benzer şekilde, vatandaşlar da zaman zaman çevrimiçi dolandırıcılık veya kişisel kimlik hırsızlığı gibi durumlarla ilgili olaylar yaşamaktadır. Bu nedenle, kilit bir varlık olarak bilgi, ortaya çıkan tehditlerden korunmalıdır.[14]

Birçok ülkede, mevzuat ve yönetmelikler bilgi güvenliği konusunda kuruluşları cezai olarak sorumlu kılmakta ve bazı durumlarda uygun risk kontrol ve bilgi güvenliği önlemlerini uygulamaları ve sürdürmeleri konusunda başarısız olmaları durumunda hesap verebilir olmalarını istemektedir.[15] Bilgi güvenliği riski ölçüm sistemlerinin etkililiği de önemli bir konudur.[16] [17] ISO/IEC 27001, BGYS' i sağlamak, yönetmek ve geliştirme ihtiyacını belirten uluslararası bir standarttır ayrıca bilgi güvenliği kontrolünde ve ölçümünde de referans olarak kullanılmaktadır.[18]

Bilgi güvenliği, gizlilik, bütünlük ve geçerlilik sağlamak için bilgisayar sistemlerini yetkisiz erişim, kullanım, rahatsızlık ve tahribattan korumayı sağlamak olarak tanımlanabilir.[19]

Hukuk büroları da, özellikle hassas kişisel verileri işlemesinden dolayı gerek ilgili müvekkillerin gerekse kurumsal ve ilgili avukatların

---

14 Anacleto Correia, Antonio Goncalves ve M.Filomena Teodoro, "A Model-Driven Approach to Information Security Compliance", AIP Conference Proceedings, 2017.

15 Petac Eugen ve Duma Petruţ,

16 Jemal H Abawajy, "User Preference of Cyber Security Awareness Delivery Methods", Behav Inf Technol 2014, 2014, 33(1), 236-47, 2014.

17 Nader Sohrabi Safa, Rossouw Von Solms ve Steven Furnell, "Information Security Policy Compliance Model in Organizations", Comput Secur 2016, 2016, 56(1), 1-13.

18 Wendy Guwan Wang, "Measuring ınformation Security and Cyber Security on Private Cloud Computing", *Journal of Theoretical and Applied Information Technology*, 2019, 96(1), 156-168.

19 NIST, NIST Special Publication 800-30: Guide for Conducting Risk Assessments, 2012.

itibarlarının korunabilmesi için bilgi güvenliği konusunu bir öncelik olarak görmeli ve temel bir takım tedbirleri almalıdır.

Büroda giderilmesi gereken risklere karar verildiğinde, risk giderme alternatifleri belirlenmeli ve tahmin edilmelidir. Büroyu paylaşan avukatlar, riskleri giderme alternatifleri öneren teknolojik tavsiyelere ihtiyaç duyabilir. Risk değerlendirmesini yapan güvenlik uzmanı, sistemdeki mevcut güvenlik açıkları konusunda bir anlayışa sahip olduğundan, saldırganların güvenlik açıklarından yararlanmalarının nasıl önlenebileceği konusunda öneride bulunabilir.

Dosyaların şifrelenmesini bir kural haline getirmek teknik bir tedbirken bu kural sonrasında ise şifreleme ve şifre çözme konusunda insanları eğitmek teknik olmayan bir tedbirdir.[20] Her ikisinin de uygulanabilmesi için de maddi kaynak gereklidir.

Bu aşamadaki zorluk, riskleri azaltan güvenlik tedbirlerinin kalitesinin ve verimliliğinin görünmemesidir. Hukuk büroları gibi küçük kuruluşların güvenlik çözümlerinin yeteneklerini ve verimliliğini test edecek kaynakları yoktur. Çoğunlukla, kontrollerin etkinliği ile ilgili olarak erişilebilir kaynaklarda yer alan bilgilere ve kontrollerle uyumlu öz değerlendirmelere güvenmek zorundadırlar.

Birden fazla önlem birleştirildiğinde, ortak etkinlikleri değerlendirilmelidir. Örneğin, masaüstü güvenlik çözümünün %50 riski önlediği ve güvenlik duvarı güvenlik çözümünün de bazı saldırıların %80' ini önlediği tahmin ediliyorsa, bu önlemlerin her ikisi birlikte uygulandığında, koruma en az %80 olmalıdır. Eğer birbirini tamamlayıcı ürünler seçilmişse bu oran %80' inin üzerinde olmalıdır. Alternatif önlemleri seçerken ve önlemlerin etkililiğini tahmin ederken, çözümün sağlayıcısı tarafından sağlanan lisansın veya desteğin uzunluğunu göz önünde bulundurmak da önemlidir. Güvenlik riskleri her geçen gün artmakta ve çeşitlenmektedir. Bu nedenle güncel bir güvenlik sistemine sahip olmak çok önemlidir.[21] Hukuk büroları gibi küçük işletmeler bir takım güvenlik kontrolleri uygulamak için sahip oldukları veya ihtiyaç duydukları insan kaynaklarını da göz önünde bulundurmalıdır. Bilgi

---

20 Tiiu Mamers, The Art and Science of Information Security Investments For Small Enterprise, *Yüksek Lisans Tezi*, Tallinn Teknoloji Üniversitesi, Bilgi Teknolojileri Okulu, Tallinn, Estonya, 2018.

21 Wendy Guwan Wang,

sistemlerini günlük olarak takip edecek bir uzmanları yoksa günlük izleme gerektiren çözümleri düşünmemelidirler.

4. ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ VE HUKUK BÜROLARI AÇISINDAN DEĞERLENDİRME

ISO/IEC 27001 standardı, bir kuruluşun BGYS'nin etkinliğini planlamayı, uygulamayı, kontrol etmeyi, önlem almayı amaçlayan PUKÖ modeli olarak bilinen döngüsel bir model sunmaktadır.

Planlama-BGYS'nin kuruluşu: İlk adım, risklerin tanımlanacağı, analiz edilip değerlendirileceği risk değerlendirmeyi tanımlamaktır. Daha sonra risk çözüm seçeneklerinin tanımlanması ve değerlendirilmesi yapılmaktadır. Kontrol hedefleri ve kontrolleri seçildikten sonra, yönetim artık riskleri onaylamalı ve BGYS'nin uygulanmasına izin vermelidir.

Uygulama-BGYS'nin uygulanması ve işletilmesi: Yönetim işlemleri, kaynaklar, öncelikler, roller ve sorumluluklar bu adımda tanımlanacaktır. Risk gerçekleşmesi durumunda ortaya çıkabilecek zararın ne şekilde düzeltilebileceği planının ilgili risklere göre belirlemesi ve kontrollerin buna göre yapılması gerekmektedir.

Kontrol Etme-BGYS'nin izlenmesi ve gözden geçirilmesi: İzleme ve gözden geçirme prosedürleri geliştirilmeli ve yürütülmelidir. BGYS ve kontrollerin etkililiği ile risk değerlendirme metodolojisi ve gözden kaçan riskler de gözden geçirilmelidir.

Önlem Alma- BGYS'nin korunması ve iyileştirilmesi: Bu adımda hem önleyici hem de düzeltici eylemlerin uygulanması BGYS'yi daha da iyileştirebilir. Ayrıca, belge ve kayıt kontrolünü zorlar ve BGYS'yi geliştirmek için bilgi güvenliği olaylarını gözden geçirir.

