T.C.

İSTİNYE ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

ÇALIŞANLARIN BİLGİ GÜVENLİĞİ FARKINDALIĞINA İLİŞKİN ALGILARI: BANKACILIK SEKTÖRÜNDE BİR ARAŞTIRMA

YÜKSEK LİSANS TEZİ

İŞLETME

AYKUT ALEMDAROĞLU

2020

T.C.

İSTİNYE ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

ÇALIŞANLARIN BİLGİ GÜVENLİĞİ FARKINDALIĞINA İLİŞKİN ALGILARI: BANKACILIK SEKTÖRÜNDE BİR ARAŞTIRMA

AYKUT ALEMDAROĞLU

Bu Tez, İstinye Üniversitesi İşletme Anabilim Dalı İşletme Yüksek Lisans derecesi için sunulmuştur.

2020

İSTİNYE ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

ETİK BEYAN

Yüksek Lisans tezi olarak sunduğum "Çalışanların Bilgi Güvenliği Farkındalığına İlişkin Algıları: Bankacılık Sektöründe Bir Araştırma" adlı çalışmanın, proje safhasından sonuçlanmasına kadar geçen bütün süreçlerde bilimsel etik kurallarına uygun bir şekilde hazırlandığını ve yararlandığım eserlerin kaynaklar bölümünde gösterilenlerden oluştuğunu belirtir ve beyan ederim.

AYKUT ALEMDAROĞLU

ÖZET

ÇALIŞANLARIN BİLGİ GÜVENLİĞİ FARKINDALIĞINA İLİŞKİN ALGILARI: BANKACILIK SEKTÖRÜNDE BİR ARAŞTIRMA

Aykut Alemdaroğlu
İşletme Yüksek Lisans
Danışman: Dr. Öğr. Üyesi Gülhan Kalmuk
2020

Günümüz dünyasında gelişen teknoloji ile birlikte, bankalardaki süreçlerin tamamına yakını dijital ortama aktarılmış durumdadır. Bu değişimin bir sonucu olarak teknoloji, tehditleri de beraberinde getirmiştir. Bir bankanın en değerli varlıkları arasında sayılabilecek bilginin bu tehditlere karşı korunması ve bankanın bilgi güvenliğinin sağlanması adına altyapı yatırımlarının yanı sıra insan faktörü de göz ardı edilmemelidir. Bu noktada çalışanların bilgi güvenliği farkındalığı, bilgi güvenliğinin sağlanmasında önemli bir rol oynamaktadır. Güvenli bir yapının kurulması, çalışanların farkındalık seviyelerinin yüksek olması ile mümkün olabilecektir.

Bu çalışmanın amacı bankacılık sektöründe çalışanların, bilgi güvenliği farkındalığı seviyesinin belirlenmesi ve geliştirilmesi gereken alanlarda önerilerin sunulmasıdır. Bu doğrultuda, Türkiye'de bulunan özel bir bankanın genel müdürlüğünde toplam 321 çalışana araştırma anketi elektronik ortamdan ulaştırılarak uygulanmıştır.

Bilgi güvenliği farkındalık ölçeğinin faktör analizi sonucunda Kişisel Verilerin Korunması, Saldırı ve Tehditler, Güvenlik Önlemi Alma ve Bilgi Güvenliği Bilinci olmak üzere 4 farklı alt boyut elde edilmiştir. Bilgi güvenliği farkındalığı alt boyutlarının sosyodemografik özelliklere göre fark yaratıp yaratmadığını tespit etmek için uygulanan bağımsız gruplar t testi ve Anova testi uygulanmıştır. Ayrıca değişkenler ile sosyodemografik özellikler arasında ilişkiyi analiz etmek için korelasyon analizi uygulanmıştır. Analiz sonucuna göre erkek çalışanların kadın çalışanlara göre daha fazla bilgi güvenliği farkındalığına sahip olduğu tespit edilmiştir. Görev süresi ile bilgi güvenliği farkındalığının alt boyutları arasındaki ilişki incelendiğinde ise anlamlı bir fark görülmemiştir. Bu çalışma ile banka çalışanlarının bilgi güvenliği farkındalıkları analitik olarak incelenerek, banka bilgi güvenliğine etkileri değerlendirilmiştir. Buna göre verimli bir bilgi güvenliği için farkındalık çalışmaları, tüm çalışanlar ve paydaşları kapsayacak şekilde gerçekleştirilmelidir.

Anahtar kelimeler: Bilgi, Bilgi Güvenliği, Bilgi Güvenliği Farkındalığı, Bankacılık, Banka Çalışanları

ABSTRACT

EMPLOYEES' PERCEPTIONS ON INFORMATION SECURITY AWARENESS: A RESEARCH IN THE BANKING SECTOR

Aykut Alemdaroğlu
Master Of Business Administration
Advisor: Asst. Prof. Gülhan KALMUK
2020

With the developing technology in today's world, almost all of the processes in banks have been transferred to digital media. As a result of this change, technology has brought threats in its train. In order to protect the information that can be considered as one of the most valuable resources of a bank against these threats and to provide the information security of the bank, the human factor should not be ignored as well as the infrastructure investments. At this point, employees' information security awareness plays an important role in providing information security. Establishing a safe structure can only be possible with employees' high level of awareness.

The aim of this study is to determine the level of information security awareness of employees in the banking sector and to put forward suggestions in areas that need to be improved. Accordingly, the research survey was transmitted electronically and applied to total of 321 employees at the general management of a private bank in Turkey.

As a result of the factor analysis of the information security awareness scale, 4 different sub-dimensions were obtained: Protection of Personal Data, Attacks and Threats, Taking Security Measure and Information Security Awareness. Independent groups t-test and Anova test were applied to determine whether sub-dimensions of information security awareness made a difference according to sociodemographic characteristics. Moreover, correlation analysis was applied to analyze the relationship between variables and sociodemographic characteristics. According to the results of the analysis, it was determined that male employees have more information security awareness than female employees. When the relationship between tenure and the sub-dimensions of information security awareness was examined, any significant difference was not found. With this study, information security awareness of bank employees was examined analytically and their effects on bank information security were evaluated. Accordingly, for an efficient information security, awareness studies should be performed to cover all employees and stakeholders.

Keywords: Information, Information Security, Information Security Awareness, Banking, Bank Employees

TEŞEKKÜR

Yüksek lisans öğrenimim süresince hem ders hem de tez aşamasında her zaman destek olan ve gece gündüz demeden yardımını esirgemeyerek tez araştırmama çok değerli katkılar sağlayan danışmanım Dr. Öğr. Üyesi Gülhan Kalmuk hocama, ders ve tez aşamasındaki desteklerinden dolayı Dr. Öğr. Üyesi Yasemin Torun hocama, tez çalışmamda kıymetli görüşlerini sunarak katkı sağlayan Özgüven Saymaz'a ve yüksek lisans eğitimim boyunca desteklerini hep hissettiğim arkadaşlarıma ve aileme,

Sonsuz teşekkürlerimi sunuyorum…

AYKUT ALEMDAROĞLU

İÇİNDEKİLER

ETİK BEYAN ..... **iii**
ÖZET ..... **iv**
ABSTRACT ..... **v**
TEŞEKKÜR ..... **vi**
İÇİNDEKİLER ..... **vii**
ŞEKİL LİSTESİ ..... **x**
TABLO LİSTESİ ..... **xi**
KISALTMALAR LİSTESİ ..... **xiii**
1. GİRİŞ **1**
2. GENEL BİLGİLER **4**
2.1. Bilgi Güvenliği 4
2.1.1. Bilgi Güvenliği Yönetimi 5
2.1.2. Bilgi Güvenliği İle İlgili Standartlar 8
2.2. Bilgi Güvenliğinin Tarihsel Gelişimi 10
2.3. Bilgi Güvenliği Prensipleri 12
2.3.1. Gizlilik 14
2.3.2. Bütünlük 15
2.3.3. Erişilebilirlik 15
2.4. Bilgi Güvenliğine Yönelik Yeni Nesil Tehditler 16
2.4.1. İstenmeyen Elektronik Posta (Spam) 18
2.4.2. Kötü Niyetli Yazılım (Malware) 19
2.4.3. Kötü Niyetli Kod (Malicious Code) 19
2.4.4. Aldatmaca (Hoax) 19
2.4.5. Zincir E-Posta (Chain E-Mail) 19
2.4.6. Casus Yazılım (Spyware) 20
2.4.7. Kimlik Hırsızlığı (Identity Theft) 20
2.4.8. Hizmet Aksatma (DOS) 20
2.4.9. Sahte Virüs Koruma Yazılımı 21
2.4.10. Oltalama (Phishing) 21
2.4.11. Sosyal Mühendislik (Social Engineering) 22
2.4.12. Siber Zorbalık (Cyberbullying) 23
2.5. Bilgi Güvenliğine Yönelik Alınması Gereken Önlemler 23

2.5.1. Bilgi Güvenliğine Yönelik Kurumsal Önlemler 24
2.5.2. Bilgi Güvenliğine Yönelik Kişisel Önlemler 26
3. BİLGİ GÜVENLİĞİ FARKINDALIĞI 27
3.1. Bilgi Güvenliği Farkındalığı Nedir? 27
3.2. Önemi Ve Etkileri 28
3.3. Farkındalık Çalışmaları 30
4. BANKACILIK SEKTÖRÜ VE BİLGİ GÜVENLİĞİ YAPISI 33
4.1. Bankacılık 33
4.1.1. Organizasyon Yapısı 34
4.2. Bilgi Güvenliği Yönetişim Yapısı 37
4.3. Bankacılık Bilgi Güvenliği Mevzuatları 39
5. ÇALIŞANLARIN BİLGİ GÜVENLİĞİ FARKINDALIĞINA İLİŞKİN BİR ARAŞTIRMA: BANKA ÖRNEĞİ 41
5.1. Araştırmanın Amacı 41
5.2. Araştırmanın Metodolojisi 42
5.2.1. Problemin Tanımı 42
5.2.2. Evren ve Örneklem 43
5.2.3. Araştırmanın Sınırlılığı 43
5.2.4. Veri Toplama ve Araçlarının Hazırlanması 43
5.2.4.1. Kişisel Bilgi Formu 43
5.2.4.2. Bilgi Güvenliği Farkındalık Ölçeği 43
5.2.5. Faktör Analizleri 43
5.2.6. Normallik Testi 46
5.3. Araştırmanın Bulguları ve Değerlendirilmesi 47
5.3.1. Demografik Özellikler 47
5.3.1.1. Cinsiyet Kriterine Göre Dağılım 47
5.3.1.2. Yaş Kriterine Göre Dağılım 48
5.3.1.3. Öğrenim Durumu Kriterine Göre Dağılım 49
5.3.1.4. Görev Türü Kriterine Göre Dağılım 50
5.3.1.5. Çalıştığı Birim Kriterine Göre Dağılım 51
5.3.1.6. Görev Süresi Kriterine Göre Dağılım 52
5.3.1.7. İnternet Kullanım Süresi Kriterine Göre Dağılım 53
5.3.2. Analiz Sonuçları 54

5.3.2.1. Korelasyon Testi Sonucu 54
5.3.2.2. Cinsiyet Değişkeni ile Yapılan Bağımsız Gruplar t-Testi Sonuçları 55
5.3.2.3. Yaş Gruplarına Göre Tek Yönlü Varyans (ANOVA) Sonuçları 57
5.3.2.4. Öğrenim Durumuna Göre Tek Yönlü Varyans (ANOVA) Sonuçları 59
5.3.2.5. Görev Türüne Göre Tek Yönlü Varyans (ANOVA) Sonuçları 62
5.3.2.6. Çalıştığını Birime Göre Tek Yönlü Varyans (ANOVA) Sonuçları 65
5.3.2.7. Görev Süresine Göre Tek Yönlü Varyans (ANOVA) Sonuçları 70
5.3.2.8. İnternet Kullanım Süresine Göre Tek Yönlü Varyans (ANOVA) Sonuçları 73
6. SONUÇ VE ÖNERİLER..... 76
KAYNAKLAR 83
EKLER..... 89

ŞEKİL LİSTESİ

Şekil 1. PUKÖ Döngüsü 6
Şekil 2. BG Yönetim Standartları Tarihçesi (Vural & Sağıroğlu, 2008, s. 511) 9
Şekil 3. Bilgi Güvenliği Prensipleri 13
Şekil 4. Gerçek Zamanlı Siber Tehdit Haritası (Kaspersky, 2020) 18
Şekil 5. Banka Taslak Organizasyon Şeması 36
Şekil 6. Bilgi Güvenliği Yönetişim Yapısı 38
Şekil 7. Cinsiyet Dağılım Grafiği 48
Şekil 8. Yaş Dağılım Grafiği 49
Şekil 9. Öğrenim Durumu Dağılım Grafiği 50
Şekil 10. Görev Türü Dağılım Grafiği 51
Şekil 11. Çalıştığı Birim Dağılım Grafiği 52
Şekil 12. Görev Süresi Dağılım Grafiği 53
Şekil 13. İnternet Kullanım Süresi Dağılım Grafiği 54

TABLO LİSTESİ

Tablo 1. Bilgi Güvenliği Farkındalığı Faktör Analizi 44
Tablo 2. Bilgi Güvenliği Farkındalığı Faktör Analizi – 2 44
Tablo 3. Normallik Testi 46
Tablo 4. Cinsiyet Kriteri Frekans Dağılımı 47
Tablo 5. Yaş Grubuna Göre Frekans Dağılımı 48
Tablo 6. Öğrenim Durumu Frekans Dağılımı 49
Tablo 7. Görev Türü Kriteri Frekans Dağılımı 50
Tablo 8. Çalıştığı Birim Frekans Dağılımı 51
Tablo 9. Görev Süresi Frekans Dağılımı 52
Tablo 10. İnternet Kullanım Süresi Frekans Dağılımı 53
Tablo 11. Korelasyon Tablosu 54
Tablo 12. Cinsiyet ve Kişisel Verilerin Korunması t-Testi Tablosu 56
Tablo 13. Cinsiyet ve Saldırı ve Tehditler t-Testi Tablosu 56
Tablo 14. Cinsiyet ve Güvenlik Önlemi Alma t-Testi Tablosu 57
Tablo 15. Cinsiyet ve Bilgi Güvenliği Bilinci t-Testi Tablosu 57
Tablo 16. Yaş Gruplarına Göre Kişisel Verilerin Korunması Boyutu ANOVA Testi Sonucu 58
Tablo 17. Yaş Gruplarına Göre Saldırı ve Tehditler Boyutu ANOVA Testi Sonucu58
Tablo 18. Yaş Gruplarına Göre Güvenlik Önlemi Alma Boyutu ANOVA Testi Sonucu 58
Tablo 19. Yaş Gruplarına Göre Bilgi Güvenliği Bilinci Boyutu ANOVA Testi Sonucu 59
Tablo 20. Öğrenim Durumu Gruplarına Göre Kişisel Verilerin Korunması Boyutu ANOVA Testi Sonucu 60
Tablo 21. Öğrenim Durumu Gruplarına Göre Saldırı ve Tehditler Boyutu ANOVA Testi Sonucu 60
Tablo 22. Öğrenim Durumu Gruplarına Göre Güvenlik Önlemi Alma Boyutu ANOVA Testi Sonucu 61
Tablo 23. Öğrenim Durumu Gruplarına Göre Bilgi Güvenliği Bilinci Boyutu ANOVA Testi Sonucu 62

Tablo 24. Görev Türü Gruplarına Göre Kişisel Verilerin Korunması Boyutu ANOVA Testi Sonucu 63
Tablo 25. Görev Türü Gruplarına Göre Saldırı ve Tehditler Boyutu ANOVA Testi Sonucu 64
Tablo 26. Görev Türü Gruplarına Göre Güvenlik Önlemi Alma Boyutu ANOVA Testi Sonucu 64
Tablo 27. Görev Türü Gruplarına Göre Bilgi Güvenliği Bilinci Boyutu Welch Testi Sonucu 65
Tablo 28. Çalıştığı Birim Gruplarına Göre Kişisel Verilerin Korunması Boyutu ANOVA Testi Sonucu 66
Tablo 29. Çalıştığı Birim Gruplarına Göre Saldırı ve Tehditler Boyutu ANOVA Testi Sonucu 67
Tablo 30. Çalıştığı Birim Gruplarına Göre Güvenlik Önlemi Alma Boyutu ANOVA Testi Sonucu 68
Tablo 31. Çalıştığı Birim Gruplarına Göre Bilgi Güvenliği Bilinci Boyutu Welch Testi Sonucu 70
Tablo 32. Görev Süresi Gruplarına Göre Kişisel Verilerin Korunması Boyutu ANOVA Testi Sonucu 71
Tablo 33. Görev Süresi Gruplarına Göre Saldırı ve Tehditler Boyutu ANOVA Testi Sonucu 71
Tablo 34. Görev Süresi Gruplarına Göre Güvenlik Önlemi Alma Boyutu Brown-Forsythe Testi Sonucu 72
Tablo 35. Görev Süresi Gruplarına Göre Bilgi Güvenliği Bilinci Boyutu ANOVA Testi Sonucu 72
Tablo 36. İnternet Kullanma Süresi Gruplarına Göre Kişisel Verilerin Korunması Boyutu Welch Testi Sonucu 74
Tablo 37. İnternet Kullanma Süresi Gruplarına Göre Saldırı ve Tehditler Boyutu ANOVA Testi Sonucu 74
Tablo 38. İnternet Kullanma Süresi Gruplarına Göre Güvenlik Önlemi Alma Boyutu ANOVA Testi Sonucu 75
Tablo 39. İnternet Kullanma Süresi Gruplarına Göre Bilgi Güvenliği Bilinci Boyutu Welch Testi Sonucu 76

KISALTMALAR LİSTESİ

BG: Bilgi Güvenliği

BSI: İngiliz Standartlar Enstitüsü

ITGI: Bilgi Teknolojileri Yönetişim Enstitüsü

ISACA: Bilgi Etki Alanları Denetim ve Kontrol Derneği

COBIT: Bilgi ve İlgili Teknoloji için Kontrol Hedefleri

CCTA: Merkezi Bilgisayar ve Telekomünikasyon Kurumu

ITIL: Bilgi Teknolojisi Altyapı Kütüphanesi

NIST: Ulusal Standartlar ve Teknoloji Enstitüsü

SP: Özel Yayın

OGC: Devlet Ticaret Ofisi

FISMA: Federal Bilgi Güvenliği Modernizasyon Yasası

MIT: Massachusetts Teknoloji Enstitüsü

DOS: Hizmeti engelleme saldırısı

DDOS: Dağıtılmış Hizmet Reddi

BGYS: Bilgi Güvenliği Yönetim Sistemi

BDDK: Bankacılık Düzenleme ve Denetleme Kurumu

BT: Bilgi Teknolojileri

KVKK: Kişisel Verilerin Korunması Kanunu

1. GİRİŞ

Dünya üzerinde kullanılan sistemlerin birçoğu bilişimle bağdaşarak teknolojik altyapıyla insanlığa hizmet etmeye devam etmektedir. İnternete bağlı cihaz sayısının gün geçtikçe artıyor olmasının karşılığı olan bu dijital dönüşümle birlikte hayatımızın her alanına dokunur hale gelmiştir. İçinde bulunduğumuz dijital çağın kazanımları elbette çok fazladır. Fakat ne yazık ki her şey göründüğü kadar da tozpembe değildir. Özellikle internet kullanımının artması arkasından birçok tehdidi beraberinde getirmiştir. Kötücül yazılımlar, fidye saldırıları, oltalama saldırıları ve var olan her türlü siber tehdit, bu dünyada kendine yer bulmuştur.

Teknoloji kullanımı gün geçtikte artmaktadır. Hangi teknolojiyi kullanırsak kullanalım hepsinin bir güvenlik boyutu mevcuttur. Bireysel güvenlikten kurumsal güvenliğe kadar süreçlerdeki her paydaş güvenlikle ilgili veya sorumluluğa sahiptir. Kullanıcılar o teknolojiyi güvenli bir şekilde kullanmak isterken, kurumlar ise kullanıcılara güvenli bir şekilde kullanılabilecek zemini oluşturmak durumundadır. Özellikle kurumlar için belirtilmelidir ki; o teknolojiyi güvenli bir şekilde kullanacak zemini hazırlayamazlarsa, finansal boyutlardan insan hayatına kadar birçok konuda olumsuz etkilerini görmek mümkündür.

En değerli varlıklarımızdan biri olan bilgiye gösterilen hassasiyet günümüzde oldukça yüksektir. Bunun bir getirisi olarak; büyük veya küçük ölçekli olması fark etmeksizin var olan bilgiyi koruma ihtiyacı ortaya çıkmaktadır. Bu ihtiyaca binaen Bilgi Güveliği kavramı önem kazanmıştır. Basit bir şekilde kelime anlamlarının karşılığını veren bu kavram, derinlemesine incelendiğinde ise karşımıza bazı unsurlar çıkmaktadır. Bu anlamda özellikle gizlilik, bütünlük ve erişilebilirlik unsurları Bilgi Güvenliğinin temelini oluşturmaktadır.

Özellikle bankacılık sektörüne bakıldığında, barındırdığı veriler itibariyle bilgi güvenliği sağlanması için uygulanması gereken süreçlerin benimsendiğini görmek mümkündür.

Bankaların bilgi sistemleri, günlük işlerinde bilgi teknolojisi kullanan çalışanlardan kaynaklanan çok çeşitli risklerden dolayı tehdit altındadır. Çalışanların ve bilgi sistemlerinin etkileşimi ile ilgili olan beklenmeyen olaylar, genellikle çalışanların bankaların bilgi güvenliği politikasına uymamaları ile ilgili toksik nedenlerden

kaynaklanmaktadır (Padayachee, 2012, s. 674). Özellikle bankalar için çok fazla risk vardır, çünkü bilgi güvenliği ihlali muazzam itibar kaybı ve operasyon açısından zararlara yol açabilir (Goldstein, Chernobai , & Benaroch , 2011, s. 607).

Bankaların kesintisiz hizmet sunması ve güvenilir olmak adına bu hizmeti güvenli bir şekilde sağlamak gibi bir amaca sahip olması sebebiyle, bilgi güvenliği konusunu var olan süreçlerin tamamına yaymaya çalıştığını görmekteyiz. Buna ek olarak, bilgi güvenliğinin organizasyon yapılarındaki konumu ve bu alanda yapılan yatırımların büyüklüğü bu durumu destekler niteliktedir.

Bankaların analog ortamlarında bulunan bilgilerin, dijital ortamlara geçişi büyük ölçüde tamamlanmış durumdadır. Yapılan yatırımlarla teknolojik olarak her ne kadar güvenlik önlemleri alınsa da bu zincirdeki en zayıf halkanın insan faktörü olduğu bilinmektedir. Son kullanıcı olarak da adlandırılan bu faktörü, bilgi güvenliği süreçleriyle ilgili bilgilendirmek ve olası tehditlere karşı bilinçlendirmek gerekmektedir. Tam da bu noktada karşımıza farkındalık kavramı çıkmaktadır. Özellikle son kullanıcının farkındalık boyutu, kurumun sağlamış olduğu güvenlik seviyesini doğrudan etkilemektedir. Unutmamak gerekir ki; her alanda olduğu gibi güvenlik açısından da en zayıf halkanız kadar güçlüsünüzdür. Bu sebeple kurum çalışanlarının farkındalık seviyelerinin arttırılması fazlasıyla dikkat çekilmesi gereken bir konudur.

Sürekli değişerek gelişim gösteren teknoloji sonucu ortaya çıkan dijital dünyada bilgi güvenliğinin önemi her geçen gün artmaktadır. Bilgi güvenliğini sağlamak içinde eldeki en önemli materyallerden bir tanesi farkındalıktır. Sektör tabanlı bakıldığında özellikle bankacılık, finans, enerji ve sağlık gibi yapı taşı sayılabilecek alanlarda bu farkındalık oluşturulması gerekmektedir. Özellikle bankacılık sektörü bu anlamda lokomotif görevi görmektedir. Karşı karşıya kaldığı bilgi güvenliğine yönelik tehditler ve riskler düşünüldüğünde, bilgi güvenliği farkındalığı oluşturmak bankalar için elzem bir durum olarak değerlendirilmektedir.

İletişim ve küreselleşme ile yeniden oluşan düzen içerisinde, kurumların sahip olduğu bilgilerin korunmasına yönelik mevcut güvenlik sistemlerinin geliştirilmesi, stratejilerin oluşturulması ve bilgi güvenliğinin farkındalığının oluşturulması için birçok farklı çalışmalar yapılmakta ve önlemler alınmaktadır (Genç, 2019, s. 3).

Özellikle bilgi güvenliği farkındalığı açısından bankalarda devamlılık içeren çalışmalar yapılmaktadır. Bankacılıkta yasal mevzuata uymak ve standartları yerine getirmek gerekmektedir. Dolayısıyla riskleri tespit etmek ve yönetmek, işleyişi sürekli iyileştirerek yönetebilmek adına kurum içerisinde çeşitli yöntemlerle bilgi güvenliği farkındalığı oluşturmak önemli süreçlerden bir tanesidir.

Bilgi güvenliğine dair farkındalığın artırılması banka faaliyetlerinin amaca uygun ve sorunsuz bir şekilde yürütülmesinde önemli bir role sahiptir (Öztemiz & Yılmaz, 2013, s. 90). Bankalar için müşterilerine karşı oluşturulması ve yükseltilmesi gereken en önemli olgulardan bir tanesi güven duygusudur. İnsanlar güven duydukları bankalar ile çalışmak isterler. Bu doğrultuda güveni zedeleyecek her türlü olay ise bankalar için ciddi kayıplara yol açmaktadır. Bu kayıpların yaşanmaması için olası tehditlere karşı alınması gereken bir takım önlemler alınmaktadır. Alınan bu önlemlerin sadece teknolojik veya sistemsel önlemlerden ibaret olması durumunda ise tam anlamıyla koruma sağlanmış sayılmamaktadır. Bu sistemleri kullanacak olan insan faktörünün bilgi güvenliği konusunda bilgisi önem arz etmektedir. Dolayısıyla bilgi güvenliği ve farkındalığı üzerine süreçler oluşturulmasıyla ortaya çıkan güvenli yapı neticesinde güven duygusu pekiştirilmektedir.

Etkili bir bilgi güvenliği farkındalığı, bankacılık sektöründe işleyişin süreklilik kazanmasına ve kurumsal itibarın artmasına yardımcı olmaktadır. Aynı zamanda kurumsal hedeflerin başarıyla gerçekleşmesine de katkı sağlamaktadır (Qureshi, 2011, s. 3). Bu bağlamda oluşturulan süreçler ve dokümanlar ile bankaların tüm faaliyetlerinde bilgi güvenliği anlayışı çerçevesinde işletilmesi desteklenmektedir. Bilgi güvenliği farkındalığı yüksek olan kurumlarda süreçlerin daha sorunsuz ilerleyeceği öngörülmektedir. Bu doğrultuda farkındalık seviyesinin arttırılması içinde çalışmalar yapılmaktadır.

Her sektörde ve kurumda olduğu gibi bankalarda da bilgi güvenliği ile ilgili riskler bulunmaktadır. Bu çalışma öncelikle bu risklerin farkına varılması, akabinde etkilerinin değerlendirilmesi ve bu riskleri azaltmaya yönelik alınacak önlemlerle ilgili yol gösteren bir kılavuz niteliği taşıması itibariyle fonksiyonel bir çalışma olacaktır. Bu çalışmanın, benzer alanda ve konulardaki araştırmalara referans olması beklenmektedir (Öztezcan, 2017, s. 4).

2. GENEL BİLGİLER

2.1. Bilgi Güvenliği

Çağımızda veri ve bilgi kavramları çok fazla ön plana çıkmıştır. Dijitalleşen günlük yaşantımızın her alanında varlığını hissettirir hale gelmiştir. Var olan bilginin bir taraftan toplanması ve saklanması kadar güvenliğinin sağlanması da önem arz ettiği için bilgi güvenliği de önemli bir husus haline gelmiştir.

