

T.C.

GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ

MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİ GÜVENLİĞİ RİSK YÖNETİMİNDE EN
UYGUN VE OBJEKTİF YÖNTEMİN
BELİRLENMESİ

Fatma Özden AKTAŞ
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ
ANABİLİM DALI

GEBZE

2009

T.C.

GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ

MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİ GÜVENLİĞİ RİSK YÖNETİMİNDE EN
UYGUN VE OBJEKTİF YÖNTEMİN
BELİRLENMESİ

Fatma Özden AKTAŞ
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ
ANABİLİM DALI

TEZ DANIŞMANI
Doç. Dr. İbrahim SOĞUKPINAR

GEBZE

2009



YÜKSEK LİSANS TEZİ JÜRİ ONAY SAYFASI

G.Y.T.E. Mühendislik ve Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 15/01/2009 tarih ve 2009/2 sayılı kararıyla oluşturulan jüri tarafından 11/05/2009 tarihinde tez savunma sınavı yapılan Fatma Özden Aktaş'ın tez çalışması Bilgisayar Mühendisliği Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

JÜRİ

ÜYE

(TEZ DANIŞMANI) : Doç.Dr. İbrahim SOĞUKPINAR

ÜYE

: Yrd.Doç.Dr. Serdar Süer ERDEM

ÜYE

: Dr. Hidayet TAKÇI

ONAY

G.Y.T.E. Mühendislik ve Fen Bilimleri Enstitüsü Yönetim Kurulu'nun/...../20... tarih ve/..... sayılı kararı.

İMZA/MÜHÜR

ÖZET

TEZİN BAŞLIĞI : BİLGİ GÜVENLİĞİ RİSK YÖNETİMİNDE EN UYGUN VE OBJEKTİF YÖNTEMİN BELİRLENMESİ

YAZAR ADI : Fatma Özden AKTAŞ

Son yıllarda bilgi sistemleri ve ağ teknolojilerinin kullanım alanlarının yaygınlaşmasıyla beraber, bilgi güvenliğinin de önemi artmıştır. Bilgi güvenliği aktivitelerinde anahtar kavram, risk analizi ve risk yönetimidir. Sistemlerdeki güvenlik seviyesini tespit etmek ve daha iyi hale getirebilmek için, mevcut riskleri belirleyebilmek, bunları analiz etmek, karşı tedbirler geliştirebilmek, kısacası yönetmek gerekmektedir.

Risk yönetiminde uzmanlaşmış yöntemler kullanmak, organizasyonlar için gelecekteki çalışmalarına daha planlı bir anlayış getireceğinden faydalı olacaktır. Bugüne kadar geliştirilmiş, karakteristikleri ve uygulamaları farklı pek çok risk analizi yöntemi bulunmaktadır. Bu yöntemlerin salt olarak birbirlerinden üstünlüklerinden bahsedebilmek mümkün değildir. Bir yöntem uygulandığı organizasyona bağlı olarak diğerlerine göre daha avantajlı hale gelebilir. Bu amaçla, organizasyonların kendi ihtiyaçlarına en uygun şekilde cevap verebilecek olan yöntemi seçebilmelerine yol gösterecek araçlara ihtiyaç duyulmaktadır. Bu tez çalışmasında, risk analizi ve yönetimi hakkında bilgi verilmiş, mevcut yöntemlere değinilmiş, uygun yöntemin seçimini tarafsız ve nicel olarak sağlayabilecek bir model tanımlanmış ve bu model dört adet risk analizi yöntemi üzerinde test edilerek uygulanmıştır. Önerilen yaklaşım, organizasyonların risk analizi ve yönetimine olan güvenini de arttırmayı hedeflemektedir.

SUMMARY

THESIS TITLE : CHOOSING THE MOST PROPER AND
OBJECTIVE METHOD IN INFORMATION SECURITY RISK
MANAGEMENT

AUTHOR : Fatma Özden AKTAŞ

Due to spreading usage of information systems and network technologies, the importance of information security has also increased in recent years. The key concept in information security activities is risk analysis and risk management. To determine and improve the security level in the systems, one has to determine the current risks, to analyze them, to generate solution; that is to manage them.

Using specialized methods for managing risk would be useful for organizations since it will bring more planned perspective to their future work. There are several risk analysis methods developed till now, varying in their characteristics and their applications. It is not possible just to mention the superiority of one over another. A method may be more advantageous than others depending on the organization in which it is applied. For this purpose, there is need to find guiding tools for choosing a method that can satisfy organizations' needs in the most useful way. In this thesis a model has been proposed to select most proper risk analysis method. The model for selecting the most proper method neutrally and quantitatively is discussed and this model is applied by testing on four risk analysis methods. The proposed approach also targets to increase reliance to risk analysis and management method for the organizations.

TEŞEKKÜR

Öncelikle, yüksek lisans eğitimim süresince bilgi ve tecrübeleriyle bana yol gösteren ve destek olan değerli hocam Doç. Dr. İbrahim Soğukpınar'a,

Öğrenim hayatımın her aşamasında bana emek veren tüm eğitimcilere,

Ve her zaman, her konuda bana destek ve yardımcı olan anneme, babama ve ablama,

sonsuz ve içten teşekkürlerimi sunuyorum.

F.Özden Aktaş

İÇİNDEKİLER DİZİNİ

	<u>Sayfa</u>
ÖZET	iv
SUMMARY	v
TEŞEKKÜR	vi
İÇİNDEKİLER DİZİNİ	vii
SİMGELER VE KISALTMALAR DİZİNİ	ix
ŞEKİLLER DİZİNİ	x
TABLolar DİZİNİ	xi
1. GİRİŞ	1
2. BİLGİ GÜVENLİĞİ RİSK ANALİZİ VE MEVCUT YÖNTEMLER	3
2.1. Bilgi Güvenliğinde Risk	3
2.2. Bilgi Güvenliğinde Risk Yönetimi	4
2.2.1. Risk Değerlendirme	7
2.2.2. Riske Karşı Yapılabilecekler	13
2.2.3. Yeniden Değerlendirme	17
2.3. Risk Analizi Sınıflandırması	17
2.4. Risk Analizi Yöntemlerinin Karşılaştırılması ve Yöntem Seçimi İçin Mevcut Çalışmalar	19
2.5. CRAMM (CCTA Risk Analysis and Management Methodology)	28
2.6. CORAS (Construct a Platform for Risk Analysis of Security Critical Systems)	30
2.7. ISRAM (Information Security Risk Analysis Method)	31
2.8. OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)	32
2.9. Risk Analizi İçin Geliştirilmiş Standartlar	33
3. RİSK ANALİZİ VE YÖNETİMİ İÇİN YÖNTEM SEÇİMİ	36
3.1. Seçim İçin Önerilen Yöntem	36
4. ÖRNEK ÇALIŞMA VE SONUÇLARININ YORUMLANMASI	45
4.1. Örnek Çalışmanın Karar Ağacı Yöntemiyle Analizi	48
5. SONUÇ VE ÖNERİLER	50

Sayfa

KAYNAKLAR	52
ÖZGEÇMİŞ	55
EKLER	56
EK 1: Tanımlar	56
EK 2: Risk Analizinde Kullanılan Matematiksel ve İstatistiki Modeller	58

SİMGELER VE KISALTMALAR DİZİNİ

ALE	Annualized Loss Expectancy (Yıllık kayıp beklentisi)
ARO	Annualized Rate of Occurrence (Yıllık oluşma oranı)
CCTA	Central Computer and Telecommunications Agency
CERT/CC	CERT Coordination Center
COBRA	Consultative, Objective and Bi-functional Risk Analysis
CORAS	Construct a platform for Risk Analysis of Security Critical Systems
CRAMM	CCTA Risk Analysis and Management Methodology
EFF	Electronic Frontier Foundation
IEC	The International Electrotechnical Committee
ISO	The International Organization for Standardization
ISRAM	Information Security Risk Analysis Method
IST	Information Society Technologies
IST/RAMP	International Security Technology/Risk Analysis Management Program
LAVA	Los Alamos Vulnerability and Risk Assessment
LRAM	Livermore Risk Analysis Methodology
NIST	National Institute of Standards and Technology
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation
RAMEX	Risk Analysis and Management Expert System
RA/SYS	Risk Analysis System
SLE	Single Loss Expectancy/Exposure (Birim kayıp beklentisi)
UML	Unified Modeling Language

ŞEKİLLER DİZİNİ

<u>Şekil</u>	<u>Sayfa</u>
2.1 Bilgi teknolojileri güvenlik modeli	5
2.2 Risk Yönetimi Süreçleri	7
2.3 Örnek bir risk azaltma stratejisi	16
2.4 CRAMM'in yapısı	29
3.1 Yöntemin adımları	37
4.1 Organizasyonun ihtiyacının karar ağacı yapısında gösterimi	49

TABLolar DİZİNİ

<u>Tablo</u>	<u>Sayfa</u>
3.1 Organizasyon ve yöntemler için soruların cevaplarının tablo yapısıyla gösterimi	44
4.1 Örnek uygulama sonuçları tablosu	46
4.2 Önerilen yöntem için Karar Ağacı ve Tablo yapısının karşılaştırılması	49
Ek 2.1 (a) Risk Ölçek Tablosu ve (b) Risk Seviye Matrisi	58

1. GİRİŞ

Bilgi; yazılı, elektronik olarak saklı, iletilen veya görüntülü ya da sözlü çeşitli formlarda olabilen ve uygun şekilde korunması gereken bir varlıktır. Diğer önemli iş değerleri gibi, organizasyonlar için bir öneme sahiptir ve bu nedenle de gerektiği şekilde korunmaya ihtiyaç duyar. Bilgi güvenliği, işin devamlılığını, iş kaybını minimuma indirmeyi, gelirdeki ve iş fırsatlarındaki kârı maksimize etmeyi garantilemek için geniş anlamdaki tehditlerden bilgiyi; genel güvenlik şartları olan gizliliğini, bütünlüğünü, erişilebilirliğini sağlayarak korumaya çalışır [ISO/IEC 17799, 2000]. İstatistikler atakların artık hedeflenmiş, daha karmaşık ve çok daha zararlı olduklarını göstermektedirler.

Bilgi güvenliği aktivitelerinde anahtar kavram, risk yönetimi fikridir ve öncelikli olarak risk azaltımı hedef alınır [Blakley et al, 2001]. Organizasyonlar, maddi açıdan ve prestij açısından zarara uğramamak için artık, kendilerine yönelen tehditleri ve sistemlerini etkileyecek riskleri gözden geçirmek ve bir bilgi güvenlik politikası oluşturmak zorundalar. Bilgi güvenliğini sağlamak için, sadece olası zayıflıklardan kaçınmaya çalışmak, bilgiyi her zaman yüzde yüz güvenli hale getirememektedir. Bu yüzden, varlıklar üzerindeki potansiyel zayıflıklara bağlı olarak riski yönetmek, bilgi güvenliği aktivitelerinin temel parçasıdır. Risk yönetimi yaparken, sistemi olumsuz yönden etkileyebilecek şüpheli olaylar, bunların sistem üzerindeki olumsuz etkileri ve etkinin şiddeti tanımlanır, maliyet-fayda dengesi sağlanacak şekilde çeşitli koruyucu önlemler belirlenerek mümkünse riski ortadan kaldırmak veya kabul edilebilir bir seviyeye indirmek yoluna gidilir.

Günümüzde birçok risk analiz ve yönetim yöntemleri tasarlanmış ve halen de tasarlanmaya devam edilmektedir. Bu yöntemlerin hepsinin genel hedefinin, güvenlik şartlarını sağlayarak bilgiyi korumak olmasına karşın, uygulamada izledikleri yol, kullandıkları metrikler, altyapıları farklılık gösterir. Risk yönetim yöntemleri hangi temellere dayanırsa dayansın, kavramsal olarak birbirlerinden üstündür diye belirlemek mümkün değildir [NIST, 1997]. Bir organizasyon için bu yöntemlerin hangisinin seçilip kullanılacağı, bilgi güvenliği yöneticilerinin önemli

bir problemidir. En uygun olan yöntemin seçimi, etkin risk yönetimi için önemlidir ve bu amaçla organizasyona güven veren bir yaklaşıma sahip objektif araçlara ihtiyaç duyulmaktadır.

En uygun risk analizi ve yönetimi seçimi için literatürde fazla çalışma yapılmadığı ve araştırmalara açık bir konu olduğu görülür.

Bilgi güvenliği risk analizi yöntemlerinin karşılaştırmasını yapan eski çalışmalar, örneğin 1993 yılında Badenhorst'un çalışmasında da olduğu gibi, yöntemlerin organizasyonun ihtiyaçlarıyla ne şekilde örtüştüğünü anlamayı sağlayan ölçekler kullanmak yerine; genellikle yöntemdeki bilgi teknolojileri, bilgi güvenliği ve risk yaklaşımının bazı kriterlere adreslenip adreslenmediğine odaklanırlar [Vorster and Labuschagne, 2005].

Yakın bir zamanda yapılan çalışma ise, 2005 yılında yapılan Vorster'in farklı risk analizi yöntemlerini karşılaştırdığı çalışmadır (Vorster'in çalışması, Bölüm 2.4'de detaylı olarak açıklanmıştır).

Bu çalışmada, bilgi güvenliği risk analizi ve yönetimi için seçilecek yöntemin belirlenmesi amacıyla bir yaklaşım önerilmiştir. Önerilen yaklaşım, öncelikle gereksinimin ve beklentilerin saptanmasıyla uygulanmaya başlanır. Daha sonra istenilen sayıdaki alternatif yöntem, tespit edilen veriler çerçevesinde incelenerek değerlendirilir. Değerlendirmede, organizasyon harici kişilerden bir yardım gerekmemektedir ve uygulayıcılar tarafından hazırlanan sorulardan yararlanılır. Karar aşamasında en uygun olan seçeneğin belirlenmesi için, uygulanması pratik olan bir matematiksel formül kullanılmıştır. Önerilen yöntem, örnek bir vaka ile sınanarak elde edilen sonuçlar da verilmiştir.

Tezin devamında, bilgi güvenliği alanında risk, risk analizi ve yönetimi konusunda temel bilgilere ve literatürdeki ilgili çalışmalara değinilmiştir. Bölüm 3'te, önerilen risk analizi değerlendirme yöntemi anlatılmış, Bölüm 4'te ise uygulama sonuçları verilerek, sonuç bölümünde genel değerlendirme yapılmıştır.

2. BİLGİ GÜVENLİĞİ RİSK ANALİZİ VE MEVCUT YÖNTEMLER

2.1. Bilgi Güvenliğinde Risk

Bilgi teknolojileri alanında gün geçtikçe meydana gelen hızlı gelişmeler nedeniyle, güvenlik konusu da gittikçe artan bir öneme sahip oldu. Ancak organizasyonlar, ne yazık ki güvenlik konusunda yeteri kadar tedbirli davranamıyorlar. Sayısal dünyada, tehdit ve risk analizi yaparak uygun bir güvenlik yapısı geliştirmek hala çok yaygın ve tam olarak anlaşılabilir değildir. Bu durumun en önemli nedenlerinden birisi de, geliştirilmiş yöntemlerden daha iyi ya da daha uygun olanının seçiminin zorluğudur. Hatalı bir seçim, organizasyona bilgi güvenliği açısından beklenen faydalı sonuçları vermeyeceği gibi, üzerinde çalışılırken boşa harcanan emek, zaman ve para da organizasyonu zarara uğratacaktır. Günümüzde birçok şirket ve organizasyon, bu nedenle böyle bir güvenlik yapısı oluşturmaktan kaçınıyor ve bilgi güvenliği için direkt olarak tasarsız testleri veya etik bilgisayar korsanlığı yöntemini kullanıyor. Yani, periyodik olarak kendi sistemlerini, ağlarını veya uygulamalarını kırmaları için dış güçleri kiralyor. Eğer bu dış güçler, üstünde çalıştıkları sisteme yaptıkları saldırılarda başarılı olamazlarsa, şirketler kendi sistemlerinin güvenli olduğunu farzediyorlar veya umuyorlar. Saldırılar başarılı olursa, sistem güvensiz kabul ediliyor. Güvensiz olarak nitelenen sistemin zayıflıkları ve güvenlik açıkları yamanıp, sistem güvenliğinin sağlanmış olduğu umuluyor. Bu yöntemle belirlenen güvenli olup olmama durumunun rastgele olduğu açıktır ve sistemin güvenliği sadece kendisini test eden dış güçlerin kapasitesine ve gücüne bağlıdır. İlginç olan nokta, etik bilgisayar korsanlığı olarak adlandırılan bu kavramın, gerçek dünyadaki karşılığının etik hırsızlık olmasıdır ki, böyle bir kavram aslında tam bir çelişkidir.

Risk, hayatımızın her alanında karşımıza çıkan bir kavramdır. Riski, sözlük anlamıyla bir zarara, bir kayıba, bir tehlikeye yol açabilecek bir olayın oluşma olasılığı olarak tanımlayabiliriz. Riskten bahsedebilmek için belirsizlik durumu, riskin sözkonusu olduğu bir varlık ve bu varlığın bulunduğu bir ortam olmalıdır.