Hukuk büroları açısından, hizmet verilen kişilerin yani müvekkillerin dava dosyaları kapsamında mevcut tüm verilerin kişisel bilgiler olduğu, bu bilgilerin korunmasından da müvekkilin dava vekaleti kapsamında avukatı ve hukuk bürosunun sorumlu olduğu açıktır. Bir hukuk bürosu, bilgi güvenliği konusunda mevcut durumunu iyileştirmek istemesi durumunda aşağıdaki konuları ele almalıdır.

Risk değerlendirmesi: Risk değerlendirmesi, tüm risk tanımlama, risk analizi ve risk değerlendirme sürecini tanımlamaktadır. İlk aşa-

mada -Risk Belirleme- kuruluşun risk kaynaklarını, etki alanlarını, risk olaylarını ve sonuçlarını tanımlar.

Risk tanımlaması: Risk tanımlamasında, ne tür olayların olabileceği ve daha sonra kayba yol açacağı incelenmektedir. Bu, kuruluşun kontrolü altında olan olayların yanı sıra dış etkenlere dayanan olayları da içermektedir.

Risk analizi: Genel olarak, risk analizi nitel veya nicel olabilir. Nicel risk analizi kesin sayısal değerlere dayanırken, nitel yöntemler, olay senaryosunun sonuçlarını ve olasılığını tanımlamak için tanımlayıcı ölçekler (düşük, orta ve yüksek gibi) kullanmaktadır.

Bağlam kurulumu: Odak noktası risk analizi, olası sonuçların değerlendirilmesinin yanı sıra tanımlanan risklerin gerçekleşme ihtimalleri de göz önünde bulundurulmalıdır. Olasılıklar değerlendirilirken, belirli bir tehdidin ne sıklıkta ortaya çıkabileceği ve ilişkili olabilecek diğer güvenlik açıkları da alınmalıdır.

Risk değerlendirmesi: Tüm olası risklerin risk seviyeleri, tanımlanan risk değerlendirme kriterleri ile karşılaştırılır. Bu, tanımlanan risklerin birbirleriyle ilişkilendirilmesini ve kuruluş için en önemli risklerin belirlenebilmesini sağlar. Bunun sonucunda, risk değerlendirme kriterlerine göre önceliklendirilen risklerin bir listesi oluşturulabilir.

Risk gidermek: ISO/IEC 27005' te risk tedavisi dört olası (risk değişikliği, risk tutma, riskten kaçınma, risk paylaşımı) seçenekten oluşan bir yapıda tanımlanmaktadır. Bu seçenekler birbirini dışlayan seçenekler değildir. Hatta bu seçeneklerin bütünleşik olarak kullanılmasının gerektiği durumlar da olabilir.

Risk kabulü: Risklerin kabulü, kuruluşun iş süreçlerine entegrasyon için çok önemlidir ve sorumlular tarafından onaylanmalıdır.

Risk iletişimi ve danışma: Risk iletişimi, bir risk yönetimi sürecinin uygulanmasında kilit bir faktördür. Bu nedenle, bu süreç tüm risk yönetimi süreci boyunca devam etmektedir. Mevcut risklerle ilgili bilgiler sürekli olarak toplanmakta ve aynı zamanda risklerden potansiyel olarak etkilenen çalışanlar risk yönetimi sürecinin mevcut sonuçları hakkında bilgilendirilmektedir.

Bilgi güvenliği risk izleme ve gözden geçirme: Mevcut risk durumuna ilişkin doğru bakış açısı elde etmek için tüm risklerin ve bunların

faktörlerinin, yani varlıkların, varlıkların değerinin, etkilerinin, tehditlerin ve meydana gelme olasılıklarının güncel tutulması gereklidir.

Bilginin kapsamı ve değeri sürekli olarak arttığından, kuruluşların ve bireylerin, verilerin çalınması veya imha edilmesine maruz kalması riski artmaktadır. Bilgisayar ve mahremiyetle ilgili düzenlemelerin uyumluluk gereklilikleri artmakla birlikte, bilgi güvenliğine yönelik önlemler gittikçe daha karmaşık bir hale gelmiş, küresel tehditlerin yayılması, bilgi güvenliği konusunda kuruluşların daha bütünsel bir yaklaşıma yönelmesine neden olmuştur.[22]

Hukuk büroları da bunun istisnası bir ayrıcalığa sahip değildir. Aksine, dilekçe yazımından, gerekli araştırmaların yapılmasına, dava açma süreçlerinden müvekkiller ile iletişime kadar pek çok noktada, hukuk bürolarının, kişiler açısından önemli, kişiye özel hem avukat hem müvekkil açısından itibarlarının zarar görmesine yol açabilecek kritik kişisel veriler ile çalışmasından dolayı, pek çok kuruluşa kıyasla daha fazla riske sahip olduğundan bahsedilebilmek mümkündür.

Karar vericiler için, kuruluşun tüm seviyelerinde, bilgi güvenliği risklerinin nasıl ele alınması gerektiğini anlamak önemlidir. Yalnızca kapsamlı ve sistematik bir yaklaşım, bir kuruluşun ihtiyaç duyduğu bilgi güvenliği seviyesini sağlayabilmektedir. Bu yaklaşım, bilgi güvenliği yönetimi için uluslararası referans, yani bilgi güvenliği ile ilgili ISO/IEC 27K standartları ailesi tarafından verilmektedir.[23]

Faaliyet kapsamı, personel sayısı ve iş süreçlerinin çeşitliliği açısından, bir hukuk bürosunun ISO/IEC 27001 standardına tam olarak uyumlu olması beklenemeyeceği gibi, standarda uyum sağlama süreci de hem ek iş gücü ihtiyacı hem de maddi açısından yüksek bir maliyetle karşılaşılmasına neden olabilecektir. Bu nedenle, hukuk bürolarının ISO/IEC 27001 standardının tüm kontrollerine uyum sağlamaktansa, mevcut durumlarının analiz edilmesi ve teknik açıdan kabul edilebilir bir seviyede kontrollerle uyumlu hale gelmesi en düşük iş gücü ve en düşük maliyetli çözüm olacaktır. Ancak, kontrollerin seçimi ISO/IEC 27001 Ek A' ya dayandırılmalıdır.[23] BGYS, kontrollerinin seçiminin, kuruluşun bilgi varlıklarını korumak ve hizmet alanlara güven vermek için yeterli ve orantılı olması gerekmektedir.[24]

---

22 NIST,
23 Malik Motii ve Elalami Semma,
24 Ernst&Young,

5. YÖNTEM

Araştırmada, Hukuk Bürolarının ISO/IEC 27001 BGYS' ne uyumları konusunda bilgi toplamak için hazırlanan ISO/IEC 27001 Bilgi Teknolojisi- Güvenlik Teknikleri- Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler dokümanı EK-A' da yer alan Referans Kontrol Amaçları ve Kontroller başlığı altında yer alan Amaç, Alt Amaç ve Kontroller paralelinde hazırlanan Öz Değerlendirme Anketi kullanılmıştır.