İletişim kanallarımızın büyük bir çoğunluğu teknolojik altyapılar üzerinden sağlanmaktadır. Bu kanalların sayısı ve kullanım oranlarının artmasıyla birlikte, içerisinde barındırdığı kişisel veri boyutu da gün geçtikte artmaktadır. Hızla ilerleyen bu süreçte, iletişim kanalları üzerinde bilgi güvenliği sürecinin yürütülmesi hem kişisel hem de kurumsal açıdan değerlendirilmesi gerekmektedir.

Bu çalışma boyunca cümleler içerisinde fazlaca bulunacak olan iki kelime mevcuttur. Bilgi ve bu kelimenin kardeşi diyebileceğimiz veri kelimesi her ne kadar birbirine yakın dursa da aslında farklı anlamlara sahiptirler. Aralarındaki farkı kavramak, yapılacak yorum ve değerlendirmelerde önem arz etmektedir.

Özünde birbirine bağlı olan bu iki kelime farklı anlamlar içermektedirler. En basit tanımıyla bilgi işlenmiş veridir. Aralarındaki farkı basit tanımdan öte detaylıca anlamak ilgili süreçleri doğru değerlendirmek açısından önemlidir. Bu çerçevede verinin tek başına anlamsız olduğunu ve verilerin toplanıp işlenmesiyle anlamlanarak bilgiyi oluşturduğunun altını çizmek gerekir. Bilgisayar sistemleri için düşünürsek veri bu sistemler için girdi, bilgi ise bu girdinin çıktısı olarak değerlendirilmektedir. Oluşum şekli itibariyle bilgi veriye bağlı olmakta birlikte veri bağımsızdır. Anlamsız ve ham olarak düşünebileceğimiz verinin karşısında bilgi anlamlı ve bir ürün niteliği taşıyan bir şekilde durmaktadır (Limenya, 2015).

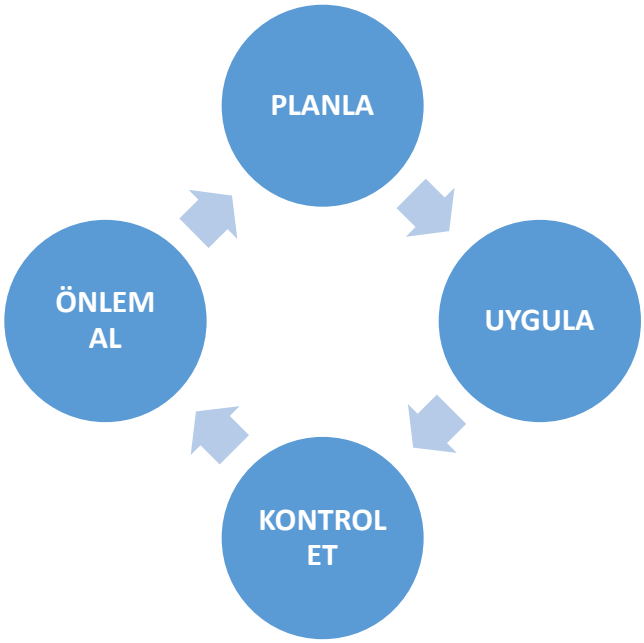
Bilginin korunması konusunda özellikle yetkisiz erişime izin verilmemesiyle birlikte bilginin değiştirilmesi, yok edilmesi ve ifşa edilmesi mutlaka kontrol altına alınmalıdır. Bilgi güvenliğinin bu çerçevede; gizlilik, erişilebilirlik ve bütünlük prensiplerine göre değerlendirilmesi gerekmektedir (Durankaya & Saymaz, 2019, s. 24).

Bilginin temelinde bulunan veriyi detaylandırırsak karşımıza kişisel veri kavramı çıkmaktadır. Kişisel veri, KVKK'da "*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" şeklinde tanımlanmaktadır (KVKK, 2016). Yalın haliyle kişisel veri, kişiyi adresleyen her türlü bilgiyi kapsamaktadır. Bu konuda önemli olan noktalardan bir tanesi kişisel verinin doğru olması gibi bir zorunluluğun olmamasıdır. Kişiyi adresliyorsa yanlışta olsa bu kişisel veri olarak değerlendirilir.

2.1.1. Bilgi Güvenliği Yönetimi

Bilgi güvenliği yönetimi kurumlar açısından değerlendirildiğinde karşımıza bir yönetim sistemi olarak çıkmaktadır. BGYS, kurumsal bilgi güvenliğinin sağlanmasında rol alan insanları ve süreçleri kapsamaktadır. Özellikle bilgi sistemlerini içine alarak üst yönetim tarafından desteklenmesi gerekmektedir. BGYS amaçları arasında bilgi varlıklarını korumak, yeterli ve orantılı güvenlik kontrollerini sağlamak vardır. Detaylandırırsak bu BGYS kurumsal yapıyı, kurum politikalarını, sorumlulukları, uygulamaları, süreçleri ve kaynakları içermektedir. Fiziksel ve elektronik bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik açısından koruyan BGYS, performans iyileşmesi sağlayarak bilgi güvenliği risklerini azalmasına ve iş sürekliliğe destek vermektedir (Durankaya & Saymaz, 2019, s. 25).

BGYS çerçevesinde ele alınması gereken yaklaşımların en başında PUKÖ döngüsü (Şekil 1) olarak bilinen yaklaşım gelmektedir. Planlama, uygulama, kontrol etme ve önlem alma maddelerinin baş harflerinden oluşan kısaltmasıyla bilinen bu döngü, BGYS'nin uygulanmasında önemli bir rol almaktadır.



Şekil 1. PUKÖ Döngüsü

İyileştirme Modellerinin kökleri, çok uzun yıllardır gelişen bilimsel yöntem ve bilim felsefesinde yatmaktadır. PUKÖ döngüsünün serüveni ise bu süreçte Dr. W. Edwards Deming'in 1950'de Japonya'daki konferansıyla başladığı bilinmektedir. Gelişiminden bu yana modelle ilgili deneyimler bazı sonuçları doğurmaktadır. Bunlardan bir tanesi döngü, her türlü kuruma ve kurum içerisindeki grup ve seviyeye uygulanabilir olmasıdır. Bilgi teorisi tarafından yönlendirilen iyileştirme yöntemlerinin ve araçlarının uygulanması için bir çerçeve sağlar:

- Döngünün ilk adımı olan planlamayı teoriye dayalı olmaya teşvik eder.
- Teori, öğrenmenin temelini oluşturan uygun sonuçlara yol açar.
- Sorular, kullanılan teoriye göre soruları cevaplamak için gerekli verileri, yöntemleri ve araçları belirlemede kullanıcıya yol gösteren tahminlere yol açar.
- Tümdengelim ve tümevarım şeklinde öğrenmenin yinelemeli öğrenme sürecine destek sağlar.

Bu sürecin öğrenilmesiyle projeye sağlanan uyum artmaktadır. Kişilerin harekete geçmesini sağlayarak faydalı sonuçlar doğuracağı ve kendilerini daha güçlü

hissedecekleri bir yol sağlar. Bu gücün ise ekip çalışmasıyla daha üst seviyelere çıkacağını ve böylece iyileştirme çalışmalarının kolaylaşacağını gösterir. (Moen & Clifford, 2009, s. 6)

PUKÖ döngüsüsün aşamaları genel hatlarıyla aşağıdaki şekilde detaylandırabiliriz (Durankaya & Saymaz, 2019, s. 26):

1) Planlama

Öncelikle amaç ve hedef belirlenmelidir. Bu amaç ve hedefleri gerçekleştirmek için ikinci faz olan uygulama planı hazırlanır. Bu hazırlık sırasında bazı sorulara cevap bulunması göz önünde bulundurulur. Bu sorular; ne yapılacak, nasıl yapılacak, nerede yapılacak, ne zaman yapılacak, kim yapacak ve kaynaklar ne olacak şeklindedir. Bu aşamada yapılan çalışmaların performansını ölçmek önem arz edeceğinden, performans göstergelerini hazırlamakta gerekmektedir.

2) Uygulama

Bu adımda ilgili taraflar bilgilendirilmektedir. Planlanan faaliyetlerin gerçekleştirilmeye başlandığı bu aşamada uygulamaya ilişkin kayıtlar tutulur ve kanıtlar oluşturulur.

3) Kontrol etme

Bu adımda ölçme, analiz ve değerlendirme çalışmaları yapılmaktadır. İzlenen uygulamaların amaç ve hedeflere uygun olup olmadığı kontrol edilir. Planlama kısmında belirlenen performans göstergeleri doğrultusunda gerekli ölçümler yapılarak amaç ve hedeflere ulaşma düzeyinin belirlenmesi sağlanır. Böylece planlanan ve hedeflenen ile gerçekleşen ve uygulanan arasındaki değişkenlik gösteren durumlar veya uygunluklar kontroller edilir.

4) Önlem alma

Tespit edilen sapmalar sonrasında bu sapmaların düzeltilmesi için gerekli faaliyetler belirlenir.

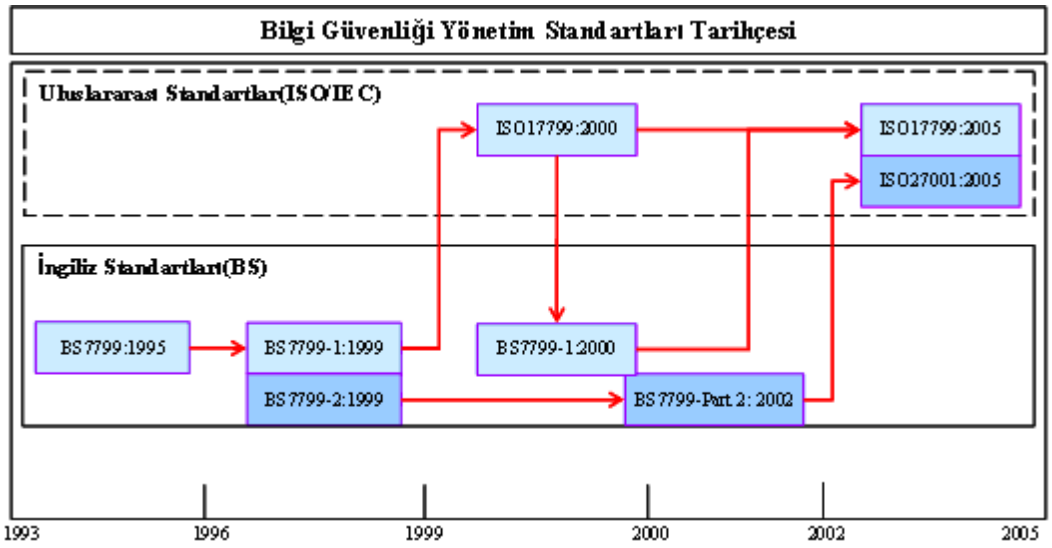
2.1.2. Bilgi Güvenliği İle İlgili Standartlar

Bilgi güvenliği yönetiminin temel amacının süreç iyileştirmeyle ilgili olduğundan bahsetmiştik. Uzun yıllardır bu alanda gerçekleştirilen çalışmalar süreçlerin daha verimli hale gelmesi ve iyileştirmelere katkı sağlaması adına bazı sonuçlar doğurmuştur. Bunların sonucunda ise bazı standartlar ortaya çıkmıştır.

Bilgi güvenliğine karşı ortaya çıkan yeni tehditlerin varlığı, kullanılan sistemlerde oluşan güvenlik açıkları ve insan unsurunun kontrolü gibi süreçler, bilgi güvenliği yönetimi için takip edilmesi gereken önemli unsurlardır. Gerçekleştirilen çalışmalar bazı standartlar doğurmuştur. Bu çerçevede BSI iki kısımda yayınladığı BS-7799 standardını oluşturmuştur. Bu standardın ilk kısmı 1995 yılında BS7799-1 adında, ikinci kısmı ise 1999 yılında BS7799-2 adında standartlar arasında yerini almıştır (Vural & Sağıroğlu, 2008, s. 511). BSI bu alanda öncü kuruluşlar arasında sayılmaktadır.

Tarihsel olarak standartlar genel olarak birbirinden dönüşerek ortaya çıkar. Bunun bir örneği olarak ISO standardı 2000 yılında BS7799-1 den faydalanılarak ISO/IEC-17799 adıyla yeni bir standart haline gelmiştir. Bu akış içerisinde ISO standartlar üzerinde geliştirmeyi sürdürmüş ve 2005 yılında ISO/IEC-17799 standardının ikinci sürümü niteliğinde ISO/IEC-17799:2005 adıyla tekrar yayınlamıştır. ISO tarafında günümüzde de hala geçerliliği olan ISO/IEC:27001 standardının doğuşu ise temelde BS7799-2 standardının üzerine inşa edilmesiyle ortaya çıkmıştır (Wikipedia, 2010).

Bilgi güvenliği yönetimi standartları tarihsel olarak incelendiğinde, zaman içerisinde birbirinden dönüşerek ortaya çıktıkları görülmektedir. Bu akışı ifade eden görsel Şekil 2' deki gibidir.



Şekil 2. BG Yönetim Standartları Tarihçesi (Vural & Sağıroğlu, 2008, s. 511)

Birbirlerinden esinlenilen ve yapılan ekleme çıkarma veya değişikliklerle ortaya çıkan standartlar dışında bazı kuruluşların özel çalışmalarıyla ortaya çıkan ve uluslararası kabul görmüş standartlarda mevcuttur. Bunlardan bazıları; ISACA tarafından yayınlanan COBIT, CCTA tarafından geliştirilen ITIL ve Uluslararası Standartlar ve Teknoloji Enstitüsü (NISP) tarafından yayınlanan NIS SP 800 standartlarıdır.

COBIT

COBIT, BT süreçlerinden kaynaklı doğan risklerin kontrol edilmesiyle birlikte iş akışını desteklemek için ortaya çıkan bir yöntemdir. COBIT için belgelendirme yetkisi ISACA kuruluşuna bağlı ITGI tarafından gerçekleştirilir. COBIT oluşturulurken ortaya çıkan düşünceler, ISO güvenlik standartlarını adresleyen bir yapıya sahiptir (BSI, 2008).

COBIT, süreçlerin ilerlemesinde kurumların önüne bazı hedefler koymaktadır. Bu hedefler yönetimsel çerçevenin de belirlenmesinde önemli rol alır. Burada altı çizilmesi gereken bir nokta vardır. COBIT hedef belirlerken, bu hedeflerin nasıl gerçekleştirileceği konusunda bir yol işaret etmez. Bu noktada ortaya koyulan hedeflerle, katma değeri yüksek olan projelerin seçilmesi sağlanarak kuruma katkı sağlamaktadır.

ITIL

ITIL, özetle BT hizmet yönetimi alanındaki birden fazla referansın bir araya gelmesinden oluşmaktadır. İngiltere devletine bağlı OGC tarafından oluşturulan ITIL standardı, BT tarafında sağlanan hizmetlerin yönetiminin tamamını kapsamaktadır. Bu noktada değerlendirilecek BT servis sağlayıcısı kurum içinden bir bölüm olabileceği gibi kurum dışı bir destek sağlayıcısı da olabilmektedir. ITIL standardının amacı, BT içerisinde verilen hizmetlerin verimliliğini arttırmak, maliyeti en uygun hale getirmek ve süreçleri bu doğrultuda iyileştirmektir (BSI, 2008).

NIST SP 800

1990 yılında NIST tarafından SP adı altında 800 serisi olarak yayınlanan standart olarak bilinmektedir. Bu standart, daha çok sistem güvenliği alanıyla ilgili bilgilere odaklıdır. İçeriğinde, NIST kuruluşunun siber güvenlik faaliyetlerine ilişkin yönergeleri, önerileri, teknik özellikleri ve yıllık raporları bulunmaktadır. SP 800 olarak bilinen serinin amacı, Amerika Birleşik Devletleri hükümetinin siber güvenlik alanındaki ihtiyaçlarını karşılamak ve desteklemektir. Aynı zamanda FISMA yasası kapsamında da geliştirilmeye devam etmektedir. İçerdiği raporlarla Amerika Birleşik Devletleri özelinde gerçekleştirilen bilgi güvenliği araştırmaları, sosyal yardım faaliyetleri, kurumlar arası işbirlikleri gibi konular hakkında bilgi vermektedir (NIST, 2018).

2.2. Bilgi Güvenliğinin Tarihsel Gelişimi

Bilginin korunmasına ilişkin gelişim süreci, zaman zaman yaşanılan olaylarla gerçekleşebildiği gibi bilirkişiler, araştırmacılar, topluluklar, kurumlar ve hatta devlet aracılığı ile de gelişim gösterebilmektedirler. Özellikle tarihsel gelişimi araştırdığımızda, bilginin korunmasına olan ihtiyacın pekte günümüze özgü bir durum olmadığını görmekteyiz.

Geçmişte, bilgi güvenliği adı altında olmasa da ülkelerini yöneten kişiler bile bu tedbire önem verdiklerini kullandıkları yöntemlerle göstermişlerdir.. Padişahların saraydan saraya gönderdikleri mektupları korumak adına mühürledikleri veya ağızlarını yapıştırdıkları bilinmektedir. Öyle ki Roma dönemi askeri komutanlarından Jül Sezar'ın kullandığı o günün şartlarına göre özel bir şifreleme yönteminin diğer

kişiler tarafından deşifre edilemediği tarih kitaplarındaki yerini almıştır. Sezar ile özdeşleşen bu yönteme ise "Sezar Şifreleme Tekniği" denilmektedir. Bu şifreleme tekniği, belli bir zaman sonra dönemin tanınmış kişilerinden Arap Hezarfen Al-Kindi tarafından kırılmış ve günümüzde de kullanılan şifreli analiz tekniği olarak bilinen frekans analizi yönteminin doğuşuna neden olmuştur. Bir diğer örnekte Eski Mısır zamanına ait kullandıkları özel alfabelerle yazışmalarının başka kişiler tarafından anlaşılmasının önüne geçerek önlem aldıkları bilinmektedir. Bu alfabenin çözümlenmesi ise 19. yüzyılın başlarında Fransız Jean-François Champollion tarafından gerçekleştirilmiştir. Yüz yıllar öncesinde bile, günümüzde olduğu gibi bilgiyi korumanın çeşitli yöntemlerle sağlandığı, çoğaltabileceğimiz bu gibi örneklerle görülmektedir (Güngör, 2015, s. 25).

Geçmişte bilgi güvenliğini sağlamak için kullanılan yöntemler, günümüz şartlarında belirlenen çözümlerin arkasında yatan analiz, ihtiyaçların belirlenmesi veya altyapıların hazırlanması gibi süreçler olmadan oluşturulmuştur. Tüm bunlar olmadığı için ilkel yöntemler gibi görünse de aslında o günün şartları düşünüldüğünde bazen önemli sonuçlarda doğurabilmektedir.

Dünya savaşlarının sonuçlarına yön verecek derecede etkiye sahip olabildiği örneklerden bir tanesi de Enigma Şifreleme Sistemi'nin kırılması olayıdır. Enigma, Nazi Almanya'sı tarafından iletişimin şifrelenmesi ve şifreli iletişimlerin çözümlenmesi için kullanılan ve o döneme göre güçlü algoritması olduğu bilinen bir makinadır. İkinci dünya savaşı öncesinde Almanya'nın savaşı kaybetmesinde rolü olduğu bilinmektedir. Şifreleme üzerine çalışan bilim adamları tarafından çözülmesinin ve savaşa yön vermesinin ardından bilgi güvenliği gelişiminde dönüm noktası olarak kabul edilmiştir (Güngör, 2015, s. 26).

Yakın tarihimizde bilgi güvenliği tarihine yeni terimler katacak olaylar yaşanmaya devam etmiştir. Bu bağlamda, 1960'lı yıllarda güvenlik alanın ilk bilgisayar korsanları ortaya çıkmıştır. Amerika'da MIT'te yaşananlar sırasında elektrikli trenler üzerinde analiz ve çalışma yapan kişiler trenlerin farklı şekilde çalışmasını sağlamıştır. Daha sonra aynı işi bilgisayarlar üzerinde de yaparak Korsan (Hacker) kavramının oluşmasını sağlamışlardır (Shinder & Tittel, 2002, s. 128).

Bilgisayarların insanların hayatına girmesi yeni bir dönüm noktası olarak değerlendirilebilir. Bilgi çağı olarak adlandırılan bu dönemde insanlar bilgi güvenliği kavramını duymaya başlamışlardır. Bilgi güvenliğinin kapsadığı alan geçmişte daha çok ülkesel veya askeri kaynakların güvenliği ile sınırlı olsa da, günümüzde bilgisayar kullanımının yaygınlaşmasıyla hem kullanılan alanlar hem de kullanılan teknik ve çözümler itibariyle modern bilgi güvenliği kavramının oluşmasına katkıda bulunmuştur (Güngör, 2015, s. 27).

Bilgi güvenliği gelişim süreci tarihsel altyapıya sahiptir. Sadece gelişen teknolojisiyle hayatımıza girmiş bir olgu değildir. Güvenliğin sağlanması için yapılan çalışmalar zamanımızda daha kolay olmasına rağmen, geçmiş dönemlerde insan ve toplum gibi daha basit olgular düşünülerek gelişim sağlamıştır. Daha geniş çerçeveden değerlendirecek olursak; bilgi güvenliği alanında yapılan incelemelerde her dönem toplumsal ve kişisel güvenlik ihtiyaçları için gerekli çalışmalar yapıldığını; farklı yol ve yöntemler kullanılarak geliştirilerek günümüze kadar geldiğini de söyleyebiliriz.

Özellikle internet kullanımının artmasıyla bilgi güvenliğine olan ihtiyaçta artmıştır. Bilgisayar kullanımının insan hayatına daha çok girmesi de bu gelişim sürecine katkıda bulunmuştur. Bu süreçte, bilginin kişisel veya kurumsal olarak korunmasının dışında, bilgiyi yasa dışı faaliyetlerde kullanmak isteyenlerde ortaya çıkmıştır. Bir tarafın haksız kazanç elde etmek istediği, bir tarafında korumak için çabaladığı bir ortamda, bilgi güvenliğinin önemi de artmaktadır (Çöp, 2017, s. 10).

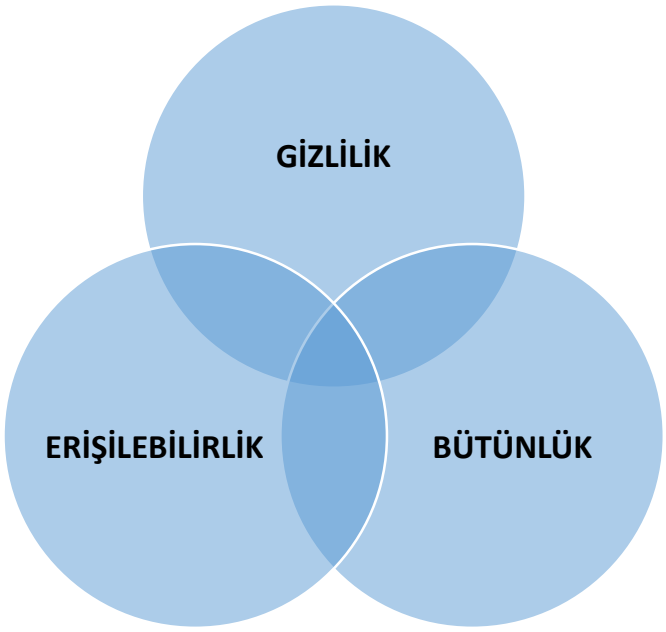
Gelişim süreci göstermiştir ki; bilgi güvenliğinin bugün ki önem arz eden halini almasının, üzerine bu denli araştırma yapılmasının ve çalışılmasının tarih boyunca bir karşılığı olmuştur. Özetle; insanoğlunun yaşam şekli ve şartları değişse de, bilgiyi koruma ihtiyacı hiç bitmediği gibi artarak devam etmektedir.

2.3. Bilgi Güvenliği Prensipleri

Bilgi güvenliği, gelişim süreciyle birlikte yapısında birçok unsur barındırmaktadır. Her ne kadar bilgi güvenliği prensipleri denilince akla gelen ilk unsurlar gizlilik, bütünlük ve erişilebilirlik olsa da, bunların dışında da bazı unsurlar vardır. Bu unsurları kimlik sınaması, yetkilendirme, kayıt tutma, süreklilik, güvenilirlik, inkâr edilememe şeklinde sıralayabiliriz.

Sorumluluk, erişim denetimi, güvenilirlik ve emniyet unsurları bilgi güvenliğinin yan unsurları olarak kabul edildiği gibi temel unsurları da göz önünde bulundurduğumuzda tamamının gereklilikleri yerine getirildiğinde gerçek anlamda bilgi güvenliği sağlanmış olarak kabul edilebilmektedir. Bu unsunlar birbirini tamamlayan nitelikte oldukları için mutlaka göz önünde bulundurulmalıdır. Bazılarının eksikliği, süreçlerde güvenlik açısından olumsuz sonuçlara yol açabilmektedir. Tüm bu unsurları değerlendirirken bu çerçeveyi önemsemekte fayda vardır (Canbek & Sağıroğlu, 2006, s. 170).

Bilgi sahip olunan en değerli varlıklar arasında olduğu düşünüldüğünde, belirtilen unsurlar çerçevesinde korunmasının sağlanması gerekmektedir. Bilgi güvenliği alanındaki standartlar özelinde değerlendirildiğinde bu unsurlar çerçevesinde korunmanın sağlanması istenmiştir. "*Bilgiye olabilecek yetkisiz erişimlerin engellenmesine gizlilik, yetkili erişimin sonucunda kendine özgü bilgi mahremiyetinin korunmasına bütünlük, ihtiyaç haline kolay ulaşılabilir olması erişilebilirlik denir.*" Bilginin korunması bu üç temel unsur üzerinde, teknik ve diğer açılardan alınan önlemlerle sağlanmaktadır (Şahinaslan, Kantürk, Şahinaslan, & Borandağ, 2009, s. 597).



Şekil 3. Bilgi Güvenliği Prensipleri

2.3.1. Gizlilik

Bilgi güvenliğinin sağlanmasının en temelinde gizlilik ilkesi yatmaktadır. Gizlilik aynı zamanda elimizdeki verinin değerini arttıran bir unsur olduğunu söyleyebiliriz. Var olan veri üçüncü taraflarla paylaşılacaksa bu paylaşımın bizim kontrolümüzde gerçekleşmesi beklenir. Tam bu noktada eğer bu paylaşım kurum veya kişilerin kontrolünde sağlanmıyorsa, para, itibar ve dolayısıyla değer kaybına neden olabilmektedir. Bu çerçevede değerlendirildiğinde bilgi güvenliğinin sağlanmasındaki en temel unsur olan gizlilik ilkesinin önemi ortaya çıkmaktadır. Kurumlar veya kişiler gizlilik unsuru çerçevesinde gereken önlemleri almaları gerekmektedir.

Bir başka ifadeyle gizlilik, bilginin yetkisiz kişilerin erişimine izin verilmemesinin ve süreçler içerisinde yetkisiz bir şekilde kullanıma sunulmamasının sağlanması olarak ifade edilebilir. Bu unsurun yerine getirilmesi için kullanılan yöntemlerden bir tanesi de şifreleme tekniklerdir. Şifreleme ile birlikte, erişim yetkisi olmayan tarafların bilgi veya verilere erişimini önlemek amacıyla kullanılmaktadır (Gelbstein & Kamal, 2002, s. 16).

Gizlilik ilkesi, bilginin disk, cd, dvd, teyp gibi fiziki veya sanal ortam üzerinde aktarımı gerçekleşirken mutlaka sağlanması gerekmektedir. Aktarılan bilgi, bazılarının yetkileri olmamasına rağmen erişmek için hedef haline gelmiş olabilir. Bu durumlarda bilgiye erişmek için birçok yol mevcuttur. Bu süreçlerde sosyal mühendislik veya çok daha basit farklı yöntemlerle yetkisiz kişiler hedeflerindeki bilgilere ulaşabilmektedir (Tekerek, 2008, s. 133).