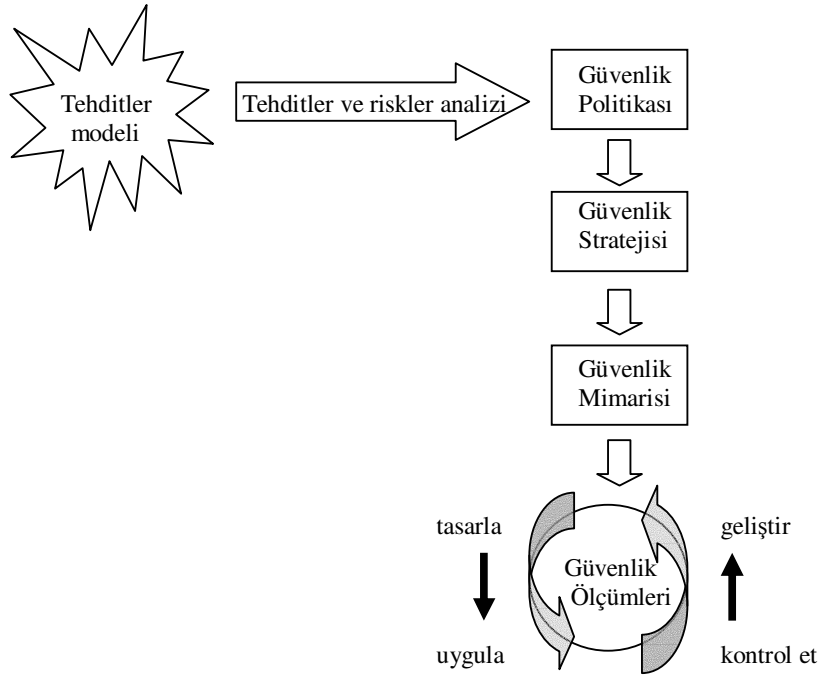
Sözkonusu olan varlık ve bu varlığın bulunduğu ortam dikkate alınarak, riski daha teknik olarak şu şekilde tanımlayabiliriz; risk, bir tehdit kaynağının, belirli bir potansiyel zayıflığı kullanma olasılığının ve bu olumsuz olayın oluşması durumunda organizasyon üzerindeki kötü etkilerin şiddetinin fonksiyonudur [Stoneburner et al, 2002]. Burada bahsedilen tehdit, zayıflık gibi kavramların tanımları ve açıklamaları, EK 1 bölümünde verilmiştir. Bilgi sistemlerinde risk; sistemin tümüne ya da bir kısmına yönelik olan ve sistemdeki bir zayıflıktan faydalanılarak zararlı sonuçlar doğurabilecek bir olayın gerçekleşmesi olasılığıdır [Swanson and Guttman, 1996].

Bilginin güvenlik koşulları olan gizlilik, bütünlük ve erişilebilirlik; bilgiye uygulanan teknolojiyle ortaya çıkan risk nedeniyle engellenmiş olabilir [Dwaikat and Parisi-Presicce, 2005]. Daha açık bir ifadeyle, herhangi bir teknolojik uygulama aracılığıyla; istenmeyen bir şekilde ifşa edilerek bilginin gizliliğinin bozulabileceğini, istemli veya istemsiz olarak hatalı bir şekilde değişikliğe uğrayarak bilginin bütünlüğünün bozulabileceğini, kasıtlı veya kasıtsız imha edilerek veya bir kısmının kaybedilerek bilginin ulaşılabilirliğinin engellenebileceğini söyleyebiliriz. Bu durumlarla bilgi güvenliğinin sağlanamaması, organizasyonda iş kaybı gibi direkt ya da işin gecikmesi gibi direkt olmayan kayıplara neden olur [Blakley et al, 2001].

2.2. Bilgi Güvenliğinde Risk Yönetimi

Birçok açıdan sayısal dünya gerçek dünyayla benzeşir. Sayısal dünyada da ne tasarlanacağını ve ne gerçekleştirileceğini, buna karşı olanların kimler olduğunu, bu kişi veya kurumların ellerindeki kaynakları, kullanacakları saldırı stratejilerini, başarılı olurlarsa ne elde edeceklerini, planlanan tepkileri, vb. açıkça anlamaya ihtiyaç vardır. İşte tüm bunların belirlenmesi ve bunlara karşı stratejilerin geliştirilmesi süreci, risk yönetimini oluşturur. Bu nedenle bilgi teknolojileri güvenlik politikaları ve mekanizmaları, Şekil 2.1’de modellendiği gibi tehditler gözönüne alınarak ve tehditlere karşı sistemi koruyacak şekilde oluşturulmalıdır. Şekilde görülen tehditler modeli, incelenen bilgi sistemleri ortamıyla bağlantılı olarak olası tehditleri sıralamalıdır. Tehditler, bağlantılı oldukları risklerle beraber detaylı bir şekilde düşünülmelidir. Daha sonra da sırasıyla bilgi güvenlik politikası, stratejisi ve mimarisi oluşturulmalıdır. Ayrıca şekilde de görüldüğü gibi güvenlik

süreci, statik yapıda değil, periyodik güvenlik ölçümleri yapılarak güncellenecek şekilde, kendini yenileyen dinamik bir yapıda olmalıdır.



Şekil 2.1 Bilgi teknolojileri güvenlik modeli

Risk yönetimi, organizasyonun bilgi güvenliği programında anahtar elemandır ve uygun güvenlik kontrollerinin seçilmesinde etkin bir çatı sağlar. Güvenlik kontrolüne risk temelli bir yaklaşım, verimliliği ve sonuçları hesaba katarak; uygulanabilir politikalar, standartlar ve direktifler tanımlamada zorlayıcı bir etki oluşturur [Ross et al, 2007].

Risk yönetimi, belirsizlikle ve risklerin kayıplarıyla ilgilenir [Wang, 1987]. Bilgi teknolojileri sistemlerinin güvenliği açısından risk yönetimi, sistemlerin işletimsel gereklilikler ve ekonomik maliyetler dengesinin sağlanmasına yardımcı olan bir yöntemdir ve organizasyonda bilginin uygun bir şekilde kontrol edilmesine imkan sağlar [Dhillon, 2007]. Bir organizasyonun risk yönetimindeki temel hedefi, sadece bilgiyi korumak değil, organizasyonu ve tüm amaçlarını gerçekleştirme yeteneğini de korumaktır. Bu nedenle, risk yönetim işlemleri sadece teknik fonksiyonu yürüten bilgi güvenliği uzmanları tarafından değil, organizasyonun

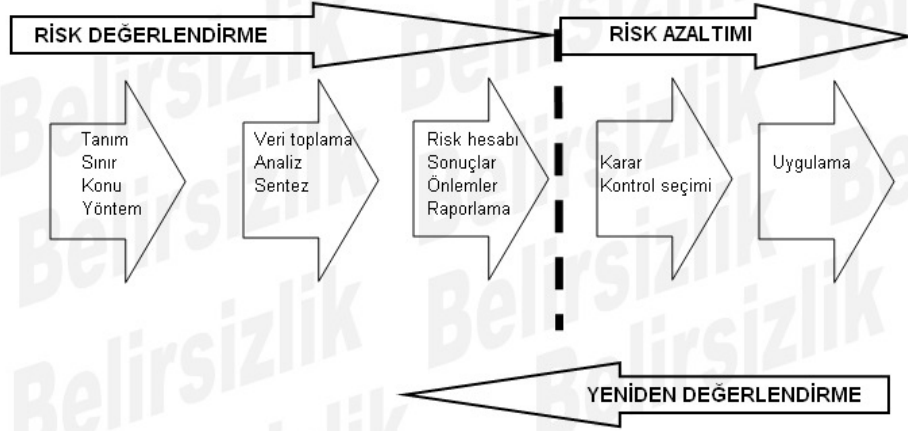
genelinde yönetim fonksiyonu olan kişilerle beraber düşünülmelidir [Bowen et al, 2006].

Risk yönetimi “sistem kaynaklarını etkileyebilecek şüpheli olayları tanımlama, kontrol etme ve ortadan kaldırma ya da en aza indirme işleri” kavramına dayanır. Eğer hiç bir zayıflık ve tehdit yoksa –sonuç olarak risk yoksa– güvenlik için ekstra zaman ve para harcanmaz. Eğer risk varsa ve risk kuvvetle muhtemelse veya beklenen kayıplar nedeniyle risk var gibi görünüyorsa, daha fazla zaman ve para harcamaya hazır olunur [Oppliger, 2007]. Bu nedenle, bilgi sistemlerinde risk yönetimi yaparken, sistemi olumsuz yönden etkileyebilecek şüpheli olaylar tanımlanır, maliyet-fayda dengesi sağlanacak şekilde çeşitli koruyucu kontroller belirlenerek riski ortadan kaldıracak ya da en aza indirgeyecek şekilde uygulanır.

Risk yönetiminin süreçleri üç temel başlıkta toplanabilir [Stoneburner et al, 2002]:

1. Risk değerlendirme
2. Riske karşı yapılabilirler
3. Yeniden değerlendirme

Şekil 2.2, genel hatlarıyla risk yönetimi süreçlerini göstermektedir. Farkedilebileceği gibi, risk yönetiminin her aşamasında belirsizlik vardır. İzleyen bölüm, bu süreçlerin detaylarını içermektedir.



Şekil 2.2 Risk Yönetimi Süreçleri

2.2.1. Risk Değerlendirme

Risk yönetiminin ilk aşaması, en hayati, en uzun süren ve detaylı çalışması olan risk değerlendirme işlemleridir. Bu aşamada risklerin tanımlanması ve risk analizinin yanı sıra potansiyel etkilerin de değerlendirilmesi yapılır, karşı önlemler belirlenir. Böylece bir sonraki adım olan riske karşı yapılabilecekler için, riski düşürücü stratejilerin önerilmesine yardımcı olunur.

Risk değerlendirmede yapılması gerekenler şu şekilde sıralanabilir [NIST, 1997] [Swanson and Guttman, 1996] [Dhillon, 2007]:

a) Risk analizi yapılacak hedef alanın ve sınırların belirlenmesi

Risk değerlendirmede öncelikle üzerinde analiz yapılan hedef çevre/konu ve sınırları belirlenmelidir. Burada belirlenen alan, hedef çevre/konu içinde ve sınırlar dahilinde bulunan değerlerin ya da varlıkların bulunduğu ortamdır. Böylece, projenin boyutu, amacı, kapsamı, uyulması gereken zorunluluklar ve sorumluluklar daha açık olarak belirlenir.

b) Sistemin tanımlanması

Eğer varsa daha önceki analiz sonuçları da dikkate alınarak analiz edilecek alandaki varlıklar ve değerleri belirlenir. Bu varlıklar; bilgi, yazılım, personel, donanım, fiziki varlıklar (bilgisayar ekipmanları gibi), vb. şeklindedir. Bir varlığın değeri, onun gerçek değerinin yanı sıra bir zarara uğradığında kısa vadedeki etkilerle uzun vadedeki sonuçları da içerecek şekilde düşünülmelidir.

c) Tehdit tanımlanması

Tehditler; sistemi olumsuz yönde etkileme potansiyeli olan mevcudiyetler veya olaylardır. Hatalar, dolandırıcılık, hayalkırıklığına uğramış çalışanlar, bilgisayar suçluları, endüstri casusları, yangın, su baskınları, bilgisayar korsanları, virüsler tehdiye örnek olarak verilebilir [NIST, 1997]. Bu adımda her bir varlık için tek tek olası tehditler ve özellikleri ortaya konur. Bu amaçla bazı sorulara verilecek cevaplardan yararlanılabilir. Örneğin, “Neler olabilir?” sorusunun cevabı, varlığa karşı olabilecek tehditleri belirlemeyi sağlar. “Eğer olursa, ne kadar kötü olabilir?” sorusu, belirlenen tehditlerin etkilerinin ve sonuçlarının değerlendirilmesini sağlar. “Ne sıklıkta olabilir?” sorusu, tehditin frekansının tespit edilmesini sağlayarak tehditin oluşma olasılığının belirlenmesine yardımcı olur. Son olarak “Bu üç sorunun cevabı ne kadar kesindir?” sorusuyla da risk için temel şart olan belirsizlik tespit edilebilir. Dört sorudan ikinci ve üçüncüsünün cevabı, tercihe göre nicel büyüklükler olabileceği gibi, nitel sıfatlar şeklinde de olabilir.

Tehditlerin belirlenmesinde gözden kaçırılacak herhangi bir şey olmaması için dış kaynakların veya bağımsız kuruluşların (Threats Research Center gibi) belirlediği ve paylaşımına açtığı olası tehditler listelerinden yararlanılabilir.

d) Önem derecelerine göre öncelik sıralaması

Kayıp veya hasar açısından daha hayati kısımlara öncelik vermek amacıyla, önem derecelerine göre önceliklerinin belirlenmesi yapılır. Risk analizi, oluşma olasılığı yüksek ve önemli varlıkları etkileyebilecek tehditlere odaklanmalıdır. Analiz edilecek bilgilerin gerekenden fazla olması durumunda önceliklerine göre sadece gerekli verinin alınması işlemine “eleme” işlemi denir. Bu işlemle, organizasyon üzerinde olumsuz sonuçlara neden olacak alanlara odaklanılır. Olumsuz bir olay

oluştduğunda, bu etkilerin sonuçları kısa vadede ifşa olma, değişiklik, yeniden kurma, hizmetin engellenmesi, vb. olabilirken uzun zamanlı olarak düşünülürse, iş kaybı, sistemin özgörevinin çökmesi, itibar kaybı, mahremiyetin bozulması, incinme veya hayat kaybı şeklinde olabilir. Önem derecesi arttıkça sistem riski, dolayısıyla da organizasyonun riski artacaktır [NIST, 1997].

e) Zayıflık tespiti ve tehditlerle ilişkilendirme

Zayıflık, tehditin sistemi zarara uğratici olarak gerçekleşmesine neden olan yani onu tetikleyen ve güvenlik prosedürlerinde, teknik koruyucularda, fiziksel koruyucularda ya da bir tehdit tarafından kullanılabilecek diğer tüm koruyucularda bulunmayan güvenlik açıklığı veya eksikliğidir. Zayıflık, tehditin sistem üzerindeki olumsuz etkilerine izin verebileceğinden, riske neden olur. Dolayısıyla bu adımda, önceki aşamada tanımlanan tehditlerin hangi zayıflıklardan kaynaklandığı tespit edilir. Tüm zayıflıkların belirlenmesi ve tehditlerle ilişkilendirilmesiyle, Tehdit-Zayıflık-Varlık eşleştirme modeli ortaya konmuş olur.

Örneğin işten ayrılan personelin sisteme giriş haklarının kapatılmaması bir zayıflıktır. Bu zayıflıkla eşleştirilecek tehdit, işten ayrılan eleman (tehdit kaynağı: insan) ve tehdit eylemi ise, şirketin sistemine bağlanarak verilere erişip bu verileri kullanmak veya verilerin bütünlüğünü bozmak olacaktır. Bu zayıflığın neden olduğu tehditin oluşması durumunda, olumsuz yönde etkilenecek varlıklar ise, veri, veri bütünlüğü, bilginin erişilebilirliği, yazılım, vs. olacaktır.

İlişkilendirme modeli için bir başka örnek, olağanüstü hal planının bulunmaması durumu zayıflığıdır. Bu zayıflığın oluşturabileceği tehditler, yangın, deprem, terörist ataklar, vs. (tehdit kaynağı: doğal); tehdit eylemi ise bu tehditlerin gerçekleşmesi halidir. Tehditlerin gerçekleşmesi durumunda olumsuz yönde etkilenecek olan değerler ise, bilgi teknolojileri donanımı, yazılımı, bilginin erişilebilirliği, itibar, vs. olacaktır.