ISO/IEC 27001 BGYS, 14 Amaç, 35 Alt Amaç ve 113 Kontrolden oluşmaktadır. Hazırlanan ankette hiçbir kontrol atlanmamak şartıyla, kontrolün yapısına göre değişen sayıda, toplam 294 anket maddesi hazırlanmıştır. ISO/IEC 27001 BGYS amaç ve alt amaçlarına ilişkin anket madde sayıları Çizelge 1' de gösterilmiştir.

Literatürde BGYS' lerini etkileyen ana faktörlerin İnsan Kaynakları, kullanılan Bilgi Teknolojileri Ekipmanı (BTE) ve Bilgi Teknolojileri İletişimi (BTİ) ile ilgili olmasından dolayı, ankette hukuk bürolarının bu özellikleri de tespit edilmiştir.

Çizelge 1. ISO/IEC 27001 referans kontrol amaçları ile alt amaç, kontrol ve anket madde sayıları

ISO/IEC 27001 Kontrol Amaçları ve Alt Amaçları	Alt Amaç Sayısı	Kontrol Sayısı	Anket Madde Sayısı
5. Bilgi Güvenliği Politikaları	1	2	8
5.1. Bilgi güvenliği için yönetimin yönlendirmesi		2	8
6. Bilgi Güvenliği Organizasyonu	2	7	12
6.1. İç organizasyon		5	8
6.2. Mobil cihazlar ve uzaktan çalışma		2	4
7. İnsan Kaynakları Güvenliği	3	6	15
7.1. İstihdam öncesi		2	3
7.2. Çalışma esnasında		3	10
7.3. İstihdamın sonlandırılması ve değiştirilmesi		1	2
8. Varlık Yönetimi	3	10	18
8.1. Varlıkların sorumluluğu		4	6
8.2. Bilgi sınıflandırması		3	7

ISO/IEC 27001 Kontrol Amaçları ve Alt Amaçları	Alt Amaç Sayısı	Kontrol Sayısı	Anket Madde Sayısı
8.3. Ortam işleme		3	5
9. Erişim Kontrolü	4	14	25
9.1 Erişim kontrolünün iş gereklilikleri		2	3
9.2. Kullanıcı erişim yönetimi		6	13
9.3. Kullanıcı sorumlulukları		1	2
9.4. Sistem ve uygulama erişim kontrolü		5	7
10. Kriptografi	1	2	5
10.1. Kriptografik kontroller		2	5
11. Fiziksel ve Çevresel Güvenlik	2	15	42
11.1. Güvenli alanlar		6	12
11.2. Teçhizat		9	30
12. İşletim Güvenliği	7	13	42
12.1. İşlem prosedürleri ve sorumlulukları		4	9
12.2. Kötücül yazılımlardan koruma		1	2
12.3. Yedekleme		1	7
12.4. Kaydetme ve izleme		3	13
12.5. İşletimsel yazılımının kontrolü		1	2
12.6. Teknik açıklık yönetimi		2	6
12.7. Bilgi sistemleri tetkik hususları		1	3
13. Haberleşme Güvenliği	2	7	22
13.1. Ağ güvenliği yönetimi		3	10
13.2. Bilgi transferi		4	12
14. Sistem Temini, Geliştirme ve Bakımı	3	13	47
14.1. Bilgi sistemlerinin güvenlik gereksinimleri		3	10
14.2. Geliştirme ve destek süreçlerinde güvenlik		9	31
14.3. Test verisi		1	6
15. Tedarikçi İlişkileri	2	5	18
15.1. Tedarikçi ilişkilerinde bilgi güvenliği		3	8
15.2. Tedarikçi hizmet sağlama yöntemi		2	10

ISO/IEC 27001 Kontrol Amaçları ve Alt Amaçları	Alt Amaç Sayısı	Kontrol Sayısı	Anket Madde Sayısı
16. Bilgi Güvenliği İhlal Olayı Yönetimi	1	7	14
16.1. Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi		7	14
17. İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları	2	4	12
17.1. Bilgi güvenliği sürekliliği		3	8
17.2. Yedek fazlalıklar		1	4
18. Uyum	2	8	14
18.1. Yasal ve sözleşmeye tabi gereksinimlerle uyum		5	9
18.2. Bilgi güvenliği gözden geçirmeleri		3	5
TOPLAM	35	113	294

Katılımcılara hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özellikleri ile ilgili sorular yöneltilen ilk bölümünde 1-5 sorularda sayısal değerler girmeleri istenmiştir. 6-15 aralığında yine İnsan Kaynakları, BTE ve BTİ özelliklerine ilişkin evet ve hayır şeklinde yanıtlamaları istenen sorular yöneltilmiştir.

ISO/IEC 27001 kontrollerine ilişkin 14 amaç anket içerisinde alt amaçlar paralelinde hazırlanan 35 soru grubu olarak katılımcılara yöneltilmiştir. Her bir alt amaca ait soru grubunun başlangıcında, katılımcılara gruptaki soruları cevaplayıp cevaplamamalarının gerektiğini belirlemek üzere evet/hayır seçenekli sorular sorulmuştur.

Örneğin, "12.2. İşlem Güvenliği" alt amacı için, katılımcıya öncelikle "Büro hizmetlerinde kullanılan bilişim teknolojileri varlıklarını kötücül yazılımlara karşı koruma amacıyla tedbirler alınıyor mu?" sorusu yöneltilmiştir. Katılımcı bu soruya Evet cevabını vermişse, ISO/IEC 27001 Standardının bu alt amaca ait kontrolleri ile ilişkili olarak "Büro hizmetlerinde kullanılan bilişim sistemleri ekipmanlarını kötücül yazılımlardan korunması için tedbirler alınıyor mu?" ve "Büro ağına bağlanan kişisel kullanıcıların kötücül yazılımlardan korunması için tedbirler alınıyor mu?" sorularını yanıtlaması istenmiştir. Katılımcı bu soruya Hayır cevabını vermiş ise, alt amaç kontrolleri ile ilişkili evet cevabını verebileceği bir anket maddesi bulunmamaktadır.

Soruları alt amaçlar halinde gruplandırarak, toplam 294 maddeden oluşan anketin daha kısa süre içerisinde, katılımcıların dikkatini dağıtmadan ilgili alt amaçlara odaklanarak cevaplayabilmeleri amaçlanmıştır.

Grup sorusuna hayır cevabını veren katılımcılar, grup içerisindeki evet cevabını verebilecekleri bir soru olmaması nedeni ile grup altındaki soruların tamamına hayır cevabını verdikleri kabul edilmiştir.

Grup içerisindeki anket maddelerine katılımcılardan her soruya karşılık evet, kısmen ve hayır cevaplarından birini işaretlemeleri istenmiştir. Evet cevapları 2, kısmen cevapları 1 ve hayır cevapları 0 puan olacak şekilde her bir katılımcının anketteki alt amaçlarda bulunan sorulara verdikleri puanlar toplanmış ve o alt amaçtaki soru sayısına bölünerek katılımcıların alt amaçlardaki düzeyleri belirlenmiştir. Bu şekilde bir katılımcının herhangi bir alt amaçtaki düzeyi maksimum 2, minimum 0 puan olabilmektedir. Aynı durum 452 katılımcı bazında düşünülerek katılımcıların genel alt amaçlardaki seviyeleri tespit edilmiştir. Yani alt amaçlardaki genel düzeyleri hesaplanırken, katılımcıların o alt amaçtan elde ettiği puanlar toplanarak katılımcı sayısına bölünmüştür.