Bu çerçevede karşımıza çıkan tehditlere karşı alınabilecek bazı önlemler vardır. En çok kullanılan yöntemlerden bir tanesi veri şifrelemedir. Artık standart olarak kullanıcı parolaları olsa bile günümüzde iki faktörlü doğrulama yöntemi de sıkça kullanılmaktadır. Bununla birlikte biyometrik doğrulama yöntemleri de bu kapsamda çözüm önerileri arasında bulunmaktadır. Bu ve bunun gibi sayısını arttırabileceğimiz bazı yöntemleri kullanarak, hem gizlilik ilkesinin gereklilikleri yerine getirilmiş olup hem de bilginin yetkisiz kişilerce ele geçirilmemesi için gerekli önlemler alınmış olunmaktadır (Rouse, 2019).

2.3.2. Bütünlük

Bütünlük ilkesi, verilerin yetkisi olmayan kişilerce değiştirilmesi, yok edilmesi ve kaybolmamasının engellenmesini ifade eder. Bütünlük ilkesine dair uygulama alanları, veri değerlerine olan güvenle birlikte bu değerlerin temsil ettiği bilgiler ve değerlerin kaynağının güvenilirliği gibi ele alınması gereken yönlere sahiptir (Gelbstein & Kamal, 2002, s. 15).

Var olan bilginin eksiksiz, doğru ve tutarlı olması gerektiğini ifade eder. Bilginin bütünlüğünün bozulması durumunda bilinçli veya bilinçsiz bir şekilde gerçekleştirilmiş olmasının bir önemi yoktur. Bu noktada kontrol mekanizması kurulması adına sorumluluk yetkilendirilmelidir. Kurum içerisinde politika ve dokümantasyonlarla bilginin bütünlüğünün sağlanması belirtilmeli ve gerekli kontroller belirli dönemlerle gerçekleştirilmelidir (Ganbat, 2013, s. 4).

Kısa tanımıyla bütünlük, verilerin yetkisiz bir şekilde değiştirilmemesi gerektiğini ifade etmektedir. Bir bilgisayara virüs bulaştırılması, çalışanın bordro bilgilerine ulaşarak ücret değişikliği yapması, bir kullanıcının bir internet sitesini tahrip etmesi, bir kişinin yanlışlıkla ve bilerek verileri ortadan kaldırması gibi durumlarda bütünlük ilkesi ihlal edilmiş sayılmaktadır (Keung, 2014, s. 1).

2.3.3. Erişilebilirlik

Erişilebilirlik ilkesi, bir sistemin veya belirli bir sistem kaynağının yetkili taraflarca istendiğinde, sisteme uygun performans özelliklerine göre erişilebilir ve kullanılabilir olması şeklinde ifade edilir (Gelbstein & Kamal, 2002, s. 15).

Bilginin, her zaman hazır bulundurulması gerekmektedir. Hizmetin devamı veya sistemin çalışma amacı doğrultusunda ihtiyaç halinde kullanılabilmesi sağlanmalıdır. Tüm bilgi işlem sistemleri, bilgileri depolayan ve işleyen sistemler, güvenlik tarafında kullanılan ürünler, kontrol mekanizmaları ve bilgiye erişim sağlayan sistemlerin tamamının aktif ve sorunsuz bir şekilde çalışması gerekmektedir. Erişilebilirlik seviyesi yüksek olan sistemler, zaman zaman meydana gelen elektrik, donanım arızası veya güncellemelerden kaynaklı sistem kesintilerini önleyici niteliğe sahip olabilmektedir. Örnek olarak, sistemlerde erişilebilirlik tam anlamıyla sağlanmış

olursa, DOS tehditlerine karşı bir önlem olarak algılanabilmektedir (Keung, 2014, s. 1)

2.4. Bilgi Güvenliğine Yönelik Yeni Nesil Tehditler

Bilgi güvenliğini sağlaması amacıyla yapılan çalışmalar gün geçtikçe gelişim göstermektedir. Aslında bunun altında yatan sebep mevcut tehditlerinde aynı doğrultuda gösterdiği gelişimdir. Tarihsel gelişim sürecinde de gördüğümüz bilgi güvenliğe yönelik tehditler, günümüzde de mutasyona uğrayarak sürekli varlığını sürdürmektedirler.

Gelişim gösteren bu tehditlerin kaynakları farklılık göstermektedir. Bu doğrultuda var olan tehditleri kaynaklarına göre gruplanması mümkündür. Bilgi güvenliğine yönelik tehditleri yazılım kaynaklı tehditler, fiziksel tehditler ve kullanıcı kaynaklı tehditler olmak üzere üç ana başlık altında inceleyebiliriz. Gruplandırdığımız bu tehditleri ve alt kırınımlarının detayları hakkında bilgi sahibi olmak, hem bilgi güvenliğinin sağlanması hem de farkındalık oluşturulması adına önem arz etmektedir (Taner, 2019, s. 23). Bu doğrultuda tehditlerin nitelikleri bakımında değerlendirilerek benimsenmesi ve alınacak önlemlerin bu bilinçle oluşturulması gerekmektedir.

Saldırı türleri özelinde çeşitli sınıflandırmalarda mevcuttur. Tehditler, sayısına veya kullanılan araçlara göre sınıflandırılabilmektedir. Sayısına göre sınıflandırılan tehditlerde; solo ve çoklu saldırı seçenekleri bulunmaktadır. Adından da anlaşılacağı üzere solo saldırılar tek kişi tarafından yapılmaktadır. Çoklu saldırılar ise toplu yapılan saldırı çeşitlerini kapsamaktadır. Örnek vermek gerekirse; yetkisiz erişim solo saldırı olarak değerlendirilmekte olup, zincir elektronik posta saldırısı çoklu saldırı kategorisine girmektedir (Kapanoğlu, 2016, s. 19). Bu sınıflandırma çeşidinde kullanılan araçlara göre de benzer örnekler verilebilir. Bu noktada önemli olan, tehditlere karşı alınabilecek önlemleri bu sınıflandırmalardan faydalanarak belirlemektir.

Yeni nesil tehditler arasında siber saldırıların önemli bir yeri vardır. Teknolojik gelişmelerle birlikte artan güvenlik riskleri şirketler için göz ardı edilemez bir noktaya gelmiştir. Maruz kalınan siber saldırılar karşısında maddi manevi kayıplar yaşamaktadır. Birçok sektörde artarak devam eden bu saldırılar özellikle en çok havacılık, finans ve telekomünikasyonu hedef almaktadır. Siber saldırılar birçok

şekilde gerçekleştirilebilmektedir. Ülkemizde son dönemde özellikle sahte mail yoluyla çok sayıda siber saldırı gerçekleştiği bilinmektedir. Saldırganlar bu yöntemde oluşturdukları sahte bir e faturayı kullanıcıya mail yoluyla gönderiyor. Fatura tutarının yüksek olmasıyla dikkat çekici hale getirilerek kullanıcının belirtilen linke tıklaması hedefleniyor. Belirtilen linkte bulunan zararlı içerikli dosya, tıklamayla birlikte bilgisayar inen dosya çalıştırıldığında zararlı, bilgisayardaki tüm dosyalara ulaşabilir hale geliyor. Bunun gibi yaşanan örnekler sonucunda şahıslar ve şirketler zor durumda kalabilmektedir. Siber fidye saldırısı olarak da bilinen bu tip olaylara maruz kalanlarda kalmayanlarda bu saldırıların artarak devam edeceği düşüncesine sahip olduğu bilinmektedir. Yapılan araştırmalar ise Türkiye'nin siber fidye saldırılarında Avrupa'da birinci, uluslararası sıralamada ise altıncı olduğunu göstermektedir. Bu sıralama ülkemizde bu saldırı tipinin ne kadar fazla olduğuna işaret etmektedir. Dolaysıyla bu tehditlerden korunma yolları üzerinde de fazlaca durulması gerekmektedir (ZeroSecond, 2020).

Her zaman dile getirilen durumlardan bir tanesi, kurumların varlıklarını elektronik ortama aktarmasıyla ve süreçler teknolojiyle birleştikçe var olan tehditlerde aynı oranda artış göstermesidir. Özellikle internet uygulamaları, zafiyet açısından düşünüldüğünde güvenlik derecesi düşük olmasından dolayı güncel gelişmelerin en çok yaşandığı alan olarak karşımıza çıkmaktadır. Her bir şirket hatta şahıs için kolay ulaşılabilir bir mecra olma özelliği taşımaktadır. Sık kullanımı artan internet uygulamaları beraberinde hedef haline gelerek tehditlerinde artmasına neden olmuştur.

İnternet uygulamaları bu noktada güvenli yazılım geliştirme doğrultusunda oluşturulmalı ve üzerinde önlem alınması mutlak alanlar olarak değerlendirilmelidir (Vural & Sağıroğlu, 2008, s. 517).

Mevcut tehditler dünya üzerinde milyonlarca harekete neden olmaktadır. Her tehdit türünde binlercesi anlık olarak yaşanmaktadır. Öyle ki bu hareketlilik günümüz şartlarında anlık olarak izlenip takip edilebilmektedir. Dünyada günlük ortalama yirmi milyona yakın saldırı gerçekleşmektedir. Tehditler bu süreçte hem gelişmekte hem de tekrar tekrar denenmektedir. Teknoloji kullanımının artması bu hareketliliğin artarak devam edeceğini işaret etmektedir. Şekil 4'te, dünya üzerinde gerçekleşen bu saldırıların hareketliliğin anlık olarak gösteren görseli bulunmaktadır.

2.4.2. Kötü Niyetli Yazılım (Malware)

Kötü niyetli yazılım, tüm kötü niyetli program veya kötü niyetli kodu kapsayacak şekilde ifade edilen genel bir tanımdır. Alt kırınımlarındaki her türlü kötü niyetli oluşumların ortak noktaları, teknolojik sistemlere veya cihazlara zarar vermeleri olduğu görülmektedir. Tüm bu zararlı yazılımlar, bulaştıkları sistemleri normal çalışmalarının önüne geçerek amaca hizmet etmesini sağlamaktadır. Aynı zamanda gerçekleştirmesi gereken fonksiyonlarının da kaybolmasına yol açmaktadırlar (Malwarebytes, 2020).

2.4.3. Kötü Niyetli Kod (Malicious Code)

Bilgisayarlarda kontrol dışı eylemlerin gerçekleşmesini sağlayan ve tam olarak amaçladığı görev doğrultusunda çalışmak için tasarlanmış ve birkaç biçimde varlığını gösterebilen kodlara kötü niyetli kod tanımı yapılmaktadır. Kötü niyetli kodun en çok bilinen çeşitleri virüsler ve solucanlardır. Virüslerin çoğalabilmesi için tetiklenmeleri gerekmektedir. Solucanlarda ise durum farklıdır. Solucanlar bulaştıkları bilgisayarlarda kendi kendilerine çoğalabilme özelliğine sahiptirler. Virüs ve solucanlar dışında bazı resmi ürünlerin içerisine yerleştirilen ve makro ismi verilen bir biçimi de vardır. Daha sık duyulan bir çeşidi de arka kapı olarak bilinmektedir (Gelbstein & Kamal, 2002, s. 48).

2.4.4. Aldatmaca (Hoax)

Kişiler veya kurumlar hakkında yalan yanlış haberler uydurulmasıyla ortaya çıkmaktadır. Gerçekleştirilen bu hikâyelerle kişi veya kurumlar zarara uğratılması hedeflenmektedir. Bu bazen ülke bazında yaşanabilmektedir. Böyle bir durumda da ulusal güvenlik söz konusu olmaktadır. Böylece tehdit etki alanını genişleterek halk üzerinde de olumsuz bir hava yaratabilmektedir. Bu yönüyle güçlü bir tehdit seçeneği olabilmektedir (Schryen, 2007, s. 19).

2.4.5. Zincir E-Posta (Chain E-Mail)

Temelde atılan e postalar üzerinden kişilerin bu e postaları başka kişilere göndererek paylaşmasını amaçlayan iletileri ifade eder. Bu e postalar insanların duygusal boşluklarından yararlanabilecek veya herhangi bir şekilde dikkat çekici içerikli olmaktadırlar. Bu e postalar genelde güvenilir bir kaynaktan geliyormuş gibi

gösterilmektedir. Böylece kullanıcı oluşan güvenle birlikte bu e postayı başkalarına da iletebilmesinin yolu açılmaktadır. Zincir bir şekilde iletilen bu e postalarla aslında kullanıcılarında adres listelerinden faydalanılarak daha çok kişiye ulaşmak hedeflenmektedir. Ulaşılan bu kişi listeleri daha sonra ticari amaçlı kullanılmaktadır (Schryen, 2007, s. 19).

2.4.6. Casus Yazılım (Spyware)

Casus yazılım, kullandığımız bilgisayarlar, telefonlar ve tabletlerde kendini gösterebilmektedir. Tüm bu cihazlar üzerinde sahip olduğumuz her türlü bilgiye erişerek, izinsiz bir şekilde toplanmasının ardından saldırganlara veya bu bilgileri hedefleyen kişilere gönderilmesini amaçlanmaktadır. Kullanıcının internet kullanım bilgileri, kredi kartı bilgileri, sahip olduğu e posta listesi ve mevcut şifre bilgileri bu noktada hedef olmaktadır. Çeşitleri bakımından amaca yönelik isimlendirilmiş türleri mevcuttur. Bunlardan birkaç tanesi parola çalıcılar, bankacılık truva atları, emotet, bilgi çalıcılar ve tuş kaydediciler olarak bilinmektedir (Özkaya, Sarıca, & Durmaz, 2019, s. 48).

2.4.7. Kimlik Hırsızlığı (Identity Theft)

Kimlik hırsızlığı, kişi veya kurumlara ait önemli bilgilerin yetkisiz kişilerce, kötüye kullanma amacı doğrultusunda elde etmesiyle başka bir yere aktarılması, korunması veya faydalanılması olarak tanımlanmaktadır. Bu tehdit hem kişileri hem de kurumları kapsamasına rağmen, kişileri etkileyen kimlik hırsızlıkları kurumlara nazaran daha fazla ön plana çıkmaktadır (OECD, 2008, s. 2).

2.4.8. Hizmet Aksatma (DOS)

Kullanılan uygulamaları kullanılamaz hale getirmeyi amaçlayan saldırı türüdür. Genelde kurumları hedef alarak hizmet sağlayıcıları üzerinden gerçekleşmektedir. Her ağın belli bir kapasitesi vardır. Bu tehdit türünde ağ bant genişliği, hafıza kapasitesi ve işlemci gücü tükenene kadar saldırının devam etmesi planlanır. Hedef altındaki uygulama, asıl amaç olan hizmet dışı kalması durumu gerçekleşene kadar saldırı devam eder. Bu saldırı çeşidinde bazen tek kaynak üzerinden bazen de birden fazla kaynak kullanılarak gerçekleştirilmektedir. Daha çok kullanılan ve daha sık

duyduğumuz, birden çok kaynak kullanılarak gerçekleştirilen DOS saldırılarına da DDOS adı verilmektedir (Özkaya, Sarıca, & Durmaz, 2019, s. 68).

2.4.9. Sahte Virüs Koruma Yazılımı

Bilinen virüs koruma programlarının taklit edilmesiyle oluşturulan kötü amaçlı kod içeren yazılımlar olarak tanımlanmaktadır. Sahte virüs koruma yazılımları, meşru virüs koruma yazılımlarının bulunduğu konumda bulunarak benzer davranışları sergilediğinden dolayı, normal virüs koruma yazılımları tarafından tespit edilmesi de bu doğrultuda kolay değildir. Davranış biçimi olarak program kısa yollarında, kayıt defteri üzerinde ve sahte virüs koruma yazılımı tarafından kullanılan dosyalarda, program simgelerini ve anahtar kelimeleri algılamakta meşru virüs koruma yazılımlarının kullandığı algoritmaları kullanmaktadırlar. Dolayısıyla bu simgeler ve anahtar kelimeler sahte virüs koruma yazılımları tarafında değiştirilebilir. Aynı zamanda sıkılaştırılarak taşınabilme özelliğine de sahip olmakta birlikte, meşru virüs koruma yazılımlarının grafik ara yüzlerini de kullanarak kendini saklayabilmektedir. Bunlar da yine tespit edilmesini zorlaştıran özellikleri arasındadır (KVKK, 2016).

2.4.10. Oltalama (Phishing)

Oltalama saldırısı, e posta yoluyla kişilere gönderilen ve gerçekçi bir hikâye içeriğiyle kullanıcıları kandırmaya yönelik hazırlanan bir saldırı çeşididir. İlk amaç kullanıcıyı, güvenli bir e posta gibi oluşturulan sahte içeriğe inandırarak, içerikteki yönlendirmeleri takip etmesini sağlamaktır. Asıl amaç ise bu yolla kullanıcıya veya kuruma ait kişisel bilgilere erişmektir. Oltalama e postaları çeşitli içeriklere sahip olabilmektedir. Bir problemi açıklayan ve çözüme kavuşmak için izlenmesi gereken yol şeklinde olabildiği gibi, yüksek miktarda bir para kazandığınızı ve buna ulaşmak için izlemeniz gereken yolu gösteren bir şekilde de olabilmektedir. Daha zor ayırt edilebilen içerik türü ise; kurum çalışanlarına gönderilen kuruma ait bir bölümden gönderiliyormuş gibi gösterilen e postalardır. Bu noktada son kullanıcının farkındalığı fazlasıyla önem arz etmektedir.

Bu saldırı çeşidinde örnekler çoğaltılabilir. Özellikle günümüzde kullanıcılara kredi kartı hesap özeti ödemesi, parola yenileme veya fatura ödeme içerikli e postalar gönderilmektedir. Bu e postalarda gösterilen adımların izlenmesiyle saldırganlar rahat bir şekilde kullanıcı parolalarını ele geçirme, bilgisayarlara kötü niyetli yazılım

bulaştırma ve istenilen linke tıklatma gibi sonuçlarına ulaşabilmektedirler (Sağıroğlu & Alkan, 2018, s. 31).

2.4.11. Sosyal Mühendislik (Social Engineering)

Sosyal mühendislik; kullanıcıların belli amaçlar doğrultusunda kandırmayı ve sonucunda özel bilgileri elde etmeyi hedefleyen bir yöntem olarak tanımlanabilir. Burada insan faktörünün bu zincirdeki önemli bir unsur olduğunu unutmamak gerekmektedir. Çünkü insan, güvenlik zincirinin en zayıf halkası olarak tanımlanmaktadır. Bunun dışında insan faktörünün hedef olmasının altında, duygusal olarak zafiyet gösterebilme olasılığı yüksek olmasıdır. Bundan dolayı günümüzde teknik önlemleri aşmakta zorlanan saldırganlar, bu seçenek üzerinde fazlaca durmaktadır ve saldırılarını bu en zayıf halkayı hedefleyerek gerçekleştirmektedirler (Özkaya, Sarıca, & Durmaz, 2019, s. 117).

Bu yöntemi kullanan saldırganların en önemli güçleri karşısındaki kişileri ikna edebilmeleridir. Bu noktada kendini güvenlik uzmanı olarak tanıtabilirler, yardımsever görüntüsü verebilirler, kişilerin herhangi bir alandaki zafiyetlerini doğru tahmin edebilirler ve bu çerçevede yakınlık kurabilirler. Bunlar gibi örneklendirebildiğimiz sosyal mühendislik aktiviteleri önemli saldırılar arasında yer bulmaktadır (Sağıroğlu & Alkan, 2018, s. 34).

Birçok saldırı tekniğini içerisinde barındıran Sosyal Mühendislik saldırıların hepsi belli adımlar çerçevesinde oluşturulur. Bir döngü olarak düşünülmekte olan adımlar aşağıdaki gibi sıralanabilir (Özkaya, 2018, s. 161):

- Bilgi Toplama
- Çıkarım
- Başkasının yerine geçme
- İkna
- Hedef seçme
- Keşif

2.4.12. Siber Zorbalık (Cyberbullying)

Siber zorbalık bir davranış biçimi olarak karşımıza çıkmaktadır. Temel amaç teknik veya kişisel olarak zarar vermektir. Bu saldırılarda kişi kurum ya da gruplar hedef olarak belirlenebilmektedir. Elektronik ve psikolojik olmak üzere iki tür seçeneği bulunmaktadır. Bu saldırı tipinde teknolojik imkânlar direk olarak hedef haline gelmesinin yanında, kişilere dolaylı yoldan olumsuz olarak etki etmektedir (Arıcak, 2011, s. 11).

2.5. Bilgi Güvenliğine Yönelik Alınması Gereken Önlemler

Gözümüzde bir bant olduğunu ve uçurumun kenarında dolaştığımızı düşünelim. Böyle bir durumda olası tehlikelerden haberdar olmamız mümkün değildir. Örneğin bir saniye sonrasında aşağı düşebiliriz. En önemlisi de bu olasılıktan haberimiz olmamasıdır. Bilgi güvenliği kavramı tam da böyle bir noktada hayatımıza katılmış olmakta birlikte; gözümüzdeki bu bandı çıkartan, var olan tehditlerle insan faktörünü karşı karşıya getiren ve alınması gereken önlemlerle geliştirilebilecek çözümleri gözler önüne seren bir araç niteliği taşımaktadır. Tehlikelerden haberdar olunmasına rağmen olası bir tehlikeye karşı gerekli hazırlıkları tamamlamamak, herhangi bir zamanda gelişebilecek bir aksiyonda ortaya azımsanmayacak derecede zarar verici sonuçlar çıkartabilir. Dolayısıyla gerekli önlemleri almakta en az durumun farkına varmak kadar önemlidir.

Bilgi güvenliğine yönelik alınması gereken önlemler, hem kişisel hem de kurumsal açıdan değerlendirilmektedir. Kişisel önlemlerin odağında insan olduğu gibi, her türlü teknolojik önlemin alındığı kurumsal önlemlerin odağında da insan bulunmaktadır. Altını çizmek gerekiyor ki, hem kişisel hem de kurumsal önlemlerin alınmasında ortak payda insan faktörüdür. Sadece teknolojik önlemlerin sağlanmasıyla güvenliğin sağlanması oldukça zordur. Öneminin altını çizdiğimiz insan faktörünün, bilgi güvenliğine yönelik alınacak önlemlerde bu sürece dâhil edilmesi ve ihtiyaç duyulan farkındalığa sahip olmasının sağlanması gerekmektedir. Bu adım mevcut risklerin minimize edilmesinde önemli bir rol oynayacaktır. Alınacak önlemler noktasında etkili olan faktörler devreye alınsa bile riskler sıfıra indirilememektedir. Hedef, riskleri kabul edilebilir bir seviyeye indirmek olmalıdır (Çetinkaya, Güldüren, & Keser, 2017, s. 49).

2.5.1. Bilgi Güvenliğine Yönelik Kurumsal Önlemler

Güncel tehditler, varlıklarını gelişerek sürdürmeye devam etmektedirler. Yapılan araştırmalar bilgi güvenliğini bozmaya yönelik saldırıların son on yılda 27 kat arttığını ve günde ortalama bir milyon altı yüz bin saldırıya ulaştığını göstermektedir. Böylesi büyük rakamların konuşulduğu bir dünyada, elbette kurumlar altyapılarını teknik anlamda her türlü senaryoya hazırlamak durumunda kalmaktadırlar. Sadece teknik anlamda değil düşünce olarak da yenilikçi, ön görü sahibi ve güvenliğin önemini kavramış bir durumda olmak gerekmektedir. Bu çerçevede kurumsal açıdan bilgi güvenliğine yönelik alınabilecek önlemler şu şekildedir (Glasshouse, 2020):

- Alanında uzman kişilerden oluşturulmuş ekipler kurulması
- Bilgi güvenliği çalışanları dışında kalan tüm çalışanların bu alanda gerekli eğitimleri alması
- Büyük ya da küçük ölçekli bir kurum olmak fark etmeksizin bu sürece hazırlıklı olunması
- Verilerin şifrelenmesi
- Mevcut verilerin yedeklenmesinin sağlanması
- Yeni teknolojilerin takip edilerek mevcut sistemle dâhil edilmesi
- Bulut uygulamalarının değerlendirilmesi
- Güvenlik alanına yapılacak yatırımların desteklenmesi
- İş sürekliliğin sağlanması

Bilgi güvenliğinin sağlanması adına alınması gereken kurumsal önlemler hakkında ne yapılması gerektiği konusunda genel hatlarıyla birkaç maddeden bahsedilmiştir. Bu doğrultuda belirtilen önlemlerin "nasıl" gerçekleştirebileceği de önemlidir. Kurumsal olarak güvenli bir yapı oluşturulmak isteniyorsa, güvenlik mimarisi planlaması yapılmalıdır. Güvenlik mimarisi oluşturulurken bazı noktalara dikkat etmek gerekmektedir. Güvenlik mimarisi bilginin gizlilik, bütünlük ve erişilebilirlik ilkelerine uygun oluşturulmalıdır. Kullanıcılar işlemlerini yeterli seviyede erişim hakkıyla gerçekleştirmeli ve bu işlemler denetlenebilir olmalıdır. Tüm sorumluluklar

önceden tanımlanmalı ve gerçekleştirilen işlemler için izleme sistemi kurulmalıdır. Bu çerçevede, güvenlik mimarisi oluşturabilmesi için gerekli unsurlar altı başlık altında sıralanabilir (Özkaya, Sarıca, & Durmaz, 2019, s. 305):

- Erişim Kontrol Mekanizmaları: Belli bir varlığa, yeterli seviyede belirlenen haklar çerçevesinde, belli kişi veya gruplara sağlanan erişim hakkı olarak tanımlanmaktadır. Özetle, kimin, neye, hangi hakla, ne kadarına erişilebileceğinin belirlenmesinin sağlanmasıdır.

- Kriptografik Güvenlik Kontrolleri: Bu gereksinim aslında bilgi güvenliği unsurlarından gizlilik ve bütünlüğün sağlanması olarak özetlenebilir. Bilgiye, sadece yetkili kişilerin erişebilmesi ve üzerinde değişiklik yapılmadığının garantisinin sağlanması olarak da ifade edebilir.

- Bilgisayar Sistemleri Güvenliği: Kurumda bulunan donanım veya yazılımlara ait güvenliğin sağlanması şeklinde özetlenebilir. Günümüzde özellikle sıkça kullanılmaya başlanan sanallaştırma ortamları da bu kapsamda değerlendirilmekte olup, güvenli mimaride üzerinde durulması gereken bir alan olarak karşımıza çıkmaktadır.

- Ağ Güvenliği: Teknik olarak detaylandırılabilecek bir alan olup, katmanlı ağ güvenliği yapısının oluşturulduğu, güvenlik duvarları, saldırı tespit ve önleme sistemlerinin kurulduğu bir alan olarak değerlendirilmektedir. Teknolojik açıdan alınan önlemlerin omurgası şeklinde bir benzetme yapabilir.

- Değişiklik Yönetimi: Güvenlik mimarisi üzerinde yapılacak bir cihaz ekleme ya da çıkarma işlemi, politika değişikliği, uygulamada farklılık gibi herhangi bir değişikliğin belli izinler veya gözetim kapsamında gerçekleştirilmesi olarak ifade edilmektedir.

- İzleme Sistemleri: Kurumu hedef alan saldırı veya tehditleri önceden belirleyebilmek amacıyla oluşturulan ve sürekli sağlanan takip ile güvenlik seviyesinin arttırıldığı sistemleri kapsamaktadır.

2.5.2. Bilgi Güvenliğine Yönelik Kişisel Önlemler

Bilgi güvenliği zincirinin en zayıf halkası olarak her zaman insan gösterilmektedir. İnsan faktörünün oluşturduğu zafiyet, kurumlar için mevcut riski oldukça arttırmaktadır. Bu riski asgari seviyeye indirmek için kurumsal önlemler yanında kişisel önlemlerde mevcuttur. Bu önlemlerden en güçlüsü, konuyla ilgili oluşacak farkındalıktır. Bilgi güvenliği ile ilgili farkındalık seviyesini artıracak eğitimler ve kurslar bu noktada destekleyici olabilmektedir. Hayatımızın her alanına girmiş olan teknolojiyi yakından takip etmek, gelişmelere kayıtsız kalmamak bile bu farkındalık seviyesinin artmasına katkıda bulunacaktır. Özetlemek gerekirse, bilgi güvenliğine yönelik alınması gereken kişisel önlemler aşağıdaki başlıklar altında şu şekilde detaylandırabilir (Taner, 2019, s. 26):

- Sosyal Mühendislik: İnsani zaaflardan yararlanılarak gerçekleştirilen bu saldırı türüne karşı en etkili silah farkındalıktır. Yüksek farkındalık seviyesiyle birlikte oluşan algı açıklığı ile gerekli önlem büyük ölçüde alınmış sayılmaktadır.