Tehdit-Zayıflık-Varlık ilişkilendirmesi, risk değerlendirme modelini daha detaylı ifade etmeyi ve bütün olasılıkları değerlendirmeyi sağlayacaktır.

f) Kontrollerin analizi

Bu adımın amacı, zayıflık nedeniyle gerçekleşme potansiyeline sahip olan tehditin oluşma olasılığını azaltacak, dolayısıyla da varlığa yönelik olası olumsuz etkiyi ortadan kaldıracak veya şiddetini düşürecek olan önlemleri, koruyucuları – bunlar kontroller olarak da ifade edilir – ortaya koymak ve analiz etmektir. Kontroller, herhangi bir eylem, aygıt, prosedür, teknik veya bir tehdite karşı sistem zayıflığını indirgeyebilen herhangi bir şey olabilir. Yetkilendirme mekanizması, şifreleme yöntemleri, nüfuz tespit yazılımı gibi teknik önlemlerin yanı sıra, güvenlik politikaları, fiziksel güvenlik ya da personel güvenliği gibi teknik olmayan önlemler koruyucuya örnek olarak verilebilirler. Koruyucu analiziyle, mevcut güvenlik önlemlerinin etkinliği de kontrol edilmiş olur. Özellikle pahalı koruyucuların seçimi veya önem derecesi belirlenemeyen sistemleri için, derinlemesine analizler daha garantili olacaktır [NIST, 1997].

g) Olasılık belirleme ve etkilerin analizi

Zayıflık nedeniyle gerçekleşebilecek tehditin olasılığı; tehdit kaynağı ve kapasitesi, zayıflığın özelliği ve mevcut önlemlerin etkinliğine bağlı olarak tespit edilmelidir. Olasılık tespit edildikten sonra, her bir zayıflığın sistem üzerindeki varlıklarda meydana getirebileceği olumsuz etkilerin de şiddeti belirlenmelidir. Etkinin şiddeti, sistemin ve varlıkların misyonuna, kritikliğine ve hassaslığına bağlı olacaktır. Şiddetin belirlenmesi için bazı sorulardan yararlanılabilir. Örneğin, “Kasıtsız hataların etkileri ne olabilir?”, “Organizasyon içindeki kişilerin suistimallerinden kaynaklanabilecek kayıpların derecesi ne olabilir?”, “Dıştan gelen saldırılarda neler yaşanabilir?” ve “Doğal felaketlerin etkileri nelerdir?” gibi sorular, olumsuz etkilerin derecelendirilmesinde yardımcı olabilirler.

h) Risk belirleme

Bu aşamanın amacı, analiz edilen sistemin risk seviyesini belirlemektir. Belirli bir tehdit-zayıflık ikilisi için risk, şu üç parametrenin fonksiyonu olarak bulunur: tehdit kaynağının zayıflığı kullanma olasılığı, gerçekleşen kötü olayın yaptığı olumsuz etkinin şiddeti ve bu şiddeti azaltan veya ortadan kaldıran güvenlik kontrollerinin yeterlilik derecesi [Dhillon, 2007]:

$$R \text{ (Risk)} = F \text{ (Tehditin Gerçekleşme Olasılığı, Tehditin Olumsuz Etkisinin Şiddeti, Kontrollerin Yeterliliği)} \quad (2.1.)$$

Burada tehdidin gerçekleşmesinden oluşan olumsuz etki, neden olduğu kaybın maliyeti olarak değerlendirilebileceğinden, riskin dolaylı olarak varlığın değerine bağlı olduğu da söylenebilir. Ayrıca, bir risk nedeniyle uygulanan koruyucu güvenlik kontrollerinin yeterliliği, riski oluşturan tehdidin gerçekleşme olasılığını değiştiriyor olacağından genel olarak risk aşağıdaki gibi parametrelerin fonksiyonu olarak düşünülebilir:

$$R \text{ (Risk)} = F \text{ (Tehditin Gerçekleşme Olasılığı, Tehditin Olumsuz Etkisinin Şiddeti)} \quad (2.2.)$$

Risk ölçümünde kullanılan en yaygın ölçüt, yıllık kayıp beklentisidir (ALE) [Blakley et al, 2001]. Bu yaklaşımda, nicel risk değeri hesaplanırken formül, tehdit etkisi maliyet cinsinden olmak üzere;

$$R \text{ (Risk)} = P \text{ (Olasılık)} \times C \text{ (Maliyet)} \quad (2.3.)$$

şeklinde genelleştirilebilir ve varlığa karşı tehditin beklenen yıllık parasal kayıp maliyeti:

$$ALE = SLE \times ARO \quad (2.4.)$$

formülüyle hesaplanır. Formülde kullanılan ARO, tehditin bir yıl içindeki oluşma sıklığıdır. Örneğin, bir tehdit 10 yılda 1 kez gerçekleşebilecek bir tehditse, bu tehdit için ARO değeri 1/10 olacaktır. Benzer şekilde, yılda 50 kere gerçekleşebilecek bir tehditin ARO değeri ise, 50 olacaktır. SLE, Varlık için birim parasal kayıp beklentisidir ve parasal bir değerdir. SLE değerini bulmak için;

$$SLE = \text{Varlık değeri [mali]} \times \text{Korunmasızlık faktörü [\%]} \quad (2.5.)$$

formülü kullanılır. Burada korunmasızlık faktörü yüzdesi, varlığın risk içeren kısmının yüzde miktarına karşılıktır. Örnek olarak 1000 \$'lık bir varlık için eğer bir riske karşı

% 90 koruma varsa, bu risk için korumasızlık faktörü % 10 olacaktır. Bu durumda bu varlık için birim parasal kayıp beklentisi Eşitlik 2.5. dolayısıyla,

$$SLE = 1000 \times 0,10 = 100 \$$$

olarak bulunacaktır. Bu varlığa yönelik ARO değeri 0,10 olan bir tehdit dolayısıyla oluşan yıllık kayıp beklentisinin değeri ise, Eşitlik 2.4. dolayısıyla,

$$ALE = 100 \times 0,10 = 10 \$$$

olarak bulunur.

Risk değeri sayısal bir büyüklük olarak bulunabileceği gibi, yüksek, orta, düşük, vb. şeklinde nitel bir ifadeyle de belirlenebilir.

i) Kontrol önerileri ve dokümantasyon

Belirlenmiş riskleri kabul edilebilir seviyeye indirecek veya ortadan kaldıracak uygun kontrollerin önerilmesi ve bunların karar vericilere sunulacak şekilde raporlanması işlemleridir. Risk değerlendirmede dokümantasyon çok önemli bir kavramdır. Elde edilen sonuçlar, mutlaka organizasyon için nelerin önemli olduğunu yansıtabilecek anlamlı çıktılar şeklinde rapor haline getirilmelidir. Bu raporlar sert kurallar içeren şekilde değil, güvenlik yapısı iskeletini geliştirici nitelikte olarak düşünülmelidir. İyi dokümante edilmiş bir risk değerlendirme, daha sonraki risk değerlendirmelerinde daha az zaman harcanmasını ve eğer daha sonra belirli bir güvenlik kararıyla ilgili bir soru gündeme gelirse kolaylıkla cevaplanarak açıklığa kavuşturulmasını sağlayacaktır [NIST, 1997]. Ayrıca bu dokümanlar, bilgi sistemleri ortamını ayrıntılı bir şekilde tanımlayacağı için sistemle ilgili yeni kararlar vermek amacıyla referans olarak da kullanılabilirler [Fung et al, 2003].

Risk değerlendirme sürecinde yapılan işlemleri üç bölümde düşünülürse; yukarıda açıklandığı gibi ilk bölümde, değerlendirilecek olan sistem, sınırları ve bu kapsamdaki mevcut varlıklar belirlenir. İkinci bölümde, riski oluşturan kaynaklar (yani tehditler, zayıflıklar) ve riski ortadan kaldıran veya azaltan kontroller tespit edilir ve riskin büyüklüğü belirlenir. Bu yüzden bu adıma, Risk Analizi adı

verilmektedir. Risk deęerlendirmenin son bölümünde ise, Riske Karşı Yapılabilecekler süreci için elde edilen sonuçlar rapor haline getirilir.

2.2.2. Riske Karşı Yapılabilecekler

Riske karşı yapılabilecekler adımı, riski önceliklerine göre sıralama, yapılabilecekleri kararlaştırma, karar vericiler tarafından riski kabul edilebilecek seviyeye indirgeyecek güvenlik kontrollerinin ve koruyucularının seçilmesi, bunların uygulanması işlemleri ile ilgilidir [Swanson and Guttman, 1996]. Öncelikli hedef, riski kabul edilebilir seviyeye getirmektir. Bu amaçla risk kontrol işlemleri ve kontrollerin maliyet-fayda analizleri gözden geçirilir. Risk kontrolleri, iş ünitelerinden bağımsız olarak yapılmalıdır.

Riskler ve bunlara karşı yapılabileceklerin deęerlendirilmesi sonrasında neler yapılacağına yetki sahibi kişiler tarafından karar verilip, bu karar hayata geçirilir. Uygun kontrolleri seçebilmek için yöneticiler birçok etkeni gözönüne almalıdırlar. Örneğin; organizasyonun politikası, yasaları, düzenleyici kuralları, emniyet, güvenilirlik, kalite ihtiyaçları, sistem performans ihtiyaçları, zaman, tamlik ve bütünlük ihtiyaçları, koruyucuların maliyeti, teknik gereksinimler, kültürel zorlayıcılar, gözönüne alınması gereken kavramlardır [NIST, 1997].

Koruyucuların seçiminde kullanılan yöntemlerden biri, “Eđer” analizidir. Bu yöntem yardımıyla, çeşitli koruyucuların uygulanmasının sonuçları; maliyet, etkinlik ve yukarıda listelenen etkenlerle baęlı dięer faktörler açısından farklılıklarının görölmesi amacıyla test edilir. Böylelikle, faktörler arasındaki farklılıklar, maliyet ve fayda açısından koruyucu seçimi sonrasında kalan riskler, ortaya konur. Bir dięer yöntem de, koruyucu tiplerini sınıflandırmak ve farklı risk seviyeleri için uygulamalar önermektir. Örneğin daha güçlü kontrol mekanizmaları, düşük riskli sistemler yerine yüksek riskli sistemler için uygulanabilir. Başka bir bakış açısı da, yüksek riskli alanlara odaklanarak eleme yapmaktır [NIST, 1997].

“Eğer” analizinde, belirli bir durum için en iyi bileşeni belirlemek amacıyla çeşitli bileşenlerin maliyet ve faydalarına bakılır. Örneğin bir organizasyonda bilgisayar korsanlarına karşı tedbir olarak daha iyi bir şifre kullanımı kontrol yapısı oluşturma durumu gözönüne alınsın. Bu durumda organizasyon, tanımlama ve yetkilendirmenin daha güçlü olabileceği bir şifreleme sistemine geçebilir veya şifreleme prosedürlerini daha kuvvetli hale getirebilir. “Eğer şifreler daha kuvvetli hale getirilirse” durumunda neler yapılabileceği düşünüldüğünde, personelin şifrelerini daha sık periyotlarda değiştirmesi veya şifrelerde sayısal veya alfabetik olmayan bir karakter kullanma zorunluluğu getirilmesi bir çözüm olacaktır. Bu durumda mali bir harcamaya direkt olarak ihtiyaç duyulmayacaktır. Ancak, personelin konuyla ilgili eğitimi, sık değişen şifrelerin unutulması durumunda yapılacak işlemler gibi, çalışan maliyeti ve idari maliyetler gündeme gelecektir. Bu çözümle, bilgisayar korsanlarının sistemi başarılı olarak kırabilme sayısı mutlaka azalacaktır. “Eğer daha kuvvetli tanımlama ve yetkilendirme teknolojisi kullanılırsa” durumunda ise organizasyonun tek kullanımlı şifre üretme gibi daha profesyonel bir şifreleme sistemi kurması düşünülebilir. Böylelikle, şifreler üçüncü şahıslar tarafından elde edilseler bile, kullanılamayacaklardır. Bu sistem için gereken maliyet; direkt maliyet, yıllık bakım maliyeti ve personelin eğitim maliyeti değerlerinin hesaplanıp, toplanmasıyla bulunabilir. Profesyonel şifre sisteminde sistemin başarılı kırılma durumunun hemen hemen tümünden engelleneceğini söyleyebiliriz. Bu analiz sonuçları ve önerileri karar verici makam olan yönetime iletildiğinde, yönetim herhangi birini bütçe sınırlarına göre daha rahat seçebilecektir.

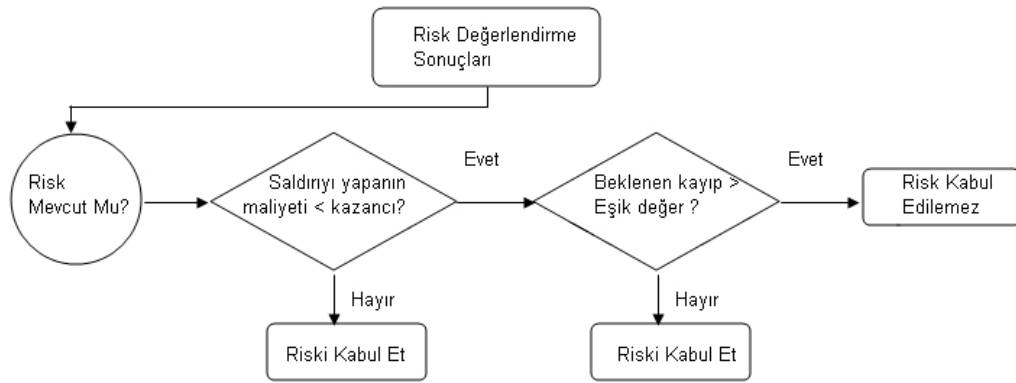
Karar vericilerin hedefi, daima harici sistemlerin güvensiz olduğu varsayımına dayanarak riski kabul edilebilir bir seviyeye indirgeyerek organizasyonun iş ve öz görev kapasitesini artırmak olmalıdır [Stoneburner et al, 2004]. Bazı durumlarda karar vericiler, kalan riskin kabul edilebilir olduğunu onaylamak durumunda kalabilirler. Koruyucunun gerek parasal, gerek parasal olmayan açılardan çok fazla maliyetli olması da riski kabul etme seçeneğini uygulamada önemli rol oynar [NIST, 1997].

Riske karşı yapılabilecekler aşamasında verilebilecek kararlar şunlar olabilir:

- Hiçbir şey yapmamak:
Analiz edilerek belirlenen riskin kabul edilir seviyede olduğu düşünülerek, bir önlem alınmadan risk olduğu gibi kabul edilebilir ve riskle yaşanır. Diğer yandan, olumsuz etkiyi ortadan kaldıracak veya etkisini azaltacak koruyucu etkin değilse de bu seçenek tercih edilebilir. Yani, riski ortadan kaldıracak veya kabul edilebilir seviyeye indireyecek koruyucuların maliyetinin, riskin gerçekleşmesi durumunda oluşacak zararlardan daha fazla olduğuna hükmedilerek de bu karar uygulanabilir.
- Riskten kaçınmak:
Söz konusu riski taşıyan varlık bir süreliğine ya da daimi olarak kullanım dışı bırakılır. Riske karşı uygulanabilecek önlemler karşılanamayacak kadar maliyetliyse veya teknolojik kısıtlar nedeniyle uygulanamaz durumdaysa ve risk nedeniyle olabilecek zararlar çok büyük boyuttaysa, bu seçenek düşünülür.
- Riski azaltmak:
Analiz sırasında tespit edilen riski azaltıcı, dolayısıyla da olumsuz etkilerin şiddetini azaltıcı koruyucular kullanılarak, risk kabul edilebilir düzeye getirilebilir.
- Riski ortadan kaldırmak:
Eğer risk tamamen ortadan kaldırılabilir durumdaysa, gerekli kontrolleri uygulayarak riski tamamen yok etme yoluna gidilebilir.
- Risk transferi:
Bu kararda, risk üçüncü şahıslara aktarılır. Sigorta, risk transferi için bir örnek olarak verilebilir. Ancak bu seçenek her varlık türü için uygulanabilir bir seçenek değildir.

Şekil 2.3'de bir saldırıya uğrama riski için, risk azaltma kararı uygulamaya gerek olup olmadığını belirlemek amacıyla kullanılan bir strateji gösterilmiştir.

Saldırıya uğranması tehditi için risk değerlendirme çalışmasından sonra elde edilen sonuca göre, eğer risk yoksa, birşey yapılmasına gerek yoktur. Ancak risk bulunmuşsa, saldırıyı yapanın bu saldırıyı yapabilmesi için gereken maliyet, elde ettiği kârdan daha fazlaysa, risk kabul edilebilir; çünkü bu durumda saldırıyı yapan, bilginin değerinden daha çok uğraş vermektedir, bu da caydırıcıdır. Tersı durumda, organizasyonun kaybı, daha önceden belirlenmiş bir eşik değeriyle karşılaştırılır ve bu değeri den daha büyük kayıp bulunursa; uygulanacak strateji, riski kabul edilemez diye nitelendiriyor. Bu durumda riski azaltmak için önlemler alınması gereklidir.



Şekil 2.3 Örnek bir risk azaltma stratejisi

Hangi risklerin azaltılacağına karar verildikten sonra, güvenlik kontrollerinin seçiminde yedi adımlı bir yaklaşım kullanılır [Bowen et al, 2006] [Dhillon, 2007]:

1. Eylemleri önceliklerine göre sıralama
2. Önerilen kontrol seçeneklerini değerlendirme
3. Maliyet-fayda analizini oluşturma
4. Kontrolleri seçme
5. Sorumlulukları atama
6. Korumacı uygulama planı geliştirme

7. Seçilen kontrolleri uygulama.

2.2.3. Yeniden Değerlendirme

Zaman içerisinde sisteme yönelik yeni tehditler ve yeni zayıflıklar ortaya çıkabilir. Organizasyonlardaki kişiler, iş prosedürleri ve uygulamaları veya sistemin yapısı değişebilir. Yazılımlarda farklılaştırmalar veya yenilemeler yapılabilir. İçsel faktörler veya yasal değişiklikler gibi dışsal faktörler nedeniyle güvenlik politikalarında düzenlemelere gidilebilir. Tüm bu durumlar, güvenlik ihtiyaçlarını ve risk değerini değiştireceğinden, risk yönetim işlemlerinin düzenli aralıklarla yeniden değerlendirilmesi gerekecektir. Bu nedenle, risk yönetim işlemleri sürekli bir yapıda olmalıdır. Risk yönetim adımları ancak periyodik ve düzenli tekrarlamalı olarak uygulanırsa başarılı bir risk yönetimine ulaşılabilir [Dhillon, 2007].

Değerlendirme sürecinde riskle ilgili değişikliklerin tespitinin yanı sıra, alınan kararların uygulanıp uygulanmadığı, sonrasında uygulamadaki sonuçları da gözden geçirilmiş olur. Risk yönetiminin dinamik olması bu süreç yardımıyla sağlanır.

