Sosyal Bilimler Dergisi / Journal of Social Sciences 4(1), 2010, 1-16

İŞLETMELERDE BİLGİ TEKNOLOJİLERİNDEKİ GELİŞMELERİN İŞLETME VE YÖNETİM FONKSİYONLARI ÜZERİNE ETKİLERİ

Yrd. Doç. Dr. Atik KULAKLI[*] ve Serpil ASLAN[**]

ÖZET

Günümüzde teknolojinin gelişmesiyle birlikte bir çok kuruluş kendisi için hayati derecede önem taşıyan operasyonlarını bilişim sistemleri yoluyla gerçekleştirmektedir. Teknolojinin hızla gelişmesiyle, iş süreçlerinin karmaşıklaşmasıyla, kuruluşların sistemlerinin ve sahip oldukları önemli verilerin üzerindeki denetim gittikçe zorlaşmaktadır. Bu sebepten dolayı kurum ve kuruluşlar bir "Felaket Kurtarma Planına" sahip olmalıdırlar. Bu çalışmanın amacı; kurumların sahip olduğu bilgi sistemlerinin muhafaza ettiği iş süreçleri ve verilerin korunmasını sağlamak amacıyla geliştirilmiş olan İş Sürekliliği ve Felaket Kurtarma Planlarının tanımlanması, önemi, amacı, uygulanan stratejiler ve kurumlar üzerindeki faydalarını açıklamaktır.

Anahtar Kelimeler*:* İş Sürekliliği Planı, Felaket Kurtarma Planı, Veri Koruma, İş Süreçleri Etkinliği.

ABSTRACT

Nowadays, a lot of institutions have carried through its operations, which are vitally matters, via information systems thanks to today's developed technology. Auditing on important data that they owned, and on the systems of the institutions, have been becoming increasingly difficult by becoming work processes complex, and rapid improvement of the technology. Because of this reason, agencies and institutions should have a plan of disaster recovery. The aim of this study is to define, explain and exemplify the benefits of Disaster Recovery Plans that have been developed for protecting institutional data and business processes which are kept by the institution's information systems, their applied strategies for institutions, and finally their aims and importance for the institutions.

Keywords: Business Continuity, Disaster Recovery Planning, Business Process Efficiency, Data Protection and Recovery.

[*] Yrd. Doç. Dr. Beykent Üniversitesi, İİBF, akulakli@beykent.edu.tr

[**] Beykent Üniversitesi Mezunu, İİBF, serpilaslannn@beykent.edu.tr

1. GİRİŞ

Günümüzde teknolojinin gelişmesiyle ve buna paralel olarak kullanılan verinin gittikçe artmasıyla, bir çok kurum ve kuruluş kendileri için hayati derecede önem taşıyan operasyonların ve sahip oldukları verilerin muhafaza edilmesini bilişim sistemleri yoluyla gerçekleştirmektedir. Bu sistemlere her hangi bir nedenle ulaşılamıyor olması, söz konusu kuruluşun hem finansal açıdan hem de rekabetçi ortamda rakipleri arasındaki pozisyonu açısından ciddi derecede olumsuz sonuçların yaşanmasına yol açabilmektedir.

