

### Bülten – 2

#### Bilgi Güvenliđi ve BT Risk Analizi Hakkında Bilmeniz Gereken 10 Şey

##### 1. İş Bağlamı'nın (Etki Deđerinin) Önemi

Tüm kurumsal riskler gibi bilgi güvenliđi ve BT riskleri de iş hedefleri bağlamında bir anlam ifade etmektedir. Riskleri etki deđerleri ile ilişkilendirmediğimizde yaptığımız çalışma bir zafiyet analizi olarak kalacak, dolayısıyla önem derecesinin anlaşılması ve kontrol yatırım kararlarının alınmasına somut bir katkı sağlayamayacaktır. Zafiyetler bir iş hedefine olan olumsuz etkileri nispetinde önem kazanmaktadır. Risk bilgisinin karar verme noktasında olan kişilerin işini kolaylaştırmak için her zafiyetin doğuracağı etki bilgisi ile birlikte sunulması gereklidir. Aksi takdirde (özellikle önerilen kontroller mali yatırım gerektiriyor ve hayatı zorlaştırıyor ise) “yapmasak ne olur ki” sorusu kaçınılmazdır.

##### 2. Analiz Metodu

Risk analizinin farklı zamanlar ve kurumun farklı birimleri arasında karşılaştırılabilir sonuçlar üretebilmesi, belli bir kalitede gerçekleştirilmesi için kurumun uyguladığı risk analiz metodu, kullandığı etki ve zafiyet kriterleri tanımlanmış olmalıdır. Mümkün olduğunca ölçülebilir kriterleri içeren ve tekrar edilebilir bir metodun tanımlanmamış olması zaten objektif deđerlere ulaşmanın çok zor olduğu risk analiz sonuçlarını daha da sorgulanır hale sokacaktır.

##### 3. Öğrenmeye İmkan Tanımak

Risk analiz metodu tanımlanmalı ve risk analizi mümkün olduğunca sanat niteliğinden sıyrılıp bilim niteliğine kavuşmalıdır. Sadece bir rehber niteliğine sahip bir doküman olmaktan tam teşekkülü bir metod olarak nitelendirilmeyi haketmeye kadar pek çok metod yayınlanmıştır. Ancak tüm kurumlara uyacak kalıba sahip bir metod bulunmamakta, her kurumun kendine has bir metod geliştirme zarureti bulunmaktadır. Bunun sebebi farklı büyüklüklere, farklı nitelikte personele, farklı iş hedefleri ve bilgi kaynaklarına, farklı iş ortaklık yapılarına sahip kurumlar için temel şablonlar üzerinde gerekli deđişiklikler yapılma ihtiyacıdır. Bu nedenle ilk risk analizinde mükemmel bir sonucu veya pürüzsüz bir süreci beklemek hem doğru deđildir, hem de beklenen faydanın elde edilmesini engelleyici bir sebep olabilir. Risk analizinde bu süreci yaşamamanın risk farkındalığını edinmeye katkı sağlayacağına ve bizzat risk analizinin bir eğitim imkanı olduğuna inanılırsa daha gerçekçi ve faydalı bir süreç yaşanacaktır.

##### 4. Olasılık

Etki bilgisi iş bağlamının öneminde de belirtildiđi üzere bir risk analizinin olmazsa olmazıdır. Klasik risk tanımında risk olumsuz bir durumun gerçekleşme olasılığı olarak tanımlanır. Ancak geleneksel risk analiz yaklaşımının bilgi güvenliđi ve bilgi teknolojilerine uyarlanması maalesef pratikte sorunlara yol açmaktadır. Örneğin yabancı bir ülkeden bir öğrencinin internete açık servislerinizi port taramasından geçirip açıklık tespit etmesi ve saldırması olasılıđını bilimsel olarak hesaplamak çok da mümkün deđildir. Bu nedenle bilgi güvenliđi ve BT risk analizlerinde olasılıđın yerini zafiyet düzeyinin aldığını gözlemledik. Bazı durumlarda sadece risk kriterleri kullanılarak kısmen etki bilgisini barındıran ancak olasılık deđerini bulmaktan kaçınan yaklaşımlar

kullanıldığı da gözlenmektedir. OCTAVE ailesi gibi en gelişmiş risk analiz metodları dahi olasılığı etki bilgisine nazaran ikincil olarak değerlendirmekte ve bu bilginin analiz edilmemesine imkan tanımaktadır.