2.3. Risk Analizi Sınıflandırması

Risk analizi, temel olarak iki sınıfa ayrılır: nitel risk analizi ve nicel risk analizi. Nitel yöntemlerde analiz, sıfatlar kullanılarak yapılır. Örneğin, düşük riskli, orta riskli, yüksek riskli şeklinde nitelendirmek gibi. Nicel yöntemlerde ise, matematiksel ve istatistiksel ifadeler kullanılır ve sayısal değerler ortaya konur [Hamdi and Boudriga, 2003] [Karabacak and Soğukpınar, 2004]. Uygulamada bu iki temel sınıfı bir arada kullanan karma yöntemlere de rastlanmaktadır. Karma yapıdaki yöntemlerde bile, nitel veya nicel özelliklerden bir tanesi daha ağırlıklı olmakta, yöntem bu özelliğiyle daha nicel veya daha nitel olarak sınıflandırılabilir [Dwaikat and Parisi-Presicce, 2005]. Kullandığı yöntem ister nitel, ister nicel olsun, genel olarak bütün risk analiz yöntemlerinin ana hedefi, toplam risk değerini tahmin etmektir [Vorster and Labuschagne, 2005].

Nitel ve nicel yöntemlerin kendilerine özgü bazı avantajları ve dezavantajları bulunmaktadır. Her iki yöntemin avantaj olarak sıralanabilecek özellikleri şunlardır [Tipton and Krause, 2000]:

Nitel yöntemlerin avantajları:

- Riskleri önceliklere göre sıralamada daha başarılıdırlar. Riskler uygulanan skalaya göre kolayca önceliklendirilebilecektir.
- Zayıflığa işaret etmede daha hızlıdırlar. Riskler yüksek, düşük, orta olarak etiketleneceğinden, yüksek riskler, dolayısıyla da en şiddetli zayıflık hemen göze çarpacaktır.
- Yoğun matematiksel işlem kullanılmadığından hesaplama açısından, kolay anlaşılır ve hızlıdırlar.
- Parasal değerleri ve sayısal frekansları kullanmak zorunlu değildir.

Nicel yöntemlerin avantajları:

- Olumsuz etkilerin şiddetinin nicel değerleri, birbirlerinden bağımsız olarak elde edilebilir.
- Bilginin bütünlüğü, güvenilirliği ve erişilebilirliği gibi soyut durumlarını parasal olarak ifade edebilmek, anlaşılabilirliğin artmasını sağlayacaktır.
- Nesnel (objektif) bir yaklaşım sağlar.
- Bilgi güvenliği bütçesi kararı için destekleyicidir.
- Risk yönetiminin performansının ölçülmesini ve değerlendirilmesini mümkün kılar.

Her iki yöntemin dezavantaj olarak sıralanabilecek özellikleri de şu şekilde listelenebilir [Tipton and Krause, 2000] [Li et al, 2006]:

Nitel yöntemlerin dezavantajları:

- Olumsuz etkinin şiddetinin, sayısal büyüklüğünü veremez. Etki değeri, sayısal aralıklara bağlı olarak ifade edilebilir. Bu nedenle açık olmayabilir. Elde edilen sonuçlar sıfatlar şeklinde olduğundan aynı kategoride sınıflanan iki tehditin, birbirleriyle karşılaştırılıp kendi aralarında önceliklerinin belirlenmesi mümkün olmayacaktır.
- Maliyet analizi yapmak zordur.
- Öznel yaklaşımlıdır. Dolayısıyla risk yönetimi performansını, nesnel olarak değerlendirmek mümkün olmayacaktır.

Nicel yöntemlerin dezavantajları:

- Yoğun matematiksel işlemler kullanıldığından, hesaplama açısından yavaşlardır.
- Daha uzun zaman harcanarak uygulanabilirler, dolayısıyla da daha maliyetlidirler.
- Büyük ölçüde bilgi toplanmasını gerektirir. Yeterli miktarda veri toplamak oldukça zordur.

2.4. Risk Analizi Yöntemlerinin Karşılaştırılması ve Yöntem Seçimi İçin Mevcut Çalışmalar

İlk kuşak risk analizi yöntemleri, 1970'lerin başlarında kullanılmaya başlanan ve kontrol listesi şeklinde bir yapıda olan yöntemlerdi [Baskerville, 1993]. Bilgisayarların çok güçlü olmadığı bu dönemlerde zaman açısından avantajlı olan nitel yöntemlerin kullanımı olağandır. Zaman içinde teknik altyapının gelişmesi paralelinde ve ihtiyaçlar çerçevesinde nicel yöntemler de nitel yöntemlerin yanında geliştirilip uygulanmaya başlandı [Tipton and Krause, 2000].

Nicel yöntemlerde kullanılan matematiksel ve istatistiki yöntemler EK 2'de açıklanmıştır.

Nitel ya da nicel, bir risk analiz yöntemi, yazılımla desteklenebilir. Özellikle nicel yöntemlerin, yoğun matematik işlemler içermeleri dolayısıyla oluşan zaman dezavantajları nedeniyle, yazılım kullanmaları oldukça anlamlı olacaktır. Yazılımla desteklenmeyen yöntemler ise, doküman temelli yöntemler olarak adlandırılırlar. SPRINT bu türe örnek bir risk analiz yöntemidir [Vorster and Labuschagne, 2005].

Günümüzde bilgi güvenliği için risk analizi uygulamalarında nitel ve nicel olarak geliştirilmiş birçok yöntem ve bu yöntemleri uygulayan pek çok risk yönetim araçları da bulunmaktadır. Özellikle riski oluşturan belirsizlikten ve tehdit frekansı, koruyucu etkinliği, risk değeri gibi risk modeli elemanlarının tam değerlerinin belirlenme güçlüğünden kaynaklanan problemleri ortadan kaldırmak için, Monte-Carlo Simülasyonu, Stokastik Yöntem, Bayes Teoremi gibi matematiksel ve istatistiki modelleri kullanan yöntemler geliştirilmiştir.

Sadece özel durumlar için geliştirilmiş yöntemler de bulunmaktadır. Gerçek Zamanlı Risk Analizi yöntemi böyle bir yöntemdir. Bu yöntem, iki uç nokta arasındaki iletişimden kaynaklanan riski gerçek zamanlı olarak belirlemekte ve bu riske karşı önlemler almaktadır ve ancak sadece bu özel durum için uygulanabilmektedir. Benzer şekilde sadece yazılım geliştirme riskleri ve bilgi sistemleri projelerinin riskleri için de bazı özel risk analizi yöntemleri bulunmaktadır.

Amaçları aynı olsa da –riski belirleyip azaltmaya çalışmak ve böylece bilgi güvenliğini sağlamak– risk sürecini farklı yorumlayan, hazırlık aşamasını detaylı ve zaman maliyetli tutan veya tutmayan, risk değerini hesaplarken uygulanan formülü basitleştiren ya da karmaşıktıran, nitel veya nicel olan, koruyucu kontrol önerileri için yaklaşımları birbirinden farklı, pek çok yöntem bulunmaktadır.

Örneğin COBRA, organizasyon dışından destek almayı gerektirmeden ve bilgi güvenliğini öncelikle teknik bir konu olmaktan çok bir iş konusu olarak göstererek anlaşılır hale getiren bir yöntemdir. Bu yapıyla da maliyete odaklanır. ISO/IEC 17799'deki işleyişle uyumludur. Tehditler ve zayıflıkların göreceli önemlerini

derecelendirerek uygun öneriler ve çözümler üretir. Düzenlenebilir ve değerlendirilebilir alt bölümlere sahip iki temel kısımdan oluşur: Risk Çözümleme ve ISO Uyumluluğu. Risk çözümleme için hazır soruları bulunmasına karşın, uygulayıcıların kendi sorularını hazırlayabilmesi seçeneğini de sunar [C&A, 2003].

RAMEX ise, risk analizi ve risk kontrolleri için uygulanabilen nitel bir yöntemdir. Küçük veya orta ölçekli organizasyonlar için önerilir. Veri toplama, analiz ve sonuçların raporlanması şeklinde üç süreçten oluşur. Bu süreçler beraberce yedi adıma bölünmüştür. İlk dört adım veri toplanması sürecini, beşinci ve altıncı adımlar bu verilerin analizini, yedinci ve son adım da raporlama kısmını oluşturur. RAMEX, diğer yöntemlerden farklı olarak, insan kaynaklı tehditlere de oldukça önem verir [Kailey, 1995].

IST/RAMP, karma bir yöntemdir. Nicel açıdan bakıldığında, yazılımı birim kayıp değerinin yanı sıra yıllık kayıp beklentisini de hesaplar. Ayrıca nitel analiz yapması da mümkündür. Risk analizi yapmak için, incelenen sistemle ilgili mevcut veri kümesini düzenleyip kontrol ederek bir yapı kurar. Analiz sırasında riskin neden olabileceği kayıpları beş sınıfa ayırarak inceler: (1) hizmet kesintileri, (2) fiziksel kayıp veya hasarlar, (3) sahtekarlık, (4) yetki dışı açığa çıkma ve (5) fiziksel hırsızlık. Analizcinin en iyi maliyet etkin güvenlik ölçümü yapabilmesi için, eğer analizlerini kullanır.

BUDDY SYSTEM, Countermeasures Inc. Firması tarafından mikrobilgisayarlı ortamlar için geliştirilmiş yazılımla desteklenmiş, karma bir yöntemdir. Karşı önlemler için anket çalışmaları ve güvenlik analizleri yapar. Zayıflıkları değerlendirmek için, kendi veri tabanında bulunan yüzden fazla koruyucuyu temel alır ve böylece zayıflığın kabul edilebilir ya da kabul edilemez düzeyde olduğuna karar verir. Daha sonra da, “eğer” analizini kullanarak kabul edilemez zayıflıklar için, raporlar ve takip yordamlarıyla izlenmek üzere analizcilere çeşitli düzenleyici faaliyetler önerir. Bilgi toplama aşamasında kullandığı anket yapısı, kolay ve çok karışık olmayan sistemler için kısa sürede tamamlanabilen bir çalışma içerir. Ardından gelen analiz çalışmalarında ise, zayıflıkların belirlenmesi ve bunlara karşı koruyucular, koruyucuların etkinliklerinin ölçümü yapılır. Ayrıca, yöntemde bulunan

bakım aşamasında ihtiyaca göre yeni varlık, zayıflık ve koruyucuların eklenmesi de mümkün kılınmıştır.

CRITI-CALC, The Zeta Group tarafından özellikle kritik yapıların tanımlaması, sınıflandırılması ve bu yapıların birbirine bağlı olarak kritikliklerinin değerlendirilmeleri için geliştirilmiş risk yönetimi ve acil durum hazırlık planlama yöntemidir. Kullanımı anlaşılır ve basittir. Bir yapının ait olduğu sınıfı tespit edebilmek için kullanıcı, basit sorular ve seçeneklerle yönlendirilir. Ağların, sistemlerin veya uygulamaların yanı sıra, dönemsel, periyodik ya da ara sıra kullanılan varlıkların tanımlanması yapılabilir. Sınıflandırmada; kapsam, etki şiddeti, etkilenen alanın büyüklüğü, bağıllık vb. gibi kriterler kullanılır. Yöntem değerlendirme sonrasında kritik yapıları A, B, C, D ve E diye isimlendirilmiş beş sınıfa ayırır. Bu sınıflandırma yardımıyla yetkililer, acil durumlar karşısında yapacakları hazırlıkların ve uygulayacakları çözümlerin etkin olmasını sağlamış olurlar [The Zeta Group, 2009].

RA/SYS Nander Brown & Co. tarafından geliştirilmiş nicel bir yöntemdir. Altmıştan fazla tehditle yaklaşık elli kadar zayıflık ve varlığı birbiriyle bağlantılı olarak kullanan bir risk analizi sisteminden oluşmaktadır. Tehdit derecelendirme ve tehdit frekansını hesaplamak için tehdit/zayıflık eşleştirmelerini göz önüne alır. Ürettiği sonuç raporlarında kayıp beklentisi, maliyet-fayda analizi ve yatırımların geri dönüşlerini gösterir [Tipton and Krause, 2000] [EFF, 2009].

GRA/SYS yöntemi de Nander Brown & Co. tarafından geliştirilmiştir. İç denetçiler ve güvenlik uzmanlarının, organizasyonel riskleri gözden geçirmeleri ve önceliklere göre çalışma planı geliştirebilmeleri için tasarlanmış yazılımı olan bir nitel risk analizi yöntemidir. Yazılım, riski belirlemek için uygulama ve bilgisayar aktivitesi envanteri hazırlar. Risk değeri, 1 ile 9 arasında bir sayıyla hesaplanır. Burada 9 en kötü durumu yani en yüksek riski temsil eder. Yazılımdan elde edilen raporlarla koruyuculara gerek duyulan riskler tespit edilmiş olur [Tipton and Krause, 2000] [EFF, 2009].

MINIRISK de yine Nander Brown & Co. tarafından mikrokompüter ortamlar için güvenlik zayıflıklarını deęerlendirmek amacıyla geliştirilmiş nitel bir yöntemdir. Bu amaçla yazılım zayıflık deęerlendirme anketi kullanır. Anketle deęerlendirdięi zayıflıklar, kullanıcının elliye kadar ayrılmış zayıflık kategorilerindeki (örneğin, şifre yönetimi, olasılık planlama, iç denetleme kontrolleri kategorileri gibi) eksik koruyucuları tespit etmesine yardımcı olur. Belirli koruyucuların bulunmayışı, zayıflık seviyesini ortaya koyar. Zayıflık seviyesi için kullanılan ölçek 0 ile 9 arasındadır. 0 deęeri en iyi duruma, 9 deęeri ise güvenlik açısından en kötü duruma işaret eder. Her bir koruyucunun yeterlilięi deęerlendirilirken, tespit edilen eksik koruyucular uygulamaya konulduktan sonra bunların tekrar deęerlendirilmeleri de mümkündür [EFF, 2009].

PRISM, Palisade şirketi tarafından geliştirilmiş, risk analizi modelleme, risk benzetim çalışmaları ve hassaslık analizi yapan nitel bir yöntemdir. Raporlamasında grafik gösterim yapısından da faydalanılması, sonuçların kullanıcılar tarafından anlaşılabilirliğinin artmasına yardımcı olur. Hesaplamalarında basit cebirsel denklemler kullanılmasının yanı sıra, daha karmaşık uygulamalar için programsal ifadeler kullanılması da mümkündür [EFF, 2009].

LAVA, Los Alamos National Laboratory tarafından geliştirilmiştir ve karma bir yöntemdir. Şifre yönetiminden personel güvenliği ve iç denetleme uygulamalarına kadar otuz dört alanda bulunan kontrol eksikliklerinin tanımlanması için anket yöntemini kullanır. Bu şekilde toplanan veriler, yazılımı tarafından deęerlendirilerek, organizasyon üzerindeki olası sonuçlar, şiddetleri ve beklenen kayıp deęeri (yani risk) hesaplanır. LAVA yöntemi, üç çeşit tehdiye odaklanır: (1) doğal ve çevresel tehlikeler, (2) kasdi veya kasdi olmayan dahili insan tehditleri, (3) harici insan tehditleri. Analizler sonrası hazırlanan detaylı raporlar, tanımlanan riskin hem nicel, hem de nitel deęerlerini ortaya koyar. Yöntem, risk deęerlendirme çalışmasında takım çalışması yaklaşımına önem verir. Ayrıca, titiz bir deęerlendirme için, ekipteki kişilerin tecrübe ve bilgi bakımından geniş bir yelpazede olmasını ve deęerlendirme sırasında ortak karar vermelerini önerir [EFF, 2009].

LRAM, nicel bir yöntemdir ve Lawrence Livermore National Laboratory tarafından geliştirilmiştir. Yöntem, varlık/tehdit/olay eşleştirmesi ile sadece yüksek etki şiddetindeki risklerin gözlemlenmesini sağlamaktadır. LRAM'da mevcut güvenlik kontrollerinin yanında, önerilen kontrollerin de etkinliğine odaklanılır. Yöntemin üç ana adımı vardır: (1) proje planlama, (2) risk analizi, (3) karar verilmesi. Proje planlama adımı analiz edilecek alanın çerçevesi ve ihtiyaç duyulan kaynaklar ve personel tanımlanır. Risk analizi adımı, ilk adımda toplanan veriler değerlendirilir. Değerlendirilme işlemi sırasında tehditler, kontroller ve varlıklar eşleştirilerek risk elemanları belirlenmiş olur. Son aşama olan karar verme adımı için, ikinci aşamada elde edilen sonuçlar değerlendirilir. Yani bu adım, bilgi güvenliği yönetimine destekleyicidir ve öncelik sırasına göre önerilen koruyucuları listeleyip, maliyet-fayda tahminlemesi gibi karar vermeye yardımcı ölçütler yardımıyla seçme yapılmasını sağlar [EFF, 2009].