Katılımcıların amaç puanlarının hesaplanmasında da aynı yöntem kullanılmış, her bir katılımcının anketteki amaçta bulunan sorulara verdikleri puanlar toplanmış ve o amaçtaki soru sayısına bölünerek katılımcıların amaçtaki düzeyleri belirlenmiştir. Bu şekilde bir katılımcının herhangi bir amaçtaki düzeyi maksimum 2, minimum 0 puan olabilmektedir. Aynı durum 452 katılımcı bazında düşünülerek katılımcıların genel amaç seviyeleri tespit edilmiştir. Yani amaçtaki genel düzeyleri hesaplanırken, katılımcıların o amaçtan elde ettiği puanlar toplanarak katılımcı sayısına bölünmüştür.

ISO/IEC 27001 BGYS kontrolleri aracılığı ile hukuk bürolarının BGYS Puanı olarak isimlendirilen, ISO/IEC 27001 BGYS kontrollerine uyum düzeylerini ifade etmek üzere hesaplanan puan değerinin tespiti için regresyon analizi yapılmıştır. Regresyon analizi yaparak edilen formül ile bir BGYS Puanı hesaplamaktaki amaç, öz değerlendirme anketini herhangi bir zamanda yanıtlayan hukuk büroları için de ISO/IEC 27001 BGYS' ne uyum seviyelerini, diğer hukuk büroları ile kıyaslanabilir bir puan olarak hesaplayabilmektir.

6. BULGULAR

Anket sorusunu cevaplayan 452 hukuk bürosunun İnsan Kaynakları, BTE ve BTİ özelliklerine ait bilgiler analiz edilerek yüzde ve frekans değerleri Çizelge 2' de sunulmuştur.

Çizelge 2. Hukuk bürolarına ait insan kaynakları, bilgi teknolojileri ekipman ve bilgi teknolojileri iletişim özellikleri yüzde oranları çizelgesi

İnsan Kaynakları, BTE ve BTİ Özellikleri			N	%
1. Bürodaki çalışan avukat sayısı?		Bir	48	10,6
		İki	196	43,4
		Üç	92	20,4
		Dört	52	11,5
		Beş+	64	14,2
2. Bürodaki çalışan personel sayısı?		Bir	144	31,9
		İki	112	24,8
		Üç	108	23,9
		Dört+	88	19,5
3. Bürodaki çalışan yardımcı personel sayısı?		Sıfır	84	18,6
		Bir	68	15,0
		İki	252	55,8
		Üç	48	10,6
4. Büroda kullanılan bilgisayar sayısı?		İki	116	25,7
		Üç	76	16,8
		Dört	40	8,8
		Beş	84	18,6
		Altı+	136	30,1
5. Büroda kullanılan yazıcı sayısı?	Bir		256	56,6
	İki		132	29,2
	Üç		64	14,2
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır		232	51,3
	Evet		220	48,7

İnsan Kaynakları, BTE ve BTİ Özellikleri			N	%
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	240	53,1	
	Evet	212	46,9	
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	236	52,2	
	Evet	216	47,8	
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	264	58,4	
	Evet	188	41,6	
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	196	43,4	
	Evet	256	56,6	
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	240	53,1	
	Evet	212	46,9	
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	208	46,0	
	Evet	244	54,0	
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	272	60,2	
	Evet	180	39,8	
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	236	52,2	
	Evet	216	47,8	
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	220	48,7	
	Evet	232	51,3	

452 hukuk bürosunun İnsan Kaynakları, BTE ve BTİ özellikleri incelendiğinde büyük oranda 2 avukatın (%43,4) çalıştığı, 1 personelin (%31,9) çalıştığı ve 2 yardımcı personelin (%55,8) çalıştığı tespit edilmiştir. Büroda kullanılan bilgisayar sayısının büyük oranda 6 ve üzeri (%30,1) olduğu, yazıcı sayısının ise büyük oranda 1 (%56,6) olduğu anlaşılmıştır.

452 hukuk bürosunun %48,7' si büroda bilgisayar ağına bağlı mobil cihazlar kullandığını, %46,9' u çalışanlarına büro ağında kişisel mobil cihazlarını kullanmalarına izin verdiğini, %47,8' i büro ve avukatlık hizmetleri için özel bir paket programı kullandığını, %41,6' sı büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi sahibi olduğunu, %56,6' sı büroda kullanılan bilişim teknolojileri ekipmanı için teknik

destek, bakım, onarım ve benzeri hizmetlerinin alındığı anlaşmalı bir tedarikçilerinin olduğunu, %46,9' u büro bilişim güvenliği konusunda danışmanlık aldıkları bir tedarikçilerinin olduğunu, %54' ü büroda kablolu bilgisayar ağı kullandıklarını, %39,8' i büroda kablosuz bilgisayar ağı kullandıklarını, %47,8' i büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop ve cep telefonu bağlanmasına izin verdiklerini, %51,3' ü büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop ve cep telefonu bağlanmasına izin verdiklerini belirtmiştir.

Çok Değişkenli Regresyon Analizi ile bir BGYS Puanı hesaplamaktaki amaç, öz değerlendirme anketini herhangi bir zamanda yanıtlayan hukuk büroları için de ISO/IEC 27001 BGYS' ne uyum seviyelerini diğer hukuk büroları ile kıyaslanabilir bir puan olarak hesaplayabilmektir. .

Analiz sonrasında, Çizelge 3' de görülen veriler elde edilmiş ve sonuçların formüle edilebilir olduğu, formülün anketin tamamını kapsayabileceği ve bir sabite ihtiyaç olmadığı (R Square=1,000) görülmüştür.

Her ne kadar R Square değeri 0 ile 1 aralığında bir değer olması gerektiği bilinse de, SPSS 25.0 ile yapılan analizlerde elde edilen R Square 1,000 değerinin, tam sayı "1" değerine üç ondalıkta, değerin yuvarlanması sonucu elde edilmiş olduğu değerlendirilmiştir.

Çizelge 3. ISO/IEC 27001 BGYS amaçlar regresyon analizi sonuçları

Amaçlar	Beta Katsayısı	B Katsayısı	p
Bilgi Güvenliği Politikaları	,138	,071	,000
Bilgi Güvenliği Organizasyonu	,088	,071	,000
İnsan Kaynakları Güvenliği	,186	,071	,000
Varlık Yönetimi	,238	,071	,000
Erişim Kontrolü	,169	,071	,000
Kriptografi	,278	,071	,000
Fiziksel ve Çevresel Güvenlik	,140	,071	,000
İşlem Güvenliği	,140	,071	,000

Amaçlar	Beta Katsayısı	B Katsayısı	p
Haberleşme Güvenliği	,178	,071	,000
Sistem Temini, Geliştirme ve Bakımı	,106	,071	,000
Tedarikçi İlişkileri	,136	,071	,000
Bilgi Güvenliği İhlal Olayı Yönetimi	,174	,071	,000
İş Sürekliliğinin Bilgi Güvenliği Hususları	,211	,071	,000
Uyum	,288	,071	,000

Katılımcılar açısından Çizelge 3' de görüleceği üzere ISO/IEC 27001 BGYS amaçlarından en önem verileninin Uyum (,288) ve en az önem verilenin ise Bilgi Güvenliği Organizasyonu (,088) olduğu görülmüştür.

