



Teknoloji Risk Yönetimi
Kıdemli Müdürü

Cem MESÇİ
cmesci@gmail.com

KIRMIZI ÇİZGİLER

Teknoloji, Yatırım ve Risk - 3



Şirketlerin, hedeflerine engel olabilecek tehlikelere karşı önlem alabilmelerinin yolu, teknoloji alanında “Bilgi İşlem Yönetiminden” “Bilgi Yönetimine” geçmekte yatmaktadır. Bu ayki yazımızda, iş yönetim birimleri ile teknoloji yönetiminin birbirlerini duyamamalarından dolayı ortaya çıkabilecek büyük riskleri, yaşanmış olan örnek olaylar ile sizlere aktaracağım. Bedel ödmeden önce “fark etmeye” hazır mısınız?

KIRMIZI ÇİZGİLER

Teknoloji kullanımı şirketlerin hem bünyelerinde hem de pazardaki hedeflerini gerçekleştirmelerinde etken bir araçtır. Buna “güç” demek de mümkündür. Teknoloji kullanımında diğer güç unsurlarında olduğu gibi zayıflıklar ve zafiyetler de vardır. Sonuçta her şey insan üretimi; doğüstü bir şey mevcut değil. Dolayısı ile ilk düşünmemiz gereken, kullandığımız teknoloji unsurlarının (Yazılım, donanım, servis vb) kendisine ait zayıflıklardır. Şirketler hedeflerini gerçekleştirmek için çıktıkları yolda, kullandıkları her teknoloji parçasının bakım ihtiyaçlarını karşılamalı, zafiyetler ve zayıflıklarını bertaraf etmeyi bilmelidirler.

Hata, arıza, zafiyet veya zayıflıklarının olmasına rağmen, iş adamları neden teknolojiyi daha fazla kullanma eğilimindedir? Neden teknolojiye yatırım yaparak para harcarlar. Neden dersiniz? Hemen kendi cevabımı söylemeliyim: Teknoloji insanların iş yerlerindeki potansiyel enerjilerini kinetik enerjiye çevirmeye yarar da ondan. Çalışanların hareketi, bilgi üretir. Bu bilgileri barındıran ve kullanan teknoloji ise bir şirketin ne kadar çevik davranabileceğini, müşterisini ne kadar iyi analiz edebileceğini, servis hatalarını ne kadar kontrol edebileceğini, hatta yılsonunda ne kadar kar yapabileceğini söyleyebilir size. Pazar belirsizliklerinden dolayı strateji savaşı veren CEO’ların, kendi şirketi ve yapabildikleri ile ilgili bulanık bir ortam görmek hoşlarına gitmez diye düşünüyorum.

İşte bu nedenle 90’lı yıllarda IT, şirkette üretilebilecek veya üretilemeyecek raporlara, yapılabilecek analizlerin çeşidine karar veren olmuştur. Hatta öyle bir hal almıştır ki, teknolojiyi yönetenler (teknolojinin ne yapabileceğini daha iyi bildikleri için) şirketin pazarlama politikasını da yönlendirebilmişlerdir. İstenen analiz raporlarının yanında, farklı bakışla oluşturulan raporlar sunmuşlardır. Bu durum günümüzde, diğer ana alan yöneticilerine teknolojinin dışında kalmalarını gerektirdiğini öğretmiştir. Biz bu duruma kısaca “Eski ama güzel günler” diyoruz.

Teknoloji yönetimi tıpkı hoyrat bir kısırağa hakim olmaya benzer. Ne zaman ne yapacağı belli olmaz; kontrol edemediğiniz her an düşüp kemiklerinizi kırabilirsiniz. Bugün teknoloji yöneticileri, binlerce beygir gücünde bir otomobil kullanır durumdadır. Herhangi bir anda “ama” ile başlayan hiçbir cümle işe yaramaz. Halen her sistem konfigürasyonu kendi başına ayrı bir örnektir. Sistemlerin kendi içlerinde tutarlı ve sürekli aynı seviyede hizmet verebilmeleri için, üreticiler hep üretimlerini uzun soluklu testlere tabi tutmak zorundadırlar. Teknoloji yöneticileri, kullanılan tüm teknoloji unsurlarının CEO’nun gösterdiği hedefle aynı yönde olduğunu sürekli kontrol altında tutarlar.

Teknoloji, Yatırım ve Risk üçgeninde CEO’nun karar vermekte ana destek noktası CIO olmaya hızla yaklaşmıştır.