MARION, Coopers & Lybrand tarafından geliştirilmiş karma bir yöntemdir. Öncelikle organizasyonun mevcut güvenlik profilini ortaya koymayı hedefler. Kendi veri tabanında bulunan sorularla, yirmi yedi güvenlik kategorisi için mevcut sistemin güvenliğini analiz eder ve sonuçlarını grafiklerle gösterir. Bu şekilde bir güvenlik profili tespit edildikten sonra, yine veri tabanındaki örneklerle karşılaştırma yaparak güvenlik bütçesi için tahmini bir masraf tutarı hesaplar. Hesaplanmış tutarlar güvenlik kategorileri için eğer yöntemiyle analiz edilerek güvenlik profilinin etkinliği incelenir. Bu şekilde güvenlik profilini daha iyi seviyeye getirebilecek bir önlem önerir [EFF, 2009].

MicroSecure Self Assessment, kişisel bilgisayar kullanıcılarına güvenlik değerlendirmesi için rehberlik eden, yazılımı olan nitel bir yöntemdir ve Boden Associates tarafından geliştirilmiştir. Yazılımı kişisel bilgisayar ortamını analiz ederek zayıflıkları tespit eder ve uygun güvenlik kontrollerini önerir. Önerilen koruyucular güvenlik seviyesini yükseltmenin yanında altı alan için korunmasızlığı da düşürmeyi hedeflemektedir. Bu alanlar şunlardır: (1) sistem bütünlüğü, (2) veri güvenliği, (3) güvenilirlik, (4) veri bütünlüğü, (5) yedekleme ve geri kazanım, (6) gizlilik. Yazılım, güvenlik seviyesinin ihtiyaç duyulan ve belirlenmiş bir duruma getirebilmesini sağlayacak şekilde de ayarlanabilir [EFF, 2009].

Başka bir nitel yöntem ise QUICKRISK'tir. Bu yöntemde, analiz aşamasının başında kullanıcıdan senaryo formunda sistemle ve özellikleriyle ilgili giriş bilgileri alınır. Senaryo şeklindeki bu formlar, analiz edilecek sistemin potansiyel tehditleri, mevcut koruyucuları ve varlıkları ile ilgilidir. Toplanan veriler, yazılım yardımıyla yıllık kayıp beklentisini ve her bir uygulanan koruyucu için yapılan yatırımının geri dönüşünü hesaplamakta kullanılır. Yazılım, birçok tehdit ve sıklıklarını içeren ve gerektiğinde kullanıcıların yenilerini de ekleyebileceği bir tehdit dosyasına sahiptir. Yöntemin önemli bir özelliği olarak, ihtiyaç dahilinde analiz aşamasında toplanan giriş verileri, sonradan güncellenerek daha önce hesaplanan sonuçları yenilemek de mümkündür [EFF, 2009].

RANK-IT, Delphi tekniğini kullanan bir risk değerlendirme yazılım paketidir. Jerry FitzGerald & Associates firması tarafından geliştirilmiştir. Delphi yöntemi risk derecelendirmede kullanılan bir uzman sistemdir. RANK-IT; tehditler, kontroller, zayıflıklar, bileşenler veya istenen başka kriterler için sistemin risk sıralamasını elde etmek için kullanılır. Yazılım yardımıyla, Delphi'yle beraber Karşılaştırmalı Risk Derecelendirme yaklaşımı kullanılarak sıralanmış bir liste elde edilir veya risk değer yüzdesi hesaplanır. Derecelendirilmiş her bir varlık, ağırlık katsayısı ya da asıl sayı değeri olarak kullanılacak bir sayısal değere sahiptir. Uygulanması pratik ve oldukça süratlidir. Yöntem, nicel olarak ifade edilsin veya edilmesin, işle ilgili başka karar seçeneklerini sıralamak amacıyla da kullanılabilir [EFF, 2009].

RiskCALC, Hoffman Business Associates tarafından geliştirilmiş karma bir yöntemdir. Hazır formdaki anket soruları yardımıyla ALE yıllık kayıp beklentisini veya istenen başka bir metrik değerini hesaplamayı sağlar. Yöntem yazılımında mevcut bulunan bu soruları cevaplamak ve raporlamak mümkündür. Yöntemin risk azaltma modülüyle en belirgin riskler tespit edilir. Kullanıcı, isteğe bağlı olarak en uygun maliyet-fayda etkinliğine sahip koruyucuları belirlemek amacıyla değerler üzerinde değişiklik yaparak sonuçlarını ekrandan takip edebilir [EFF, 2009].

RISK-PAC yöntemi, sorular, anketler ve raporlar olarak üç bileşenden oluşan nitel bir yöntemdir. Sorular bölümü, organizasyonun politikalarını, fiziki çevresini, donanımını, uygulamalarını ve verilerini gözden geçirmek yoluyla sistemi oluşturan bu ayrık kategorileri tek tek inceler. Sorular sektöre bağlı olarak çeşitlendirilebilir. Bu bölümde elde edilen sonuçlar, analizin temelini oluşturan anket bölümünde kullanılırlar. Yöntemde ağırlıklandırma ve skotlama algoritmasında, Kepner/Tregoe analizi kullanılır. Elde edilen raporlar, 1 ile 5 arasında ölçeklendirilmiştir. 5 derecesi, güvenlik için en kötü duruma işaret eder [EFF, 2009].

Diğer bir yöntem ise karma özellikli RISKWATCH yöntemidir. Büyük ya da küçük ölçekli organizasyonları, sistemleri, uygulamaları, ağıları analiz etmeye yardımcı olur. Özellikle finansal, kritik, hassas ve sınıflandırılmış sistemlerde önemli ölçüde kullanışlıdır. Tehditler, varlıklar, zayıflıklar, kayıplar ve koruyucular arasında binin üzerinde ilişki kurulmuş veri tabanına sahiptir. Yöntem, seçilen herhangi bir tehdit, varlık, zayıflık veya koruyucu için sorgulama yapmaya izin verir. Raporlamaları varlık envanteri, detaylı zayıflık listesi, yıllık kayıp beklentilerini gösteren tehdit analizi ve yatırımın geri dönüş değerini de içeren koruyucu önerme raporu şeklindedir [EFF, 2009].

Yöntemlerin en iyisini bulmak için, altyapıları farklı yaklaşımlara ve matematiksel ve istatistiksel temellere dayanan yöntemleri karşılaştırmak, anlamlı değildir. İhtiyaç ve beklentiler doğrultusunda, farklı organizasyonlar için farklı yöntemler daha kullanışlı olabilirler.

En uygun risk analizi ve yönetimi seçimi için Vorster'in farklı risk analizi yöntemlerini karşılaştırdığı çalışmadan ilk bölümde bahsedilmiştir. Vorster'in çalışmasında, örnek olarak seçilen nitel ve nicel sınıftan, beş farklı yöntem üzerinde incelemeler yapılmıştır. İnceleme sırasında uygulanan karşılaştırma kriterleri şu şekildedir:

- *Risk analizinin tekli varlıklar veya varlık grupları üzerinde yapılması:*

Yöntemin sonuçlarından, tek tek varlıklar ya da varlık grupları üzerinde yapıldığını anlayabiliriz. Varlıklar üzerinde tekil analiz yapılması, zaman açısından organizasyona maliyet getireceğinden organizasyonun yöntem seçiminde etkili olacaktır. Bu nedenle çoğu organizasyon, varlık grupları üzerinde risk analizi gerçekleştirebilecektir.

- *Risk analizinin uygulandığı yöntemin bulunduğu yer:*

Risk analizi için gereken bilgi ve çalışmaların miktarını belirleyen kriterdir. Yöntemde bu kriter, iki alternatifle değerlendirilir: (1) *zaman*, ya da daha kritik sistemler için (2) *sonucun tamlığı*. Bu kriter, organizasyonun önceliğine göre belirlenip ölçeklendirilebilir.

- *Risk analizine katılan kişiler:*

Analizin, organizasyonun dahilindeki kişilerle veya harici kişilerin katılımıyla olması, maliyet ve uzmanlık açısından farklılık yaratacaktır. Burada da kriter olarak organizasyonun maliyet veya uzmanlık önceliğine göre ölçekleme yapılmasına imkan sağlanmıştır.

- *Kullanılan ana formül:*

Uygulanan yöntemdeki matematiksel formülün karmaşıklığı, zaman ve sonucun güvenilirliği açısından değerlendirilir. Organizasyon, isteğe bağlı olarak bu kriteri kolaylık ve sonucun tamlığı seçeneklerinden birini gözönüne alarak değerlendirebilir.

- *Sonuçların bağlı ya da mutlak olması:*

Uygulanan yöntem ile bulunan sonuçlar, her zaman karşılaştırılabilir olmayabilir. Örneğin, bir yöntemde iki varlığa yönelik bulunan risk sonucu da yüksek ise, hangisinin daha büyük risk taşıdığını söylemek mümkün olmayacaktır. Ama başka bir yöntemde bulunan iki risk değeri

200 ve 100 ise, birincinin ikinciye göre daha yüksek risk taşıdığını söylemek mümkündür.

Vorster, analiz ettiği yöntemleri bu kriterler bazında değerlendirmiş, ölçeklendirmiş ve karşılaştırma için bir tablo oluşturmuştur. Yöntem, beş kriterden her birinin önem derecesine bağlı olarak, organizasyon tarafından ağırlık katsayısı seçilmesini olanaklı kılmıştır (eşit ağırlıklı bir değerlendirme için beş kriterin ağırlık katsayısı, 0,2 alınabilir). Her bir yöntem için; kriterlerin değeri, bu ağırlık katsayısıyla çarpılıp sonuçları toplandığında, o yöntem için bir değer bulunacaktır. En büyük değere sahip olan yöntem, organizasyonun ihtiyaçlarıyla en iyi örtüşen yöntem olarak değerlendirilir.

Vorster'ın çalışması, farklı özelliklerdeki risk analiz yöntemlerine uygulanabileceği ve organizasyonun ihtiyaçları doğrultusunda katsayılarla şekillendirilebileceği için olumlu bir tablo çizmesine rağmen, Vorster'in makalesinde de belirttiği gibi bazı zayıflıklara sahiptir. Örneğin, makale ile belirlenen kriterler haricinde en uygun yöntem seçiminde etkin olabilecek farklı kriterler de tespit edilebilir. Ayrıca, çalışmada seçenekli hale getirilmiş bazı kriterler, uygulayıcıları iki özellikten birini seçmeye zorlamaktadır. Organizasyonun ihtiyaçlarını belirleme ve tatmin için sadece ağırlık katsayılarının kullanılması yeterli olmayacağı gibi, bu katsayıların belirlenme yöntemi de net ve objektif değildir.

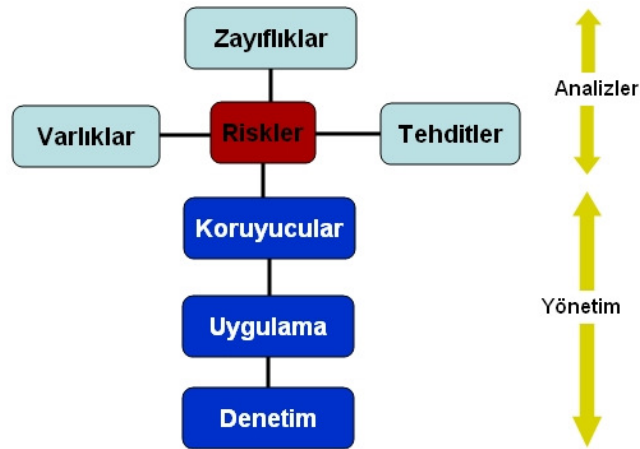
Bu bölümün devamında mevcut bazı ticari ve akademik risk analiz ve yönetim yöntemleri daha detaylı olarak incelenmiştir.

2.5. CRAMM (CCTA Risk Analysis and Management Methodology)

İngiliz hükümeti tarafından görevlendirilen CCTA tarafından öncelikle İngiliz resmi dairelerinde kullanılmak üzere geliştirilmiştir. Günümüzde özel sektörde de yaygın olarak kullanılmaktadır. BS7799'la tam uyumlu ve ayrıntılı risk değerlendirme

araçlarından oluşan, nitel bir yöntemdir. Organizasyonun varlıklarını, süreçlerini, uygulamalarını, sistemlerini, tehdit ve zayıflıklarını, risk seviyelerini, koruyucuları güvenlik yönünden analiz etmek için sorular kullanır. Bu sırada yapılan analizin daha detaylı (ve uzun) ya da hızlı (ve kısa) olarak yapılabilmesinin seçimli olmasıyla, geniş kapsamlı konulara değinen soru yapısıyla kullanımı esnekliklidir. Potansiyel problemleri (virüsler, kırıcılar, ekipman veya yazılım eksiklikleri, kasıtlı zararlar, insan hataları gibi) dikkate alarak nitel analiz yapar. Ancak, istenirse sonuçların nicel değerlere çevirilebilmesi de mümkündür. Kullanıcıların verdiği yanıtlar doğrultusunda “eğer” yöntemini kullanarak koruyucu değerlendirme yapar ve bu koruyucuların birbirlerine göre önceliklerini belirler. Koruyucu maliyetlerini tahminler, güvenlik politikası geliştirilmesine yardımcı olur ve denetleme yapılmasını olanaklı kılar [CRAMM, 2001].

CRAMM, bilgi güvenliğine, hem teknolojik (donanım, yazılım gibi) hem de teknik olmayan (fiziksel çevre, insan gibi) açılardan disiplinli bir yaklaşım sağlar. Güvenlik bileşenlerini, varlık tanımlama ve değerlendirme, tehdit ve zayıflık değerlendirmesi, koruyucu önlemlerin seçimi ve öneriler olarak 3 adımda değerlendirir. Şekil 2.4’de CRAMM’in risk analizi ve risk yönetimi yapısı görülmektedir.



Şekil 2.4 CRAMM’in yapısı

Bilgi sistemlerindeki varlıklar, varlık tanımlama ve değerlendirme aşamasında; fiziksel, yazılım, veri ve konum varlıkları olarak gruplandırılarak tanımlanır ve her bir varlığın değer analizi yapılır. Fiziksel varlıklarda varlığın değeri, yerine koyma maliyeti iken, diğer varlıklarda ise bilgi sisteminde bu varlıklar kullanılamaz hale geldiğinde, değişmiş veya yok edilmiş olduğunda oluşan etkinin değeri şeklinde düşünülür. Bu değerler, 1 ile 10 arasında bir skala yardımıyla ölçeklendirilir. Yöntem, varlık değeri 3 ve daha büyük olarak sınıflandırılmış varlıklarla işleme devam eder.

CRAMM’de, tehdit ve zayıflık analizinde bilgi sistemlerine karşı kasıtlı veya kasıtsız olası tüm tehdit ve zayıflıklar listelendiği için, mevcut riskin hesaplanması mümkündür. Riski hesaplama aşamasında tehdit ve zayıflıkları 1 ile 5 arasında ölçeklendirerek, aralarındaki bağlantıyı kurar, tehdit-zayıflık ikilisinin oluşturduğu riskin seviyesini hesaplar.

Öneriler ve karşı önlemler adımı için kullanılmak üzere, 70’den fazla mantıksal grupta altında 3000’in üstünde koruyucu içeren detaylı bir koruyucu kütüphanesi vardır. Son aşamada CRAMM yazılımı, önceki adımda belirlenmiş risk değerini kullanarak belirlenen bir eşik değeri güvenlik seviyesi için, kütüphanesindeki uygun koruyucuları karşılaştırır ve detaylı raporlar sunar. Bu şekilde karar verilmesini kolaylaştırır [CRAMM, 2001].

2.6. CORAS (Construct a Platform for Risk Analysis of Security Critical Systems)

CORAS, nitel risk analizi yöntemini kullanır. IST programı dahilinde geliştirilmiştir. Temel amacı, risk analizi için yöntemler, nesneye dayalı modelleme için yarı formal yöntemler, güvenliğin kritik olduğu sistemlerde kesin, belirgin ve etkin bir risk analizi sağlayan hesaplayıcı araçları sıyan bir çerçeve geliştirmektir [Vorster and Labuschagne, 2005]. Yöntemde varlıklar, tehditler ve zayıflıklar arasındaki ilişkileri ve riskin bulunduğu ortam arasındaki bağlantıları göstermek için görsel diyagramlar (UML) kullanılır.

Risk analizi sırasında toplanan bilginin çoğu, beyin fırtınası, seminer ve tartışmalarla, farklı alanlar ve düzeylerde uzman olan kişilerin (kullanıcı, sistem geliştiricisi, sistem yöneticisi, vb.) bir araya gelmesi ve fikirlerin, bilgilerin paylaşılmasıyla ortaya konur. Uygulanan işlemler açısından, biri risk yönetim süreçlerinden olan analiz sonrası çalışmalar olmak üzere dört ana katmandan ve yedi adımdan oluşur. Bir kararın temel alındığı final sonuç, her bir varlık için farklı UML sınıfı diyagramı şeklindedir [Braber et al, 2007]. Bu görsel diyagramlarda, varlıklar için söz konusu tüm kaynakları, mevcut riskleri, bunların birbirleriyle olan etkileşimlerini ve bu şekilde riskin derecesini nitel sıfatlarla görmek mümkündür.