## 5. Kabul Edilebilir Risk

Geleneksel risk analiz metodunda kabul edilebilir riskin analiz öncesinde belirlenmesi öngörülür. Ancak bu durum gerçek hayatla çalışmaktadır. Zira bir kişi veya kurumun tüm inisiyatiflerinde belli bir kaybın üstünde riskleri almaması gibi bir durum söz konusu değildir. Her risk ilgili getiri beklentisi ile ilişkilendirilerek risk kabul kararı verilir. Bu nedenle standart bir kayıp seviyesinin üstündeki risklerin kabul edilmeyeceği varsayımı gerçek hayat ile uyumlu değildir. Bu nedenle etki değerlerine göre risklerin sıralanması ve her riski kendi başına ele alma yaklaşımı gerçek hayat gereksinimlerine daha uygundur.

## 6. Nesnellik İhtiyacı

İnsan doğasının belirsizliğe tahammülü malesef yüksek değildir. Bu durum bir birey veya bir kurum açısından en temel problemlerden biridir. Yine insan doğası bir işe girişecekse mükemmel yakın bir sonuç elde etme hedefini taşır. Malesef bu yaklaşım da gerçek hayatta sıkıntılara yol açar. Bu sorundan en muzdarip kişilere yazarlar örnek verilebilir, mükemmel bir roman veya senaryo yazmak istediklerinden bir türlü yazmaya başlayamazlar. Risk analizini yapmanın çok mekanik bir yolu bulunmamakta ve sonuçları çoğu zaman tartışmaya açık durumdadır. Böyle bir süreci işletmek için şu prensibi taşımak gereklidir: "Eğer bir iş yapılmaya değerse kötü yapılmaya da değerdir". O nedenle risk analizi sürecinde mükemmel asla hedeflenmemelidir. Çünkü böyle bir hedefle iyinin de elde edilememe riski yüksektir.

## 7. Katılım

Risk analizi sonuçlarına dayanılarak alınacak önlemler itibarıyla kapsam içinde bulunan herkesin yaşamını etkileyecek sonuçlar doğurabilir. Bu sonuçlar belli riskleri azaltmak için yaşamın zorlaşmasını da içerebilir (tıpkı havaalanında sayısız defa güvenlik taramasından geçmemiz gibi). İnsanlar kendi koşulları üzerinde söz sahibi olmak isterler. Bu nedenle risk analizi gibi bir süreçte süreç, varlık ve kontrol sahiplerinin söz sahibi ve karar mercii olmaları risk analizinin bir araç olarak kullanıldığı risk yönetimi açısından kritik bir başarı faktörü olabilir. Ek olarak bir riskin etkilerini değerlendirmek açısından en doğru kaynağın iş süreci sahipleri olduğunu da not etmek gerekir. Bir diğer taraftan bilgi güvenliği, çevre güvenliği veya başka bir konuda yapılacak risk analiz çalışması tehditler, zafiyetler ve kontroller açısından belli bir uzmanlık gerektirmektedir. Yani risk analizine katılım sağlayacak kişilerin sadece katılmaları yetmez, katıldıkları süreçte etkin olabilmeleri için belli bir bilgi düzeyine de sahip olmaları gerekir. Risk analiz ekibinin kompozisyonu veya sürece kimin hangi düzey ve şekilde dahil edilmesine ilişkin bir başka parametre de kurum büyüklüğü ve coğrafi dağılımıdır. Büyük kurumlarda tüm süreçleri iyi tanıyan tek bir kişiyi veya bu kişilerden oluşan bir ekibi oluşturmak daha zordur. Bu nedenle bazı bilgileri elde etmek için mutlaka belli kişilerden bilgi toplama ihtiyacı vardır. Sadece risk analiz ekibinin kompozisyonu ve analiz sürecinde kimlerle hangi çalıştayların yapılması gerektiğinin tespiti dahi risk analiz yaklaşımı konusunda standart bir metod uygulamanın zorluğunu ortaya koyar. Genel kaide kurum büyüdükçe risk analiz sürecine daha fazla kişiyi dahil etme zorunluluğu olduğudur. Ancak bu kişilerden bilgi alma yöntemi olarak uzman risk analiz ekibi tarafından yönlendirilen çalıştaylar düzenlemek ihtiyacı ortaya çıkmaktadır. Çünkü sadece anket gönderimi ile bilgi toplamak çok çok büyük oranda nfile bir çabadır.