- Oltalama: Bu saldırı çeşidinden korunmanın ilk adımı bilinmeyen bir adresten gelen e postalarda bulunan ek veya linkleri açmamaktır. Yapılan yönlendirmeyle açılan sayfada ise size ait kişisel bilgilerin girilmemesi gerekmektedir. Gidilen adresin adres çubuğunda bir imla hatası veya yanlış yazım olup olmadığı kontrol edilmelidir.

- Parola Güvenliği: Kullanıcılar sistemlere giriş yapabilmek için bazen tek bazen ise çoklu doğrulamadan geçmektedirler. Bu noktada oluşturulan parolalar kolay tahmin edilebilir olmamalıdır. Karışık ve kişisel bilgi içermeyen parolalar oluşturulmasının yanı sıra aynı parola başka sistemlerde kullanılmamalıdır. Böylece daha güvenli bir parola yönetimi sağlanmış olabilecektir.

- Sosyal Medya Kullanımı: Her yaştan kullanıcıyı içerisinde barındıran sosyal medyalar, kişilerin hayatı hakkında her bilginin paylaşıldığı mecralar haline gelmiştir. Bundan dolayı kişisel bilgiler, sosyal medya hesaplarında herkesin görebileceği açık bir şekilde yayınlanmaması gerekmektedir. Özellikle paylaşılan konum bilgileri, kişilere yönelikte oluşabilecek tehditlerin

oluşmasına vesile olmaktadır. Bu doğrultuda sosyal medya hesaplarında asgari kişisel bilgi paylaşılması, paylaşılan bilgilerinde kimler tarafından erişilebilir olduğunun kontrol altına alınması gerekmektedir.

- Cihaz Güvenliği: Günümüzde kişisel olarak sahip olunan her türlü cihaz (Telefon, Bilgisayar, Tablet) üzerinden birçok işlem yapılmaktadır. Yapılan işlemlerin yanında bu cihazlarımız özel hayatımıza dair birçok veriyi barındırmaktadır. Bu doğrultuda cihazlara güçlü bir giriş parolası eklenerek güvenlik seviyesi arttırılmalıdır. Sanal marketler üzerinden indirilen uygulamalarda verilen izinlere dikkat edilmelidir. Cihazlara gelen güvenlik güncellemeleri takip edilerek bekletilmeden yapılmalıdır.

- Bilgi güvenliğine yönelik alınması gereken önlemlerin hem kurumsal hem de kişisel boyutta birçok yöntemi mevcuttur. Tüm bu önlemler alınmış olsa bile, sürekli gelişen tehdit çeşitlerinin varlığından dolayı, hiçbir zaman riskler sıfıra inmeyecektir. Bu anlayışla ve farkındalıkla alınması gereken önlemler, bu tehditlere karşı ya hiç etkilenmemek ya da asgari şekilde etkilenmek amacıyla oluşturulmaktadır. Bu doğrultuda hem dünyada hem de ülkemizde ortak çözüm olarak, bilgi güvenliğine gereken önemin verilmesi ve farkındalık seviyesinin arttırılması olarak gösterilmektedir (Canbek & Sağıroğlu, 2006, s. 172).

3. BİLGİ GÜVENLİĞİ FARKINDALIĞI

3.1. Bilgi Güvenliği Farkındalığı Nedir?

Bilgi güvenliğinin oluşumu ve gelişimi, güvenliğe yönelik mevcut tehditler ve alınabilecek önlemler gibi konuların, tesis edilmiş olan bilgi güvenliğinin sürdürülebilir olmasındaki rolü büyüktür. Geniş bir çerçeveden bakmak gerekirse, yapılan yatırımlar, teknolojik hamleler, kurulan güvenlik sistemleri ve tüm bilgi güvenliği standartları göz önüne alındığında, karşımızdaki en temel etkenin insan olduğu görülmektedir. Yapılan çalışmalar da göstermiştir ki, bilgi güvenliğini sağlamak adına odak noktamız insan olmalıdır. İnsan faktörünün neden olduğu riskleri en aza indirmenin yolu da farkındalık seviyesini arttırmaktır.

Farkındalık seviyesinin artmasında bazı destekleyici unsurlar vardır. Bu noktada ilk olarak farkındalıkla birlikte sürece hâkim olabilmek adına daha önce benzer süreçlere aşina olmaktır. Bu da deneyerek veya deneyimle mümkündür. Bir diğer ve en önemli unsur ise eğitimdir. Farkındalığı arttırmaya yönelik verilmekte olan eğitimler, uzmanlık seviyesini arttırır ve tehditler karşısında farkındalık sonrası atılması gereken adımları doğru belirlemek adına önem arz etmektedir. Bu üç unsur aslında birbirinden bağımsız gözükse de, birbirini etkileyen unsurlar olarak karşımıza çıkmaktadır. Etkili bir bilgi güvenliği sistemi oluşturulmak isteniyorsa, farkındalık seviyesinin arttırılması ve destekleyici unsurların sağlanması gerekmektedir (Peltier, 2005, s. 37).

Bilgi güvenliği farkındalığı, bilgi güvenliğine ilişkin mevcut riskler ve bu risklere karşı alınabilecek önlemler konusunda bilgi ve beceri sahibi olabilme durumu şeklinde tanımlanabilmektedir (Şahinaslan, Kandemir, & Şahinaslan, 2009, s. 193).

Kişilerin teknoloji kullanımları sırasında bazı tehditler oluşmaktadır. Bu tehditlere karşı alınabilecek önlemler, doğru analizler yapılarak ortaya koyulmalıdır. Bu süreçte doğru analizlerle, alınması gereken önlemlerin bilincinde olma durumu, bilgi güvenliği farkındalığı olarak değerlendirilmektedir (Vural & Sağıroğlu, 2008, s. 509).

Bir diğer deyişle, kişisel veya kurumsal bilgi güvenliğinin sağlanmasına yönelik tehditlerin ve bu tehditlere karşı alınacak önlemlerin oluşturacağı süreçlerin kavranması olarak da belirtilebilir (Sağıroğlu & Alkan, 2018, s. 119). Literatürdeki tanımlar genel olarak değerlendirildiğinde; farkındalık, kişinin mevcut tehditler ve bu tehditlere karşı verilen tepkinin ortak paydada buluşacak şekilde değerlendirilmesi olarak tanımlanabilir.

3.2. Önemi Ve Etkileri

Kurumlarda bilgi güvenliği farkındalığı oluşturmanın bazı amaçları vardır. Bu konudaki temel amaç; özellikle çalışanların kurumun değerli varlıkları arasında sayılan bilgi varlıklarının korunmasına ilişkin tüm sorumluluklarının bilincinde olması şeklinde açıklanır. Bu noktada farkındalığın oluşması gereken tek grup çalışanlar da değildir. Aynı zamanda kurumun kendi çalışanları dışındaki tüm paydaşlarda bu sorumluluğa sahip olmalıdır. Dolayısıyla oluşturulması gereken farkındalığın kapsamı çalışanlarla sınırlı değildir. Kurumun bilgi alışverişi sağladığı her kişi veya kurum üzerinde bu farkındalığın oluşturulması gerekmektedir. Çalışanlar için bilgi güvenliği

farkındalığının ek bir iş olarak görülmemesi ve iş sorumlulukları arasında değerlendirilmesi, kurumlardaki bilgi güvenliği farkındalık seviyesini olumlu yönde etkilemektedir. Bu durumdan dolayı çalışanların farkındalık çalışmalarını içselleştirmeleri daha başarılı sonuçlar doğurmaktadır. Bu noktada amaçlardan bir tanesi de farkındalık çalışmalarının, çalışanların özümseyecekleri şekilde organize edilmesi olmalıdır (Şahinaslan, Kantürk, Şahinaslan, & Borandağ, 2009, s. 598).

Bilgi güvenliği farkındalığı, bir kurumum oluşturması gereken en önemli adımlar arasında olup, hem kişisel hem de kurumsal açıdan sağlanan başarının faktörlerinden bir tanesidir. Seviyesi yüksek bir bilgi güvenliği oluşturulmak isteniyorsa, farkındalık çalışmaları gerçekleştirilmelidir. Kurumsal çatı altındaki tüm faaliyetler bu farkındalık ışığında başlatılmadı ve sürdürülmelidir. Bu doğrultuda planlanacak farkındalık eğitimleri, çalışmalar, bilgilendirmeler gibi aktivitelerle farkındalık seviyesi arttırılabilir. Bu tip çalışmalara devlet desteği de sağlandığı takdirde ülke genelinde bir farkındalıkta oluşmuş olacaktır. Sadece kurumsal olarak düşünmenin ötesinde, ülkenin tüm bileşenlerinin destek olması ve sorumlu hissetmesi gereken bir alan olarak karşımıza çıkmaktadır (Eminağaoğlu & Gökşen, 2009, s. 13). Dolayısıyla bilgi güvenliği farkındalığı, kişiden başlayarak koca bir toplumu etkileyecek derece de bir etkiye sahip önemli bir husustur.

Bilgi güvenliği farkındalığının önemi, bilgi güvenliği standartlarında da karşımıza çıkmaktadır. ISO 27001 BGYS maddeleri arasında, kurumsal farkındalığın sağlanması adına belirli aralıklarla ilgili eğitimlerin düzenlemesi maddesi bulunmaktadır (Ganbat, 2013, s. 81). Standardın gerekliliklerinin tesis edilmesi ve korunabilmesi adına bu eğitimlerin sürekli gerçekleştirilmesiyle farkındalık seviyesinin arttırılması hedeflenmektedir. Özetle, farkındalığın önemi ve etkisi bilgi güvenliği standartlarıyla da ortaya konulmuştur.

İnsan faktörünün öneminin yüksek olduğu bilinen bilgi güvenliği uygulamalarında, yapılacak yatırımlarda insan odaklı planlanmaktadır. Bu doğrultuda insana yapılacak en doğru yatırım eğitim olarak karşımıza çıkmaktadır. Bilgi güvenliği farkındalığını arttırmak amacıyla da kurumlar eğitim yolunu izlemektedirler. Bu eğitimlerin uygulanması kadar, sonuçlarının değerlendirilip analiz edilmesi de önemlidir. Bu eğitimler sonucu, etkilerinin ölçülmesi adına kişinin hem kendine hem kuruma değer katıp katamadığının değerlendirilmesi de önem arz etmektedir. Bu etkiler

ölçüldüğünde, kurulan teknik altyapının da daha verimli kullanılmasına katkı sağlaması beklenmektedir. Günümüzde bu analizler kurumlar tarafından şimdilik eğitim ve anket yoluyla gerçekleştirilmektedir. Dolayısıyla bu noktada belki de bu etkileri tespit edebilecek bir araca veya daha çok araştırmaya ihtiyaç olabilir (Gökce, 2010).

3.3. Farkındalık Çalışmaları

Bilgi güvenliği farkındalığını oluşturmanın çeşitli yolları vardır. Bu yollar belirlenmeden önce hedef kitle belirlenmelidir. Daha önce tüm paydaşların bu farkındalığın bir parçası olması gerektiğini belirtmiştik. Bu doğrultuda kurum çalışanlarının tamamının yanı sıra kuruma dışardan hizmet verenlerde bu kapsamda değerlendirilmelidir.

İşe yeni başlayan bir çalışana kurumlar tarafından oryantasyon adı altında bir eğitim verilmektedir. Bu eğitimin içeriğinde bilgi güvenliği farkındalığı mutlaka yer almalıdır. Çalışanın kuruma giriş yapmasından itibaren, belli bir zaman aralıklarıyla farkındalığa ilişkin eğitimlere devam edilmelidir. Bu eğitimlerin dışında da uygulanabilecek birçok yol bulunmaktadır. Bu yolları aşağıdaki şekilde sıralayabiliriz (Şahinaslan, Kantürk, Şahinaslan, & Borandağ, 2009, s. 601):

- Bilgisayar üzerinden sanal eğitimler gerçekleştirilebilir.
- Bölüm ya da pozisyona göre değişkenlik gösteren eğitimler hazırlanabilir.
- Çalışanlara dağıtılmak üzere mini kitapçık, broşür ve posterler hazırlanabilir.
- Her birimin çalışma alanındaki güvenlik boyutunun değerlendirilebileceği mini toplantılar düzenlenebilir.
- Kurum içi ekranlarda oynatılmak üzere animasyonlar oluşturulabilir.
- Geniş çaplı kitlelerin bulunduğu ortamlar için kısa filmler çekilip yayınlanabilir.
- Belli zaman aralıklarıyla gönderilmek üzere e-bülten hazırlanabilir.
- Kurum cihazlarının ekran koruyucularında veya masa üstü arka planına yerleştirilmek üzere görseller hazırlanabilir.

- Bilgi güvenliği içerikli oyunlar hazırlanarak yarışmalar düzenlenebilir.
- Çalışanların günlük kullanımlarına uygun, güvenlik risklerini veya önlemlerini hatırlatan aksesuarlar hazırlanıp dağıtılabilir.
- Bilgi güvenliğinin önemini arttıracak ve farkındalığı hatırlatacak etkinlik, oyun veya turnuvalar düzenlenebilir.

Kurumların en önemli varlıkları arasında olarak bilinen bilginin, gizlilik, bütünlük ve erişilebilirlik unsurları açısından değerlendirilerek korunmasının sağlanması gerekmektedir. Bu unsurların sağlanmasında en önemli adımlardan bir tanesi bilgi güvenliği farkındalığıdır. Bilgi güvenliği farkındalık eğitimleri üzerinde yapılan bir araştırmada, bu eğitimin içeriğinde bulunan temel bilgi güvenliği prensiplerinin, temel farkındalık programlarının yer almasıyla oluşabilecek farkındalık etkisi incelenmiş ve farkındalık seviyesine olumlu katkılar sağladığı görülmüştür. Temel seviyede bir farkındalık eğitimi bile kurum güvenliğine ve farkındalık seviyesine etkisi olmaktadır. Çünkü her türlü teknolojik ve sistemsel önlemlerin alındığı kurumlarda nihai olarak temelde insan faktörü karşımıza çıkmaktadır. Risklerin asgariye indirilmesinde de insana yapılacak yatırım fazlasıyla önem arz etmektedir (Şahinaslan, Kandemir, & Şahinaslan, 2009, s. 193).

Yapılan bir araştırmada; bilgi güvenliği bilincinde kültürel faktörlerin rolü araştırılmıştır. İki farklı kültüre sahip üniversite öğrenci grupları üzerinde gerçekleştirilen çalışma sonucunda öğrencilerin virüs, oltalama saldırısı ve e posta güvenliği gibi konularda bilgi sahibi oldukları, fakat sosyal mühendislik konusunda herhangi bir fikirleri olmadıkları ortaya çıkmıştır. Aynı araştırmanın bir diğer sonucuna göre, sosyal mühendislik konusunda bilgi sahibi olmamalarına rağmen, bilgi güvenliği konusunda sergiledikleri davranışlarda bilinçli hareket ettikleri görülmüştür. Tüm sonuçların odağında ise doğup büyüdükleri ortam, yaşam tarzları, sahip oldukları kültürleri gibi kavramların bilgi güvenliğine ilişkin davranışları üzerinde etkisinin olduğu tespit edilmiştir. Bu tespitler ışığında güvenlik seviyesini yükseltmek için sosyal mühendislik bilinci konusunda öğrencilere farkındalık eğitimleri verilmesi sonucuna varılmıştır (Kruger, Flowerday, Drevin, & Steyn, 2011).

Toplumsal açıdan yapılan bir araştırmada; yaş, cinsiyet, eğitim seviyesi gibi değişkenler dikkate alınarak, toplumun güvenlik tehditlerine karşı olan duyarlılığı

incelenmiştir. Araştırma sonucu toplumun güvenlik konusunda bilgi eksikliğini belirleyecek bir politika çerçevesinde farkındalık eğitimleri verilerek tamamlanması gerektiği belirtilmiştir. Böylece toplumsal güvenlik risklerinin de azalmasına katkıda bulunulacağı savunulmuştur (Schmidt, Johnston, Arnett, Chen, & Li, 2008, s. 95).

Gençler üzerinde yapılan bir araştırmada; internet dünyasında var olan güvenlik risklerine karşı katılımcıların farkındalık seviyeleri incelenmiştir. Çalışmaya katılımlarıyla destek olanların yüzde seksen oranında erkek olmasının yanında, yaşlarının 20-29 arasındadır. Ortaya çıkan sonuçlara göre güvenlik alanında eğitim almış kişilerin mevcut risklere karşı bilgi sahibi oldukları ve bu konudaki farkındalık seviyelerinin fazla olduğu gözlemlenmiştir (Shehri & Clarke , 2007, s. 21).

Yapılan uluslararası bir araştırmada dünya üzerinde etkin iki devlet olan Amerika ve Kore gibi iki farklı kültüre sahip ülke arasındaki, teknolojik yaklaşımlar ve internet kullanımına ilişkin oranlar ve güvenlik riskleri incelenmiştir. İlgili çalışma, teknoloji kullanımı, zararlı yazılımlar ve bu tehditlere karşı oluşan farkındalık olmak üzere 3 ana başlık altında değerlendirilmiştir. Araştırmada Amerika'nın teknoloji kullanım oranı ve bilgi güvenliği farkındalığı konusunda seviyesi Kore'ye nazaran daha düşük olduğu sonucu ortaya çıkmıştır (Kwak, Kizzier, Zo, & Jung, 2011, s. 63).

Japon kurumları üzerinde yapılan bir araştırmada çalışanların bilgi güvenliği farkındalıkları incelenmiştir. Araştırmada kişisel özellikler baz alınarak yapılan karşılaştırmada, kişisel özelliklerinde farkındalık üzerinde etkisi olduğu görülmüştür. Ek olarak çalışanların bilgi güvenliği farkındalıklarının artması için bu konuda eğitim alınması gerektiği de ortaya çıkmıştır (Takemura, Tanaka, & Matsuura, 2011, s. 260).

Norveç'teki bir banka üzerinde gerçekleştirilen bir çalışmada, çalışanların bilgi güvenliği konusundaki yetkinlikleri incelenmiştir. Araştırma sonucu bilgi güvenliğini sağlamakla sorumlu olan kişilerle diğer çalışanlar arasında bir kopukluk olduğu görülmüştür. Bilgi güvenliğinde ortaya çıkan risklerin sebebinin, çalışanların bilgi güvenliği yetkinliklerinin düşük ve farkındalıklarının eksik olduğu sonucu ortaya çıkmıştır (Albrechtsen, 2007, s. 277).

Avustralya'da bulunan bir banka çalışanları üzerinde gerçekleştirilen çalışmada hem çalışanların bilgi güvenliği farkındalık seviyelerini etkileyen faktörler hem de başka sektör çalışanlarıyla banka çalışanları arasındaki bilgi güvenliği bilinci araştırılmıştır.

Banka çalışanı olarak 200 kişi ve çeşitli sektörlerden 500 kişi üzerinde anket çalışması yapılmış. Araştırmada çalışanların bilgi güvenliği farkındalıkları, alınan eğitimler çerçevesinde değerlendirilmiştir. Daha sık eğitim alanlarla, daha az eğitim alanlar arasında bilgi güvenliği farkındalığına ilişkin ciddi bir fark olmadığı görülmüş. Bu sonuç, eğitim sıklığının bir çalışanın bilgi güvenliği farkındalık seviyesine katkıda bulunan önemli bir faktör olmadığını göstermiştir (Pattinson, Butavicius, Parsons, McCormac, & Calic, 2017, s. 182).

Almanya'da 183 banka çalışanı üzerinde gerçekleştirilen bir araştırmada bilgi güvenliği farkındalık eğitimlerinin bilgi güvenliğine uyum konusundaki etkileri üzerinde çalışılmıştır. Araştırma sonucunda bilgi güvenliği eğitimlerinin çalışanlar üzerinde koruma arzusunu arttırması ve konuyla ilgili bilinçlendirmesi itibariyle olumlu katkıları olduğu ortaya çıkmıştır. Bu sonucu güçlü kılan önemli koşullardan bir tanesi ise, bu eğitimlerin çalışanları güvenlik tehditleriyle nasıl başa çıkacakları konusunda bilgi sahibi yapması olarak değerlendirilmektedir (Bauer & Bernroider, 2015, s. 154).

Avrupa'da bulunan büyük bir bankada gerçekleştirilen çalışmada bilgi güvenliği politikalarına çalışanların gösterdiği uyum ve bu uyumun geliştirilmesine yönelik yapılması gerekenler araştırılmıştır. Araştırma sonucunda bilgi güvenliği farkındalığını sosyal normların yanı sıra kişisel normlarında etkilediği ortaya koyulmuştur. Bu çerçevede kişisel olarak bilgi güvenliği farkındalığını arttırmaya yönelik eğitimlerin önemine vurgu yapılmıştır (Bauer & Bernroider, 2017, s. 59).

4. BANKACILIK SEKTÖRÜ VE BİLGİ GÜVENLİĞİ YAPISI

4.1. Bankacılık

Yaşadığımız topraklarda bankacılık faaliyetleri ilk olarak Osmanlı döneminde azınlıklar tarafından ortaya çıkartılmıştır. Daha sonra Tanzimat dönemiyle hız kazanan bankacılık faaliyetleri Cumhuriyetin ilanıyla birlikte gelişmeye başlamış ve bugün ki Türk Bankacılığı halini almıştır. Türk bankacılık sektörü günden güne gelişmekte olan, güçlü sermayeye sahip, özerk, denetim altında ve güvenli bir yapıya sahiptir. Yaşanan ekonomik kriz ve bu krizlerin yarattığı olaylar vesilesiyle Türk Bankacılık

Sektörü günümüzde oldukça sağlam bir duruma kavuşmuştur. Bankacılık faaliyetlerinin teknolojiyle birleşmesi bakımından da Türk Bankacılığı tüm bu gelişmelere ve yeniliklere ayak uydurmuş ve hatta bazı alanlarda da öncülük edebilecek altyapıya sahip hale gelmiştir. Bu anlamda Türk Bankacılık Sektörü yüksek büyüme potansiyeline sahip olduğu görülmektedir (Sümer, 2016, s. 487).

Bankalar, "*fon fazlası olanlardan toplanan kaynakların fon talebi olanlara kredi olarak verilmesine aracılık eden finansal kuruluşlardır*" olarak ifade edilmektedir. Bankacılık sektörü güçlü ve etkili yapısı gereği ülke ekonomisi üzerinde etki yaratabilmektedir. Bu nedenle ülke ekonomisinde bankalar önemli bir yere sahiptir. Bankaların fon sağlamak dışında ekonomik açıdan önemli başka faaliyetleri de olduğundan dolayı, ülke ekonomisi için güç kaynağı niteliği taşımaktadır. Bankacılık ne kadar büyür, gelişir ve sağlamlaşırsa o ülkenin ekonomisi de aynı derecede güçlü olacağı belirtilmektedir (Yetiz, 2016, s. 107).

Bankalar, ülke ekonomisine katkıda bulunan kuruluşlardır. Bu katkıyı belli görevler çerçevesinde gerçekleştirmektedirler. Ülkenin üretim faaliyetlerinin devamlılığını sağlayarak ekonomik büyüme ve kalkınmaya hizmet ederler. Bu çerçevede bankaların bazı görevlerini aşağıdaki şekilde sıralayabiliriz (Ayanoğlu, 2013, s. 4):

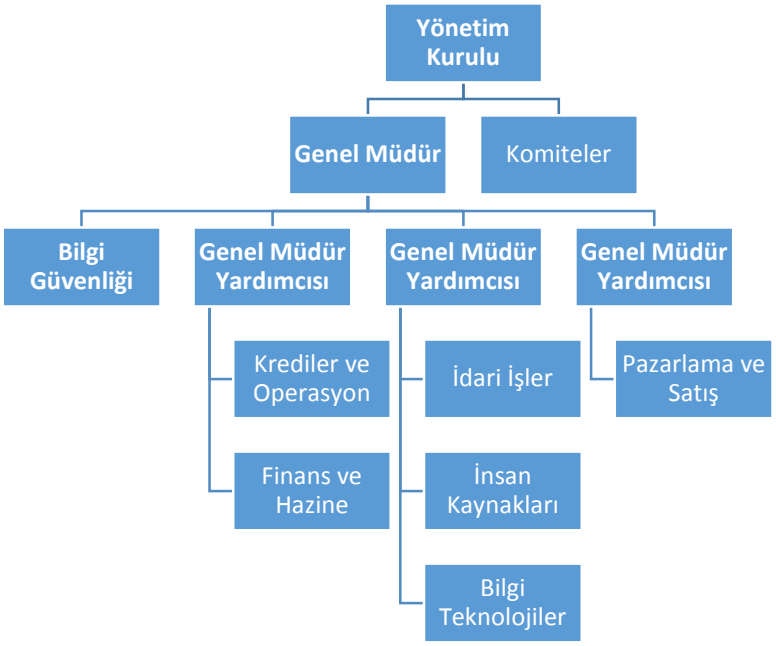
- Finansal aracılık yapmak
- Likidite sağlamak
- Kaydi para yaratmak
- Para politikasının etkinliğini arttırmak
- Sermaye piyasalarının gelişimine ve yatırımların finansmanına katkıda bulunmak
- Gelir ve servet dağılımını etkilemek
- Dış ticareti geliştirmek

4.1.1. Organizasyon Yapısı

Ekonomik yaşamın sürdürülebilmesi amacıyla yapılan üretimde ve gerçekleştirilen hizmetlerde insanların bir araya gelmesiyle oluşan yapıların önemi büyüktür. Bazı

faaliyetlerin tek bir kişi tarafından yürütülemeyeceği veya verimli olamayacağı açıktır. Buradan doğan ihtiyaçla gücü birleştirerek, verimi arttırmanın ve bir anlamda örgütlü bir yapı oluşturarak faaliyetlerin hız kazanmasının sağlanabileceği ortaya çıkmıştır. Sanayinin gelişmesiyle gerçekleşen hızlı büyümeyle birlikte, gerçekleştirilen işlerin bölünmesi ihtiyacı doğurmuştur. Bazı işlerin tek kişi değil, gruplar ile birlikte yapılması bile tek başına yetersiz kalmıştır. Bu doğrultuda hem kişilerin hem de grupların belirtildiği organizasyon yapısı ihtiyacı ortaya çıkmıştır. Organizasyon yapısının oluşturulmasının amacı, faaliyetlerin asgari maliyetle, gerekli düzen ve uyum içerisinde gerçekleştirilmesidir. Ek olarak, mevcut varlıkların arttırılması ve oluşturulan organizasyonun yenilikçi bir yapıda olması da amaçları arasında bulunmaktadır (Ülgen, 1973, s. 208).

Bir banka faaliyetlerinde gösterdiği başarının temelinde güçlü ve işlevsel bir organizasyon yapısı yatmaktadır. Bu yapının en tepesinde yönetim kurulu bulunmaktadır. Yönetim kurulu bankanın en yetkili makamı olup, politikaları belirleyerek uygulayacak ve faaliyetleri yönetecek üst düzey yöneticileri atayacaktır. Bu atamaların devamında birimlerin yöneticilerinin belirlenmesiyle güçlü organizasyon yapısının temeli oluşturulmaktadır. Yönetim kurulu dışında bu yapı dâhilinde bazı komiteler bulunmaktadır. Bu komitelerin en önemlilerinden bir tanesi denetim komitesidir (Kesebir & Mutlu, 2019, s. 323). Güçlü ve güvenli bir organizasyon yapısı için işlevsel bir denetim komitesi kurulması gerekmektedir. Bu doğrultuda genel hatlarıyla bankalardaki organizasyon yapısı Şekil 5'teki gibi oluşturulmaktadır.