2.7. ISRAM (Information Security Risk Analysis Method)

ISRAM, 2003’de geliştirilmiş nicel ve doküman temelli bir risk analizi yöntemidir. Yedi aşamadan oluşmaktadır. İlk dört aşamada ön çalışma yapılır ve tetkik testleri hazırlanır. Konuyla ilgili tüm kişilerin fikrini almak amacıyla organizasyondaki yöneticiler ve çalışanların katılımını sağlayarak, bilgi güvenliği problemlerinin neden olduğu risk değerlendirilir. ISRAM’da güvenlik açıklarını etkileyen olasılıkla ve bu açıkların etkileriyle ilgili tüm faktörler belirlenerek listelenir ve bu faktörlere ağırlık değerleri atanır. Realistik ve objektif sonuç elde etmek için en hayati bölüm bu adımdır. En az önem içeren faktör, en düşük ağırlık değeri olan 1’le derecelendirilir. En önemli faktör ise, belirlenmiş en yüksek ağırlıklı değere sahip olacaktır.

Bunu takiben tüm faktörler, riskin olasılığını ve olumsuz sonuçlarını ölçmek amacıyla çeşitli sorular ve cevap seçeneklerinin bulunduğu iki ayrı tetkik testine dönüştürülür. Bu testlerle, bilgi güvenliği probleminin sistemdeki veya organizasyondaki etkileri ve dereceleri ortaya konmuş olur. Derecelendirme yapabilmek için, her soruya verilebilecek cevap seçenekleri belirlenerek bu cevaplar numaralandırılır. Nicel analiz için hayati önem taşıyan risk tabloları hazırlanır. Her tetkik testinden elde edilebilecek tüm sonuçlar için, risk tabloları ölçeklendirilir. Bu şekilde dördüncü aşama sonlanmış olur.

Beşinci aşamada, hazırlanan her iki tetkik testi, yöneticiler, direktörler, teknik personel ve diğer kullanıcılara dağıtılarak, yanıtlanması istenir. Tetkik testlerinin uygulayıcıları veya uygulanma sayısı aynı olmak zorunda değildir. Altıncı aşamada testlerin sonuçları ISRAM yönteminde tanımlanmış olan risk formülüne uygulanır. Böylece sonuçta, risk için tek bir sayısal değer elde edilir.

Yedinci ve son aşamada ise değerlendirmeler yapılır. Bu değerlendirmeler sırasında sadece altıncı aşamada elde edilen risk değeri değil, tetkik testlerindeki soruların cevapları da analiz edilir.

ISRAM'da risk, 1 ile 25 arasında numaralandırılır. Bu sayısal değer, yüksek, orta veya düşük değer olarak risk yönetiminde karara temel oluşturacak bir nitel ifadeye karşı gelir. Eğer istenirse ALE formülü kullanılarak maliyet değeri hesaplanabilir [Karabacak and Soğukpınar, 2004].

2.8. OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)

OCTAVE, CERT/CC tarafından geliştirilmiştir. Varlıklar, tehditler ve zayıflıklara odaklanan ve risk değerlendirmesinin sadece organizasyon dahilindeki kişilerce (bilgi teknolojileri ve diğer iş ünitelerindeki personel) yürütülmesini öngören bir yöntemdir. Riski hesaplarken nitel kriterler kullanır. Uygulanması şart olan belirli aktivite işlemlerini içeren ve sekiz alt sürece ayrılan üç fazdan oluşur. Elde edilen sonuç raporu, farklı varlıkların tehdit profili şeklindedir ve risk kararları bu rapora dayanır [Vorster and Labuschagne, 2005] [CERT, 2008].

OCTAVE'da varlıklar tek tek analiz edilerek tehditleri değerlendirilir ve riskleri hesaplanır. Analiz öncesi yoğun bir hazırlık gerektirir, öyle ki bu hazırlıklar ilk altı süreç boyunca devam eder. Bu yüzden zaman açısından maliyetlidir ancak bu durum elde edilen sonuçların doğruluk oranını artırır. Yedinci ve sekizinci adımlarda toplanan verilere dayanarak risk analizi işlemleri yapılır. Risk değeri hesabı için kullanılan olasılık ve etki şiddeti parametreleri, nitel değerler alırlar

(yüksek, orta, düşük gibi) ve bu nedenle nesnel değildirler. Bu özellik, riskin değerine de yansır. Ayrıca varlıkları ayrı ayrı değerlendirdiği için sonuçlar arasında karşılaştırma yapmak mümkün değildir. Örneğin, risk seviyesi yüksek olan iki varlık için göreceli yükseklik karşılaştırması yapılamayacaktır.

2.9. Risk Analizi İçin Geliştirilmiş Standartlar

Risk analizi sırasında her kuruluş, serbest olarak bir yol izleyebilir. Ancak daha düzenli ve kontrollü bir çalışma için, bu konuda geliştirilmiş belirli standartlar ve rehberler de kullanılabilir.

Yaygın olarak kullanılan iki tane standart bulunmaktadır. Birincisi ISO ve IEC'nin ortaya koyduğu ISO/IEC bilgi teknolojileri güvenlik yönetimi için risk analizi yöntemleri bilgilerinin belirlediği standarttır. Diğeri ise American NIST tarafından düzenlenen NIST bilgi teknolojileri sistemleri için standarttır. Her iki standartta öngörülen yaklaşımlar oldukça yakındır ve genel risk analizi ve yönetimi yapısını destekler.

ISO/IEC standartı, uygulamalı bilgi güvenlik yönetimindeki temel noktaları tanımlamak için geliştirilmiştir. Standartta güvenlik risk analizleri işlemleri, farklı yaklaşımlar gözönüne alınarak yorumlamalı olarak tanımlanmıştır. Bu yaklaşımlar ve önerildikleri sistemler şunlardır:

Temel yaklaşım: Sistemin tümüne uygulanan koruyucuları baz alır. Yaygın tehditler için uygun koruyucular öneren listeleri kullanır. Küçük ölçekli ve düşük seviyede güvenliğe ihtiyaç duyan organizasyonlar için maliyet avantajlı bir yaklaşımdır.

Gündelik yaklaşım: Yapısal yöntemlere dayanmak yerine, bilgi öncelikli yaklaşım şeklindedir. Bu şekilde harcanan emeği azaltır ama böylelikle uygulayıcıların eski bilgileri direkt olarak sonucu etkileyeceğinden dezavantajlı

olabilir. Sözelimi, bazı varlıklar veya detaylar kolaylıkla unutulurak gözden kaçırılabilir.

Detaylı risk analizi yaklaşımı: Sistemin varlıklarını, tehditlerini, zayıflıklarını, bunlara karşı koruyucuları detaylı şekilde analiz etmeye dayanır. Fazla zaman alan ve emek harcanan bir yaklaşım olduğundan, sadece karmaşık sistemlere ve işlemlerin tümü yerine sadece daha hayati olanlarına uygulanmak üzere önerilir.

Birleşik yaklaşım: Temel yaklaşım ve detaylı risk analizi yaklaşımının birleştirilmesi şeklindedir. Önce kabaca bilgi sistemine temel yaklaşım uygulanır, elde edilen bulgularla daha önemli kısımlara detaylı risk analizi uygulanır.

Bu yaklaşımlar risk analizi sırasında uygulanacak işlemlerin nicel ya da nitel olmaları bilgisine sahip değildir. Tercih analizcilere bırakılmıştır. Uygun yaklaşımla risk analizi tamamlandıktan sonra koruyucular seçilebilir. Standart, gereken koruyucuların neden seçildiklerini ve nasıl çalıştıklarını açıklayan bilgi güvenliği politikası ve güvenlik seviyesinin nasıl korunacağını, koruyucuların nasıl kontrol edileceğini açıklayan ve maliyetlendiren bilgi güvenlik planı dokümanlarının yazılmasını önerir [ISO/IEC 13335-3, 1998].

NIST'in standartı ise, risk yönetimini, dokuz aşamalı olarak yapar ve Bölüm 2'de açıklanan klasik yapıya paralel bir sistemi vardır. Analizde kullanılacak yöntemin nicel ya da nitel olmasını kısıtlamaz.

ISO/IEC'nin ve NIST'in bilgi güvenliğinde risk yönetimine bakış açıları, kullandıkları terminolojiler farklı olsa da, genel çerçevede benzer nitelikler taşımaktadırlar. Temel olarak söylenebilecek farklılık, ISO/IEC detaylı risk analizi gerektirmeyen sistemler için başlangıçta farklı bir yön önererek işlemleri baştan kısaltırken, NIST analiz sırasında eleme yapmayı önermektedir. Ayrıca NIST'ten farklı olarak ISO/IEC birleşik yaklaşımla daha esnek bir yapı sağlamaktadır.

Standartlar, özellikle risk analiziyle ilgili adımlarda, ölçümlerle ilgili bir kısıtlama yapılmadan daha güvenli risk hesabı için düzenli bir şablon sunarlar.

3. RİSK ANALİZİ VE YÖNETİMİ İÇİN YÖNTEM SEÇİMİ

İlk kısımlarda da bahsedildiği gibi, günümüzde risk analizi ve yönetimi için birçok araç bulunmaktadır. Gelecekte de akademik veya ticari, risk analizi ve yönetimi için yeni yöntemler ortaya koyan farklı çalışmalar yapılması mümkündür. Risk konusunda temel kavramlar korunmakla beraber; konuya yaklaşım, süreç sıralaması, hazırlık çalışmaları, analiz ekibinin organizasyon yapısının farklı düşünülmesi, risk hesabında belirsizliğin etkisini göz önüne almak için farklı istatistiki ve matematiksel yöntemler uygulanması, ihtiyaçların değişmesi, sadece belirli konulara odaklanılması ve benzeri nedenler dolayısıyla yeni yöntemlerin ortaya konması ve yöntem sayısının artması olağandır.

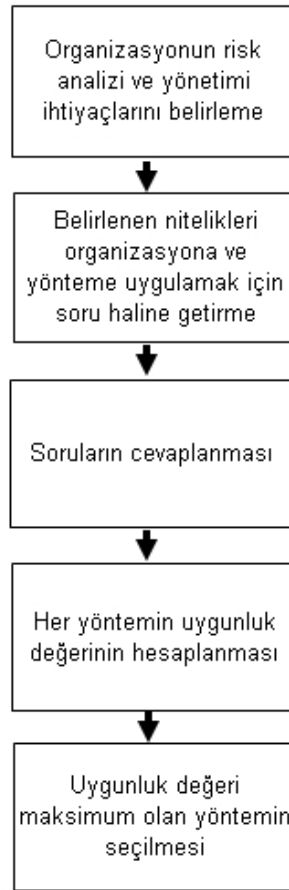
Bir organizasyon, kendi bilgi sistemlerine karşı mevcut tehditlerin riskini düşürebilmek için, birincil öncelikli olarak iyi bir risk yönetim programına ihtiyaç duyar [Myerson, 1999]. Organizasyon, kendi ihtiyaçlarını temel alarak, mevcut bulunan yöntemlerden kendisine en uygun olan yöntemi seçmelidir. Ancak, karşısında seçebileceği birçok alternatif vardır. Üstelik organizasyon, risk analizi ve yönetimi işlemleriyle zaman ve para harcayacağı için, doğru yöntemi seçmesi, oldukça kritiktir. Bu nedenle, alternatiflerini karşılaştırıp değerlendirerek, kendi ihtiyaçlarıyla örtüşen bir yöntem seçmelidir. Hangi yöntemin seçilip kullanılacağı, bilgi güvenliği yöneticilerinin önemli bir problemidir. Seçim için yapılacak en iyi şey, yöntemlerin tarafsız ve nicel olarak karşılaştırılmasıdır ve organizasyonlar bu yöntemlerden hangisini seçmeleri konusunda, objektif araçlara ihtiyaç duymaktadırlar. Bu bölümde en uygun risk analizi yöntemi seçiminde önerilen modelin kuramsal temelleri açıklanmıştır.

3.1. Seçim İçin Önerilen Yöntem

Önerilen yöntemin temelinde yatan ilke, risk analizi ve yönetimi için pek çok yöntem olmasına karşın bunların genel anlamda birbirlerine üstünlüklerinin

olmadığı, ancak uygulayan organizasyonun ihtiyaçları çerçevesinde bir organizasyon için en iyi olan yöntemin bulunması gerekliliği sonucudur. Bu bakış açısıyla ortaya konan yaklaşımda, bir yöntemi diğerlerinden üstün kılacak nitelikleri belirlemek yerine, öncelikle uygulanacak ortamın risk analizi ve yönetimi için beklentilerini ve gereksinimlerini tespit etmek gerekir. Yaklaşım daha sonra, bu niteliklere en çok cevap verebilen seçeneği tespit etmek için işleyecektir.

Yöntemin işleyiş şeması Şekil 3.1’de verilmiştir.



Şekil 3.1 Yöntemin adımları

Herhangi bir organizasyon için ihtiyaç olan yöntemin belirlenmesi amacıyla, genel olarak risk analizi ve yönetimi niteliklerini düşünmek gerekmektedir. Her organizasyon, kendi gereksinimleri çerçevesinde bu nitelikleri serbest olarak tespit

edebilir. Organizasyonun ihtiyaçları doğrultusunda belirlenip şekillenecek olan bu nitelikler, gerek organizasyon için lüzumu belirleyecek şekilde ve gerekse yöntem için niteliğin bulunup bulunmadığını tespit edecek şekilde evet/hayır cevaplı soru formuna dönüştürülebilirler. Organizasyon için hazırlanan sorulara S kodu, yöntem için hazırlanan sorulara M kodu verilirse, i. nitelik için,

S.i: Organizasyon için i. soruyu

M.i: Yöntem için i. soruyu

gösterir. Uygulayıcılara göre kritik olan sistemlerde bu nitelikler, yöntemin hassasiyeti (çok hassas ve nicel sonuç ihtiyacı vardır), sonuçların karşılaştırılabilirliği (analiz sonularının karşılaştırılabilir olma ihtiyacı vardır), koruyucu kontrolleri önerme (yöntemin koruyucu önermesi gereklidir), vb. olabilecekken; daha az kritik sistemlerde genel risk durumu (varlıkları grup olarak değerlendirmek ihtiyaç olacaktır), düşük maliyet (kısa zaman ve düşük bütçe gereklidir), uzman desteği gerektirmeme (harici uzman gerekmemelidir), vb. şekilde olabilir.

Aşağıda örnek olarak bazı nitelikler ve bunlara göre tasarlanmış sorular, bu yapıyla kodlandırılarak listelenmiştir. Belirlenen nitelikler, bir organizasyonun risk analizi ve yönteminin bekleyebileceği genel kapsamlı örnek niteliklerdir, uygulanan organizasyonlar için farklılaştırılabilirler. Soru formları ise bu nitelikleri var/yok şeklinde belirleyici ölçümü sağlamak üzere şekillendirilmiştir:

Nitelik 1: *Analiz edilen varlıkların önem dereceleri*

Organizasyon için:

Soru S.1: Sistemin herhangi bir parçasındaki bir aksaklık, diğer parçaları da etkileyebilir mi?

Yöntem için:

Soru M.1: Varlıklar grup olarak mı değerlendiriliyor (tek tek değil)?

Nitelik 2: *Maliyet*

Organizasyon için:

Soru S.2: Parasal maliyetin düşük olması önemli mi?

Yöntem için:

Soru M.2: Yöntemin parasal maliyeti düşük mü?

Nitelik 3: *Sonuçların kesinliği*

Organizasyon için:

Soru S.3: Genel durum analizindense, net sonuçlara mı ihtiyaç var?

Yöntem için:

Soru M.3: Riskler hakkında genel bir çalışma niteliğinden çok, net sonuçlar ortaya koyabiliyor mu?

Nitelik 4: *Uygulanacak yöntemde kullanılan malzeme*

Organizasyon için:

Soru S.4: Hazır sorular, testler şeklinde bir yapıya mı ihtiyaç duyuluyor?

Yöntem için:

Soru M.4: Yöntemde kullanıma hazır testler ve şablonlar mevcut mu?

Nitelik 5: *Yöntemin güncellenebilir olması*

Organizasyon için:

Soru S.5: Güncellenebilir bir yöntem mi tercih ediliyor?

Yöntem için:

Soru M.5: Yöntem güncellenebilir mi?

Nitelik 6: *Uygulayıcılar*

Organizasyon için:

Soru S.6: Analizler için organizasyon dışından uzman takviyesi tercih edilir mi?

Yöntem için:

Soru M.6: Organizasyon dışından teknik uzman uygulayıcılara ihtiyaç var mı?

Nitelik 7: *Yöntemin sonucunun nitel veya nicel olması*

Organizasyon için:

Soru S.7: Risk için tercih edilen metrik nicel midir?

Yöntem için:

Soru M.7: Risk metriği nicel midir?

Nitelik 8: *Yöntemin sektör için kullanılabilirliği veya adapte edilebilirliği*

Organizasyon için:

Soru S.8: - (Cevap: Evet olmalı)

Yöntem için:

Soru M.8: Yöntem, ilgili sektörde (organizasyonun sektörü) uygulanabilir mi?

Nitelik 9: *Yöntemin standart dışı durumlara uygulanabilirliği*

Organizasyon için:

Soru S.9: Organizasyonda analiz edilmesi gereken standart dışı durumlar var mı?

Yöntem için:

Soru M.9: Yöntem standart dışı durumları analiz edebilecek yapıda mıdır?

Nitelik 10: *Yöntemin koruyucu seçimindeki durumu*

Organizasyon için:

Soru S.10: Koruyucu seçimi için önerilere ihtiyaç duyuluyor mu?

Yöntem için:

Soru M.10: Koruyucu öneri modülü mevcut mu?