## 8. Risk Analizi'nin Risk Yönetim Sürecindeki Yeri

Çoğu zaman risk analizi ilgiyi o kadar üstüne çeker ki aslında risk yönetimi açısından belki de daha önemli olan yönetim gözden geçirme, artık riskin onaylanması, risk tedavi planının geliştirilmesi, onaylanması, uygulanması ve takibi gibi süreçlere nispeten gerekli düzeyde önem

atanmaz. Dolayısıyla bu adımlar yine nispeten geçiştirilir veya hiç gerçekleştirilmez. Risk analizi risk yönetim süreci için bir araçtır. Eğer amaç haline gelirse sadece entellektüel olarak bize çekici gelen ama harcanan kaynağın değer üretmediği bir çaba olarak kalır. Risk analiz sürecindeki bir diğer tehlike de (özellikle kontrol sahiplerinin yoğun katıldığı bölümlerde) akılların endişe alanı belirlenir belirlenmez risk yanıt stratejilerine kaymasıdır. Bu durumda risk analiz sürecinde zaman kayıpları ve motivasyon kaybı yaşanır. Risk yanıt stratejileri geliştirilmiş olan risk analiz metodu gereği olması gereken sıra ve zamanda belirlenmelidir.

## 9. Üst Çıta

Belli bir büyüklüğün üstündeki kurumlarda gerçekleştirilen risk analizlerinde risk analiz ekibinin de sayıca artması beklenebilir. Farklı kişilerin farklı deneyimlere sahip olmasından dolayı ve çeşitli faktörlerle farklı etki, tehdit ve olasılık algılarına sahip olması olağandır. Bu algıların aynı kişi için bile zaman içinde dalgalanması şaşılacak bir durum değildir. Farklı algıların etkilediği risk analiz sonuçları bir araya geldiğinde aslında yan yana zikredildiğinde aynı risk seviyesinde bulunmaması gereken risklerin benzer seviyelerde bulunduğu görülebilmektedir. Ekibin bu nedenle algılarını değerlendirebilecekleri bir mihenk taşına ihtiyaç bulunmaktadır. Bu taş analizin başında analiz kapsamında gerçekleşebilecek en kötü risk sonucunu veya farklı etki kriterleri açısından oluşabilecek en kötü durumları belirleyerek sağlanabilir. Böylece bir analist ulaştığı risk değerini bu üst çıta ile karşılaştırarak sonucunu daha doğru bir göreceli hizaya yerleştirebilir.

## 10. Teknoloji Riskleri

Risk analizleri veya denetimlerde masa başında "belirlenen" zafiyet tespitleri ile sistem odasında taşınan zafiyetler arasında fark olması beklenmedik bir durum değildir. Bu açıdan eğer risk analiz ekibi teknik zafiyet denetimi gerçekleştirme kabiliyetine sahipse daha doyurucu zafiyet bilgisi edinme amacıyla teknik zafiyet denetimi risk analizinin bir parçası olmalıdır. Ancak bu denetimin sonuçlarının birebir risk analizine yansıtılması ve teknik varlıklar ile sıkı sıkıya ilişkilendirilmesi de denetim çalışmasının en etkin şekilde kullanılmasını engelleyecektir. Öncelikle tüm sonuçların risk analizine birebir yansıtılması birbirini tekrar eden ve sunumu sırasında dinleyicilerin (özellikle üst yönetimin) ilgisinin kaybedilmesine yol açabilir. Bu nedenlerle teknik zafiyet denetim sonuçlarının risk analizinde nicelik olarak değil nitelik olarak değerlendirilmesi, bulunan zafiyetlerin sonuç olmaktan ziyade semptom olarak ele alınması daha faydalı sonuç üretecektir. Bu şekilde kök sebeplere odaklanma ve veri kalabalığı içinde dikkatin dağılmaması sağlanabilir. Zira teknik zafiyet denetiminin de bilinen zafiyetler içinde bir alt kümeyi tespit edeceği unutulmamalıdır.