Şekil 5. Banka Taslak Organizasyon Şeması

Bankaların temel faaliyetlerin yönetildiği genel müdürlükleri bulunmaktadır. Oluşturulan organizasyon yapısı gereği genel müdürlük çatısı altında bulunan bazı birimleri aşağıdaki gibi sıralayabiliriz:

- Krediler ve Operasyon
- Finans ve Hazine
- İdari İşler
- İnsan Kaynakları
- Bilgi Teknolojileri
- Pazarlama ve Satış

Bankalarda, BT güvenlik fonksiyonlarının yönetildiği bir bölüm bulunmaktadır. Banka organizasyon şemasında genelde bilgi güvenliği birimi olarak yer almaktadır. Bilgi güvenliği biriminde bankanın tüm güvenlik politikaları oluşturulmaktadır. Bu koşullar BDDK mevzuatlarında açıkça belirtilmektedir. BDDK, Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik başlığı altında

bir mevzuat yayınlamıştır. Bu mevzuattaki Bilgi Güvenliği Yönetimi bölümünde bulunan 8. maddenin 5 fıkrasında ilgili kısım "Banka bünyesinde, bilgi sistemlerinden sorumlu üst düzey yönetici ve ona bağlı birimlerden meydana gelen BT fonksiyonundan ayrı ve bağımsız olacak şekilde bir BT güvenlik fonksiyonu oluşturulur. BT güvenlik fonksiyonunun doğrudan yönetim kuruluna veya genel müdüre bağlı olması esastır. Bankanın BT güvenlik fonksiyonu, bilgi güvenliği sorumlusu tarafından yönetilir." şeklinde belirtilmiştir (BDDK, 2020). Bu noktada, bilgi güvenliğinin direk üst yönetime bağlanması bu birimin bir banka için ne kadar önemli olduğunu göstermektedir.

4.2. Bilgi Güvenliği Yönetişim Yapısı

Günümüzde, organizasyon yapısı geçmişe nazaran daha işlevsel bir şekilde oluşturulmaktadır. Özellikle özel sektör, özel sektörde ise finans ve bankacılık alanlarında karşımıza çıkan bu organizasyon yapısı üç temel parçadan oluşmaktadır. Bu katmanlar stratejik seviye, taktiksel seviye ve operasyonel seviye şeklinde belirtilmektedir. Bu katmanları açıklamak gerekirse;

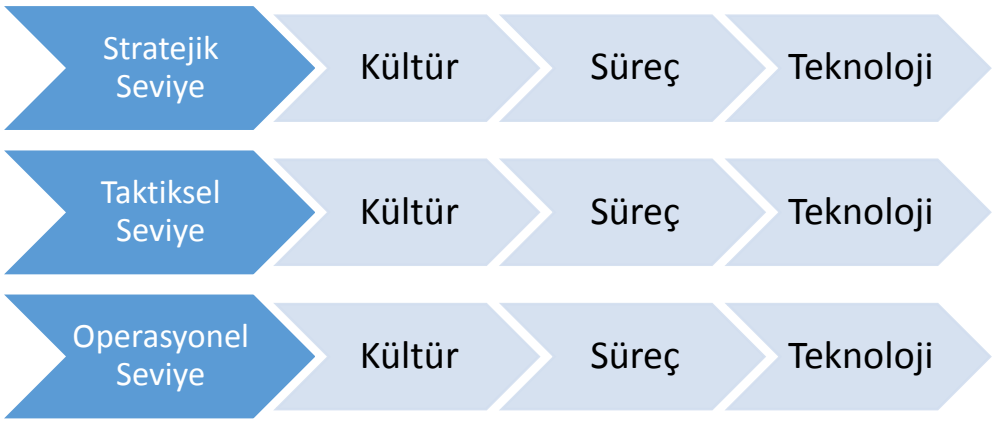
- Stratejik seviye; yönetim kurulu ve üst yönetim seviyesindeki rollerden oluşmakta olup, yatay düzlemde tek bir ekiptir. Temel görevleri; politika üretme, hedef ve stratejileri belirleme, organizasyon içi koordinasyonu sağlama, yatırım kararları alma, performans izleme ve değerlendirme şeklinde sıralanabilir. Bunun yanı sıra yasal kuruluşlar, birlikler ve diğer organizasyonlarla iletişim ve koordinasyonu sağlamak da yine stratejik seviye rollerinin arasında bulunmaktadır.

- Taktiksel seviye, ilgili iş kollarındaki genel müdür yardımcısı ve o iş kolunda yer alan birim ve bölüm yöneticileri rollerinden oluşur. Yatay düzlemde, organizasyondaki iş kolu kadar taktiksel ekip oluşmaktadır. Örnek olarak, merkezi operasyon/üretim işkolu, kredi ve izleme iş kolu, bilgi ve iletişim teknolojileri iş kolu olarak söyleyebiliriz. Temel görevleri; stratejik seviyede alınan kararların nasıl uygulanacağına dair plan ve program yapmak ve uygulanmasını sağlamaktır. Kendi iş kollarında, planlama, koordinasyon, izleme ve değerlendirme yapmaktır. Bu seviye ağırlıklı olarak 'ne, nasıl yapılacak' sorularının cevabına odaklı çalışmalar yürütür.

- Operasyonel seviye; ilgili iş kolundaki birimlerin veya bölümlerin kendi içindeki servislerden ve buradaki rollerden oluşmaktadır. Buradaki ekip sayısı, birim, bölüm veya içlerinde alan servisler kadardır. Örnek olarak, bilgi ve iletişim teknolojileri iş kolu, BT Alt Yapı Birimi, network yönetimi servisi, yönetici ve uzman rolü şeklinde söyleyebiliriz. Temel görevi, kendi alanındaki işin nasıl yapılacağını belirlemek, gerekli süreç, yöntem ve talimatları oluşturarak bunu fiilen gerçekleştirmektir.

Bu noktada bahsedilen her bir katman, kendi içinde de yine üç boyutta incelenebilmektedir. Bu üç boyut kültür, süreç ve teknoloji boyutu olarak sıralanmaktadır. Buna göre;

- Kültür boyutu; var olan birim veya bölümlerdeki roller ile bu rollerde yer alan insanlar ve bunların yetkinliklerinden oluşmaktadır.
- Süreç boyutu; ürün veya hizmet sağlamanın nasıl yapılacağının belirlenmesi ve bunun gerçekleştirilmesini kapsamaktadır.
- Teknoloji boyutu, ürün veya hizmet sağlanması sürecinde otomasyon, yazılım, donanım, makine araç ve gereçlerinin kullanılmasını kapsamaktadır.



Şekil 6. Bilgi Güvenliği Yönetişim Yapısı

Bilgi güvenliği yönetişim yapısı da kendi içinde üç katmandan ve her bir katman üç boyuttan oluşmaktadır. Bilgi güvenliği yönetişim yapısını bu katman ve boyutlar açısından iki bölümde inceleyebiliriz.

1. Stratejik Katman

   Bilgi güvenliği yönetimine yönelik üst seviye politikaların belirlenmesi, tabi olunan yasal mevzuatın takibi ve politikalarla uyumlu hale getirilmesi ve BGYS'nin performansının izlenmesi çalışmaları yürütülmektedir. Bu seviyede, bir birim ve burada görev yapacak yönetici ve uzman roller yer almaktadır. Süreç olarak; mevzuat takip, performans izleme, raporlama, politika yazma gibi süreçler işletilmektedir. Teknolojik olarak Office uygulamaları ve varsa süreçlerde kullanılan diğer uygulamalar kullanılmaktadır.

2. Taktiksel ve Operasyonel Katman

   Bilgi güvenliği yönetişim yapısında bu iki katman ayrı ayrı olabileceği gibi birlikte de ele alınabilir. Mevcut organizasyonda birlikte ele alınmasın daha etkili olacağı düşünüldüğünden burada da birlikte ele alınmaktadır. Bu noktada belirlenen politikaların süreçlerde uygulanması sağlanmakta, her bir bilgi güvenliği sürecinin fiili uygulanmasına ve geliştirilmesine odaklanılmaktadır. Bu seviyede bir birim ve burada görev yapacak yönetici ve uzman roller yer almaktadır. Süreç olarak; kayıt yönetimi, ağ güvenliği yönetimi, sertifika yönetimi, zararlı analizi, zafiyet tarama gibi tüm bilgi güvenliği süreçleri yürütülmektedir. Teknolojik olarak ise süreçlerin gerçekleştirilmesine yardımcı araçlar kullanılmaktadır. Örnek olarak; zafiyet tarama araçları, zararlı yazılım analiz etme araçları, kayıt tutma araçları, ağ güvenliği saldırı önleme araçları gibi teknolojik imkânlardan yararlanılmaktadır.

4.3. Bankacılık Bilgi Güvenliği Mevzuatları

Bankacılık Düzenleme ve Denetleme Kurumu tarafından bankacılık sektöründe bilgi güvenliğini düzenlemek için, Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik yayınlanmış olup tüm gereksinimler bu yönetmelikte belirtilmektedir. Bu mevzuata göre temel gereksinimler aşağıdaki başlıklar altında belirtilmiştir (BDDK, 2020):

- Başlangıç Hükümleri
- Bilgi Sistemlerine İlişkin Risk Yönetimi Ve Kontrollerinin Tesisi
    - Bilgi sistemleri yönetişimi

    - Bilgi sistemleri risklerinin yönetilmesi
    - Bilgi güvenliği yönetimi
    - Sistem geliştirme ve değişiklik yönetimi
    - Bilgi sistemleri sürekliliği ve erişilebilirlik yönetimi
    - Dış hizmet alımı
    - Bilgi sistemleri iç kontrol ve iç denetim faaliyetleri
- Elektronik Bankacılık Hizmetleri
    - Ortak hükümler
    - İnternet bankacılığı
    - Mobil bankacılık
    - Telefon bankacılığı
    - Açık bankacılık servisleri
    - ATM bankacılığı
- Çeşitli ve Son Hükümler
    - Çeşitli hükümler
    - Son hükümler

Çalışmamızın temelini oluşturan bilgi güvenliği farkındalığı, bu mevzuat içerisinde belirtilen gereksinimler arasında yer almaktadır. Özellikle 'bilgi güvenliği farkındalığını arttırma' isimli madde içerisinde bu gereksinimler açıklanmıştır. Mevzuat gereği, bilgi güvenliği farkındalık seviyesini arttıracak çalışmaların yapılması gerekmektedir. Bu çalışmalar, üst yönetim de dâhil olmak üzere tüm banka çalışanlarını, müşterileri ve destek alınan dış firmaları kısaca bilgi güvenliğinin tüm paydaşlarını kapsamalıdır.

5. ÇALIŞANLARIN BİLGİ GÜVENLİĞİ FARKINDALIĞINA İLİŞKİN BİR ARAŞTIRMA: BANKA ÖRNEĞİ

Bu bölümde, araştırmanın amacı ve araştırmanın metodolojisi ile ilgili bilgiler verilmektedir. Aynı zamanda, araştırma sonucunda elde edilen bulgular ve bu bulguların sonuçları değerlendirilmektedir.

5.1. Araştırmanın Amacı

Gelişen teknolojiyle bilgi güvenliğinin önemi gün geçtikçe artmaktadır. Bilgi güvenliğinin sağlanmasında ilk olarak teknolojik önlemler akla gelmektedir. Bu noktada unutulmamalıdır ki kurulan tüm bu teknik altyapıyı nihayetinde insan kullanmaktadır. Alınan önlemlerin gelişmesinde genel olarak teknolojik alanlara yatırım yapılmaktadır. Kaynakların çoğu sistemsel gelişmelere aktarılmaktadır. Fakat tüm bu teknik gelişmeler kadar insan faktörünün gelişimi de önemlidir. Bu çalışma kapsamında, insanın sosyal anlamdaki gelişimine dikkat çekilerek; araştırma konusu, bilgi güvenliği farkındalığına ilişkin algı zemini üzerine oturtulmuştur.

Özellikle bankacılık ve finans sektörlerinde bilgi güvenliğinin sağlanmasına fazlasıyla önem verilmektedir. Bir bankanın bünyesinde barındırdığı bilgi ve kaynaklar düşünüldüğünde, bunların zarar görmesi durumunda ortaya tahribat yaratacak sonuçlar çıkabilmektedir. Kazanılması zor, kaybedilmesi kolay olarak bilinen güven duygusuna zarar gelmesi, hem anlık vereceği zararlar hem de gelecekte oluşturacağı olumsuz intibadan dolayı bir bankanın asla istemeyeceği bir durumdur. Hiçbir müşteri, bilgisini sızdıran, emanet ettiği parasına sahip çıkamayan veya bilgisiz olduğunu düşündüğü personele sahip bir banka ile çalışmak istemez. Dolayısıyla bankalar, hem banka olarak itibar kaybı yaşamamak, hem mevcut müşteri kaybına neden olmamak, hem de maddi zarara uğramamak içi gerekli tüm güvenlik önlemlerini almaktadır ve personeline de bu anlamda yatırım yapmaktadır. Tüm bu nedenlerden ötürü çalışanların bilgi güvenliği farkındalığı yüksek derecede öneme sahiptir.

Literatür incelendiğinde ülkemizde bir banka özelinde çalışanların bilgi güvenliği farkındalığa ilişkin algılarının ölçülmesine yönelik bir çalışmaya rastlanmamıştır. Gerçekleştirilen çalışmalarda BGYS, kişisel veya kurumsal BG, siber güvenlik gibi konularda üzerinde değerlendirmeler yapıldığı görülmüştür. Daha çok teknolojik anlamda yapılması gerekenler ve alınması gereken önlemler üzerinde durulan

çalışmalarda, çalışanların bilgi güvenliği farkındalığının etkilerini yeterli düzeyde incelenmediği görülmüştür. Bu araştırma alanyazında bulunan bu eksiği tamamlamak amacıyla hazırlanmıştır.

Bu araştırma, ülkemizde bulunan özel bir bankanın genel müdürlüğünde bulunan çalışanların bilgi güvenliği farkındalığının ölçülmesini amaçlamaktadır. Bu amaç doğrultusunda aşağıdaki sorulara cevap aranacaktır.

Bilgi güvenliği farkındalığı personellerin;

- Cinsiyetine göre farklılaşmakta mıdır?
- Yaşına göre farklılaşmakta mıdır?
- Öğrenim durumuna göre farklılaşmakta mıdır?
- Kurumdaki görev türüne göre farklılaşmakta mıdır?
- Çalıştığı birime göre farklılaşmakta mıdır?
- Görev süresine göre farklılaşmakta mıdır?
- İnternet kullanım süresine göre farklılaşmakta mıdır?

5.2. Araştırmanın Metodolojisi

5.2.1. Problemin Tanımı

Bilgi güvenliğinin sağlanmasında en önemli faktörlerden biri insandır. İnsan, önem seviyesi yüksek olması sebebiyle eğer gerekli farkındalık oluşturulmazsa aynı zamanda en büyük tehdit unsuru haline de dönüşebilmektedir. Alınan tüm teknolojik önlemler insan tarafından kullanılmakta ve yönetilmektedir. Bu çerçevede değerlendirildiğinde çalışanların bilgi güvenliği farkındalığı, kurumsal BG oluşmasında etkili bir unsur olarak karşımıza çıkmaktadır.

Başarılı ve süreklilik arz edecek bir şekilde bilgi güvenliği yönetiminin işletilmesi, çalışanların bilgi güvenliği konusunda farkındalık seviyelerinin yüksek olmasıyla sağlanabilmektedir. Bilgi güvenliğinin önemli bir süreç olarak işletildiği bankalarda da, farkındalık seviyelerine ilişkin çalışmaların yapılması gerekmektedir.

Bu araştırmanın problemi, bilgi güvenliğinin sağlanması için alınan önlemlerin genelde teknolojik açıdan değerlendirildiği ve bu süreçte insan faktörünün etkisinin yeterince incelenmediği şeklindedir.

5.2.2. Evren ve Örneklem

Bu araştırmanın evrenini Türkiye'de bulunan özel bir bankanın genel müdürlüğünde çalışan 3791 personel oluşturmaktadır. Çalışmanın örneklemini ise uygun örneklem yöntemi ile seçilmiş olan 321 personel oluşturmaktadır.

5.2.3. Araştırmanın Sınırlılığı

Bu araştırmanın en önemli sınırlılığı bankacılık sektörü içerisinde sadece bir bankanın genel müdürlüğünde çalışan personellerini kapsıyor olmasıdır.

5.2.4. Veri Toplama ve Araçlarının Hazırlanması

Bu araştırmada Keser ve Güldüren tarafından geliştirilen Bilgi Güvenliği Farkındalık Ölçeği kullanılmıştır. Bu ölçek EK-2'de yer almaktadır (Keser & Güldüren, 2015, s. 1167). Aynı zamanda çalışanların demografik özelliklerini belirlemek amacıyla Kişisel Bilgi Formu oluşturulan ilgili form ise EK-1'de yer almaktadır.

5.2.4.1. Kişisel Bilgi Formu

Araştırmada kullanılan kişisel bilgi formu kapsamında çalışanlara 7 tane soru sorulmuştur. Bu sorular ile çalışmaya katılan personelin demografik özellikleri belirlenmiştir.

5.2.4.2. Bilgi Güvenliği Farkındalık Ölçeği

Araştırmada kullanılan Bilgi Güvenliği Farkındalık Ölçeği, 5'li likert tipinde toplam 34 maddeden oluşmaktadır. Ölçekte "hiç katılmıyorum", "katılmıyorum", "kararsızım", "katılıyorum" ve "tamamen katılıyorum" derecelerine ayrılmış olumlu ve olumsuz ifadeler bulunmaktadır.

5.2.5. Faktör Analizleri

Bilgi güvenliği farkındalık ölçeğinin alt boyutlarını tespit etmek amacıyla faktör analizi yapılmıştır. Verilen faktör analizine uygunluğunun test edilmesi için, Kaiser-Meyer-Olkin (KMO) örneklem yeterliliği testi ve Bartlett küresellik testi uygulanmıştır. Bu değerlerden KMO değerinin 0,50'nin üzerinde ve Bartlett testinin de 0,05'in üzerinde olmasından dolayı (KMO=0,957, χ2Bartlett test =11418,56,

p=0,000) veri seti analize uygun bulunmuştur. Tüm değişkenlerin dâhil edildiği ölçeğin Cronbach α değeri (0,974), 0,70 kritik eşik değerinin oldukça üzerindedir.(Bkz. Tablo 1.)

Tablo 1. Bilgi Güvenliği Farkındalığı Faktör Analizi

	Cronbach α	**KMO**	**Açıklanan Toplam Varyans**
Bilgi Güvenliği Farkındalığı	0,974	0,957	72,180

Temel bileşenler yöntemi ve Varimax döndürme yöntemi kullanılarak ölçekte bulunan sorular analiz edilmiştir. Faktör ağırlığı 0,50 değerinin altında kalan, faktör altında tek kalan veya birbirine yakın faktör ağırlıkları olan soru bulunmadığından dolayı ölçekten soru çıkartılmamıştır. Toplam 34 soru sorudan oluşan dört ayrı faktör elde edilmiştir. Elde edilen faktörlerin güvenilirlik analizleri sonucu dördünün de 0,70 güvenilirlik düzeyinin üstünde olduğu görülmüştür. Faktörler aşağıdaki gibi isimlendirilmiştir:

- Kişisel Verilerin Korunması
- Saldırı ve Tehditler
- Güvenlik Önlemi Alma
- Bilgi Güvenliği Bilinci

Faktörlerin içsel tutarlılıklarının hesaplanmasında Cronbach α değerleri kullanılmıştır. Tüm bu değerler Tablo 2'de belirtilmektedir.

Tablo 2. Bilgi Güvenliği Farkındalığı Faktör Analizi – 2

Faktör Adı	**Faktör Soruları**	**Faktör Ağırlıkları**	**Faktörün Açıklayıcılığı**	**Güvenilirlik**
Kişisel Verilerin Korunması	Dijital imza (digital signature) nedir biliyorum.	0,550	21,681	0,947
	Şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum.	0,688		
	E-posta gönderirken "Gizli" (BCC) alanının sağladığı avantajları biliyorum.	0,557		

	İstenmeyen elektronik posta (spam) nedir biliyorum.	0,749		
	İstenmeyen elektronik posta miktarını azaltmak için gerekli bilgiye sahibim.	0,645		
	Sosyal ağ sitelerini (social networking sites) güvenli olarak nasıl kullanacağımı biliyorum.	0,695		
	USB sürücülerini (USB drives) kullanırken dikkat edilmesi gereken hususları biliyorum.	0,730		
	Taşınabilir cihazlara (portable devices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum.	0,735		
	Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.	0,708		
	Kişisel mahremiyet nedir biliyorum.	0,750		
	Çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum.	0,733		
	Mavidiş (Bluetooth) teknolojisi ile veri aktarımı konusunda bilgi sahibiyim.	0,593		
Saldırı ve Tehditler	Kimlik hırsızlığı (identity theft) nedir biliyorum.	0,618	21,512	0,959
	Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.	0,620		
	Hizmet aksatma (Denial of Service - DoS) saldırısı nedir biliyorum.	0,692		
	Kimlik avı (phishing) saldırısı nedir biliyorum.	0,708		
	Sosyal mühendislik (social engineering) saldırısı nedir biliyorum.	0,744		
	Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum	0,736		
	Siber zorbalık (cyberbullying) nedir biliyorum.	0,838		
	Siber zorbalığa karşı kendimi nasıl koruyacağımı biliyorum.	0,837		
	Siber zorbalığa karşı çocuklarımı nasıl koruyacağımı biliyorum	0,807		
Güvenlik Önlemi Alma	Bilgisayarıma casus yazılım yüklenmesini engelleme yöntemlerini biliyorum.	,738	20,268	0,944
	Bilgisayarımda casus yazılım (spyware) olup olmadığını anlayabilirim.	0,719		
	Kötü niyetli yazılımlara (malware) karşı alınması gereken güvenlik tedbirlerini biliyorum.	0,716		
	Bilgisayarıma kötü niyetli kod (malicious code) bulaşıp bulaşmadığını anlayabilirim.	0,700		
	Bilgi sistemlerinde kullanılan virüs koruma yazılımını nasıl kullanacağımı biliyorum.	0,655		

	Sahte virüs koruma yazılımının ne olduğunu biliyorum.	0,645		
	Bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (realtime protection) özelliğini kullanmaktayım.	0,611		
	Zincir e-postalara (chain e-mail) karşı nasıl hareket etmem gerektiğini biliyorum.	0,602		
	Bilgisayarımdaki virüs koruma yazılımının otomatik güncelleştirme yapmasını sağlayabilirim.	0,574		
	Aldatmaca (hoax) nedir biliyorum.	0,571		
Bilgi Güvenliği Bilinci	Bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum.	0,797	8,719	0,877
	Kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum.	0,776		
	Bilgi güvenliğinin ne anlama geldiğini biliyorum.	0,657		

5.2.6. Normallik Testi

Bir dağılımın simetrisinin ölçülmesi yapılan analiz açısından önemlidir. Yapılan karşılaştırmalar normal bir dağılımla yapılması gerekmektedir. Bu dağılımların pozitif eğimli olanları büyük değerlere ve sağa doğru kuyruklara sahiptir. Negatif eğimli bir dağılım ise nispeten küçük değerlere ve sola doğru kuyruklara sahiptir. Çarpıklık değerleri -1 ile +1 dışında kalması durumunda, büyük ölçüde çarpık bir dağılımı gösterir ve normal bir dağılıma sahip olmadığını ifade eder (Hair, Black, Babin, & Anderson, 2013, s. 34). Bu doğrultuda tüm alt boyutlarımıza ait çarpıklık(Skewness) ve basıklık(Kurtosis) değerleri(Tablo 3) incelendiğinde, -1 ile +1 arasında olduğu görülmüştür. Buna bağlı olarak verimizin tüm boyutlar için normal dağıldığını söyleyebiliriz.

Tablo 3. Normallik Testi

Normallik Testi			
		İstatistik	**Standart Sapma**
	Skewness	-0,689	0,136

Kişisel Verilerin Korunması	Kurtosis	0,124	0,271
Saldırı ve Tehdit	Skewness	-0,413	0,136
	Kurtosis	-0,386	0,271
Bilgi Güvenliği Bilinci	Skewness	-0,630	0,136
	Kurtosis	-0,526	0,271
Güvenlik Önlemi Alma	Skewness	-0,313	0,136
	Kurtosis	-0,303	0,271

5.3. Araştırmanın Bulguları ve Değerlendirilmesi

5.3.1. Demografik Özellikler

5.3.1.1. Cinsiyet Kriterine Göre Dağılım

Araştırmaya katılanların %19,6'sı kadın, %80,4'ü erkektir.

Tablo 4. Cinsiyet Kriteri Frekans Dağılımı

Cinsiyet		
	Frekans	**Yüzde**
Kadın	63	19,6
Erkek	258	80,4
Toplam	321	100

İnternet Kullanım Süresi	,177**	,310**	,185**	-,263**	,160**	,243**	1				
Kişisel Verilerin Korunması	0,098	-0,075	-0,058	0,087	-0,102	-0,077	0,005	1			
Saldırı ve Tehditler	0,101	-0,078	-0,055	0,087	-,161**	-0,065	-0,019	,707**	1		
Güvenlik Önlemi Alma	,188**	-0,035	-,119*	0,094	-,142*	-0,051	0,015	,736**	,824**	1	
Bilgi Güvenliği Bilinci	0,072	0,074	-0,033	0,019	-0,077	0,020	0,078	,653**	,485**	,516**	1
**. Korelasyon 0.01 düzeyinde anlamlıdır.											
*. Korelasyon 0.05 düzeyinde anlamlıdır.											

Korelasyon tablosundaki değerler incelendiğinde, gruplar ile alt boyutlar arasında aşağıdaki ilişkiler tespit edilmiştir.

- Cinsiyet ile güvenlik önlemi alma arasında (r=0,18, p<0,01) düşük düzeyde pozitif yönlü anlamlı bir ilişki bulunmaktadır.
- Öğrenim durumu ile güvenlik önlemi alma arasında (r=-0,11, p<0,05) düşük düzeyde negatif yönlü anlamlı bir ilişki bulunmaktadır.
- Çalıştığı birim ve güvenlik önlemi alma arasında (r=-0,14, p<0,05) düşük düzeyde negatif yönlü anlamlı bir ilişki bulunmaktadır.
- Çalıştığı birim ve saldırı ve tehditler arasında (r=-0,16, p<0,01) düşük düzeyde negatif yönlü bir ilişki bulunmaktadır.

5.3.2.2. Cinsiyet Değişkeni ile Yapılan Bağımsız Gruplar t-Testi Sonuçları

H_{2a}: Cinsiyete göre Kişisel Verilerin Korunması farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan kişisel verilerin korunmasının, cinsiyet değişkenine göre bağımsız grup t-Testi gerçekleştirilmiştir. Analiz sonucu istatiksel olarak farklılık gösteren grup ortalama değerlerinin anlamlı olup olmadığı incelenmiştir. Tablo 12'de görüleceği üzere p değeri 0.05'ten büyük olduğu için grup ortalamaları arasındaki farkın anlamlı bir fark olmadığı tespit edilmiştir. Bu doğrultuda, kişisel verilerin korunması yönünde cinsiyet açısından herhangi bir fark bulunamamış ve H_{2a} hipotezi reddedilmiştir.

Tablo 12. Cinsiyet ve Kişisel Verilerin Korunması t-Testi Tablosu

		N	Ort.	S.S.	t değeri	p değeri
Kişisel Verilerin Korunması	**Kadın**	63	4,09	0,67	-1,760	0,079
	Erkek	258	4,26	0,65		

H_{2b}: Cinsiyete göre Saldırı ve Tehditler farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan saldırı ve tehditlerin, cinsiyet değişkenine göre bağımsız grup t-Testi gerçekleştirilmiştir. Analiz sonucu istatiksel olarak farklılık gösteren grup ortalama değerlerinin anlamlı olup olmadığı incelenmiştir. Tablo 13'de görüleceği üzere p değeri 0.05'ten büyük olduğu için grup ortalamaları arasındaki farkın anlamlı bir fark olmadığı tespit edilmiştir. Bu doğrultuda, saldırı ve tehditler yönünde cinsiyet açısından herhangi bir fark bulunamamış ve H_{2b} hipotezi reddedilmiştir.