Nitelik 11: *Yöntemin raporlama durumu*

Organizasyon için:

Soru S.11: Detaylı raporlara ihtiyaç var mı (Sadece riski bilmek yerine zayıflık ve tehditlerle ilgili raporlar, vs. isteniyor mu?) ?

Yöntem için:

Soru M.11: Detaylı raporlama modülü mevcut mu?

Nitelik 12: *Yöntemin uygulanma zamanı*

Organizasyon için:

Soru S.12: Risk analizi ve yönetimi çalışma süresinin kısa olması önemli mi?

Yöntem için:

Soru M.12: Yöntemin uygulanma süresi kısa mı?

Nitelik 13: *Yöntemin bakımı (satın alınma sonrası destek gerekliliği)*

Organizasyon için:

Soru S.13: Organizasyon zaman içerisinde bakım gerektiren bir yöntemi kullanabilir mi?

Yöntem için:

Soru M.13: Yöntemin zaman içerisinde bakıma ihtiyacı var mı?

Nitelik 14: *Analiz sonuçlarının karşılaştırılabilir olması*

Organizasyon için:

Soru S.14: Organizasyon yöntem sonuçlarının aynı birimden, dolayısıyla karşılaştırılabilir olmasını mı istiyor?

Yöntem için:

Soru M.14: Yöntemin sonuçları aynı birimden ve karşılaştırılabilir mi?

Belirlenen nitelikler ve bunlardan yola çıkarak hazırlanan sorular, ihtiyaca göre örnek olarak verilenden daha az ya da daha fazla sayıda olacak şekilde düzenlenebilirler. Burada listelenen sorulardan istenilenler değerlendirme dışı bırakılabilir. Yukarıda verilen örnek nitelik ve sorular, genel açıdan ihtiyaç duyulabilecek niteliklerdir, ancak her organizasyonun özgörevi ve beklentileri farklı olacağından, önerilen yaklaşımda nitelikler ve sayıları esnek bırakılmıştır, organizasyon bazında düşünülerek belirlenmelidir. Sayının artması, ihtiyacın geniş kapsamlı analiz edildiğini ve daha fazla detay içerdiğinden seçim sonucunun da daha isabetli olacağını gösterir. Tüm nitelikler, yukarıda örnek verilenlerle benzer şekilde evet/hayır cevaplı sorulara dönüştürülebilir.

Hazırlanan S kodlu sorular, organizasyon tarafından ihtiyaçlar doğrultusunda sırayla evet veya hayır değerleri ile değerlendirilir. Evet cevapları 1 ile, hayır cevapları 0 ile temsil edilirler. Dolayısıyla, toplam soru sayısı n ve

$i = 1, \dots, n$ için,

S_i : Her bir niteliği karakterize eden organizasyon tarafındaki S.i sorusunun cevabı

olmak üzere, S_i 'ler 1 veya 0 şeklinde değerler alabilirler.

Diğer taraftan da, organizasyon için değerlendirilen tüm niteliklerle aynı sırada olmak üzere, incelenmek istenilen k nolu yöntem, hazırlanan evet/hayır cevaplı sorularla değerlendirilir. Benzer şekilde evet cevapları 1 ile, hayır cevapları 0 ile belirlenir. Dolayısıyla, değerlendirilen soruların toplam sayısı yine n olacağından,

$i = 1, \dots, n$ için,

M_{ki} : k nolu yöntem için, her bir niteliği karakterize eden yöntem tarafındaki

M_i sorusunun cevabı

olmak üzere, M_{ki} 'ler 1 veya 0 şeklinde değerler alabilirler.

Organizasyon için en uygun yöntemi belirlemek amacıyla, incelenen m adet yöntemin her biri için,

$k = 1, \dots, m$ olmak üzere, k yönteminin uygunluğu:

$$TM_k = \sum_i^n (S_i \Leftrightarrow M_{ki}) \quad (3.1.)$$

formülüyle hesaplanır. En büyük TM_k değerini veren yöntem, organizasyona en uygun ve önerilen yöntemdir.

Sonuçları daha iyi analiz edebilmek için, organizasyon ve yöntemlerle ilgili sorulara verilen cevaplar ve her yöntem için uygunluk değeri, bir tablo ile gösterilebilir. Tablo 3.1'de bu şekilde düzenlenmiş tablonun yapısı görülmektedir. Tablo $n \times (2m + 2)$ büyüklüğünde bir matris yapısındadır. İlk sütun, soru numaralarını göstermektedir (n adet soru için). İkinci sütunda organizasyon sorularına verilen cevaplar işlenmiştir (S_1 : Birinci soruya verilen cevap, ..., S_i : i . soruya verilen cevap, ..., S_n : n . soruya verilen cevap şeklinde). Üçüncü sütundan başlayarak alternatif m adet yöntem için yöntem sorularının cevapları, tek tek ayrı sütunlarda görülmektedir. Bu sütunların ardından da, her bir yöntem cevap sütununun organizasyon cevabını içeren ikinci sütunla çift gerektirme işlemine tabii olması neticesi sıralanmıştır. Her bir yöntemin uygunluk değeri, tüm sorular için organizasyonun ve yöntemin cevabının çift gerektirme işlemiyle bulunan bu değerlerin toplamı olduğundan, bu değerleri gösteren sütununun toplamı alınarak bulunabilir ve tabloda da ek olarak en alt satırda gösterilmiştir.

Soru	Org	Y ₁		Y _k		Y _m	Y ₁ ⇔ Org.		Y _k ⇔ Org.		Y _m ⇔ Org.
1	S ₁	M ₁₁		M _{k1}		M _{m1}	S ₁ ⇔ M ₁₁		S ₁ ⇔ M _{k1}		S ₁ ⇔ M _{m1}
2	S ₂	M ₁₂		M _{k2}		M _{m2}	S ₂ ⇔ M ₁₂		S ₂ ⇔ M _{k2}		S ₂ ⇔ M _{m2}
3	S ₃	M ₁₃		M _{k3}		M _{m3}	S ₃ ⇔ M ₁₃		S ₃ ⇔ M _{k3}		S ₃ ⇔ M _{m3}
.											
.											
i	S _i	M _{1i}		M _{ki}		M _{mi}	S _i ⇔ M _{1i}		S _i ⇔ M _{ki}		S _i ⇔ M _{mi}
.											
.											
n	S _n	M _{1n}		M _{kn}		M _{mn}	S _n ⇔ M _{1n}		S _n ⇔ M _{kn}		S _n ⇔ M _{mn}
TM							TM ₁		TM _k		TM _m

Tablo 3.1 Organizasyon ve yöntemler için soruların cevaplarının tablo yapısıyla gösterimi

4. ÖRNEK ÇALIŞMA VE SONUÇLARININ YORUMLANMASI

Bölüm 3’de açıklanan yöntem, bu bölümde örnek bir organizasyona uygulanmıştır. Örnek organizasyon, sanal bir organizasyondur ve sadece yöntemin çalışmasını daha iyi anlaşılır hale getirmek için kullanılmaktadır. Bu organizasyon, bilgi güvenliği için dört alternatif risk analiz ve yönetim yönteminden kendi ihtiyaçlarına en iyi cevap verebilecek olanını seçmek istiyor. Alternatif yöntemler; CRAMM, CORAS, ISRAM ve OCTAVE’ dır.

Organizasyon, yöntemleri şu şekilde sıralamıştır:

Yöntem 1: CRAMM

Yöntem 2: CORAS

Yöntem 3: ISRAM

Yöntem 4: OCTAVE

Organizasyonun ihtiyaçları doğrultusunda sıraladığı ve üçüncü bölümde açıklanan yaklaşıma uygun olarak soru formuna getirdiği nitelikler, Bölüm 3.1’deki belirtilmiş on dört niteliktir. Yine soru formları da, aynı bölümde hazırlanan sorulardır. Bu soruları sırasıyla organizasyon ve alternatif yöntemlerin cevaplamasıyla elde edilen sonuçlar, Tablo 4.1’de verilmiştir. Tablo, genel yapısı Tablo 3.1’in açıklanması sırasında anlatıldığı gibi düzenlenmiştir ve 14 x 10 büyüklüğünde bir matris yapısındadır.

Tablonun ilk sütunu, soru numaralarını göstermektedir (14 adet soru bulunmaktadır). İkinci sütunda, organizasyonun kendi için düzenlediği sorulara verdiği cevaplar gösterilmektedir. Üçüncü, dördüncü, beşinci ve altıncı sütunlarda alternatif dört yöntemin, yöntem için düzenlenmiş sorulara cevapları sırayla

görülmektedir. Bu sütunların ardından gelen sütunlarda da, her bir yöntem cevap sütununun, ikinci sütunla (organizasyonun cevapları) çift gerektirme işlemi neticesi verilmiştir. Her bir yöntemin uygunluk değeri, TM, kendine ait olan bu işlem sütununun değerleri toplamı olduğundan, bu değer tablonun sonunda gösterilmiştir.

Soru No	Org	CRAMM	CORAS	ISRAM	OCTAVE	CRAMM ⇔ Org	CORAS ⇔ Org	ISRAM ⇔ Org	OCTAVE ⇔ Org
S.1	0	0	0	1	0	1	1	0	1
S.2	1	0	1	1	1	0	1	1	1
S.3	0	1	0	1	0	0	1	0	1
S.4	1	1	0	0	0	1	0	0	0
S.5	1	1	0	0	0	1	0	0	0
S.6	0	0	0	0	0	1	1	1	1
S.7	0	1	0	1	0	0	1	0	1
S.8	1	1	1	1	1	1	1	1	1
S.9	0	1	1	1	1	0	0	0	0
S.10	1	1	0	0	0	1	0	0	0
S.11	0	1	0	0	0	0	1	1	1
S.12	1	1	0	0	0	1	0	0	0
S.13	1	1	0	0	0	1	0	0	0
S.14	1	1	0	0	0	1	0	0	0
TM						9	7	4	7

Tablo 4.1 Örnek uygulama sonuçları tablosu

Daha açıklayıcı olması için; örnek incelendiğinde, cevaplanan dördüncü soru, uygulanacak yöntemin kullandığı malzemeye ilgilidir:

Organizasyon için:

Soru S.4: Hazır sorular, testler şeklinde bir yapıya mı ihtiyaç duyuluyor?

Yöntem için:

Soru M.4: Yöntemde kullanıma hazır testler ve şablonlar mevcut mu?

Organizasyon kendi sorusuna “Evet” diye cevap vermiştir ve bu cevap tabloda organizasyonun cevapları bölümünde (dördüncü satır, ikinci sütun) “1” ile görülmektedir. Her bir yöntem, yöntem sorusu için kendi içerisinde değerlendirildiğinde, sadece CRAMM’de uygulama sırasında hazır bir şablon yapı mevcut olduğundan, yöntemler için sadece CRAMM’in dördüncü cevabı “1” ile gösterilmiş (dördüncü satır, CRAMM sütunu), diğer yöntemler için “0” değeri verilmiştir.

Başka bir soru ise, on ikinci nitelik olan yöntemin uygulanma süresiyle ilgili sorudur:

Organizasyon için:

Soru S.12: Risk analizi ve yönetimi çalışma süresinin kısa olması önemli mi?

Yöntem için:

Soru M.12: Yöntemin uygulanma süresi kısa mı?

Organizasyonun ihtiyacı, zaman yönünden ekonomiklidir. Dolayısıyla bu soruya “Evet” cevabını verdiğinden tabloda organizasyon için cevaplar sütununda “1” ile gösterilmiştir (on ikinci satır, ikinci sütun). Tüm yöntemlere bu niteliğe ilişkin olan yöntem sorusu uygulanırsa, yine sadece CRAMM’de uygulama süresi kısa olduğu için CRAMM’in on ikinci cevabı “1” ile gösterilmiş (on ikinci satır, üçüncü sütun), diğer yöntemlerde ise yoğun ön çalışma yapılması gerekliliği ve uygulanma sürelerinin uzun olması dolayısıyla “Hayır” cevabına karşılık “0” değeri verilmiştir.

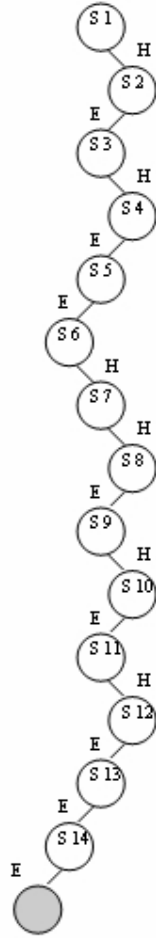
Tablonun en altındaki ek satırda da görüldüğü gibi, yöntemlerin uygunlukları, Eşitlik 3.1.'deki formül dolayısıyla $TM_1 = 9$, $TM_2 = 7$, $TM_3 = 4$ ve $TM_4 = 7$ şeklinde olacaktır. Dolayısıyla, örnek organizasyonun risk yönetiminde kullanması için, ihtiyaçlarına daha çok cevap veren birinci alternatif olan CRAMM yöntemi, daha uygundur.

4.1. Örnek Çalışmanın Karar Ağacı Yöntemiyle Analizi

Uygulanan yöntemi başka bir açıdan değerlendirmek için, anket sorularına verilen cevaplar, bir sınıflandırma tekniği olan Karar Ağacı yöntemiyle analiz edilsin. Karar Ağacı Sınıflandırma tekniğiyle hiyerarşik bir yapıda geliştirilen ağaçta, kök düğüm, kök düğümüne bağlı yaprak veya alt düğümler bulunabilirler. Düğümlere hazırlanan sorular yerleştirilsin ve verilen cevaplar da ağacın dallarını oluşturmada kullanılsın. Önerilen yöntem dahilinde düzenlenen sorular, evet/hayır şeklinde iki cevap değeri alabileceğinden, bir kök veya düğümden sadece iki dal ya da son soru için iki yaprak oluşturulabilir. Böylece oluşturulacak ağaç, soru sayısı kadar derinliğe (ya da yüksekliğe) sahip olacaktır. Ağaç daha anlaşılır ve sade hale getirilmek için, olası tüm cevapları değil de, sadece organizasyonun verdiği cevapları gösteren yapıda geliştirilirse, Şekil 4.1'deki gibi bir ağaç elde edilir.

Ağaç üzerinden düğümleri takip ederek de, alternatif yöntemlerin her biri için aynı cevapları içeren düğümlerin sayısı, yine o yöntem için uygunluk değerini verecektir. Bu yaklaşımla da CRAMM en yüksek olan 9 uygunluk değeriyle organizasyonun ihtiyaçlarına en fazla cevap veren yöntem olarak bulunacaktır.

Önerilen yöntem için iki modelin karşılaştırılması Tablo 4.2'de görülmektedir. Tablodan da anlaşılacağı gibi, karar ağacı yapısı, sorulara verilen cevapları görsel olarak daha bütünsel yansıtmakla beraber, uygulanan model için tablo yapısı daha anlaşılır ve genel analiz yapabilmek için daha uygundur. Uygulamalarda geniş ölçüde kullanıma sahip olan Karar Ağacı Sınıflandırma tekniği, özellikle organizasyonun ihtiyacını modelleyecek risk analizi ve yönetimi niteliklerinin fazlalığı durumunda karmaşıklığın da artacak olması nedeniyle uygun değildir.



Şekil 4.1 Organizasyonun ihtiyacının karar ağacı yapısında gösterimi

Özellikler	Tablo Modeli	Karar Ağacı Modeli
Yönteme uygunluğu	***	*
Uygulama kolaylığı	***	**
Görüntüsel anlaşılabilirlik	**	***
Hatalara eğilimsizlik	**	**
Sonuçları yansıtma	***	***
Güncelleme kolaylığı	**	**

(Ölçek: ***: Çok iyi; **: Orta; *: Zayıf)

Tablo 4.2 Önerilen yöntem için Karar Ağacı ve Tablo yapısının karşılaştırılması

5. SONUÇ VE ÖNERİLER

Günümüzde organizasyonlar, bilgi güvenliğini sağlamak için risk yönetiminin önemini ve uzman bir yöntem kullanımının gerekliliğinin farkındalar. Ancak risk analizi ve yönetimi için seçebilecekleri pek çok yöntem bulunduğundan, bu alternatiflerden hangisinin kendileri için en uygun olduğu konusunda karar vermek zordur. Bu çalışmada, söz konusu problem için bir model ortaya konularak örnek bir sanal organizasyona uygulanmıştır.

Riskin doğasında olan belirsizliğin nedenlerinden birisi, risk elemanlarının (tehdit frekansı, koruyucu etkinliği ve sonuç gibi) tam değerlerini belirlemek için yeterli verinin olmaması iken, diğer bir neden de risk yönetim modeli veya yöntemine olan güven eksikliği veya yöntemin sonuçlarının doğruluğunun şüphesidir. Risk elemanlarının belirsizliğini kaldırmak, risk analizi ve yönetimi araçlarının işidir. Bu işi de, uyguladıkları yöntemlerde istatistiki ve matematiksel yapıları kullanarak yapmaya çalışırlar. Belirsizliğin diğer nedeni olan risk yönetimine olan güveni sağlamak ise, ancak gerçekten organizasyona en uygun yöntemi bulmakla mümkündür. Bir organizasyona en uygun risk yönetim yöntemini seçmek için, organizasyona güven veren bir yaklaşım bulunmalıdır. Literatürdeki daha önceki çalışmalarda ortaya konan yaklaşım, belirli özellikleri sağlayan en iyi yöntemi bulma ya da sadece belirli yönlerden organizasyona en uygun yöntemi bulma şeklinde iken, bu çalışmada organizasyonun ihtiyaçları yine organizasyon tarafından belirlenerek, ihtiyaçları karşılayan en iyi yönteme esnek bir şekilde ulaşma yaklaşımı açıklanmıştır.