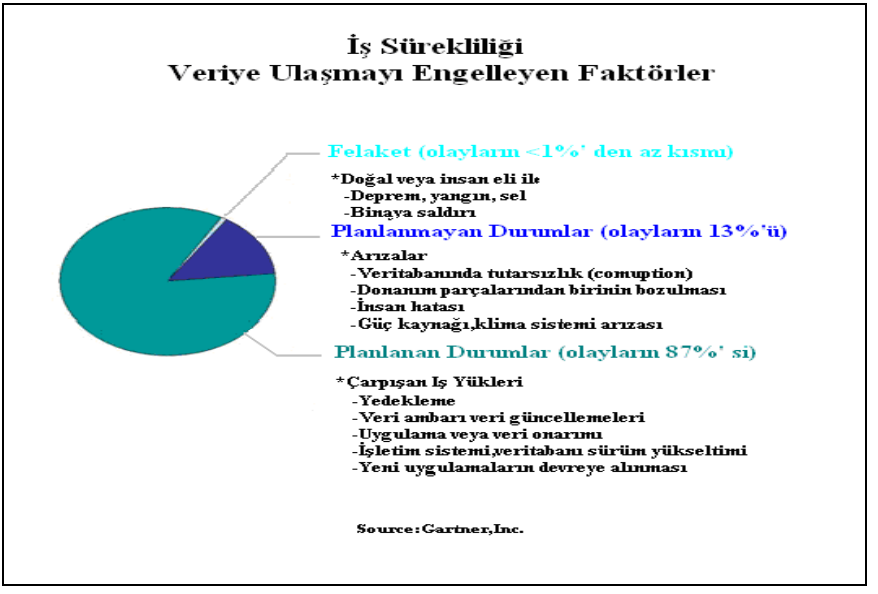
Şüphesiz ki bir çok kuruluş, sahip olduğu süreç ve verilerini koruma konusunda olası bir felaket ile her gün karşı karşıya kalma riskini taşımaktadır. Bunlar,doğal afetler, yerel afetler ve insana bağlı hatalar olabildiği gibi, kurumun gözden kaçırdığı küçük gibi görünen fakat meydana geldiğinde ciddi sonuçlar doğurabilen felaketler de olabilmektedir.

Bu çalışmada kurumların ve kuruluşların sahip oldukları süreçler ve verilerin aslında kendileri için ne kadar önemli olduğu ve olası bir felakete karşı nasıl bir hazırlık planı içinde olmaları gerektiği hem "İş Sürekliliği" hem de "Felaket Kurtarma Planı" açısından ele alınmıştır.

2. İŞ SÜREKLİLİĞİ

İş sürekliliği kavramı ilk kez 2000 Milenyum yılı sırasında yaşanması beklenen bilgisayar tarihlerine ilişkin hata olasılıkları olarak gündeme geldi. O dönemde eski bilgisayarın donanım ve yazılımlarında sıkça kullanılan iki rakamlı yıl bilgisinin (örneğin 1964 yılı için 64) 2000 yılında sıfırlanmasının yaratacağı sorunlar gündemdeydi. Tüm donanım ve yazılımlar elden geçirilerek sorun yaratabilecekler değiştirildi, sınandı. Ancak geriye bir risk kalıyordu. Acaba gözden kaçan başka donanım ve yazılım sorun yaratabilir miydi? İşte bu riski göze almak istemeyen kuruluşlar daha önce pek önem vermedikleri Acil Durum Planları'nı (Contingency Plan) geliştirmeye başladılar (Ergil, 2009). İş

sürekliliği bir kurumun herhangi bir bölümünde veya birden çok bölümünde meydana gelen ve kurumun günlük operasyonlarını gerçekleştirdiği süreçleri kesintiye uğratan sekmelerdir. Böylesi bir durumda kurumun süreçlerini devam ettirmesini sağlamak için önceden hazırlanmış olan plan İş Sürekliliği Planı olarak adlandırılır. İş Sürekliliği konusunda veriye ulaşmayı engelleyen olaylar; felaketler, planlanan durumlar ve planlanmayan durumlar olarak üç kategoride toplanabilir.



Şekil.1. Veriye Ulaşmayı Engelleyen Faktörler (www.datateknik.com /a)

Günümüzün iş ortamında başarılı olmak için, iş operasyonlarının sürekliliğinin sağlanması, veri kaybının önlenmesi, beklenmedik olaylar geliştiğinde hızlı ve çevik bir şekilde davranabilme imkanı sunan stratejilere sahip olunması büyük önem taşımaktadır (Özenç, 2009).