Tablo 13. Cinsiyet ve Saldırı ve Tehditler t-Testi Tablosu

		N	Ort.	S.S.	t değeri	p değeri
Saldırı ve Tehditler	**Kadın**	63	3,46	0,99	-1,811	0,071
	Erkek	258	3,71	0,96		

H_{2c}: Cinsiyete göre Güvenlik Önlemi Alma farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan güvenlik önlemi alma, cinsiyet değişkenine göre bağımsız grup t-Testi gerçekleştirilmiştir. Analiz sonucu istatiksel olarak farklılık gösteren grup ortalama değerlerinin anlamlı olup olmadığı incelenmiştir. Tablo 14'te görüleceği üzere p değeri 0.05'ten küçük olduğu için grup ortalamaları arasındaki farkın anlamlı bir fark olduğu tespit edilmiştir. Bu doğrultuda, güvenlik önlemi alma yönünde cinsiyet açısından fark bulunmuş ve H_{2d} hipotezi kabul edilmiştir. Buna göre ortalama değeri daha büyük olduğu için, güvenlik önlemi alma konusunda kadınlara göre erkeklerin daha fazla farkındalığı olduğu görülmüştür. (Kadın Ort.=3,27, Erkek Ort.=3,70)

Tablo 14. Cinsiyet ve Güvenlik Önlemi Alma t-Testi Tablosu

		N	Ort.	S.S.	t değeri	p değeri
Güvenlik Önlemi Alma	**Kadın**	63	3,27	0,93	-3,425	0,001
	Erkek	258	3,70	0,85		

H_{2d}: Cinsiyete göre Bilgi Güvenliği Bilinci farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan bilgi güvenliği bilinci, cinsiyet değişkenine göre bağımsız grup t-Testi gerçekleştirilmiştir. Analiz sonucu istatiksel olarak farklılık gösteren grup ortalama değerlerinin anlamlı olup olmadığı incelenmiştir. Tablo 15'de görüleceği üzere p değeri 0.05'ten büyük olduğu için grup ortalamaları arasındaki farkın anlamlı bir fark olmadığı tespit edilmiştir. Bu doğrultuda, bilgi güvenliği bilinci yönünde cinsiyet açısından herhangi bir fark bulunamamış ve H_{2d} hipotezi reddedilmiştir.

Tablo 15. Cinsiyet ve Bilgi Güvenliği Bilinci t-Testi Tablosu

		N	Ort.	S.S.	t değeri	p değeri
Bilgi Güvenliği Bilinci	**Kadın**	63	4,39	0,59	-1,295	0,196
	Erkek	258	4,49	0,53		

5.3.2.3. Yaş Gruplarına Göre Tek Yönlü Varyans (ANOVA) Sonuçları

Bilgi güvenliği farkındalığı alt boyutları ile yaş grupları arasındaki analizde, 2den fazla grup sayısına sahip olunması sebebiyle ANOVA yöntemi kullanılmıştır. Alt boyutların tümü için homojenlik testi incelendiğinde Levene p değerinin 0,05'ten büyük olmasında dolayı ANOVA'ya uygun bulunmuştur. Bu analizlerle birlikte aşağıdaki hipotezler değerlendirilmiştir.

H_{3a}: Yaşa göre Kişisel Verilerin Korunması farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan kişisel verilerin korunmasının, yaş gruplarına göre farklılık gösterip göstermediği Tablo 16'daki veriler doğrultusunda

incelenmiştir. Kişisel verilerin korunması p değeri 0,05'ten büyük olduğu için yaş grupları ile arasında fark bulunamamış ve H_{3a} hipotezi reddedilmiştir.

Tablo 16. Yaş Gruplarına Göre Kişisel Verilerin Korunması Boyutu ANOVA Testi Sonucu

	Yaş Grupları	N	Ort.	df	F değeri	p değeri
Kişisel Verilerin Korunması	23-27	43	4,30	3	1,18	0,316
	28-32	112	4,23			
	33-37	75	4,30			
	38 ve üzeri	91	4,12			

H_{3b}: Yaşa göre Saldırı ve Tehditler farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan saldırı ve tehditlerin, yaş gruplarına göre farklılık gösterip göstermediği Tablo 17'deki veriler doğrultusunda incelenmiştir. Saldırı ve tehditler p değeri 0,05'ten büyük olduğu için yaş grupları ile arasında fark bulunamamış ve H_{3b} hipotezi reddedilmiştir.

Tablo 17. Yaş Gruplarına Göre Saldırı ve Tehditler Boyutu ANOVA Testi Sonucu

	Yaş Grupları	N	Ort.	df	F değeri	p değeri
Saldırı ve Tehditler	23-27	43	3,75	3	1,13	0,334
	28-32	112	3,69			
	33-37	75	3,75			
	38 ve üzeri	91	3,51			

H_{3c}: Yaşa göre Güvenlik Önlemi Alma farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan güvenlik önlemi almanın, yaş gruplarına göre farklılık gösterip göstermediği Tablo 18'deki veriler doğrultusunda incelenmiştir. Güvenlik önlemi alma p değeri 0,05'ten büyük olduğu için yaş grupları ile arasında fark bulunamamış ve H_{3c} hipotezi reddedilmiştir.

Tablo 18. Yaş Gruplarına Göre Güvenlik Önlemi Alma Boyutu ANOVA Testi Sonucu

	Yaş Grupları	N	Ort.	df	F değeri	p değeri
Güvenlik Önlemi Alma	23-27	43	3,52	3	1,73	0,160
	28-32	112	3,66			
	33-37	75	3,76			
	38 ve üzeri	91	3,47			

H_{3d}: Yaşa göre Bilgi Güvenliği Bilinci farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan bilgi güvenliği bilincinin, yaş gruplarına göre farklılık gösterip göstermediği Tablo 19'daki veriler doğrultusunda incelenmiştir. Bilgi güvenliği bilinci p değeri 0,05'ten büyük olduğu için yaş grupları ile arasında fark bulunamamış ve H_{3d} hipotezi reddedilmiştir.

Tablo 19. Yaş Gruplarına Göre Bilgi Güvenliği Bilinci Boyutu ANOVA Testi Sonucu

	Yaş Grupları	N	Ort.	df	F değeri	p değeri
Bilgi Güvenliği Bilinci	23-27	43	4,37	3	0,83	0,478
	28-32	112	4,46			
	33-37	75	4,52			
	38 ve üzeri	91	4,50			

5.3.2.4. Öğrenim Durumuna Göre Tek Yönlü Varyans (ANOVA) Sonuçları

Bilgi güvenliği farkındalığı alt boyutları ile öğrenim durumu grupları arasındaki analizde, 2den fazla grup sayısına sahip olunması sebebiyle ANOVA yöntemi kullanılmıştır. Alt boyutların tümü için homojenlik testi incelendiğinde Levene p değerinin 0,05'ten büyük olmasında dolayı ANOVA'ya uygun bulunmuştur. Bu analizlerle birlikte aşağıdaki hipotezler değerlendirilmiştir.

H_{4a}: Öğrenim durumuna göre Kişisel Verilerin Korunması farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan kişisel verilerin korunmasının, öğrenim durumu gruplarına göre farklılık gösterip göstermediği Tablo 20'deki veriler

doğrultusunda incelenmiştir. Kişisel verilerin korunması p değeri 0,05'ten büyük olduğu için öğrenim durumu grupları ile arasında fark bulunamamış ve H_{4a} hipotezi reddedilmiştir.

Tablo 20. Öğrenim Durumu Gruplarına Göre Kişisel Verilerin Korunması Boyutu ANOVA Testi Sonucu

	Öğrenim Durumu Grupları	N	Ort.	df	F değeri	p değeri
Kişisel Verilerin Korunması	Lise	17	4,27	4	0,65	0,621
	Ön Lisans	28	4,38			
	Lisans	213	4,21			
	Yüksek Lisans	58	4,22			
	Doktora	5	3,96			

H_{4b}: Öğrenim durumuna göre Saldırı ve Tehditler farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan saldırı ve tehditlerin, öğrenim durumu gruplarına göre farklılık gösterip göstermediği Tablo 21'deki veriler doğrultusunda incelenmiştir. Saldırı ve tehditler p değeri 0,05'ten büyük olduğu için öğrenim durumu grupları ile arasında fark bulunamamış ve H_{4b} hipotezi reddedilmiştir.

Tablo 21. Öğrenim Durumu Gruplarına Göre Saldırı ve Tehditler Boyutu ANOVA Testi Sonucu

	Öğrenim Durumu Grupları	N	Ort.	df	F değeri	p değeri
Saldırı ve Tehditler	Lise	17	3,86	4	1,08	0,365
	Ön Lisans	28	3,94			
	Lisans	213	3,60			
	Yüksek Lisans	58	3,72			
	Doktora	5	3,46			

H_{4c}: Öğrenim durumuna göre Güvenlik Önlemi Alma farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan güvenlik önlemi alma, öğrenim durumu gruplarına göre farklılık gösterip göstermediği Tablo 22'deki veriler doğrultusunda incelenmiştir. Güvenlik önlemi alma p değeri 0,05'ten küçük olduğu için öğrenim durumu grupları ile arasında fark bulunmuş ve H_{4c} hipotezi kabul edilmiştir.

Tukey karşılaştırma testi sonucunda, güvenlik önlemi alma konusunda ön lisans ve lisans öğrenim durumuna sahip çalışanlar arasında anlamlı bir fark olduğu görülmüştür(Ön Lisans=4,08, Lisans=3,54). Analiz sonucunda ön lisans öğrenim durumuna sahip personelin lisans öğrenim durumuna sahip olanlara göre güvenlik önlemi alma konusunda daha fazla farkındalığa sahip oldukları tespit edilmiştir(Ort. fark=0,54).

Tablo 22. Öğrenim Durumu Gruplarına Göre Güvenlik Önlemi Alma Boyutu ANOVA Testi Sonucu

	Öğrenim Durumu Grupları	N	Ort.	df	F değeri	p değeri
Güvenlik Önlemi Alma	Lise	17	3,86	4	2,86	0,023
	Ön Lisans	28	3,94			
	Lisans	213	3,60			
	Yüksek Lisans	58	3,72			
	Doktora	5	3,46			

Tukey Sonuçları		Ort. Farkı	Standart Sapma	p değeri
Lise	Ön Lisans	-0,21	0,27	0,928
	Lisans	0,32	0,22	0,580
	Yüksek Lisans	0,26	0,24	0,820
	Doktora	0,53	0,44	0,759
Ön Lisans	Lise	0,21	0,27	0,928
	Lisans	0,54*	0,17	0,019
	Yüksek Lisans	0,47	0,20	0,127
	Doktora	0,74	0,42	0,402
Lisans	Lise	-0,32	0,22	0,580
	Ön Lisans	-0,54*	0,17	0,019
	Yüksek Lisans	-0,06	0,13	0,986
	Doktora	0,20	0,39	0,986
Yüksek Lisans	Lise	-0,26	0,24	0,820

	Ön Lisans	-0,47	0,20	0,127
	Lisans	0,06	0,13	0,986
	Doktora	0,27	0,40	0,965
Doktora	Lise	-0,53	0,44	0,759
	Ön Lisans	-0,74	0,42	0,402
	Lisans	-0,20	0,39	0,986
	Yüksek Lisans	-0,27	0,40	0,965

H_{4d}: Öğrenim durumuna göre Bilgi Güvenliği Bilinci farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan bilgi güvenliği bilinci, öğrenim durumu gruplarına göre farklılık gösterip göstermediği Tablo 23'deki veriler doğrultusunda incelenmiştir. Bilgi güvenliği bilinci p değeri 0,05'ten büyük olduğu için öğrenim durumu grupları ile arasında fark bulunamamış ve H_{4d} hipotezi reddedilmiştir.

Tablo 23. Öğrenim Durumu Gruplarına Göre Bilgi Güvenliği Bilinci Boyutu ANOVA Testi Sonucu

	Öğrenim Durumu Grupları	N	Ort.	df	F değeri	p değeri
Bilgi Güvenliği Bilinci	Lise	17	4,56	4	1,79	0,129
	Ön Lisans	28	4,66			
	Lisans	213	4,43			
	Yüksek Lisans	58	4,49			
	Doktora	5	4,80			

5.3.2.5. Görev Türüne Göre Tek Yönlü Varyans (ANOVA) Sonuçları

Bilgi güvenliği farkındalığı alt boyutları ile öğrenim durumu grupları arasındaki analizde, 2'den fazla grup sayısına sahip olunması sebebiyle ANOVA yöntemi kullanılmıştır. Alt boyutlardan kişisel verilerin korunması, saldırı ve tehditler ve güvenlik önlemi alma için homojenlik testi incelendiğinde Levene p değerinin 0,05'ten büyük olmasında dolayı ANOVA'ya uygun bulunmuştur. Alt boyutlardan bilgi güvenliği bilinci için homojenlik testi incelendiğinde Levene p değerinin 0,05'ten

küçük olmasında dolayı Brown-Forsythe ve Welch'e uygun bulunmuştur. Bu analizlerle birlikte aşağıdaki hipotezler değerlendirilmiştir.

H_{5a}: Kurumda çalıştığı görevine göre Kişisel Verilerin Korunması farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan kişisel verilerin korunmasının, görev türü gruplarına göre farklılık gösterip göstermediği Tablo 24'deki veriler doğrultusunda incelenmiştir. Kişisel verilerin korunması p değeri 0,05'ten küçük olduğu için görev türü grupları ile arasında fark bulunmuş ve H_{5a} hipotezi kabul edilmiştir.

Tukey karşılaştırma testi sonucunda, kişisel verilerin korunması konusunda, üst düzey ve orta düzey yönetici görev türüne sahip çalışanlar arasında anlamlı bir fark olduğu görülmüştür.(Üst Düzey Yönetici=4,70, Orta Düzey Yönetici=4,12). Analiz sonucu üst düzey yönetici görev türüne sahip personelin orta düzey yönetici görev türüne sahip olanlara göre kişisel verilerin korunması konusunda daha fazla farkındalığa sahip oldukları tespit edilmiştir(Ort. fark=0,58).

Tablo 24. Görev Türü Gruplarına Göre Kişisel Verilerin Korunması Boyutu ANOVA Testi Sonucu

	Görev Türü Grupları	N	Ort.	df	F değeri	p değeri
Kişisel Verilerin Korunması	Üst Düzey Yönetici	4	4,70	2	3,49	0,031
	Orta Düzey Yönetici	132	4,12			
	Uzman/Yetkili/Diğer	185	4,29			

Tukey Sonuçları		Ort. Farkı	Standart Sapma	p değeri
Üst Düzey Yönetici	Orta Düzey Yönetici	0,58	0,33	0,192
	Uzman/Yetkili/Diğer	0,41	0,33	0,423
Orta Düzey Yönetici	Üst Düzey Yönetici	-0,58	0,33	0,192
	Uzman/Yetkili/Diğer	-0,16	0,07	0,073
Uzman/Yetkili/Diğer	Üst Düzey Yönetici	-0,41	0,33	0,423
	Orta Düzey Yönetici	0,16	0,07	0,073

H_{5b}: Kurumda çalıştığı görevine göre Saldırı ve Tehditler farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan saldırı ve tehditlerin, görev türü gruplarına göre farklılık gösterip göstermediği Tablo 25'deki veriler doğrultusunda incelenmiştir. Saldırı ve tehditler p değeri 0,05'ten büyük olduğu için görev türü grupları ile arasında fark bulunamamış ve H_{5b} hipotezi reddedilmiştir.

Tablo 25. Görev Türü Gruplarına Göre Saldırı ve Tehditler Boyutu ANOVA Testi Sonucu

	Görev Türü Grupları	N	Ort.	df	F değeri	p değeri
Saldırı ve Tehditler	Üst Düzey Yönetici	4	4,02	2	2,11	0,122
	Orta Düzey Yönetici	132	3,53			
	Uzman/Yetkili/Diğer	185	3,75			

H_{5c}: Kurumda çalıştığı görevine göre Güvenlik Önlemi Alma farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan güvenlik önlemi almanın, görev türü gruplarına göre farklılık gösterip göstermediği Tablo 26'daki veriler doğrultusunda incelenmiştir. Güvenlik önlemi alma p değeri 0,05'ten büyük olduğu için görev türü grupları ile arasında fark bulunamamış ve H_{5c} hipotezi reddedilmiştir.

Tablo 26. Görev Türü Gruplarına Göre Güvenlik Önlemi Alma Boyutu ANOVA Testi Sonucu

	Görev Türü Grupları	N	Ort.	df	F değeri	p değeri
Güvenlik Önlemi Alma	Üst Düzey Yönetici	4	4,02	2	2,70	0,068
	Orta Düzey Yönetici	132	3,48			
	Uzman/Yetkili/Diğer	185	3,70			

H_{5d}: Kurumda çalıştığı görevine göre Bilgi Güvenliği Bilinci farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan bilgi güvenliği bilincinin, görev türü gruplarına göre farklılık gösterip göstermediği Tablo 27'deki veriler doğrultusunda

incelenmiştir. Bilgi güvenliği bilinci Welch testi p değeri 0,05'ten küçük olduğu için görev türü grupları ile arasında fark bulunmuş ve H_{5d} hipotezi kabul edilmiştir.

Tamhane karşılaştırma testi sonucunda, bilgi güvenliği bilinci konusunda, üst düzey ve orta düzey yönetici görev türüne sahip çalışanlar arasında anlamlı bir fark olduğu görülmüştür.(Üst Düzey Yönetici=4,83, Orta Düzey Yönetici=4,44). Analiz sonucu üst düzey yönetici görev türüne sahip personelin orta düzey yönetici görev türüne sahip olanlara göre bilgi güvenliği bilinci konusunda daha fazla farkındalığa sahip oldukları tespit edilmiştir(Ort. fark=0,39).

Tablo 27. Görev Türü Gruplarına Göre Bilgi Güvenliği Bilinci Boyutu Welch Testi Sonucu

	Görev Türü Grupları	N	Ort.	df	F değeri	p değeri
Bilgi Güvenliği Bilinci	Üst Düzey Yönetici	4	4,83	2	9,57	0,018
	Orta Düzey Yönetici	132	4,44			
	Uzman/Yetkili/Diğer	185	4,49			

Tamhane Sonuçları		Ort. Farkı	Standart Sapma	p değeri
Üst Düzey Yönetici	Orta Düzey Yönetici	0,39*	0,10	0,049
	Uzman/Yetkili/Diğer	0,33	0,10	0,087
Orta Düzey Yönetici	Üst Düzey Yönetici	-0,39	0,10	0,049
	Uzman/Yetkili/Diğer	-0,05	0,06	0,796
Uzman/Yetkili/Diğer	Üst Düzey Yönetici	-0,33	0,10	0,087
	Orta Düzey Yönetici	0,05	0,06	0,796

5.3.2.6. Çalıştığını Birime Göre Tek Yönlü Varyans (ANOVA) Sonuçları

Bilgi güvenliği farkındalığı alt boyutları ile çalıştığı birim grupları arasındaki analizde, 2'den fazla grup sayısına sahip olunması sebebiyle ANOVA yöntemi kullanılmıştır. Alt boyutlardan kişisel verilerin korunması, saldırı ve tehditler ve güvenlik önlemi alma için homojenlik testi incelendiğinde Levene p değerinin 0,05'ten büyük olmasında dolayı ANOVA'ya uygun bulunmuştur. Alt boyutlardan bilgi güvenliği bilinci için homojenlik testi incelendiğinde Levene p değerinin 0,05'ten küçük olmasında dolayı Brown-Forsythe ve Welch'e uygun bulunmuştur. Bu analizlerle birlikte aşağıdaki hipotezler değerlendirilmiştir.

H_{6a}: Çalıştığı birime göre Kişisel Verilerin Korunması farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan kişisel verilerin korunmasının, çalıştığı birim gruplarına göre farklılık gösterip göstermediği Tablo 28'deki veriler doğrultusunda incelenmiştir. Kişisel verilerin korunması p değeri 0,05'ten küçük olduğu için çalıştığı birim grupları ile arasında fark bulunmuş ve H_{6a} hipotezi kabul edilmiştir.

Tukey karşılaştırma testi sonucunda, kişisel verilerin korunması konusunda, BT birimi çalışanları ile pazarlama/satış ve krediler ve operasyon birimleri çalışanları arasında anlamlı bir fark olduğu görülmüştür (BT=4,47, Pazarlama/Satış=3,92, Krediler ve Operasyon=4,08). Analiz sonucu BT birimi çalışanlarının hem pazarlama/satış hem de krediler ve operasyon birimleri çalışanlarına göre kişisel verilerin korunması konusunda daha fazla farkındalığa sahip oldukları tespit edilmiştir (BT ile Pazarlama/Satış Ort. Fark=0,55, BT ile Krediler ve Operasyon Ort. Fark=0,38). Aynı zamanda finans ve hazine birimi çalışanları ile krediler ve operasyon çalışanları arasında anlamlı bir fark olduğu görülmüştür(Finans ve Hazine=4,34). Analiz sonucu finans ve hazine birimi çalışanlarının krediler ve operasyon çalışanlarına göre kişisel verileri korunması konusunda daha fazla farkındalığa sahip oldukları tespit edilmiştir (Ort. Fark=0,26).

Tablo 28. Çalıştığı Birim Gruplarına Göre Kişisel Verilerin Korunması Boyutu ANOVA Testi Sonucu

	Çalıştığı Birim Grupları	N	Ort.	df	F değeri	p değeri
Kişisel Verilerin Korunması	BT	49	4,47	4	5,48	0,000
	IK ve İdari İşler	50	4,32			
	Pazarlama/Satış	22	4,92			
	Krediler ve Operasyon	127	4,08			
	Finans ve Hazine	73	4,34			

Tukey Sonuçları		Ort. Farkı	Standart Sapma	p değeri
BT	IK ve İdari İşler	0,14	0,12	0,785
	Pazarlama/Satış	0,55*	0,16	0,008
	Krediler ve Operasyon	0,38*	0,10	0,004
	Finans ve Hazine	0,12	0,11	0,824

IK ve İdari İşler	BT	-0,14	0,12	0,785
	Pazarlama/Satış	0,40	0,16	0,105
	Krediler ve Operasyon	0,24	0,10	0,169
	Finans ve Hazine	-0,02	0,11	1,000
Pazarlama/Satış	BT	-0,55*	0,16	0,008
	IK ve İdari İşler	-0,40	0,16	0,105
	Krediler ve Operasyon	-0,16	0,14	0,808
	Finans ve Hazine	-0,42	0,15	0,055
Krediler ve Operasyon	BT	-0,38*	0,10	0,004
	IK ve İdari İşler	-0,24	0,10	0,169
	Pazarlama/Satış	0,16	0,14	0,808
	Finans ve Hazine	-0,26*	0,09	0,047
Finans ve Hazine	BT	-0,12	0,11	0,824
	IK ve İdari İşler	0,02	0,11	1,000
	Pazarlama/Satış	0,42	0,15	0,055
	Krediler ve Operasyon	0,26*	0,09	0,047

H_{6b}: Çalıştığı birime göre Saldırı ve Tehditler farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan saldırı ve tehditlerin, çalıştığı birim gruplarına göre farklılık gösterip göstermediği Tablo 29'daki veriler doğrultusunda incelenmiştir. Saldırı ve tehditler p değeri 0,05'ten küçük olduğu için çalıştığı birim grupları ile arasında fark bulunmuş ve H_{6b} hipotezi kabul edilmiştir.

Tukey karşılaştırma testi sonucunda, saldırı ve tehditler konusunda, BT birimi çalışanları ile krediler ve operasyon birimleri çalışanları arasında anlamlı bir fark olduğu görülmüştür (BT=4,12, Krediler ve Operasyon=3,42). Analiz sonucu BT birimi çalışanlarının krediler ve operasyon birimi çalışanlarına göre saldırı ve tehditler konusunda daha fazla farkındalığa sahip oldukları tespit edilmiştir (Ort. fark=0,70).

Tablo 29. Çalıştığı Birim Gruplarına Göre Saldırı ve Tehditler Boyutu ANOVA Testi Sonucu

	Çalıştığı Birim Grupları	N	Ort.	df	F değeri	p değeri
Saldırı ve Tehditler	BT	49	4,12	4	5,48	0,000
	IK ve İdari İşler	50	3,78			
	Pazarlama/Satış	22	3,50			
	Krediler ve Operasyon	127	3,42			
	Finans ve Hazine	73	3,75			

Tukey Sonuçları		Ort. Farkı	Standart Sapma	p değeri
BT	IK ve İdari İşler	0,33	0,19	0,394
	Pazarlama/Satış	0,62	0,24	0,079
	Krediler ve Operasyon	0,70*	0,16	0,000
	Finans ve Hazine	0,37	0,17	0,205
IK ve İdari İşler	BT	-0,33	0,19	0,394
	Pazarlama/Satış	0,28	0,24	0,759
	Krediler ve Operasyon	0,36	0,15	0,144
	Finans ve Hazine	0,03	0,17	0,999
Pazarlama/Satış	BT	-0,62	0,24	0,79
	IK ve İdari İşler	-0,28	0,24	0,759
	Krediler ve Operasyon	0,07	0,21	0,997
	Finans ve Hazine	-0,25	0,23	0,816
Krediler ve Operasyon	BT	-0,70*	0,16	0,000
	IK ve İdari İşler	-0,36	0,15	0,144
	Pazarlama/Satış	-0,07	0,21	0,997
	Finans ve Hazine	-0,32	0,13	0,132
Finans ve Hazine	BT	-0,37	0,17	0,205
	IK ve İdari İşler	-0,03	0,17	0,999
	Pazarlama/Satış	0,25	0,23	0,816
	Krediler ve Operasyon	0,32	0,13	0,132

H_{6c}: Çalıştığı birime göre Güvenlik Önlemi Alma farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan güvenlik önlemi almanın, çalıştığı birim gruplarına göre farklılık gösterip göstermediği Tablo 30'daki veriler doğrultusunda incelenmiştir. Güvenlik önlemi alma p değeri 0,05'ten küçük olduğu için çalıştığı birim grupları ile arasında fark bulunmuş ve H_{6c} hipotezi kabul edilmiştir.

Tukey karşılaştırma testi sonucunda, güvenlik önlemi alma konusunda, BT birimi çalışanları ile pazarlama/satış ve krediler ve operasyon birimleri çalışanları arasında anlamlı bir fark olduğu görülmüştür (BT=4,05, Pazarlama/Satış=3,42, Krediler ve Operasyon=3,42). Analiz sonucu BT birimi çalışanlarının hem pazarlama/satış hem de krediler ve operasyon birimleri çalışanlarına göre güvenlik önlemi alma konusunda daha fazla farkındalığa sahip oldukları tespit edilmiştir (BT ile Pazarlama/Satış Ort. fark=0,62, BT ile Krediler ve Operasyon Ort. fark=0,62).

Tablo 30. Çalıştığı Birim Gruplarına Göre Güvenlik Önlemi Alma Boyutu ANOVA Testi Sonucu

	Çalıştığı Birim Grupları	N	Ort.	df	F değeri	p değeri
Güvenlik Önlemi Alma	BT	49	4,12	4	5,13	0,001
	IK ve İdari İşler	50	3,78			
	Pazarlama/Satış	22	3,50			
	Krediler ve Operasyon	127	3,42			
	Finans ve Hazine	73	3,75			

Tukey Sonuçları		Ort. Farkı	Standart Sapma	p değeri
BT	IK ve İdari İşler	0,41	0,17	0,130
	Pazarlama/Satış	0,62*	0,22	0,041
	Krediler ve Operasyon	0,62*	0,14	0,000
	Finans ve Hazine	0,34	0,16	0,190
IK ve İdari İşler	BT	-0,41	0,17	0,130
	Pazarlama/Satış	0,21	0,22	0,869
	Krediler ve Operasyon	0,21	0,14	0,558
	Finans ve Hazine	-0,06	0,15	0,995
Pazarlama/Satış	BT	-0,62*	0,22	0,041
	IK ve İdari İşler	-0,21	0,22	0,869
	Krediler ve Operasyon	0,00	0,20	1,000
	Finans ve Hazine	-0,27	0,21	0,684
Krediler ve Operasyon	BT	-0,62*	0,14	0,000
	IK ve İdari İşler	-0,21	0,14	0,558
	Pazarlama/Satış	-0,00	0,20	1,000
	Finans ve Hazine	-0,28	0,12	0,181
Finans ve Hazine	BT	-0,34	0,16	0,190
	IK ve İdari İşler	0,06	0,15	0,995
	Pazarlama/Satış	0,27	0,21	0,684
	Krediler ve Operasyon	0,28	0,12	0,181

H_{6d}: Çalıştığı birime göre Bilgi Güvenliği Bilinci farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan bilgi güvenliği bilincinin, görev türü gruplarına göre farklılık gösterip göstermediği Tablo 31'deki veriler doğrultusunda incelenmiştir. Bilgi güvenliği bilinci Welch testi p değeri 0,05'ten küçük olduğu için çalıştığı birim grupları ile arasında fark bulunmuş ve H_{6d} hipotezi kabul edilmiştir.