Önerilen modele göre öncelikle, organizasyonun yapısını ve uygulayacağı yöntemden beklentilerini ortaya koymak için, gerekli olan anahtar nitelikler belirlenmektedir. Daha sonra bu niteliklerden yola çıkılarak, her bir nitelik için bir soru formu oluşturulmalıdır. Hazırlanan sorular, organizasyonun ihtiyaçları ve önceliklerini yansıttığından, sonuçta belirlenen yöntem, risk analizine olan güvenin de güçlenmesine de yardımcı olacaktır.

Sorular; yöntemleri analiz edecek şekilde yeniden düzenlenerek bu yeni sorularla da, istenilen sayıda alternatif yöntem tarafsız olarak değerlendirilebilir. Tüm alternatifler için sorular cevaplandıktan sonra, organizasyonun ihtiyaçlarına en uygun risk analizi yöntemi, modelde tanımlanan ve uygulanması pratik olan uygunluk formülü yardımıyla tespit edilebilir.

Organizasyon için yeni bir risk analiz yöntemi değerlendirilmek istendiğinde, eğer ihtiyaçlar değişmemişse, sadece yeni yöntem için aynı sorular kullanılarak, yöntemin uygunluğu hesaplanır ve yöntemin değerlendirilmesi yapılır. Elde edilen sonuç, daha önceki yöntemlerin uygunluk değerleri ile karşılaştırılarak yeni yöntemin organizasyon için daha iyi olup olmadığına karar verilir.

Organizasyonun tercihleri değiştiği takdirde, sadece organizasyon için aynı değerlendirme soruları tekrar uygulanarak, tüm yöntemlerin tekrar analiz edilmesine gerek kalmadan, sadece yöntemlerin uygunluk değerleri güncellenir ve karşılaştırma yapılabilir.

Modelin belirsizlik durumu, bir veya daha fazla alternatif yöntemin eşit ve en büyük uygunluk değeri vermesiyle olabilir. Bu durumda organizasyon yöntemlerden birini seçmek için, yeni kriter nitelikleri belirleyip, bunları ilave soru olarak formuna ekleyebilir. Başka bir yol da, cevap tablosunu incelemek olabilir. Tablodaki sonuçlar yardımıyla organizasyon, dikkate alınan kriterlerden daha öncelikli olanlarını göz önüne alarak, yöntemlerden birini seçebilir. Organizasyon için kesinlikle gerekli olan bir kritere uymayan alternatif yöntemler, bu devrede tablodan da yararlanılarak tespit edilir ve elenebilirler.

Modelin geliştirilmesi gereken yanı, organizasyon için risk analizi ve yönetimi yönteminde bir gereksinimi ifade eden her niteliğin, eşit ağırlık derecesine sahip olarak düşünülmesi zayıflıktır. Organizasyon için bazı nitelikler, diğerlerine göre daha kritik olabilirler. Bu farkı dikkate alabilen bir sistemin geliştirilmesi, modeli daha başarılı hale getirebilecektir.

KAYNAKLAR

ISO/IEC 17799, 2000, International Standard, Information technology - Code of practice for information security management, Switzerland

Bob Blakley, Ellen McDermott, Dan Geer, 2001, "Session 5: less is more: Information security is information risk management", Proceedings of the 2001 workshop on New security paradigms NSPW '01

NIST, 1997, An Introduction to Computer Security: The NIST Handbook Special Publication 800-12

Anita Vorster, Les Labuschagne, 2005, "A framework for comparing different information security risk analysis methodologies", Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries SAICSIT '05

Gary Stoneburner, Alice Goguen, Alexis Feringa, 2002, "Risk Management Guide for Information Technology Systems", NIST, Special Publication 800-30

Marianne Swanson, Barbara Guttman, 1996, "Generally Accepted Principles and Practices for Securing Information Technology Systems", NIST, Special Publication 800-14

Zaid Dwaikat, Francesco Parisi-Presicce, 2005, "Risky trust: risk-based analysis of software systems", ACM SIGSOFT Software Engineering Notes, Volume 30 Issue 4

Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, George Rogers, 2007, Recommended Security Controls for Federal Information Systems, NIST SP 800-53 rev. 2

Tung-chien Wang, 1987, "Some problems arising out of the cross-disciplinary nature of information systems security", ACM SIGCPR Computer Personnel, Volume 11 Issue 2

Gurpreet Dhillon, 2007, Principles of Information System Security, Wiley

Pauline Bowen, Joan Hash, Mark Wilson, 2006, Information Security Handbook: A Guide for Managers NIST SP 800-100

Rolf Oppliger, 2007, "Technical opinion: IT security: in search of the Holy Grail", Communications of the ACM, Volume 50 Issue 2

Peggy Fung, Lam-for Kwok, Dennis Longley, 2003, "Electronic information security documentation", ACSW Frontiers '03: Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003 - Volume 21, Volume 21 Publisher: Australian Computer Society, Inc.

Gary Stoneburner, Clark Hayden, and Alexis Feringa, 2004, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A, NIST SP 800-27 rev. A

Mohamed Hamdi, Noureddine Boudriga, 2003, "Algebraic specification of network security risk management", Proceedings of the 2003 ACM workshop on Formal methods in security engineering FMSE '03

Bilge Karabacak, Ibrahim Sogukpinar, 2004, "ISRAM: Information Security Risk Analysis Method", Computers&Security 24(2) 147-159

Harold F.Tipton, Micki Krause, 2000, "Information Security Management HandBook", Auerbach

Mingshu Li, Meng Huang, Fengdi Shu, Juan Li, 2006, "Experience papers: risk analysis: A risk-driven method for eXtreme programming release planning", Proceeding of the 28th international conference on Software engineering ICSE '06

Richard Baskerville, 1993, Information systems security design methods: implications for information systems development, ACM Computing Surveys (CSUR), Volume 25 Issue 4

C&A Security Risk Analysis Group, 2003, <http://www.security-risk-analysis.com/cobproc.htm>

Muninder P. Kailey, Peter Jarrat, 1995, “RAMEX: a prototype expert system for computer security risk analysis and management”, Computers & Security, Volume 14, issue 5, page 449-463

The Zeta Group, 2009, <http://www.zetagroup.ca/zeta-criticalc.html>

EFF, 2009, http://w2.eff.org/Privacy/Newin/New_nist/risktool.txt

CRAMM, 2001, UK Central Computer and Telecommunication Agency (CCTA), Risk Analysis and Management Method, *CRAMM User Guide*, Issue 2.0
<http://www.cramm.com/overview/howitworks.htm>

F. den Braber, I. Hogganvik, M.S. Lund, K. Stolen, F. Vraalsen, 2007, “Model-based security analysis in seven steps - A guided tour to the CORAS method”, BT Technology Journal, v 25, n 1, p 101-117

CERT, 2008, <http://www.cert.org/octave/>

ISO/IEC 13335-3, 1998, Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security

Judith Myerson, 1999, “Risk management”, International Journal of Network Management, Volume 9 Issue 5

ÖZGEÇMİŞ

Fatma Özden AKTAŞ

1973 yılında Niğde’de doğdu. İlk ve orta öğrenimini İstanbul’da tamamladı. 1989 yılında girdiği İstanbul Teknik Üniversitesi Matematik Mühendisliği Bölümünden, 1993 yılında mezun oldu. Çeşitli firmalarda bilgisayar programcı, sistem analisti ve proje sorumlusu olarak çalıştı. Halen Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği anabilim dalında yüksek lisans eğitimine devam etmektedir.

EKLER

EK 1: Tanımlar

Varlık: Organizasyonun özgörevini ya da işini yürütebilmesi amacıyla bulunması şart olduğundan organizasyon için değer ifade eden ve bu nedenle de korunması gereken her şey.

Zayıflık: Tesadüfi veya kasti olarak tetiklenebilme potansiyeli olan yetersizlik, yani riski azaltan ya da etkisiz kılan koruyucunun yokluğu veya yetersiz kalma durumudur [Tipton and Krause, 2000]. Güvenlik politikalarındaki eksiklikler veya güvenlik potikasının hiç olmaması, bir zayıflık örneğidir. Genel olarak oluşabilecek zayıflıklar dört sınıfa ayrılırlar:

1. Davranışsal veya fikirsel zayıflıklar
Zorlamalara karşı gelme veya hayal kırıklıklığına uğrama gibi nedenlerle oluşabilecek, genellikle insandan kaynaklanan zayıflıklardır.
2. Yanlış yorumlama zayıflıkları
Hatalı veya eksik tanımlanmış kurallar nedeniyle olan zayıflıklardır.
3. Yazılım problemleri
Programlama hataları veya kusurları nedeniyle ortaya çıkan zayıflıklardır. Örneğin, Y2K sorununa neden olan zayıflık, yazılımlardan kaynaklanan bir zayıflıktır.
4. Fiziksel zayıflıklar
Denetim yetersizliği, ihmalkar kişiler veya yangın, erozyon gibi doğal felaketler nedeniyle oluşabilecek zayıflıklardır.

Tehdit: Özel bir tehdit kaynağının, istenmeyen etki veya etkiler meydana getirebilecek belirli bir zayıflığı kullanma potansiyelidir. Yani tehditin var olması

için, bir zayıflık ve bu zayıflığı kullanma amacıyla olan bir tehdit kaynağı olmalıdır ve olay gerçekleşirse bu olayın sonucunda zayıflığa sahip olan varlık olumsuz olarak etkilenmelidir. Tehdit kaynakları üç kısma ayrılırlar [Stoneburner et al, 2002]:

1. Doğal tehditler

Sel, deprem, çığ, toprak kayması ve benzeri doğa olayları

2. İnsan tehditleri

İnsan tarafından yapılan veya insanın neden olduğu eylemlerdir. Dikkatsizlik sonucu (hatalı veri girişi, vb.) olabilecekleri gibi kasti olarak da (gizli bilgilere yetkisiz erişim, ağa yapılan saldırılar, kötü niyetli yazılım yüklemek, vb.) yapılabilirler.

3. Çevresel tehditler

Uzun süreli enerji kesintisi, kirlilik, zararlı kimyasal maddeler, vb. örnek olarak verilebilir.

Risk: Belirli bir ortamdaki somut veya soyut bir varlık (veya değeri) olumsuz yönde etkileyecek bir zayıflık ve bu zayıflığı kullanma potansiyelinde olan bir tehdit mevcut olsun. Bu zayıflık ve tehditin, varlığı (veya değeri) olumsuz yönde etkileyecek şekilde birleşme olasılığı, o varlık (veya değer) üzerindeki riski oluşturur. Eğer ortamda bir zayıflık yoksa, bir tehdit kaynağı tek başına riski oluşturmaz.

EK 2: Risk Analizinde Kullanılan Matematiksel ve İstatistikî Modeller

Belirsizlikten kaynaklanan riskin değerini belirlemek zordur. Bu nedenle nicel risk analizi yöntemlerinde risk değerini daha kesin hesaplayabilmek için matematiksel ve istatistikî bazı yöntemlerden faydalanılmaktadır. Bu yöntemler aşağıda listelenmiştir:

1- Risk Tabloları

Risk tabloları, belirlenmiş bir şablon yardımıyla riski formülize etmeye yararlar. Riski belirleyen varlık değeri, tehdit etki şiddeti, tehditin gerçekleşme olasılığı parametreleri ve risk değerinin kendisi, matris yapısı kullanarak tespit edilir. Bu yöntem, tablonun girdi verileri analizi yapanlar tarafından belirlendiğinden ve soyut değerler olduğundan objektiflik açısından zayıf bir yöntem olmasına ve statikliğine karşın, kolaylığı nedeniyle tercih edilebilir. Ancak, riski belirlemede güvenilir sonuçlar vermesi ve ihtiyaçları tam manasıyla karşılaması garantili değildir. Tablo Ek 1.1 (a) ve (b)'de risk ölçek tablosu ve risk seviye matrisi için birer örnek verilmiştir [Dhillon, 2007]. Buradaki verilen ölçeklerin sayısı arttırılabilir. Örneğin tablolara, “Çok Yüksek” ve “Çok Düşük”, “İhmal edilebilir” gibi kriterler de eklenebilir.

Tehdit Olasılığı	Etki Derecesi		
	Düşük (10)	Orta (50)	Yüksek (100)
Yüksek (1.0)	Düşük $10 \times 1.0 = 10$	Orta $50 \times 1.0 = 50$	Yüksek $100 \times 1.0 = 100$
Orta (0.5)	Düşük $10 \times 0.5 = 5$	Orta $50 \times 0.5 = 25$	Orta $100 \times 0.5 = 50$
Düşük (0.1)	Düşük $10 \times 0.1 = 1$	Düşük $50 \times 0.1 = 5$	Düşük $100 \times 0.1 = 10$

Risk Ölçeği: Yüksek (>50-100); Orta (>10-50); Düşük (1-10)

(a)

Risk Seviyesi
Yüksek
Orta
Düşük

(b)

Tablo Ek 2.1 (a) Risk Ölçek Tablosu ve (b) Risk Seviye Matrisi

2- Bulanık Mantık

Risk değerini belirlerken, sadece risk var ya da yok şeklinde bir sonuç çıkarmak uygulamada istenilen bir şey değildir. Risk analizinde amaç, risk değerini daha hassas bir şekilde ortaya koymaktır. Yani riskin seviyesini, ne kadar var veya ne kadar yok olduğunu belirlemek önemli bir ihtiyaçtır. Bu durum, matematikteki bulanık mantık kavramı ile benzerlik teşkil ettiğinden, riski belirlemek için bulanık mantık teorisinden yararlanılabilir. İnanç temelli bir yaklaşım sağlayan bulanık mantık, riski daha esnek ve kolay bir şekilde ifade etmeye yarar.

Belirsiz, zamanla değişen, karmaşık, iyi tanımlanmamış sistemlerin denetimine basit çözümler getirebilen ve basit matematik modellerle tanımlı sistemlerde ekonomik olan bulanık mantıkta, kullanılan kurallar deneyime bağlıdır. Bu nedenle bu yöntem kullanılarak yapılan risk hesabında risk analizi yapan kişilerin sezgi ve inaçları ön plana çıkar. Ancak risk parametrelerinin alabileceği değer arttıkça bulanık sayılarla yapılan işlem sayısı fazlalaşacak, zorlaşacaktır. Böylece risk analiz işlemleri daha karmaşık ve uzun süreli olacaktır.

3- Hata Ağaçları

Risk Yönetimi süreçlerinde daha önce de açıklandığı gibi, normal şartlarda risk analizi; önce varlıkları, daha sonra bunlara yönelik tehditleri ve zayıflıkları tespit ederek, bu zayıflıkların etkilerini ve riskin ne olduğunu belirler, bunlara yönelik karşı tedbirler önerir. Ancak hata ağaçları gibi bunun dışında ilerleyen risk analizi yöntemleri de uygulanmaktadır. Bazı hallerde riskten yola çıkılarak bu riski oluşturabilecek faktörler sıralanabilir. Bu şekilde yaklaşım, modelin ağaç yapısı ile benzetilmesini sağlar. Böylelikle, riske yönelik tehditler daha detaylı ve kolay anlaşılır olarak görülür.

4- Eğer Analizi

Eğer analizinde bir değişkenin bağlı olduğu parametrelere belirli değerler verilip bu durumda değişkenin değerindeki değişiklikler analiz edilir. Bu yöntem kullanılarak yapılan risk analizinde, riskin bağlı olduğu parametreler değiştirilerek risk değerindeki değişimler incelenmekte ve buna bağlı olarak riski azaltıcı kontroller önerilebilmektedir. Genellikle en iyi durum, en kötü durum ve orta

durumlar, vb. için varlıkların riski bulunup, bu değerler arasında karşılaştırılmaya gidilir. Ancak, analiz edilen durum sayısı ve varlık sayısı fazlalaştıkça bu yöntemdeki işlem sayısı da artacaktır.

5- Benzetim

Benzetim, gerçek hayattaki bir yapıya benzeyen bir yapı inşa etmek, gerçek hayatı taklit etmektir. İstatistiksel ve matematiksel tekniklerle bir deneyi veya çözülmesi gereken bir fiziksel olayı rastgele oluşturulan sayıları defalarca kullanarak benzeştirip, bir model oluşturarak çözme esasına dayanır. Benzetim yöntemi, eğer yöntemine benzer bir yapıdadır. Bir değişkenin bağlı olduğu parametreleri değiştirerek, değişkenin aldığı değerleri hesaplar. Ancak benzetimde çok sayıda deneme yapılır. Parametrelerin her biri için çok sayıda değer denenir ve bir model kurulur. Risk analizinde de bu yaklaşımla bir risk modeli oluşturulabilir. Böylece gerçeğe benzeyen bir model inşa edilmiş olur. Benzetim yöntemlerinden risk analizinde en çok kullanılan Monte-Carlo benzetimidir. Monte-Carlo yönteminde değişkenin alabileceği çok sayıda değer yanında bu değerlerin olasılıkları da gözönüne alınır.