Bu rolleri ile Teknoloji, Yatırım ve Risk üçgeninde CEO’nun karar vermekte ana destek noktası CIO olmaya hızla yaklaşmıştır. Yanlış bir ürün ile yanlış işletilen teknolojinin vereceği zararlar karşılaştırılırsa, teknolojinin verdiği zarar ölümcül boyutlarda olabilir.

Teknoloji yönetimi sadece operasyon, yazılım ve donanımdan sorumlu genel müdür yardımcısı algılamasından çıkmaktadır. Teknolojiyi bilen, ancak şirketin karına odaklanmış, en az diğer yönetim unsurları kadar kartal gözlü olmak zorundadır.

Pekala teknoloji yönetimi ve yatırımlarını CIO desteği ile aldığımız kararlarla başardığımızda konu sonlanıyor mu? Elbette hayır. Bu kısım sadece gelecekte oluşturmaya çalıştığımız karlarımız içindi. Peki ya bugün ya da yakın gelecekte olabilecekler? Bunlara göz atmamız gerekmez mi? Konu şu ki, tüm insanlar içerisinde bence en zekileri çok ileriye görerek kar realizasyonunu engelleyebilecek tehlikeleri ortaya koyanlardır. Ama en akıllıları, sürekli bugünü ve iki adım sonrasını koruyanlar olacaktır.

Geçmişte kalmış ama çok çarpıcı bir örnek ile açıklayım; ABD’nin bölgesel uçuşlar yapan Comair adlı bir havayolları şirketinin, 2004 yılı Noel tatil başlangıcına yakın bir tarihte “uçuş düzenle-

KIRMIZI ÇİZGİLER



lam 3.900 uçuşun ertelenmesi veya iptaline, 200.000 yolcunun yolda kalmasına sebep olmuştur. 27 milyon USD yıllık kar yapan Comair, toplam 20 milyon USD hasar almış, zarar görmüştür. Dahası da var; tüm bu olanlardan dolayı itibar kaybetmiş olması yetmiyormuş gibi Ulaştırma Bakanlığı tarafından da denetlenmiştir.

Olayın olması sonrasında görülen bir gerçek ise; "iş" ve "teknoloji" yönetimlerinin, birbirlerine karşı ne kadar sağır olduklarıdır. Söz konusu yazılım 1986 yılında satın alınmış, 18 yıldır yeni geliştirme ve düzenlemeler ile kullanılmaktaymış.

me" yazılımı bozuluyor. Komik bir tabir ama gerçekten de bozuluyor. Uçuş düzenleme yazılımının ana görevi, pilotların ve hosteslerin devlet tarafından konulan kurallar dahilinde ve belirlenen süre kadar uçuş yapmalarını garanti altına almaktadır. Dolayısıyla kilit uygulamadır. Sonuç üç gün içerisinde bulunuyor; yazılımın ayda 32.000 adet düzenleme yapabilme sınırı aşılmış ve yazılım arıza yapmıştır. IT dünyasındaki herkes buna gülecektir eminim. Kullanılan verinin tipinden dolayı limitler aşılmış. Ancak bu basit hatalı durum uygulama çalışmadığından sistemin tekrar yüklenmesine ve bu arada hatanın gerçek sebebinin bulunması için harcanan iki güne mal olmuştur. Kayıplar teknik dille ifade edilirse durum bundan ibarettir. Bir de diğer tarafın, yani iş kolunun dilini kullanalım; hata, top-

Teknoloji yönetimi değişim talep etmişse de sürekli ertelenmiştir. Bu örnek, bir IT Risk'inin şirketin geleceğine etkisini çok iyi yansıtmaktadır.

Comair'de olaylar bunlarla da bitmemiş; 17 Ocak'ta 20 yıllık emektar Genel Müdür istifa etmiştir. Yine de sanmayın ki Comair çareyi hemen yazılımı değiştirmekte buldu. Mart 2005'ten itibaren Comair aynı yazılımı iki modüle bölerek kullanmaya devam etti. Bunların her biri 32.000 kapasiteli olduğundan sorun ortadan kalkmıştı. Ancak buna rağmen, günlük hacmin kontrolü için alınan raporlarla ve yapılan kontrollerle çok dikkatle kullanılmaya devam etti.