Regresyon analizi amaç seviyesinde formüle edildiğinde;

BGYS Puanı = 0,071 * (Bilgi Güvenliği Politikaları Puanı + Bilgi Güvenliği Organizasyonu Puanı + İnsan Kaynakları Güvenliği Puanı + Varlık Yönetimi Puanı + Erişim Kontrolü Puanı + Kriptografi Puanı + Fiziksel ve Çevresel Güvenlik Puanı + İşlem Güvenliği Puanı + Haberleşme Güvenliği Puanı + Sistem Temini, Geliştirme ve Bakımı Puanı + Tedarikçi İlişkileri Puanı + Bilgi Güvenliği İhlal Olayı Yönetimi Puanı + İş Sürekliliğinin Bilgi Güvenliği Hususları Puanı + Uyum Puanı)

olarak yazılabildiği görülmüştür.

Regresyon analizi sonucu amaçlara ait katsayıların eşit olması nedeni ile bu formül uygulanabilir olmakla birlikte, regresyon katsayılarını kullanarak aynı formülü aşağıdaki şekilde yazmak da mümkündür.

KAP_m = Bir BGYS amacı için anket katılımcılarının toplam puanı.

Formülde görüleceği üzere regresyon analizi sonucunda elde edilen katsayılar ile bütün katılımcıların, bütün BGYS amaçlarından alabileceği 0-100 aralığına indirgenmiş puanı hesaplanabilmektedir.

Çizelge 4' de tüm katılımcılar için hesaplanan BGYS Puanları ile 30 ve 50 sıra numaralı katılımcılara ait BGYS Puanları görülmektedir.

Çizelge 4. Tüm katılımcılara, 30 ve 50 sıra numaralı katılımcılara ait ISO/IEC amaç BGYS puanları

ISO/IEC 27001 Kontrol Amaçları	KAP_m	BGYSP	BGYSP100	$BGYSP100_{30}$	$BGYSP100_{50}$
Bilgi Güvenliği Politikaları	0,105088	0,007461	0,373	0,000	0,000
Bilgi Güvenliği Organizasyonu	0,065634	0,004660	0,233	0,000	0,000
İnsan Kaynakları Güvenliği	0,134513	0,009550	0,478	0,000	0,000
Varlık Yönetimi	0,331858	0,023562	1,178	1,775	0,197
Erişim Kontrolü	0,099469	0,007062	0,353	0,000	0,852
Kriptografi	0,394690	0,028023	1,401	0,000	2,840
Fiziksel ve Çevresel Güvenlik	0,100927	0,007166	0,358	0,000	1,099
İşletim Güvenliği	0,213654	0,015169	0,758	1,099	2,874
Haberleşme Güvenliği	0,318986	0,022648	1,132	1,130	1,291
Sistem Temini, Geliştirme ve Bakımı	0,139145	0,009879	0,494	0,000	1,964
Tedarikçi İlişkileri	0,114553	0,008133	0,407	0,000	2,761
Bilgi Güvenliği İhlal Olayı Yönetimi	0,187105	0,013284	0,664	1,521	0,000
İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları	0,206490	0,014661	0,733	0,000	0,000
Uyum	0,512010	0,036353	1,818	6,339	5,832
ORTALAMA			0,741		
TOPLAM		0,207613	10,381	11,864	19,710

Herhangi bir katılımcının 0-100 aralığında hesaplanan BGYS Puanının, katılımcıların tamamının 0-100 aralığında hesaplanan BGYS Puanı ile kıyaslanması herhangi bir hukuk bürosunun diğer hukuk büroları arasındaki durumunu değerlendirmeyi sağlamaktadır. Bu yöntem ile, diğer hukuk bürolarına ait BGYS Puanları bilinmeksizin de herhangi bir hukuk bürosunun ISO/IEC 27001 BGYS' ne göre Bilgi Güvenliği Yeterliliğini, standardın amaçları seviyesinde değerlendirebilmek mümkündür.

Örneğin 30 sıra numaralı katılımcı ile anketi yanıtlayan tüm katılımcılar arasında bir kıyaslama yapılmak istenirse, katılımcıların tamamı ve 30 sıra numaralı katılımcı için hesaplanan BGYS Puanları kullanılabilecektir.

Çizelge 4 incelendiğinde, bütün katılımcıların BGYS Puanı (10,381) ile 30 sıra numarasındaki katılımcının BGYS Puanı (11.864) karşılaştırıldığında, 30 sıra numaralı katılımcının BGYS puanının daha yüksek olduğu görülmüştür.

30 sıra numaralı katılımcının her ne kadar BGYS Puanı, tüm katılımcıların puanından yüksek olsa da, 14 amacın dokuzundan (1) Bilgi Güvenliği Politikaları, 2) Bilgi Güvenliği Organizasyonu, 3) İnsan Kaynakları Güvenliği, 4) Erişim Kontrolü, 5) Kriptografi, 6) Fiziksel ve Çevresel Güvenlik, 7) Sistem Temini, Geliştirme ve Bakımı, 8) Tedarikçi İlişkileri, 9) İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları) hiç puan alamadığı, puan aldığı amaçlardan ise Haberleşme Güvenliği (1,130) amacında, tüm katılımcılara (1,132) kıyasla daha düşük puana sahip olduğu ancak, Varlık Yönetimi (1,775/1,178), İşletim Güvenliği (1,099/0,758), Bilgi Güvenliği İhlal Olayı Yönetimi (1,521/0,664) ve Uyum (6,339/1,818) amaçlarından daha yüksek puan aldığı görülmüştür. 30 sıra numaralı katılımcının özellikle Uyum amacından aldığı puanın, diğer katılımcılardan oldukça yüksek olması dikkat çekmiştir.

Benzer şekilde bütün katılımcılar arasında istenen herhangi iki katılımcı hukuk bürosunun kıyaslanması bu hukuk bürolarının ayrı ayrı hesaplanacak BGYS Puanı ile yapılabilecektir.

Örneğin 30 sıra numaralı katılımcı ile 50 sıra numaralı katılımcı arasında bir kıyaslama yapılmak istenirse, 30 sıra numaralı katılımcı için hesaplanan BGYS puanı ile 50 sıra numaralı katılımcı için hesaplanan BGYS Puanları kullanılabilecektir.

Çizelge 4 incelendiğinde, 30 sıra numaralı katılımcının BGYS Puanı (11,864) ile 50 sıra numaralı katılımcının BGYS Puanı (19,710) karşılaştırıldığında, 50 sıra numaralı katılımcının BGYS Puanının daha yüksek olduğu, 50 sıra numaralı katılımcının, 14 amacın beşinden (1) Bilgi Güvenliği Politikaları, 2) Bilgi Güvenliği Organizasyonu, 3) İnsan Kaynakları Güvenliği, 4) Bilgi Güvenliği İhlal Olayı Yönetimi, 5) İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları) hiç puan alamadığı,

puan aldığı amaçlardan ise Varlık Yönetimi (0,197/1,775) ve Uyum (5,832/6,339) amaçlarından 30 sıra numaralı katılımcıya kıyasla daha düşük puana sahip olduğu ancak, Erişim Kontrolü (0,852/0,000), Kriptografi (2,840/0,000), Fiziksel ve Çevresel Güvenlik (1,099/0,000), İşletim Güvenliği (2,874/1,099), Haberleşme Güvenliği (1,964/0,000),Sistem Temini, Geliştirme ve Bakımı (1,964/0,000) ile Tedarikçi İlişkileri (2,761/0,000) amaçlarından 30 sıra numaralı katılımcıya kıyasla daha yüksek puanlara sahip olduğu görülmüştür.