Kurumlarda iş sürekliliği planıyla, hizmetlerin kesilmesini engellemek, müşteri kayıplarını engellemek, kurumun itibarını korumak, ticari işletmeler için pazar kayıplarını engellemek hedeflenmiştir. İş sürekliliği planlaması sadece bilişim sistemleri departmanına ait bir sorun olmayıp, mevcut kurumların hangi iş süreçleriyle uğraşıyorlarsa o iş süreçlerine yönelik bir bir iş sürekliliği planı geliştirmesi gerekmektedir. İş Sürekliliği Planlamasında dikkat edilecek bir husus sadece veri depolama merkezlerinin korunması değil, bir kurum içindeki e-posta yazışmalarından müşteri ilişkileri yönetimine kadar, şirket içi ve şirket dışı süreçleri gibi birbirlerine bağlı olarak ilerleyen tüm süreçlerin korunmasını sağlamaktır. Kurum içindeki bu süreçlerden herhangi bir servisin kesintiye uğraması zincirleme olarak diğer servislerin işlemesindeki aksaklıklara yol açabilir ve bu durum sadece maddi zararla kalmayıp, kurumun rekabetçi ortamda imajının zedelenmesine neden olabilmektedir. Özellikle finansal kuruluşların bilgi sistemlerinin kesintiye uğraması ve veri kaybetmesi sonucunda ortaya çıkan maliyetler milyon dolarlarla ölçülmektedir.

İş sürekliliği kavramını ciddiye alan ve bu konuda yatırım yapan firmalar olası bir kesinti veya felaket durumunda ayakta kalacaklardır, sürekliliklerini ve imajlarını bu şekilde koruyacaklardır. Bunun yanında kurumların karşı karşıya kaldığı iş kesintileri sonucunda meydana gelen zararlar çok ciddi boyutlara ulaşabilmektedir. Buna çarpıcı bir örnek vermek gerekirse bazı endüstrilerde kesinti maliyeti gelirin %16'sına kadar çıkabilmektedir. Sadece 4 saatlik bir kesinti organizasyonların %32'si için ciddi biçimde zarar verici olabilmektedir (Demirbaş, 2009).

Aşağıdaki tabloda sektörel olarak işlerin bir saat durmasının ortaya çıkardığı yaklaşık maliyetleri gösterilmektedir.

Tablo.I. Kurumlarda 1 Saatlik Kesinti Maliyeti (www.datateknik.com /b)

Uygulama	**Sektör**	**Kesintinin Saatlik Maliyeti**
Borsa İşlemleri, Brokerage	Finans	6.45 milyon $
Kredi Kartı Provizyonu	Finans	2.60 milyon $
Katalog Satışı	Perakende	90,000.- $
Uçak Rezervasyonu	Ulaştırma	89,500.- $
Elektronik Bilet Satışı	Medya	69,000.- $

İş sürekliliği planlarında temel amaç yaşanılan durum süresini en uygun maliyetlerle minimum seviyeye düşürmek ve felaket sonrası ortaya çıkabilecek kayıpları kabul edilebilir bir seviyeye indirmektir. Bunun yanında bir İş Sürekliliği Planında, planlama ve test aşamalarında sadece deprem senaryosu ele alınmamalı, aşağıdaki örnekleri sıralanan diğer senaryoların yaşanması durumunda da çalışmaların devamlılığı için gerekli hazırlıklar göz önünde bulundurulmalıdır (Bestel, 2008). Diğer felaket senaryolarına bakacak olursak;

- İletişim alt yapısının kesilmesi ya da aşırı yavaşlaması,
- Sağanak yağmur veya şiddetli kar sebebi ile personelin çalışma yerine geç ulaşması,
- Telekom'un yurtdışı çıkış hatlarının kesilmesi,
- Toplumsal hareketler veya salgın hastalıklar sebebi ile personelin büyük bölümünün bir kaç gün boyunca işe gelememesi,
- Uzun süreli elektrik kesintileri, jenaratör yakıtının bitmesi,
- Bir şubenin felaket sebebi ile kullanılamaz duruma gelmesi,
- Şubelerin iletişiminin kesilmesi,

- Yangın sonucu bazı katların kullanılamaz duruma gelmesi v.b gibidir.

İş sürekliliği konusu, günümüzde kuruluşların iş süreçlerini devam ettirmesi açısından son derece önemli rol oynamaktadır. Kurumlarda iş sürekliliğinin sağlanması için daha önceden hazırlanan bir plan içerisinde *maksimum kabul edilebilir kesinti süresi*, *kabul edilebilir kesinti süresi, kabul edilebilir veri kaybı* ve *iş etki analizi* gibi kurumun süreçleri üzerinde ciddi etkiye sahip kavramların açıklanması gereklidir.