Başka bir örnek ile konunun sadece teknolojinin kendisi veya onun yapımındaki "kasıtsız" ha-

KIRMIZI ÇİZGİLER

tarlar ile sınırlı olmadığını, “kasıtlı” yapılan hareketlerin de teknolojinin riskini oluşturduğunu anlatmak isterim.

Yine ABD’den bir örnek vermek istiyorum. Sürekli örneklemelerin bu ülkeden olmasının sebebi, sadece istatistiki olarak çok sayıda olay gerçekleşmesi ve etki alanının çok geniş olmasıdır.

Mart 2007’de JTX şirketlerinin sistemine sayısı belirlenemeyen ölçüde atak yapılmış ve sistemden toplam 45,6 milyon müşterinin kredi kartı veya nakit kartı numaralarının çalındığını açıklanmıştır. Olay 2005’in ortalarında Card Systems Solution adlı şirketin 40 milyon kaydın çalınmasını gölgede bırakacak kadar büyük olmuştur. Buna ek olarak JTX, 451.000 müşterisinin 2003 yılında şirkete yapılan bağlantı ile müşterilere aktarılan kişisel bilgilerin de çalınmış olduğunu bildirmiştir. Şirket, etkilenen müşterilerini arayarak bilgi vermeye uzunca bir süre devam etmek durumunda kalmıştır. 2007 yılı Ocak ayında şirket yetkilileri tarafından yapılan açıklamada bu olay farkına varılmış, ancak başlangıcının Mayıs 2006’ya dayandığı tahmin edilmekte olduğu bildirilmişti. Bu kısım çok ilginç; şirketin olay için görevlendirdiği uzmanlar, müşteri bilgilerinin çalınmaya başladığı zamanı Temmuz 2005 olarak tahmin etmişlerdir. Yani şirket, ödeme sistemlerine biri veya birilerinin yasa dışı erişimini uzunca bir süre fark edememiştir. Ayrıca 18 Aralık 2006’da durum anlaşıldıktan sonra da hiçbir kaydın çalınmadığı da görülmüştür.

Resmin bütününe baktığınızda, biri veya birileri fark edilmeyecek şekilde sisteme giriyor ve fark edilene kadar 45,6 milyon müşterinin kişisel bilgilerini çalıyor. Anlaşıldığını fark edip anında kesiyor çalmayı. Bütün şüpheler bilginin şirket içerisinden çalındığını söylese de pek bir şey bulunamıyor.

Teknolojiyi hem kendinden hem de onu kullanan çalışanların da “iyi niyetle” kullanmaların-

dan emin olacak seviyede risklerimizi görmemiz gerekiyor. Şirket gitmek istediği yere gidemez, hedefleri yarı yolda kalırsa bundan yine o şirketin çalışanları ve çalışanların hayatları etkilenmektedir. Yani risk sadece maddi olmamakta, toplumsal sonuçlar da içermektedir.

Teknoloji ve iş yönetimlerinin ekip olabilmeleri, iletişimlerinin her iki tarafça doğru ve anlaşılır olabilmesi çok önemlidir. Bugün şirketlerin Pazarlama & Satış fonksiyonları ne kadar hayati ise Teknoloji Yönetimi de o kadar hayati olmuştur. Bu arada belirtmeliyiz ki, teknoloji yönetimi donanım ve yazılım operasyonundan çok daha büyük bir boyutta stratejiyi de içine alacak bir yönetime dönüşmektedir.

Teknoloji yönetimi, donanım ve yazılım operasyonundan çok daha büyük bir boyutta stratejiyi de içine alacak bir yönetime dönüşmektedir.

Şirketlerin, hedeflerine engel olabilecek tehlikelere karşı önlem alabilmelerinin yolu, teknoloji alanında “Bilgi İşlem Yönetiminden” “Bilgi Yönetimine” geçmekte yatmaktadır. CIO risk

yönetimini, kendi yönetim alanının verimli ve etkinliği için ne kadar çok kullanabiliyorsa, CEO o kadar rahat uyur.

Teknoloji boyutundan bakıldığında, uygulama mimarisinde yapılan küçük bir öngörü eksikliği veya tahmin yetersizliği olarak görülebilir. Bu küçük teknik hata, ne zaman ki şirketin diğer fonksiyonlarını da içine çeken, onların da canını yakan bir olay olur, işte o zaman durumun sadece teknik olmadığı anlaşılır.

Bedel ödmeden önce fark etmek hepsinden daha akılcıdır...