Benzer şekilde, katılımcı herhangi bir hukuk bürosunun katılımcı diğer tüm hukuk büroları ile veya belirli hukuk bürolarının karşılıklı olarak hesaplanan Bilgi Güvenliği Puanları aracılığı ile genel puan veya ISO/IEC 27001 BGYS amaç puanları bazında kıyaslanması mümkün olabilmekte ve iyileştirme yapılması gereken bilgi güvenliği alanları net olarak belirlenebilmektedir.

7. SONUÇ VE ÖNERİLER

Çizelge 4' de görüleceği üzere katılımcıların BGYSP puanları 0,233 ile 1,818 arasındadır. BGYSP' lerin toplamı ile elde edilen BGYSP100 puanının ise 10,381 olduğu hesaplanmıştır.

1,818 puanla en yüksek amaç değerinin "Uyum" amacına ait olduğu görülmüştür. Bu amacın alt amaçları olan "Yasal ve sözleşmeye tabi gereksinimlerle uyum" ve "Bilgi güvenliği gözden geçirmeleri" ile birlikte değerlendirildiğinde, hukuk bürolarının, yasal mevzuat uyumlulukları ve veri gizliliği sorumluluklarından dolayı bu amaca ait puanlarının, diğer amaçlardan çok daha yüksek olduğu değerlendirilmiştir.

En düşük BGYSP olan 0,233 puanının "Bilgi Güvenliği Organizasyonu" amacına ait olduğu görülmüştür. Bu amacın alt amaçları olan "İç organizasyon" ve "Mobil cihazlarla uzaktan çalışma" ile birlikte değerlendirildiğinde, hukuk bürolarında belirli bir yönetim hiyerarşisinin olmaması, büroda çalışan avukatların birbirine denk olması, elektronik imza kullanımı nedeni ile büro faaliyetlerinin büro içinden veya herhangi bir yerden, büro ağına bağlanma gereksinimi olmadan yapılabiliyor olması nedenlerinden dolayı bu amaca ait puanlarının, diğer amaçlardan çok daha düşük olduğu değerlendirilmiştir.

Ancak, 0-100 aralığına indirgenmiş BGYSP100 puanının 10,381' de kalması, hukuk bürolarının, ISO/IEC 27001 BGYS açısından oldukça yetersiz olduğunu göstermektedir.

ISO/IEC 27001 BGYS' de Uyum amacına bağlı iki alt amaç Yasal ve Sözleşmeye Tabi Gereksinimlerle Uyum ve Bilgi Güvenliği Gözden Geçirmeleri düzeyleridir. Çizelge 4' de görüleceği üzere hukuk bürolarının BGYSP100 puanı olan 10,381 içerisinde, Uyum amacının puanı 1,818 olup, amaçlara ait ortalama puan olan 0,741' den yüksek olması nedeni ile yeterli olduğu değerlendirilmiştir.

Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre, anlamsal farklılık gösteren ISO/IEC 27001 BGYS alt amaç sayıları incelendiğinde;

- Bürodaki çalışan avukat sayısına göre, 25 alt amacın,
- Bürodaki çalışan personel sayısına göre, 24 alt amacın,
- Bürodaki çalışan yardımcı personel sayısına göre, 18 alt amacın,
- Büroda kullanılan bilgisayar sayısına göre, 21 alt amacın,
- Büroda kullanılan yazıcı sayısına göre, 17 alt amacın,
- Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıp kullanılmamasına göre, 5 alt amacın,
- Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin verilip verilmemesine göre, 9 alt amacın,
- Büro ve avukatlık hizmetleri için kullanılan özel bir paket program olup olmamasına göre, 10 alt amacın,
- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre, 16 alt amacın,
- Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi olup olmamasına göre, 14 alt amacın,
- Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi olup olmamasına göre, 10 alt amacın,
- Büroda kablolu bilgisayar ağı kullanılıp kullanılmamasına göre, 16 alt amacın,

- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre, 16 alt amacın,
- Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre, 12 alt amacın,
- Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre, 6 alt amacın,

anlamsal farklılık gösterdiği görülmüştür.

Hukuk bürolarının, ISO/IEC 27001 BGYS amaçlarından aldıkları BGYSP100 puanlarının kendi içerisinde ortalamaları (0,741 puan) ile karşılaştırılmaları sonucunda yeterli ve yetersiz oldukları amaçların aşağıdakiler oldukları tespit edilmiştir.

Yeterli olunan amaçlar

- Varlık Yönetimi
- Kriptografi
- İşletim Güvenliği
- Haberleşme Güvenliği
- Uyum

Yetersiz olunan amaçlar

- Bilgi Güvenliği Politikaları
- Bilgi Güvenliği Organizasyonu
- İnsan Kaynakları Güvenliği
- Erişim Kontrolü
- Fiziksel ve Çevresel Güvenlik
- Sistem Temini, Geliştirme ve Bakımı
- Tedarikçi İlişkileri
- Bilgi Güvenliği İhlal Olayı Yönetimi
- İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları

Diğer taraftan, alt amaç seviyesinde incelenen hukuk bürolarının

İnsan Kaynakları, BTE ve BTİ özelliklerine göre de ISO/IEC 27001 BGYS alt amaç sayılarının da değişken olduğu görülmekle birlikte, toplamda 35 alt amacın kriter olarak en az 15' i ile anlamsal bir ilişkinin varlığı aranacak olursa, İnsan Kaynakları, BTE ve BTİ özelliklerine ilişkin olarak aşağıdaki özelliklerin öncelikli olarak dikkate alınması gerektiği görülecektir.

- Bürodaki çalışan avukat sayısı
- Bürodaki çalışan personel sayısı
- Bürodaki çalışan yardımcı personel sayısı
- Büroda kullanılan bilgisayar sayısı
- Büroda kullanılan yazıcı sayısı
- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmaması
- Büroda kablolu bilgisayar ağı kullanılıp kullanılmaması
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmaması

Hukuk bürolarının ISO/IEC 27001 BGYS amaçlarına göre hesaplanan BGYSP100 puanlarının 0-100 aralığı için 10,381 gibi oldukça düşük bir seviyede kalmış olmasından dolayı, yeterliliklerinin artırılması için iki farklı bakış açısı geliştirilmiştir.

Birincisi, hukuk bürolarının, BGYSP puanı ortalamasına göre yeterli oldukları amaçlardan aldıkları BGYSP puanlarının artırılmasının amaçlanmasıdır.

İkincisi ise hukuk bürolarının, BGYSP puanı ortalamasına göre yetersiz oldukları amaçlardan aldıkları BGYSP puanlarının artırılmasıdır.