Tamhane karşılaştırma testi sonucunda, bilgi güvenliği bilinci konusunda, IK ve İdari İşler birimi çalışanları ile krediler ve operasyon birimleri çalışanları arasında anlamlı bir fark olduğu görülmüştür (IK ve İdari İşler=4,67, Krediler ve Operasyon=4,39).

Analiz sonucu IK ve idari işler birimi çalışanlarının krediler ve operasyon birimi çalışanlarına göre bilgi güvenliği bilinci konusunda daha fazla farkındalığa sahip oldukları tespit edilmiştir (Ort. fark=0,27).

Tablo 31. Çalıştığı Birim Gruplarına Göre Bilgi Güvenliği Bilinci Boyutu Welch Testi Sonucu

	Çalıştığı Birim Grupları	N	Ort.	df	F değeri	p değeri
Bilgi Güvenliği Bilinci	BT	49	4,49	4	2,59	0,037
	IK ve İdari İşler	50	4,67			
	Pazarlama/Satış	22	4,36			
	Krediler ve Operasyon	127	4,39			
	Finans ve Hazine	73	4,49			

Tukey Sonuçları		Ort. Farkı	Standart Sapma	p değeri
BT	IK ve İdari İşler	-0,17	0,09	0,513
	Pazarlama/Satış	0,13	0,15	0,993
	Krediler ve Operasyon	0,09	0,08	0,962
	Finans ve Hazine	-0,00	0,09	1,000
IK ve İdari İşler	BT	0,17	0,09	0,513
	Pazarlama/Satış	0,30	0,14	0,369
	Krediler ve Operasyon	0,27*	0,07	0,007
	Finans ve Hazine	0,17	0,08	0,405
Pazarlama/Satış	BT	-0,13	0,15	0,993
	IK ve İdari İşler	-0,30	0,14	0,369
	Krediler ve Operasyon	-0,03	0,14	1,000
	Finans ve Hazine	-0,13	0,14	0,991
Krediler ve Operasyon	BT	-0,09	0,08	0,962
	IK ve İdari İşler	-0,27*	0,07	0,007
	Pazarlama/Satış	0,03	0,14	1,000
	Finans ve Hazine	-0,09	0,08	0,926
Finans ve Hazine	BT	0,00	0,09	1,000
	IK ve İdari İşler	-0,17	0,08	0,405
	Pazarlama/Satış	0,13	0,14	0,991
	Krediler ve Operasyon	0,09	0,81	0,926

5.3.2.7. Görev Süresine Göre Tek Yönlü Varyans (ANOVA) Sonuçları

Bilgi güvenliği farkındalığı alt boyutları ile görev süresi grupları arasındaki analizde, 2'den fazla grup sayısına sahip olunması sebebiyle ANOVA yöntemi kullanılmıştır. Alt boyutlardan kişisel verilerin korunması, saldırı ve tehditler ve bilgi güvenliği

bilinci için homojenlik testi incelendiğinde Levene p değerinin 0,05'ten büyük olmasında dolayı ANOVA'ya uygun bulunmuştur. Alt boyutlardan güvenlik önlemi alma için homojenlik testi incelendiğinde Levene p değerinin 0,05'ten küçük olmasında dolayı Brown-Forsythe ve Welch'e uygun bulunmuştur. Bu analizlerle birlikte aşağıdaki hipotezler değerlendirilmiştir.

H_{7a}: Görev süresine göre Kişisel Verilerin Korunması farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan kişisel verilerin korunmasının, görev süresi gruplarına göre farklılık gösterip göstermediği Tablo 32'deki veriler doğrultusunda incelenmiştir. Kişisel verilerin korunması p değeri 0,05'ten büyük olduğu için görev süresi grupları ile arasında fark bulunamamış ve H_{7a} hipotezi reddedilmiştir.

Tablo 32. Görev Süresi Gruplarına Göre Kişisel Verilerin Korunması Boyutu ANOVA Testi Sonucu

	Görev Süresi Grupları	N	Ort.	df	F değeri	p değeri
Kişisel Verilerin Korunması	0-3 yıl	92	4,33	4	1,80	0,128
	4-6 yıl	80	4,15			
	7-9 yıl	60	4,19			
	10-14 yıl	47	4,32			
	15 yıl ve üzeri	42	4,07			

H_{7b}: Görev süresine göre Saldırı ve Tehditler farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan saldırı ve tehditlerin, görev süresi gruplarına göre farklılık gösterip göstermediği Tablo 33'deki veriler doğrultusunda incelenmiştir. Saldırı ve tehditler p değeri 0,05'ten büyük olduğu için görev süresi grupları ile arasında fark bulunamamış ve H_{7b} hipotezi reddedilmiştir.

Tablo 33. Görev Süresi Gruplarına Göre Saldırı ve Tehditler Boyutu ANOVA Testi Sonucu

Saldırı ve Tehditler	Görev Süresi Grupları	N	Ort.	df	F değeri	p değeri

	0-3 yıl	92	3,71	4	1,00	0,405
	4-6 yıl	80	3,65			
	7-9 yıl	60	3,76			
	10-14 yıl	47	3,70			
	15 yıl ve üzeri	42	3,39			

H_{7c}: Görev süresine göre Güvenlik Önlemi Alma farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan güvenlik önlemi almanın, görev süresi gruplarına göre farklılık gösterip göstermediği Tablo 34'deki veriler doğrultusunda incelenmiştir. Güvenlik önlemi alma Brown-Forsythe p değeri 0,05'ten büyük olduğu için görev süresi grupları ile arasında fark bulunamamış ve H_{7c} hipotezi reddedilmiştir.

Tablo 34. Görev Süresi Gruplarına Göre Güvenlik Önlemi Alma Boyutu Brown-Forsythe Testi Sonucu

	Görev Süresi Grupları	N	Ort.	df	F değeri	p değeri
Güvenlik Önlemi Alma	0-3 yıl	92	3,68	4	0,86	0,489
	4-6 yıl	80	3,56			
	7-9 yıl	60	3,65			
	10-14 yıl	47	3,70			
	15 yıl ve üzeri	42	3,42			

H_{7d}: Görev süresine göre Bilgi Güvenliği Bilinci farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan bilgi güvenliği bilincinin, görev süresi gruplarına göre farklılık gösterip göstermediği Tablo 35'deki veriler doğrultusunda incelenmiştir. Bilgi güvenliği bilinci p değeri 0,05'ten büyük olduğu için görev süresi grupları ile arasında fark bulunamamış ve H_{7d} hipotezi reddedilmiştir.

Tablo 35. Görev Süresi Gruplarına Göre Bilgi Güvenliği Bilinci Boyutu ANOVA Testi Sonucu

	Görev Süresi Grupları	N	Ort.	df	F değeri	p değeri
Bilgi Güvenliği Bilinci	0-3 yıl	92	4,47	4	1,21	0,304
	4-6 yıl	80	4,44			
	7-9 yıl	60	4,45			
	10-14 yıl	47	4,63			
	15 yıl ve üzeri	42	4,40			

5.3.2.8. İnternet Kullanım Süresine Göre Tek Yönlü Varyans (ANOVA) Sonuçları

Bilgi güvenliği farkındalığı alt boyutları ile görev süresi grupları arasındaki analizde, 2'den fazla grup sayısına sahip olunması sebebiyle ANOVA yöntemi kullanılmıştır. Alt boyutlardan saldırı ve tehditler ve güvenlik önlemi için homojenlik testi incelendiğinde Levene p değerinin 0,05'ten büyük olmasında dolayı ANOVA'ya uygun bulunmuştur. Alt boyutlardan kişisel verilerin korunması ve bilgi güvenliği bilinci için homojenlik testi incelendiğinde Levene p değerinin 0,05'ten küçük olmasında dolayı Brown-Forsythe ve Welch'e uygun bulunmuştur. Bu analizlerle birlikte aşağıdaki hipotezler değerlendirilmiştir.

H_{8a}: İnternet kullanma süresine göre Kişisel Verilerin Korunması farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan kişisel verilerin korunmasının, internet kullanma süresi gruplarına göre farklılık gösterip göstermediği Tablo 36'daki veriler doğrultusunda incelenmiştir. Kişisel verileri korunması Welch testi p değeri 0,05'ten küçük olduğu için çalıştığı birim grupları ile arasında fark bulunmuş ve H_{8a} hipotezi kabul edilmiştir.

Tamhane karşılaştırma testi sonucunda, kişisel verilerin korunması konusunda, 0-4 yıldır internet kullanım süresi grubu çalışanları ile 5-9 yıldır internet kullanım süresi grubu çalışanları arasında anlamlı bir fark olduğu görülmüştür (0-4 yıl=4,80, 5-9 yıl=4,26). Analiz sonucu 0-4 yıldır internet kullanan çalışanlarının 5-9 yıldır internet kullanan çalışanlarına göre kişisel verileri korunması konusunda daha fazla farkındalığa sahip oldukları tespit edilmiştir (Ort. fark=0,54).

Tablo 36. İnternet Kullanma Süresi Gruplarına Göre Kişisel Verilerin Korunması Boyutu Welch Testi Sonucu

	İnternet Kullanma Süresi Grupları	N	Ort.	df	F değeri	p değeri
Kişisel Verilerin Korunması	0-4 yıl	3	4,80	3	9,72	0,002
	5-9 yıl	22	4,26			
	10-14 yıl	115	4,16			
	15 yıl ve üzeri	181	4,25			

Tamhane Sonuçları		Ort. Farkı	Standart Sapma	p değeri
0-4 yıl	5-9 yıl	0,54*	0,17	0,045
	10-14 yıl	0,64	0,11	0,052
	15 yıl ve üzeri	0,54	0,11	0,078
5-9 yıl	0-4 yıl	-0,54*	0,17	0,045
	10-14 yıl	0,09	0,14	0,989
	15 yıl ve üzeri	0,00	0,14	1,000
10-14 yıl	0-4 yıl	-0,64	0,11	0,052
	5-9 yıl	-0,09	0,14	0,989
	15 yıl ve üzeri	-0,09	0,07	0,783
15 yıl ve üzeri	0-4 yıl	-0,54	0,11	0,078
	5-9 yıl	-0,00	0,14	1,000
	10-14 yıl	0,09	0,07	0,783

H_{8b}: İnternet kullanma süresine göre Saldırı ve Tehditler farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan saldırı ve tehditlerin, internet kullanma süresi gruplarına göre farklılık gösterip göstermediği Tablo 37'deki veriler doğrultusunda incelenmiştir. Saldırı ve tehditler p değeri 0,05'ten büyük olduğu için internet kullanım süresi grupları ile arasında fark bulunamamış ve H_{8b} hipotezi reddedilmiştir.

Tablo 37. İnternet Kullanma Süresi Gruplarına Göre Saldırı ve Tehditler Boyutu ANOVA Testi Sonucu

	İnternet Kullanma Süresi Grupları	N	Ort.	df	F değeri	p değeri
Saldırı ve Tehditler	0-4 yıl	3	4,59	3	1,64	0,178
	5-9 yıl	22	3,84			
	10-14 yıl	115	3,56			

	15 yıl ve üzeri	181	3,69			

H_{8c}: İnternet kullanma süresine göre Güvenlik Önlemi Alma farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan güvenlik önlemi almanın, internet kullanma süresi gruplarına göre farklılık gösterip göstermediği Tablo 38'deki veriler doğrultusunda incelenmiştir. Güvenlik önlemi alma p değeri 0,05'ten büyük olduğu için internet kullanma süresi grupları ile arasında fark bulunamamış ve H_{8c} hipotezi reddedilmiştir.

Tablo 38. İnternet Kullanma Süresi Gruplarına Göre Güvenlik Önlemi Alma Boyutu ANOVA Testi Sonucu

	İnternet Kullanma Süresi Grupları	N	Ort.	df	F değeri	p değeri
Güvenlik Önlemi Alma	0-4 yıl	3	4,33	3	1,14	0,332
	5-9 yıl	22	3,63			
	10-14 yıl	115	3,53			
	15 yıl ve üzeri	181	3,65			

H_{8d}: İnternet kullanma süresine göre Bilgi Güvenliği Bilinci farkındalığı açısından farklılık vardır.

Bilgi güvenliği farkındalığının alt boyutu olan bilgi güvenliği bilincinin, internet kullanma süresi gruplarına göre farklılık gösterip göstermediği Tablo 39'daki veriler doğrultusunda incelenmiştir. Bilgi güvenliği bilinci Welch testi p değeri 0,05'ten küçük olduğu için çalıştığı birim grupları ile arasında fark bulunmuş ve H_{8d} hipotezi kabul edilmiştir.

Tamhane karşılaştırma testi sonucunda, bilgi güvenliği bilinci konusunda 0-4 yıldır internet kullanım süresi grubu çalışanları ile 5-9 yıldır internet kullanım süresi grubu çalışanları arasında anlamlı bir fark olduğu görülmüştür (0-4 yıl=4,88, 5-9 yıl=4,33). Analiz sonucu 0-4 yıldır internet kullanan çalışanlarının 5-9 yıldır internet kullanan çalışanlarına göre bilgi güvenliği bilinci konusunda daha fazla farkındalığa sahip oldukları tespit edilmiştir (Ort. fark=0,55).

Tablo 39. İnternet Kullanma Süresi Gruplarına Göre Bilgi Güvenliği Bilinci Boyutu Welch Testi Sonucu

	İnternet Kullanma Süresi Grupları	N	Ort.	df	F değeri	p değeri
Bilgi Güvenliği Bilinci	0-4 yıl	3	4,88	3	5,10	0,020
	5-9 yıl	22	4,33			
	10-14 yıl	115	4,42			
	15 yıl ve üzeri	181	4,52			

Tamhane Sonuçları		Ort. Farkı	Standart Sapma	p değeri
0-4 yıl	5-9 yıl	0,55	0,16	0,053
	10-14 yıl	0,46	0,12	0,193
	15 yıl ve üzeri	0,36	0,11	0,331
5-9 yıl	0-4 yıl	-0,55	0,16	0,053
	10-14 yıl	-0,08	0,13	0,988
	15 yıl ve üzeri	-0,18	0,13	0,662
10-14 yıl	0-4 yıl	-0,46	0,12	0,193
	5-9 yıl	0,08	0,13	0,988
	15 yıl ve üzeri	-0,10	0,06	0,477
15 yıl ve üzeri	0-4 yıl	-0,36	0,11	0,331
	5-9 yıl	0,18	0,13	0,662
	10-14 yıl	0,10	0,06	0,477

6. SONUÇ VE ÖNERİLER

Gelişen teknolojiyle, kurumlar da süreçlerini bu gelişime ayak uyduracak şekilde düzenlemeye çalışmışlardır. Bu değişim, beraberinde bazı riskler doğurmuştur. Özellikle bilginin dijital hale gelmesiyle birlikte güvenliğinin sağlanması konusu da önem kazanmıştır. Bu doğrultuda kurumlar bilgi güvenliği konusunda daha fazla yatırım ve planlama gerçekleştirecekleri bir döneme girmişlerdir.

Günümüzde çok konuşulan bir konu haline gelen bilgi güvenliği özellikle bankalar için hayati öneme sahip bir kavramdır ve gelişen teknolojiyle önemi her geçen gün daha da artmaktadır (Gazdağı & Çetinyokuş, 2020, s. 487). Gerek bankaların sahip olduğu bilgilerin önemi, gerekse de tüm bu bilgilerin korunmasına dair denetim mekanizmasına sahip kurumların varlığı bu alandaki çalışmaları nitelikli bir konuma getirmiştir. Fakat bilgi güvenliğinin sağlanması adına alınan önlemler noktasında sadece teknolojik yatırımların yeterli kalmadığı görülmüştür. Bu noktada insan

faktörünün önemi ortaya çıkmaktadır. Nihayetinde kurulan teknolojik altyapının yönetimini de insan sağlamaktadır ve zincirin son halkası olarak insan değerlendirilir.

İnsan faktörünün, oluşturulmaya çalışılan bilgi güvenliği yapısı içerisindeki en etkili özelliği olarak bilgi güvenliği farkındalığı karşımıza çıkmaktadır. Kurumlar bu farkındalığı sağlamadan, alınan önlemlerin bilgi güvenliğini sağlama konusunda yetersiz kalındığını tecrübe ettikleri görülmektedir. Öyle ki, sektör bağımsız tüm kurumlar farkındalık üzerine çalışmalar yapmaktadırlar. Kurumların çalışanları ve tüm paydaşları üzerinde, bilgi güvenliğini sağlamak adına güçlü çıkarımlardan bir tanesi olan bilgi güvenliği farkındalığını sağladığı takdirde, kurulan tüm teknolojik altyapısının işlevselliğinin güçlendiği görülmektedir.

Bu bağlamda, bilgi güvenliği farkındalığının kurumlar için önemi yüksek olması ve göz ardı edilmemesi gereken bir süreç olması ve özellikle finans sektörünün neredeyse tüm faaliyetlerini bilişim sistemleri aracığıyla gerçekleştirdikleri kritik seviyedeki operasyonlarına etkisi düşünüldüğünde, çalışanların bilgi güvenliği farkındalığına ilişkin araştırma yapılması uygun görülmüştür.

Araştırmamız, Türkiye'de özel bir banka çalışanları arasından toplam 321 çalışan üzerinde "Bilgi Güvenliği Farkındalık Ölçeği" uygulanmıştır. Bu uygulamanın sonuçları ise IBM SPSS Statistics 25 programı aracılığı ile analiz edilmiştir. İlgili anketler personele bankanın İnsan Kaynakları birimi aracılığı ile internet üzerinden iletilmiş olup, anketin tamamını dolduranlar analize dâhil edilmiştir.

Bilgi güvenliği farkındalığı ölçeğine uygulanan faktör analizi sonucunda, 4 alt boyut ortaya çıkmıştır. Oluşan "Kişisel Verilerin Korunması", Saldırı ve Tehditler", Güvenlik Önlemi Alma" ve Bilgi Güvenliği Bilinci" alt boyutları ile demografik özellikler arasındaki ilişkiler incelenerek sonuçları değerlendirilmiştir. Oluşturulan hipotezler, genel bilgi güvenliği algısına yönelik durumlar sonucunda, alanyazında sıklıkla vurgulanan sorunsal değerler üzerine kurgulanmıştır.

Özel bir banka çalışanlarının bilgi güvenliği farkındalıklarını değerlendirilmesi için gerçekleştirilen bu çalışmadan sonra ortaya aşağıdaki gibi sonuçlar çıkmıştır:

Cinsiyet ile bilgi güvenliği farkındalığının alt boyutları arasındaki ilişki incelenmiş ve erkek çalışanlar ile kadın çalışanlar arasında özellikle güvenlik önlemi alma

konusunda farklılık gözlemlenmiştir. Ortalama değerler doğrultusunda yapılan değerlendirmeye göre erkek çalışanların kadın çalışanlara göre daha fazla farkındalığa sahip olduğu tespit edilmiştir. Bu noktada kadın ile erkek arasında oluşan fark, demografik dağılımdaki erkek yoğunluğunun fazla olması ile alakalıda olabilir. Alan yazında bulunan araştırma sonuçları ise bu araştırma sonucunu destekler niteliktedir. Farklı çalışan gruplar üzerinde yapılan araştırmalarda, diğer alt boyutlar için yine erkeklerin farkındalığının kadınlara oranla daha yüksek olduğu gözlemlenmiştir. Bir üniversitenin idari ve akademik personeli üzerinde yapılan "Bilgi Güvenliği Farkındalık Ölçeği" araştırma sonucuna göre kişisel verilerin korunması, saldırı ve tehditler, güvenlik önlemi alma ve bilgi güvenliği bilinci konularında erkek çalışanların kadın çalışanlara göre daha fazla farkındalığa sahip olduğu görülmüştür (Öztezcan, 2017, s. 138). Banka çalışanlarına yönelik yapılan araştırmada aradaki bu farkın sadece savunma alt boyutu üzerinde görülmüş olması, bankacılık faaliyetlerine ilişkin yapılan farkındalık çalışmalarının savunma ağırlıklı olması şeklinde değerlendirilebileceği gibi diğer alt boyutlarda benzer seviyede bir bilince sahip olunması şeklinde de yorumlanmaktadır.

Yaş ile bilgi güvenliği farkındalığının alt boyutları arasındaki ilişki incelenmiş ve anlamlı bir fark görülmemiştir. Alanyazında bulunan bir araştırmaya göre; genç kuşağın teknoloji ile daha iç içe olması nedeniyle, yaş ortalaması büyük olan çalışanların genç yaştaki çalışanlara göre güvenlik konusundaki farkındalık seviyelerinin daha düşük olduğu belirtilmiştir (Bostan & Akman, 2011, s. 18). Bu bağlamda Bostan'ın araştırması bu araştırmanın sonucunu desteklememektedir. Yaş ile farkındalık arasındaki ilişki konusunda farklı sonuçlar elde edilen birçok araştırma mevcuttur. Dolayısıyla gelecekteki araştırmalar için, yaş açısından detaylı bir karşılaştırma ve araştırma yapılması önerilmektedir.

Öğrenim durumu ile bilgi güvenliği farkındalığının alt boyutları arasındaki ilişki incelenmiş ve güvenlik önlemi alma konusunda ön lisans mezunları ile lisans mezunları arasında fark gözlemlenmesine rağmen diğer öğrenim durumu grupları ile diğer alt boyutlar arasında herhangi bir farka rastlanmamıştır. Bu farka göre ön lisans mezunlarının güvenlik önlemi alma konusunda lisans mezunlarından daha fazla farkındalığa sahip oldukları görülmüştür. Bu sonuç, bir bankanın yapısı düşünüldüğünde aslında öğrenim durumundaki farka rağmen güvenlik konusunda

daha hassas olunabileceğini göstermiştir. Bu durumun arka planında bankanın çalışanlarını ayırt etmeden herkese bu konuda gerekli eğitimi ve desteği verdiğini göstermektedir. Aynı zamanda genel itibariyle ön lisans mezunları işlerin operasyon kısmında çalıştıkları için bilgi güvenliğiyle ilgili yaşanan durumlarla daha çok karşılaşmaktadırlar. Dolayısıyla mevcut tehditler ve olaylar itibariyle daha çok iç içe olduklarından dolayı farkındalık seviyeleri yüksek çıkmış olabilir. Alanyazın incelendiğinde bu araştırmanın reddedilen hipotezlerini destekler nitelikle olan sonuçlara rastlanmıştır. Bir araştırma sonucuna göre katılımcıların bilgi güvenliği farkındalıkları eğitim durumlarına göre değişmemektedir (Mart, 2012, s. 69).

Görev türü ile bilgi güvenliği farkındalığının alt boyutları arasındaki ilişki incelenmesi sonucunda kişisel verilerin korunması ve bilgi güvenliği bilinci konularında üst düzey yöneticiler ile orta düzey yöneticiler arasında farklılık gözlemlenmiştir. Bu farka göre üst düzey yöneticiler kişisel verilerin korunması ve bilgi güvenliği bilinci konularında orta düzey yöneticilere göre daha fazla farkındalığa sahip oldukları görülmüştür. Alan yazın araştırmasında banka çalışanlarının görev türlerine göre bilgi güvenliği farkındalıklarının karşılaştırıldığı bir çalışmaya rastlanmamıştır. Bu nedenle bu araştırma bu farklılığı ortaya koyarak alan yazına katkıda bulunmuştur.

Çalıştığı birim ile bilgi güvenliği farkındalığının alt boyutları arasındaki ilişki incelenmiş ve her alt boyut için farklılıklar görülmüştür. Kişisel verilerin korunması konusunda Bilgi Teknolojileri çalışanlarının farkındalığı Pazarlama/Satış bölümü çalışanlarına göre daha yüksek olduğu, Krediler ve Operasyon çalışanlarının farkındalığı ise hem Bilgi Teknolojileri hem de Finans ve Hazine çalışanlarına göre daha düşük olduğu görülmüştür. Saldırı ve tehditler konusunda Bilgi Teknolojileri çalışanlarının farkındalığı Krediler ve Operasyon bölümü çalışanlarına göre daha yüksek olduğu görülmüştür. Güvenlik önlemi alma konusunda Bilgi Teknolojileri çalışanlarının farkındalığı hem Pazarlama/Satış hem de Krediler ve Operasyon çalışanlarına göre daha yüksek olduğu görülmüştür. Kişisel verilerin korunması konusunda IK ve İdari İşler çalışanlarının farkındalığı Krediler ve Operasyon çalışanlarına göre daha yüksek olduğu görülmüştür. Analiz sonuçlarına göre Bilgi Teknolojileri çalışanlarının farkındalık seviyelerinin diğer birimler karşısında ön plana çıktığı görülmektedir. Bunun nedeni gerek teknolojiyle iç içe olmaları gerekse de güvenlik başlığının bir teknoloji konusu olması şeklinde değerlendirilmektedir. Aynı

zamanda Krediler ve Operasyon bölümü çalışanlarının farkındalık seviyelerin her alt boyutta düşük kaldığı görülmektedir. Bu durum, bankacılık faaliyetlerinin kritik bir bölümünü yürüten çalışanların bilgi güvenliği farkındalığının yetersiz olduğu şeklinde değerlendirilmektedir. Genel olarak finansal faaliyetleri yürüten birimlerin algıları sadece yapılan işlemlerle sınırla kalabilmektedir. Bankacılık faaliyeti işlemlerinin tamamlanması odaklı çalışmakla beraber diğer konulara kendilerini kapatarak bir bakıma göz ardı edebilmektedirler. Bu noktada, Krediler ve Operasyon çalışanlarının bilgi güvenliği farkındalığını artırmak adına çalışmalar yapılması gerektiği önerilmektedir. Alanyazın incelendiğinde meslek dallarına göre bilgi güvenliği farkındalığı karşılaştırılması yapıldığı görülmüştür. Araştırma sonucuna göre mühendis olanların diğer meslek dallarından daha fazla bilgi güvenliği farkındalığına sahip olduğu tespit edilmiştir (Mart, 2012, s. 63). Banka nezdinde bilgi teknolojileri bölümünde çalışanların büyük bir bölümünün mühendis olduğu düşünülürse, alanyazında bulunan bu araştırma sonucu banka bünyesinde yapılan araştırma sonucunu desteklemektedir.

Görev süresi ile bilgi güvenliği farkındalığının alt boyutları arasındaki ilişki incelenmiş ve anlamlı bir fark görülmemiştir. Alanyazında bir araştırmaya göre; saldırı ve tehditler konusunda çalışanların görev sürelerine göre anlamlı bir fark görülmediği, buna karşılık olarak kişisel verilerin korunması konusunda görev süresi 8 ve üstü olan çalışanların diğer gruplara göre daha yüksek farkındalığa sahip oldukları belirtilmiştir (Taner, 2019, s. 57). Bu bağlamda Taner'in araştırma sonuçlarını bu araştırma sonuçlarını saldırı ve tehditler konusunda desteklediği, kişisel verileri korunması konusunda desteklemediği görülmüştür.