3. FELAKET KURTARMA PLANI

Günümüzde teknolojinin gittikçe gelişmesiyle, artan ihtiyaçlar doğrultusunda bilişim sistemleri oldukça kritik görevleri yerine getirmektedir. Bundan dolayı bu sistemlerin herhangi bir felaket ya da kesinti sebebiyle çalışamaz hale gelmesinin kurumlar üzerinde çok ciddi olumsuz etkileri olabilmektedir. Böylesi yoğun çalışma ortamlarında beklenmedik bir bozulma veya tabii bir afet vb. felaketlerle karşı karşıya kalmak kurumların sahip oldukları rekabet avantajlarını ya da hizmet alt yapısını tamamen yok edebilir. Böylesi bir duruma daha önceden hazırlanmış bir "Felaket Kurtama Planı" ile hazırlıklı olmak ve veri kaybını önleyecek önlemlerin alınması kurumlar için faydalı olacaktır.

Günümüzde giderek önem kazanan felaket kurtarma planları 1970'li yıllarda yedekleme yapılmak üzere kullanılan bilgisayarların geliştirilmesiyle ortaya çıkmıştır. Bu açıdan bakıldığında, "felaket" bilişim sistemi tabanlı iş süreçlerini sekteye uğratan ya da sistemlere ulaşılmasını engelleyen olaylardır. İşletmelerin geleneksel bilgi sistemlerini tehdit eden felaketler; yangın, su baskını, deprem, kasırga, iş kazaları ve vandalizm gibi unsurlar görülürken, yeni bilgi teknolojilerini ise, terörist saldırılar; kimyasal maddeler, biyolojik maddeler, virüsler; bilgisayar korsanı istilaları gibi yeni unsurlar felakete sürüklemektedir (Wilson ve Diğ, 2004).

Herhangi bir olumsuz durumla karşılaşıldığında, işletmenin üretiminin devam etmesi ve faaliyetlerin aksamadan yürütülebilmesi için yapılması gereken en önemli çalışma, bir felaketten kurtarma planı hazırlanmasıdır. Bu plan çerçevesinde tanımlanan prosedürlerin uygulanması durumunda işletmenin olası bir felaketten olabildiğince az zararla kurtulması sağlanabilir (Doğan ve diğ, 2005).

Felaket kurtarma planlarının amacı, felaket olarak nitelendirilen olaylar meydana gelmeden önce olabilecek her türlü felaket göz önünde bulundurularak gerekli önlemlerin alınması bu olayların meydana gelmesinden, sona ermesine kadar olan zaman içerisinde önlenebiliyorsa felaketlerin önlenmesi ya da sona erdirilmesi amacıyla gerekli hazırlıkların ve faaliyetlerin planlanmasıdır. Felaket Kurtarma Planın önemi özellikle aşağıdaki alanlarda ortaya çıkmaktadır (Felaketten Kurtarma ve Depolama, 2009):

- **Varlıkların ve Kayıtların Korunması:** Felaket meydana geldiğinde bilişim sistemlerinde tutulmakta olan bilgi ve kayıtların korunması, bunlara felaket sonrasında ve normal düzene geçildiğinde de erişilebilmesi gerekmektedir.

- **Faaliyetlerin Yeniden Başlaması:** Felaket sonrasında normal düzene geçişin sağlanabilmesi ve iş faaliyetlerinin felaket öncesinde olduğu gibi yürütülebilmesi sağlanmalıdır.

- **Personelin Korunması:** Bilişim sistemlerini ve iş faaliyetlerini yürüten kişilerin korunması ve sistemlerin devamlılığını felaket sonrasında da devam ettirebilmeleri sağlanmalıdır.

- **Yönetimin Sürekliliğinin Sağlanması:** Felaket olduktan sonra ve normal faaliyetlerin tekrar başlamasında kadar geçen süre içinde yönetim faaliyetlerinin işleyişi sağlanmalıdır.