Çizelge 5. 15 ve üzeri alt amaç ile anlamsal farklılığa sahip insan kaynakları, bilişim teknolojileri ekipman ve bilişim teknolojileri iletişim özellikleri ile ortalama BGYSP puanına göre yeterli olunan ISO/IEC amaç ve alt amaç sayılarının incelenmesi

		Bürodaki çalışan avukat sayısı	Bürodaki çalışan personel sayısı	Bürodaki çalışan yardımcı personel sayısı	Büroda kullanılan bilgisayar sayısı	Büroda kullanılan yazıcı sayısı	Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmaması	Büroda kablolu bilgisayar ağı kullanılıp kullanılmaması	Büroda kablosuz bilgisayar ağı kullanılıp kullanılmaması
Yeterli Olunan Amaçlar	Varlık Yönetimi	2/3	3/3	2/3	1/3	-/3	1/3	-/3	1/3
	Kriptografi	1/1	1/1	1/1	1/1	-/1	1/1	-/1	1/1
	İşletim Güvenliği	4/5	2/5	-/5	1/5	2/5	4/5	1/5	3/5
	Haberleşme Güvenliği	2/2	2/2	1/2	2/2	1/2	1/2	-/2	1/2
	Uyum	1/2	2/2	1/2	1/2	2/2	-/2	1/2	1/2
Yetersiz Olunan Amaçlar	Bilgi Güvenliği Politikaları	-/1	1/1	1/1	1/1	-/1	-/1	-/1	-/1
	Bilgi Güvenliği Organizasyonu	2/2	2/2	1/2	2/2	2/2	-/2	1/2	1/2
	İnsan Kaynakları Güvenliği	1/3	1/3	3/3	1/3	3/3	1/3	-/3	1/3
	Erişim Kontrolü	4/4	2/4	2/4	3/4	1/4	2/4	2/4	3/4
	Fiziksel ve Çevresel Güvenlik	1/2	2/2	1/2	1/2	2/2	1/2	2/2	-/2
	Sistem Temini, Geliştirme ve Bakımı	1/3	1/3	-/3	3/3	2/3	2/3	1/3	-/3
	Tedarikçi İlişkileri	1/2	2/2	2/2	-/2	-/2	-/2	1/2	2/2
	Bilgi Güvenliği İhlal Olayı Yönetimi	1/1	1/1	1/1	1/1	-/1	1/1	-/1	-/1
	İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları	2/2	2/2	1/2	2/2	1/2	1/2	-/2	2/2

Güçlendirici Model ve Öneriler

Bu modelde, BGYSP puanları, ortalama BGYSP puanlarından düşük olan amaçların, amaçlarla anlamsal farklılık gösteren İnsan Kaynakları, BTE ve BTİ özelliklerine öncelik verilerek yükseltilmesi öngörülmüştür.

Güçlendirici modelde, hukuk büroları için, Çizelge 5 incelendiğinde;

1. Varlık Yönetimi amacı için öncelikli olarak büroda kullanılan yazıcı sayısı ve kablolu ağ kullanımı, ikincil öncelikli olarak büro web sitesi ve kablosuz ağ kullanımı konularında Bilgi Güvenliğine yönelik çalışma yapılması önerilmektedir.
2. Kriptografi amacı için öncelikli olarak, büroda kullanılan yazıcı sayısı ve kablolu ağ kullanımı konularında Bilgi Güvenliğine' ne yönelik çalışma yapılması önerilmektedir.
3. İşletim Güvenliği amacı için büroda çalışan yardımcı personel sayısı, ikincil öncelikli olarak, büroda kullanılan yazıcı sayısı ve kablolu ağ kullanımı konularında Bilgi Güvenliğine' ne yönelik çalışma yapılması önerilmektedir.
4. Haberleşme Güvenliği amacı için öncelikli olarak, büroda kablolu ağ kullanımı, ikincil öncelikli olarak büroda çalışan yardımcı personel sayısı, büroda kullanılan yazıcı sayısı, büro web sitesi ve kablosuz ağ kullanımı konularında Bilgi Güvenliğine' ne yönelik çalışma yapılması önerilmektedir.
5. Uyum amacı için öncelikli olarak, büro web sitesi, ikincil öncelikli olarak büroda çalışan avukat sayısı, yardımcı personel sayısı, kablolu ağ kullanımı ve kablosuz ağ kullanımı konularında BG' ne yönelik çalışma yapılması önerilmektedir.

Tamamlayıcı Model ve Öneriler

Bu modelde, BGYSP puanları, ortalama BGYSP puanlarından düşük olan amaçların, amaçlarla anlamsal farklılık gösteren İnsan Kaynakları, BTE ve BTİ özelliklerine öncelik verilerek yükseltilmesi öngörülmüştür.

Tamamlayıcı modelde, hukuk büroları için, Çizelge 5 incelendiğinde;

1. Bilgi Güvenliği Politikaları amacı için öncelikli olarak büroda çalışan avukat sayısı, yazıcı sayısı, kablolu ağ kullanımı, büro web sitesi, kablolu ağ kullanımı ve kablosuz ağ kullanımı konularında Bilgi Güvenliğine' ne yönelik çalışma yapılması önerilmektedir.
2. Bilgi Güvenliği Organizasyonu amacı için öncelikli olarak, büro web sitesi, ikincil öncelikli olarak büroda çalışan yardımcı personel sayısı, kablolu ağ kullanımı ve kablosuz ağ kullanımı konularında Bilgi Güvenliğine' ne yönelik çalışma yapılması önerilmektedir.
3. İnsan Kaynakları Güvenliği amacı için öncelikli olarak, büroda kablolu ağ kullanımı, ikincil öncelikli olarak büroda çalışan personel sayısı, büroda kullanılan bilgisayar sayısı, büro web sitesi ve kablosuz ağ kullanımı konularında Bilgi Güvenliğine' ne yönelik çalışma yapılması önerilmektedir.
4. Erişim Kontrolü amacı için öncelikli olarak, büroda kullanılan yazıcı sayısı, ikincil öncelikli olarak büroda çalışan personel sayısı, yardımcı personel sayısı, büro web sitesi ve kablolu ağ kullanımı konularında Bilgi Güvenliğine' ne yönelik çalışma yapılması önerilmektedir.
5. Fiziksel ve Çevresel Güvenlik amacı için öncelikli olarak, büroda kablosuz ağ kullanımı, ikincil öncelikli olarak, büroda çalışan avukat sayısı, yardımcı personel sayısı, kullanılan yazıcı sayısı ve büro web sitesi konularında Bilgi Güvenliğine' ne yönelik çalışma yapılması önerilmektedir.
6. Sistem Temini, Geliştirme ve Bakımı amacı için öncelikli olarak, büroda çalışan yardımcı personel sayısı ve kablosuz ağ kullanımı, ikincil öncelikli olarak, büroda çalışan avukat sayısı, personel sayısı ve kablosuz ağ kullanımı konularında Bilgi Güvenliğine' ne yönelik çalışma yapılması önerilmektedir.
7. Tedarikçi ilişkileri amacı için öncelikli olarak, büroda kullanılan bilgisayar sayısı, yazıcı sayısı ve büro web sitesi, ikincil öncelikli olarak büroda çalışan avukat sayısı ve kablolu ağ kullanımı ko-

nularında Bilgi Güvenliğine' ne yönelik çalışma yapılması önerilmektedir.