İnternet kullanım süresi ile bilgi güvenliği farkındalığının alt boyutları arasındaki ilişki incelenmiş ve kişisel verilerin korunması konusu ile bilgi güvenliği bilinci konularında 0-4 yıldır internet kullananlar ile 5-9 yıldır internet kullananlar arasında farklılık gözlemlenmiştir. Buna göre 0-4 yıldır internet kullanan çalışanların, 5-9 yıldır internet kullanan çalışanlara göre hem kişisel verilerin korunması hem de bilgi güvenliği bilinci konularında daha fazla farkındalığa sahip oldukları görülmüştür. Aynı zamanda saldırı ve tehditler ile güvenlik önlemi alma konularında tüm gruplar için anlamlı bir farklılık görülmemiştir. Alanyazın incelendiğinde bir grup çalışan üzerinde gerçekleştirilen araştırma sonucuna göre bilgi güvenliği farkındalığı ile çalışanların

kaç yıldır internet kullandıkları arasında anlamlı bir farklılık görülmemiştir (Çöp, 2017, s. 67). Bu durumda alanyazın araştırması sonucu, banka bünyesinde yapılan araştırma sonucunu saldırı ve tehditler ile güvenlik önlemi alma konularında desteklerken, kişisel verilerin korunması ve bilgi güvenliği bilinci konularında desteklememektedir. Bu noktada internet kullanım süresi kısa olanların farkındalık seviyelerinin düşük çıkması beklenebilir. Fakat bu noktada uzun yıllardır internet kullananlarda körelme yaşanabiliyor. Yeni kullanıcıların algıları bu anlamda daha açık olabilirken, uzun yıllardır kullananlar bir nevi rehavete kapılarak ilgisiz kalabiliyor. Dolayısıyla yeni sayılabilecek internet kullanıcılarının farkındalık seviyeleri, daha uzun yıllardır internet kullananlara göre yüksek çıkması bu şekilde yorumlanabilir.

Bu araştırmada çalışanların bilgi güvenliği farkındalıklarının analitik olarak incelenmesi sonucunda, bankacılık sektöründe bilgi güvenliğinin sağlanması adına sunulan öneriler şu şekildedir:

- Banka bünyesinde etkili ve verimli bir bilgi güvenliği sağlanmak isteniyorsa, oluşturulması gereken bilgi güvenliği farkındalığı sadece bu alanla ilgili çalışanları değil, birimine veya kademelerine bakılmaksızın tüm çalışanları kapsaması gerekmektedir.

- Bilgi güvenliği farkındalığı çalışmaları sadece banka çalışanları üzerinde değil, bankanın tüm paydaşları olarak değerlendirilebilecek olan dış firmaları ve ziyaretçileri de kapsayacak şekilde gerçekleştirilmelidir.

- Kurumdaki genç çalışanlarla genç sayılmayacak çalışanları bir araya getirecek programlar düzenlenerek, teknoloji ile daha çok iç içe olan genç çalışanların bilgi güvenliği farkındalığı konusundaki algılarını paylaşmaları sağlanabilir.

- Bir alt eğitim seviyesine sahip çalışanların, bir üst eğitim seviyesine sahip çalışanlara göre bilgi güvenliği farkındalıklarının yüksek çıkması durumuna karşılık eğitim seviyesinin artması karşısında bilgi güvenliği farkındalığının artması da beklenmemelidir. Bu noktada kurumlar her çalışanı için bilgi güvenliği farkındalık beklentisini eşit düzeyde tutması gerekmektedir.

- İleride yapılacak çalışmalarda, çalışanların görev türüne göre bilgi güvenliği farkındalıklarının incelenmesi alanyazına katkı sağlayacaktır.

- Banka bünyesinde teknolojik dünyaya diğer birimlere nazaran daha uzak birimler tespit edilerek, bilgi güvenliği farkındalığı konusunda bu birimlere daha fazla odaklanılmalıdır. Bilgi güvenliği farkındalık adına gerçekleştirilen çalışmalara ek farkındalık çalışmaları yapılması gerekmektedir.

- Teknoloji ile iç içe ve bilgi güvenliği farkındalığı yüksek birimler tespit edilerek, olası riskler ve alınabilecek önlemler konusunda hem farklı bir gözden bakılması hem de kurum yapısının bilinmesi itibariyle firik alışverişinde bulunulması kurum içi çalışmalara katkı sağlayacaktır.

- Çalışanların kurumdaki görev sürelerine bakılmaksızın tüm çalışanlardan temelde seviyede bilgi güvenliği farkındalığına sahip olmaları sağlanmalıdır. 1 günlük çalışan ile 1 yıllık çalışan arasında sağlanması gereken farkındalık seviyesinde fark olmaması gerekmektedir. Mümkünse yeni başlayan çalışanlara, bazı test ve sınavlar uygulanarak, önceden belirlenmiş olan temel bilgi güvenliği farkındalığı seviyesine erişmeden göreve başlatılmamalıdır. Sonrasında alanına ve ihtiyaçlarına göre bu seviye artırılmalıdır.

- Bu çalışmada değerlendirilmeye dâhil edilmiş personel, tek bir bankanın tek bir şehrinde bulunan çalışanları ile sınırlı kalmıştır. İleride yapılacak olan çalışmalarda, Bilgi Güvenliği Farkındalığı ölçeğini birden fazla bankaya hatta mümkünse farklı illerden daha fazla katılımcıya ulaştırarak bir farkındalık analizi çalışması yapılması alanyazına katkı sağlayacaktır.

Sonuç olarak, bilgi güvenliğinin bir banka için ne derece önemli olduğu, bilgi güvenliğinin tarihsel gelişimi, prensipleri, tehditleri ve alınabilecek önlemleri ile birlikte düşünülerek ortaya koyulmuştur. Aynı zamanda banka çalışanlarının bilgi güvenliği algılarının süreçler üzerindeki olumlu veya olumsuz etkileri olduğu görülmüştür. Bu çalışma ile bankacılık sektöründe çalışanların bilgi güvenliği farkındalıkları analitik olarak incelenmiş ve alanyazındaki benzeri çalışmalar ile karşılaştırılmıştır. Kurumsal çerçevede bu kavramlar, bireysel ve örgütsel faktörlerin etkisi değerlendirilerek açıklanmıştır. Gelecek araştırmalar, bankalar arası bilgi güvenliği ve çalışanların bilgi güvenliği farkındalığını analiz edebilir, banka müşterilerinin bu noktadaki etkilerini de analiz ederek alanyazına katkı sağlayabilir.

KAYNAKLAR

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers and Security, 26*(4), 276-289.

Arıcak, O. T. (2011). Siber zorbalık: Gençlerimizi bekleyen yeni tehlike. *Kariyer Penceresi, 2*(6), 10-12.

Ayanoğlu, Y. (2013). Bankaların Kuruluşu ve Organizasyon Yapısı. A. Karapınar içinde, *Bankaların Yönetimi ve Denetimi* (s. 2-33). Eskişehir: Anadolu Üniversitesi.

Bauer, S., & Bernroider, E. (2017, August). From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization. *The DATA BASE for Advances in Information Systems, 48*(3), 44-68.

Bauer, S., & Bernroider, E. W. (2015). The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring. *Third International Conference, HAS 2015, Held as Part of HCI International 2015* (s. 154-164). Los Angeles, CA, USA: Springer.

BDDK. (2020). *Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik.* Nisan 30, 2020 tarihinde BDDK: https://www.bddk.org.tr/ContentBddk/dokuman/mevzuat_0947.pdf adresinden alındı

Bostan, A., & Akman, İ. (2011). Bilişim Güvenliği : Kullanıcı Açısından Bir Durum Tespiti. *TMMOB EMO ANKARA ŞUBESİ HABER BÜLTENİ*(6), 12-18.

BSI. (2008). *Bundesamt für Sicherheit in der Informationstechnik.* Ocak 15, 2020 tarihinde https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.html adresinden alındı

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

Çetinkaya, L., Güldüren, C., & Keser, H. (2017). Öğretmenler İçin Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması. *Milli Eğitim, 46*(216), 33-52.

Çöp, Ç. Ç. (2017). *Kalite Yöneti Direktörlerinin Bilgi Güvenliği Farkındalığı: İstanbul İli Örneği.* İstanbul: T.C. Okan Üniversitesi Sağlık Bilimleri Esntitüsü.

Çöp, Ç. Ç. (2017). *Kalite Yönetim Direktörlerinin Bilgi Güvenliği Farkındalığı: İstanbul İli Örneği.* İstanbul: Okan Üniversitesi (Yüksek Lisans Tezi).

Durankaya, İ., & Saymaz, Ö. (2019). *Bilgi Güvenliği Yönetim Sistemi Kurulum, İşletim ve Denetim* (Birinci b.). İstanbul: Cinius Yayınları.

Eminağaoğlu, M., & Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları Ve Çözüm Önerileri. *Sosyal Bilimler Enstitüsü Dergisi, 11*(4), 01-15.

Ganbat, O. (2013). *Bilgi Güvenliği Yönetim Sistemi ISO/IEC 27001 ve Bilgi Güvenliği Risk Yönetimi ISO/IEC 27005 Standartlarının Uygulanması.* İzmir: Ege Üniversitesi Fen Bilimleri Enstitüsü (Yüksek Lisans Tezi).

Gazdağı, O., & Çetinyokuş, T. (2020). Bankacılık Sektöründe Bilgi Güvenliği ve İş Sürekliğinin Sağlanması Amacıyla ISO/IEC 27001 ve ISO 22301 Standartlarının Uygulanmasına Yönelik Kavramsal İnceleme. *Journal of Humanities and Tourism Research, 10*(2), 475-491.

Gelbstein, E., & Kamal, A. (2002). *Information Insecurity.* New York: United Nations ICT Task Force and the United Nations Institute for Training and Research.

Genç, C. (2019). *Kişisel Verilerin korunması Kapsamında Bilgi Güvenliği Farkındalığı Analizi ve E-Devlet Yapısının İncelenmesi.* İstanbul: Okan Üniversitesi (Yüksek Lisans Tezi).

Glasshouse. (2020). *Siber Saldırı Riskini Azaltmanın 10 Yolu.* Mart 20, 2020 tarihinde http://otomasyondergisi.com.tr/bolumler/teknolojik-trendler/siber-saldiri-riskini-azaltmanin-10-yolu/ adresinden alındı

Goldstein, J., Chernobai , A., & Benaroch , M. (2011). An Event Study Analysis of the Economic Impact of. *Journal of the Association for Information Systems, 12*(9), 606-631.

Gökce, A. G. (2010). *Bilgi Güvenliği Farkındalığı Nasıl Ölçülür? (1).* Aralık 22, 2019 tarihinde http://www.asimgencergokce.com/bilgi-guvenligi-farkindaligi-nasil-olculur-1/ adresinden alındı

Güngör, M. (2015). *Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma.* Ankara: T.C. Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı (Uzmanlık Tezi).

Hair, J., Black, W., Babin, B., & Anderson, R. (2013). *Multivariate Data Analysis.* Harlow: Pearson Education Limited.

Kapanoğlu, G. (2016). *Öğretmenlerin Bilgi Güvenliği Farkındalığının İncelenmesi.* Ankara: Gazi Üniversitesi Eğitim Bilimleri Enstitüsü (Yüksek Lisans Tezi).

Kaspersky. (2020). *Gerçek Zamanlı Siber Tehdit Haritası*. Nisan 26, 2020 tarihinde Kaspersky: https://cybermap.kaspersky.com/tr/ adresinden alındı

Kesebir, M., & Mutlu, M. D. (2019). Türk Bankacılık Sektöründeki Yönetsel Ve Örgütsel Uygulamalar Üzerine Eleştireler Ve Yeni Görüşler. S. Sönmez, E. Özçoban, D. Balkan, & H. Karakuş içinde, *Sosyal, Beşeri ve İdari Bilimler Alanında Yeni Ufuklar* (s. 321-340). Ankara: Gece Akademi.

Keser, H., & Güldüren, C. (2015). Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması. *K. Ü. Kastamanu Eğitim Dergisi, 23*(2), 1167-1184.

Keung, Y. H. (2014). Basic Principle of Information Security. *Advances in Robotics & Automation, 3*(2).

Kruger, H. A., Flowerday, S., Drevin, L., & Steyn, T. (2011). An assessment of the role of cultural factors in information security awareness. *Information Security South Africa Conference.* Johannesburg, South Africa: IEEE.

KVKK. (2016). *Kişisel Verilerin Korunması Kanunu.* Şubat 20, 2020 tarihinde https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf adresinden alındı

Kwak, D.-H., Kizzier, D. M., Zo, H., & Jung, E. (2011, September). Understanding Security Knowledge and National Culture: A Comparative Investigation between Korea and the U.S. *Asia Pacific Journal of Information Systems, 21*(3), 51-69.

Limenya. (2015). *Veri ve Bilgi Arasındaki Fark*. Kasım 5, 2019 tarihinde Limenya: https://limenya.com/veri-ve-bilgi-arasindaki-fark/ adresinden alındı

Malwarebytes. (2020). *Cybersecurity Basics*. Ocak 30, 2020 tarihinde https://www.malwarebytes.com/malware/ adresinden alındı

Mart, İ. (2012). *Bilişim Kültüründe Bilgi Güvenliği Farkındalığı.* Kahramanmaraş: Kahramanmaraş Sütçü İmam Üniversitesi (Yüksek Lisans Tezi).

Moen, R., & Clifford, N. (2009). The History of the PDCA Cycle. *In Proceedings of the 7th ANQ Congress* (s. 1-11). Tokyo: Asian Network for Quality.

NIST. (2018). *National Institute of Standards and Technology*. Mayıs 18, 2019 tarihinde https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information adresinden alındı

OECD. (2008). *OECD Policy Guidance on Online Identity Theft.* Seoul: Korea Communications Commission.

Özkaya, E. (2018). *Learn Social Engineering.* Birmingham, England: Packt Publishing.

Özkaya, E., Sarıca, R., & Durmaz, Ş. (2019). *Siber Güvenlik Saldırı & Savunma Stratejileri.* Ankara: Buzdağı Yayınevi.

Öztemiz, S., & Yılmaz, B. (2013). Bilgi Merkezlerinde Bilgi Güvenliği Farkındalığı: Ankara'daki Üniversite Kütüphaneleri Örneği. *Bilgi Dünyası, 14*(1), 87-100.

Öztezcan, B. A. (2017). *Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma: Marmara Üniversitesi Örneği.* İstanbul: Marmara Üniversitesi (Yüksek Lisans Tezi).

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security*, 673-680.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2017). Managing information security awareness at an Australian bank: a comparative study. *Information and Computer Security, 25*(2), 181-189.

Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Security Management Practices, 14*(2), 37-49.

Qureshi, M. (2011). *Measuring Efficacy of Information Security Policies A Case Study of UAE Based Company*. Stockholm: Stockholm University (Yüksek Lisans Tezi).

Rouse, M. (2019). *Confidentiality, integrity, and availability (CIA triad)*. Nisan 25, 2020 tarihinde https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA adresinden alındı

Sağıroğlu, Ş., & Alkan, M. (2018). *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık.* Ankara: Grafiker Yayınları.

Schmidt, M. B., Johnston, A. C., Arnett, K. P., Chen, J. Q., & Li, S. (2008). A Cross-Cultural Comparison of U.S. and Chinese Computer Security Awareness. *Journal of Global Information Management, 16*(2), 91-103.

Schryen, G. (2007). *Anti-Spam Measures: Analysis and Design.* Aachen: Springer-Verlag Berlin Heidelberg.

Shehri, Y., & Clarke , N. L. (2007). Information Security Awareness and Culture. P. Dowland, & S. Furnell içinde, *Advances in Networks, Computing and Communications 6* (s. 12-22). Plymouth: Lulu.com.

Shinder, D. L., & Tittel, E. (2002). *Scene Of Cybercrime: Computer Forensics Handbook.* Rockland: Syngress Publishing Inc.

Sümer, G. (2016). Türk Bankacılık Sektörünün Tarihsel Gelişimi Ve Ab Bankacılık Sektörü İle Karşılaştırılması. *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 18*(2), 485-508.

Şahinaslan, E., Kandemir, R., & Şahinaslan, Ö. (2009). Bilgi Güvenliği Farkındalık Eğitim Örneği. *Akademik Bilişim Konferansı* (s. 189-194). Şanlıurfa: Harran Üniversitesi.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., & Borandağ, E. (2009). Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri. *XI. Akademik Bilişim Konferansı* (s. 597-602). Şanlıurfa: Akademik Bilişim.

Takemura, T., Tanaka, H., & Matsuura, K. (2011). Analysis of Awareness Gap between Security Managers and Workers in an Organization with Regard to the Effectiveness of the Information Security Measures. *Journal of Information Processing, 19*, 253-262.

Taner, E. (2019). *Güvenlik Güçlerinin Bilgi Güvenliği Farkındalığına Yönelik Bir Betimleme.* Afyon: Afyon Kocatepe Üniversitesi (Yüksek Lisans Tezi).

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

Ülgen, H. (1973). İşletmelerimizin Organizasyon Yapıları İle İlgili Uygulamaya Ait Bir Araştırma Örneği. *İstanbul Üniversitesi İşletme Fakültesi Dergisi*, 178-213.

Vural, Y., & Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 23*(2), 507-522.

Wikipedia. (2010). *BS 7799*. Ocak 15, 2020 tarihinde https://en.wikipedia.org/wiki/BS_7799 adresinden alındı

Yetiz, F. (2016). Bankacılığın Doğuşu Ve Türk Bankacılık Sistemi. *Niğde Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 9*(2), 107-117.

ZeroSecond. (2020). *Zero Second*. Nisan 20, 2020 tarihinde https://www.zerosecond.com.tr/single-post/2020/04/09/Siber-Fidye-Sald%C4%B1r%C4%B1lar%C4%B1nda-T%C3%BCrkiye-Birinci-S%C4%B1rada adresinden alındı

EKLER

EK-1 - Kişisel Bilgi Formu

Sayın Katılımcı;

Bu anket, "Çalışanların bilgi güvenliği farkındalığına ilişkin algıları: bankacılık sektöründe bir araştırm" başlıklı İstinye Üniversitesi Sosyal Bilimler Enstitüsü İşletme Bölümünde Yüksek Lisans tez çalışmasında kullanılacaktır. Çalışmanın amacına ulaşması sizlerin değerli katılımlarına bağlıdır. Bu nedenle soruları dikkatli okumanız ve cevaplamanız büyük önem taşımaktadır. Ankette 34 soru bulunmaktadır.

Katkılarınız için şimdiden teşekkür ederim.

Aykut ALEMDAROĞLU

Bölüm I.
Kişisel Bilgiler

Aşağıda kişisel özelliklerinizin belirlenmesi amacıyla sorular sorulmaktadır. Size yöneltilen her soru için durumunuza en uygun seçeneğin karşısına (X) işareti koyunuz.

1. **Cinsiyet?** [ ] Kadın [ ] Erkek

2. **Yaş?** [ ] 18-21 [ ] 23-27 [ ] 28-32 [ ] 33-37 [ ] 38 ve üzeri

3. **Öğrenim Durumu?** [ ] Lise [ ] Ön lisans [ ] Lisans [ ] Yüksek Lisans [ ] Doktora

4. **Çalıştığınız kurumdaki göreviniz?** [ ] Üst Düzey Yönetici [ ] Orta Düzey Yönetici [ ] Uzman/Yetkili/Diğer

5. **Çalıştığınız Birim/Bölüm:** [ ] BT [ ] IK ve İdari İşler [ ] Pazarlama/Satış [ ] Krediler ve Operasyon [ ] Finans ve Hazine

6. **Görev süreniz?** [ ] 0-3 yıl [ ] 4-6 yıl [ ] 7-9 yıl [ ] 10-14 yıl [ ] 15 yıl ve üzeri

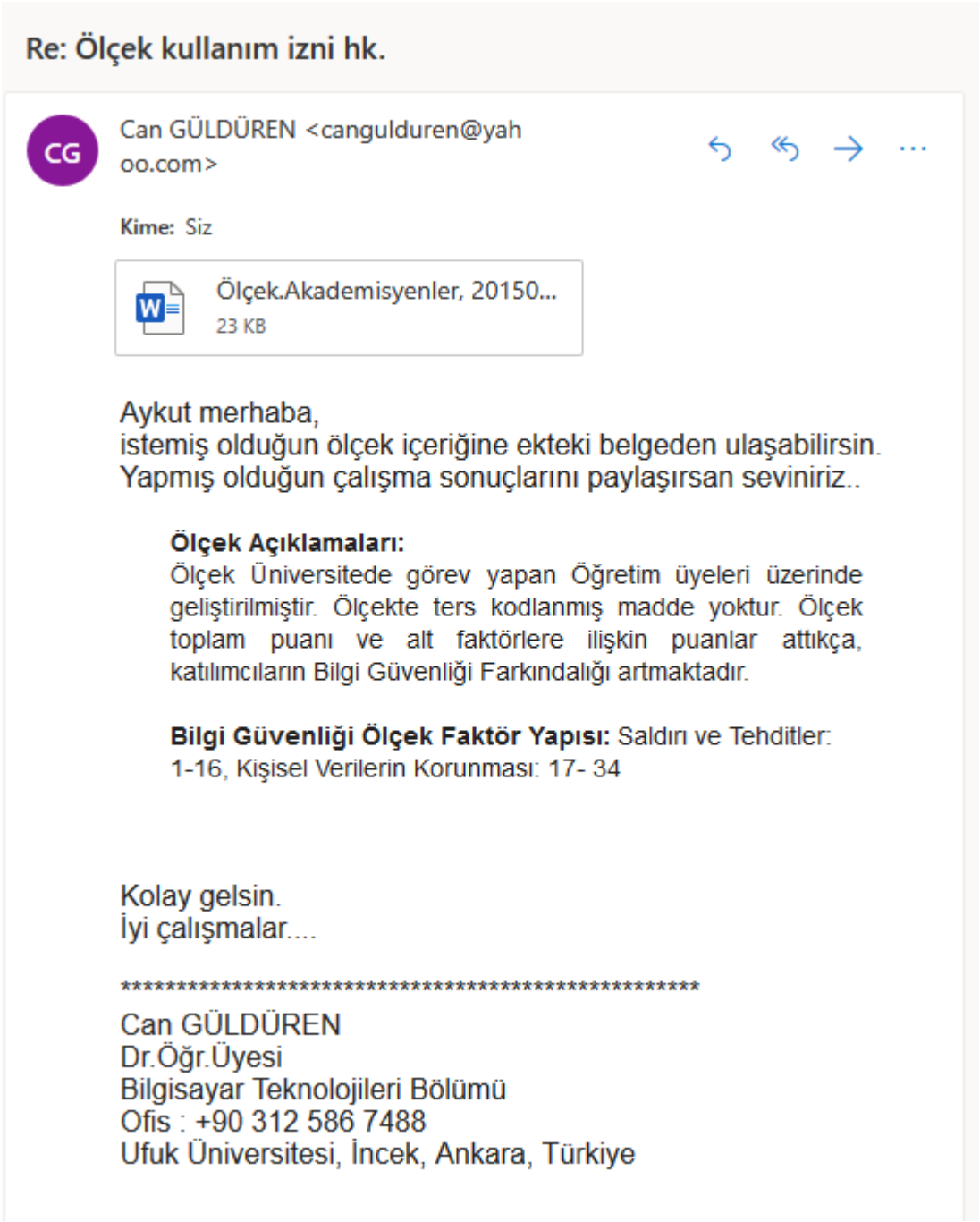
7. **Ortalana kaç yıldır internet kullanıyorsunuz?** [ ] 0-4 yıl [ ] 5-9 yıl [ ] 10-14 yıl [ ] 15 yıl ve üzeri

EK-2 – Bilgi Güvenliği Farkındalık Ölçeği

Aşağıda bilgi güvenliği farkındalığınızı belirlemek amacıyla sorular sorulmaktadır. Size yöneltilen her soru için durumunuza en uygun seçeneğin karşısına (X) işareti koyunuz.

	BİLGİ GÜVENLİĞİ FARKINDALIĞI BELİRLEME ANKETİ	Hiç Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Tamamen Katılıyorum
1.	Bilgi güvenliğinin ne anlama geldiğini biliyorum.					
2.	Bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum.					
3.	Kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum.					
4.	Bilgi sistemlerinde kullanılan virüs koruma yazılımını nasıl kullanacağımı biliyorum.					
5.	Bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (realtime protection) özelliğini kullanmaktayım.					
6.	Bilgisayarımdaki virüs koruma yazılımının otomatik güncelleştirme yapmasını sağlayabilirim.					
7.	Dijital imza (digital signature) nedir biliyorum.					
8.	Şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum.					
9.	E-posta gönderirken "Gizli" (BCC) alanının sağladığı avantajları biliyorum.					
10.	İstenmeyen elektronik posta (spam) nedir biliyorum.					
11.	İstenmeyen elektronik posta miktarını azaltmak için gerekli bilgiye sahibim.					
12.	Sosyal ağ sitelerini (social networking sites) güvenli olarak nasıl kullanacağımı biliyorum.					
13.	USB sürücülerini (USB drives) kullanırken dikkat edilmesi gereken hususları biliyorum.					
14.	Taşınabilir cihazlara (portable devices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum.					
15.	Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.					
16.	Kişisel mahremiyet nedir biliyorum.					
17.	Çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum.					
18.	Mavidiş (Bluetooth) teknolojisi ile veri aktarımı konusunda bilgi sahibiyim.					
19.	Bilgisayarıma kötü niyetli kod (malicious code) bulaşıp bulaşmadığını anlayabilirim.					
20.	Kötü niyetli yazılımlara (malware) karşı alınması gereken güvenlik tedbirlerini biliyorum.					
21.	Aldatmaca (hoax) nedir biliyorum.					
22.	Zincir e-postalara (chain e-mail) karşı nasıl hareket etmem gerektiğini biliyorum.					
23.	Bilgisayarımda casus yazılım (spyware) olup olmadığını anlayabilirim.					
24.	Bilgisayarıma casus yazılım yüklenmesini engelleme yöntemlerini biliyorum.					
25.	Kimlik hırsızlığı (identity theft) nedir biliyorum.					
26.	Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.					
27.	Sahte virüs koruma yazılımının ne olduğunu biliyorum.					
28.	Hizmet aksatma (Denial of Service - DoS) saldırısı nedir biliyorum.					
29.	Kimlik avı (phishing) saldırısı nedir biliyorum.					
30.	Sosyal mühendislik (social engineering) saldırısı nedir biliyorum.					
31	Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum					
32	Siber zorbalık (cyberbullying) nedir biliyorum.					
33	Siber zorbalığa karşı kendimi nasıl koruyacağımı biliyorum.					
34	Siber zorbalığa karşı çocuklarımı nasıl koruyacağımı biliyorum					

EK-3 – Ölçek Kullanım İzni



Re: Ölçek kullanım izni hk.

CG

Can GÜLDÜREN <cangulduren@yahoo.com>

Kime: Siz

Ölçek.Akademisyenler, 20150...
23 KB

Aykut merhaba,
istemiş olduğun ölçek içeriğine ekteki belgeden ulaşabilirsin.
Yapmış olduğun çalışma sonuçlarını paylaşırsan seviniriz..

Ölçek Açıklamaları:
Ölçek Üniversitede görev yapan Öğretim üyeleri üzerinde geliştirilmiştir. Ölçekte ters kodlanmış madde yoktur. Ölçek toplam puanı ve alt faktörlere ilişkin puanlar attıkça, katılımcıların Bilgi Güvenliği Farkındalığı artmaktadır.

Bilgi Güvenliği Ölçek Faktör Yapısı: Saldırı ve Tehditler: 1-16, Kişisel Verilerin Korunması: 17- 34

Kolay gelsin.
İyi çalışmalar....

****
Can GÜLDÜREN
Dr.Öğr.Üyesi
Bilgisayar Teknolojileri Bölümü
Ofis : +90 312 586 7488
Ufuk Üniversitesi, İncek, Ankara, Türkiye

"Bilgi güvenliği farkındalık ölçeği geliştirme çalışması" başlıklı makalede, Bilgi Güvenliği Farkındalık Ölçeği bulunmaktadır (Keser & Güldüren, 2015, s. 1171). İlgili ölçek çalışmamızda, geliştiricisi tarafından izin alınarak kullanılmıştır.