8. Bilgi Güvenliği İhlal Olayı Yönetimi amacı için öncelikli olarak, büroda kullanılan yazıcı sayısı, kablolu ağ kullanımı ve kablosuz ağ kullanımı Bilgi Güvenliğine' ne yönelik çalışma yapılması önerilmektedir.
9. İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları amacı için öncelikli olarak, büroda kablolu ağ kullanımı, ikincil öncelikli olarak büroda çalışan yardımcı personel sayısı, kullanılan yazıcı sayısı ve büro web sitesi konularında Bilgi Güvenliğine' ne yönelik çalışma yapılması önerilmektedir.

Herhangi Bir Hukuk Bürosu İçin Tamamlayıcı ve Güçlendirici Model Önerileri

ISO/IEC 27001 BGYS amaç ve alt amaçlarına bağlı olarak hazırlanan öz değerlendirme anketinin herhangi bir hukuk bürosu tarafından yanıtlanması ile hukuk bürosu için BGYSP100 puanı hesaplamak, yeterli ve yetersiz oldukları amaçları belirlemek mümkündür.

Yeterli ve yetersiz olunan amaçlar için belirli bir eşik puan değeri göz önünde bulundurulabileceği gibi, büronun amaç puanları ortalaması kullanılarak kendi içerisinde, tüm katılımcıların ortalama puanları kullanılarak hukuk büroları arasında karşılaştırmalı bir değerlendirme yapmak da mümkündür. Değerlendirmenin objektifliği için 10, 25 ve 50 puan eşikleri için belirlenen amaçlar Çizelge 6' da yer aldığı şekilde hesaplanmıştır.

Tamamlayıcı modeller uygulanmak üzere, 30 ve 50 sıra numaralı anket katılımcısı hukuk bürolarının Çizelge 4' e göre yeterli ve yetersiz oldukları amaçlar değerlendirildiğinde, Çizelge 6' da yer alan amaçlar elde edilecektir.

Çizelge 6. 10, 25 ve 50 eşik puanları için 30 ve 50 sıra numaralı anket katılımcısı hukuk bürolarının yeterli ve yetersiz oldukları ISO/IEC 27001 amaçları

	30 Sıra Nolu Hukuk Bürosu				50 Sıra Nolu Hukuk Bürosu			
ISO/IEC 27001 Kontrol Amaçları	Puan	10 p	25 p	50 p	Puan	10 p	25 p	50 p
Bilgi Güvenliği Politikaları	0,000	X	X	X	0,000	X	X	X
Bilgi Güvenliği Organizasyonu	0,000	X	X	X	0,000	X	X	X
İnsan Kaynakları Güvenliği	0,000	X	X	X	0,000	X	X	X
Varlık Yönetimi	25,000	√	√	X	2,775	X	X	X
Erişim Kontrolü	0,000	X	X	X	12,000	√	X	X
Kriptografi	0,000	X	X	X	40,000	√	√	X
Fiziksel ve Çevresel Güvenlik	0,000	X	X	X	15,479	√	X	X
İşletim Güvenliği	15,479	√	X	X	40,479	√	√	X
Haberleşme Güvenliği	15,915	√	X	X	18,183	√	X	X
Sistem Temini, Geliştirme ve Bakımı	0,000	X	X	X	27,662	√	√	X
Tedarikçi İlişkileri	0,000	X	X	X	38,887	√	X	X
Bilgi Güvenliği İhlal Olayı Yönetimi	21,423	√	X	X	0,000	X	X	X
İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları	0,000	X	X	X	0,000	X	X	X
Uyum	89,282	√	√	√	82,141	√	√	√

Kaynakça

Makaleler

Abawajy Jemal H, "User Preference of Cyber Security Awareness Delivery Methods", Behav Inf Technol 2014, 2014, 33(1), 236-47.

Ahmad Atif, Bosua Rachelle ve Scheepers Rens, "Protecting Organizational Competitive Advantage: A Knowledge Leakage Perspective", Computers & Security, 2014, 42(1), 27-39.

Eugen Petac ve Petruț Duma, "Exploring the New Era of Cybersecurity Governance", Ovidius University Annals, Economic Sciences Series, 2018, 18(1), 358-363.

Motii Malik ve Semma Elalami, "Towards a New Approach to Pooling COBIT 5 and ITIL V3 with ISO IEC 27002 for Better Use of ITG in the Morrocan Parliament", *IJCSI International Journal of Computer Science Issues,* 2017, 14(3), 49-58.

Romero Santiago Martín-Romo ve De-Pablos-Heredero Carmen, "Data Protection by Design: Organizational Integration", Harvard Deusto Business Research, 2016, 7(2), 60-71.

Sohrabi Safa Nader, Von Solms Rossouw ve Furnell Steven, "Information Security Policy Compliance Model in Organizations", Comput Secur 2016, 2016, 56(1), 1-13.

Wang Wendy Guwan, "Measuring ınformation Security and Cyber Security on Private Cloud Computing", *Journal of Theoretical and Applied Information Technology*, 2019, 96(1), 156-168.

Bildiriler

Bin Hamid Ali Firkhan Ali ve Jali Mohd Zalisham, "Human-Technology Centric In Cyber Security Maintenance for Digital Transformation ERA", 1st International Conference on Big Data and Cloud Computing (ICoBiC), 2017.

Correia Anacleto, Goncalves Antonio ve Teodoro M.Filomena, "A Model-Driven Approach to Information Security Compliance", AIP Conference Proceedings, 2017.

Paja Elda, Dalpiaz Fabiano ve Giorgini Paolo, "Modelling and Reasoning About Security Requirements in Socio-Technical Systems", 24th International Conference on Advanced Information Systems Engineering (CAiSE), 2015, 855(1).

Rapor ve Kılavuzlar

Ernst&Young, Into the Cloud, Out of the Fog: Ernst & Young' s 2011 Global Information Security Survey, Ernst&Young Raporu, Londra, İngiltere, 2011.

European Union (EU), Directive 95/46/EC, General Data Protection Regulation, 2016.

European Union (EU), European Cybersecurity Centres of Expertise Map: Definition and Taxonomy, Publications Office of the European Union, Lüxemburg, 2018.

HM Goverment, 2015 Information Security Breaches Survey, HM Raporu, Londra, İngiltere, 2015.

NIST SP 800-30, NIST Special Publication 800-30: Guide for Conducting Risk Assessments, 2012.

PWC, Turnaround and Transformation in Cybersecurity, PWC Raporu, Londra, İngiltere, 2016.

Yüksek Lisans Tezleri

Kılıç Berker, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Açısından Türkiye' de Hukuk Bürolarında Bilgi Güvenliği Yönetimi, Yüksek Lisans Tezi, Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim Anabilim Dalı, Ankara, Türkiye, Aralık-2019.

Große Christine, Towards an Integrated Framework for Quality and Information Security Management in Small Companies, Yüksek Lisans Tezi, Lulea Teknoloji

Üniversitesi, Bilgisayar Bilimi Bölümü, Elektrik ve Uzay Mühendisliği, Lulea, İsveç, 2016.

Mamers Tiiu, The Art and Science of Information Security Investments For Small Enterprise, Yüksek Lisans Tezi, Tallinn Teknoloji Üniversitesi, Bilgi Teknolojileri Okulu, Tallinn, Estonya, 2018.