Felaket kurtarma planlarında ilk adım, iş sürekliliğinin sağlanması için olası felaketlerden gelebilecek tehlike ya da riskleri, risk analizi yaparak önceden tanımlamaktır. Bir risk analizi; bir organizasyon için olası tehlikeleri belirlemeyi içerir ve bu tehlikeler karşısında organizasyonun savunmasızlığının analizi edilir (Wold and Shriver, 2008). Bir risk analizi yaparken göz önünde bulundurulması gereken hususlar; olabilecek her bir felaket türü ve meydana gelme sıklığı hakkında araştırma yapmak, felaket ile ilgili ikaz edilen durumları analiz etmek, felaketlerin sonuçlarını önceden tespit etmek, olası potansiyel maddi ve manevi kayıpları tahmin etmek ve Felaket Kurtarma Planının maliyetlerini belirlemektir (Brooks ve diğ, 2002).

4. İŞ SÜREKLİLİĞİ ve FELAKET KURTARMA PLANI STRATEJİLERİ

Teknolojinin hızla gelişmesiyle birlikte, günümüzde kurumların sahip oldukları kritik iş süreçleri ve önemli verilerinin korunması, bilginin her gün artması ve iş süreçlerinin karmaşık bir hal almasıyla gittikçe zorlaşmaktadır.

İş süreçlerinin bilgi teknolojileri ile entegre edilmeye başlamasından beri, "İş Sürekliliği" ve "Felaket Kurtarma" projeleri her bilişim sistemleri birminin en öncelikli projelerinden biri haline gelmiştir. İş sürekliliği ve dolayısıyla Bilişim Teknolojieri sürekliliği, süreçlerin bir parçası olan Felaket Kurtarma senaryoları bir veri merkezinin tamamen kullanılamaz duruma geldiğinde tüm alt yapıyı farklı bir lokasyonda ayağa kaldırma hedefini içerir (Tunç, 2009).

Bilişim teknolojilerinde meydana gelebilecek felaketler sistemin tamamen çalışabilirliğini durdurabilir ya da veriyi kullanılamaz hale getirebilir. Bu felaketler elektrik kesilmesi, soğutma sistemlerinde bir bozukluk meydana gelmesi ya da donanımsal bir arıza gibi küçük çapta olabilirken, kasırga, su basması, deprem gibi çok geniş çapta da olabilir. Burda en önemli nokta kurumların sahip olduğu önemli veriler, iş süreçleri ve fonksiyonlar için

planlanan ya da planlanmayan kesintilere ve arızalara karşı felaketten kurtarma stratejilerine sahip olunup olunmadığıdır.

Günümüz çalışma ortamlarında en sık karşılaşılan problemlerden bazıları; bilgi güvenliği, iş sürekliliği, önemli verilerin yedeklenmesi ve yedekleme üniteleri üzerinde meydana gelebilecek arızalardır. Bilgi güvenliği konusunda en önemli noktalar; bilginin erişilebilirliği, gizliği ve bütünlüğüdür. Bilgi gizliliği ile kast edilen şey bir bilgiye sadece izin verilen bir grup insanın erişmesinin sağlanmasıdır. Bunu sağlamak bilgiyi kilitli bir kutuya koymak ve bu kilidinde sadece izin verilen kişilerde bulunması gibidir. Bunu sağlamak için değişik şifreleme teknikleri kullanılmaktadır. Bilginin bütünlüğü ise sahip olunan bilginin tahrip edilmemesinin garanti altına alınmasıdır. Örneğin bilgisayar ağlarında aktarılan bilginin tahrip edilmeden yani eksiltilmeden ya da değiştirilmeden elimize ulaştığından emin olmak isteriz. Bu güvenceyi sağlamak için farklı şifreleme teknikleri kullanılmaktadır.

Günümüzde şifreleme olayı bir anahtar kelime yoluyla yapılmaktadır. Gizlemek istediğimiz bilgi anahtar kelime ile ilişkili olarak yeni bir bilgiye dönüştürülür. Bu bilgiyi ilk ham haline dönüştürmek için yine anahtar kelimeye ihtiyaç duyulur. Bunun için güncel olarak kullanılan teknoloji açık anahtar alt yapısı ve sayısal imzadır (Güngören, 2008). Açık anahtar şifrelemesi gerçek hayattaki bir posta kutusu örneğine benzetilebilir. Buna göre ilgili kişinin adresini bilen herkes bu kişinin posta kutusuna bir mektup bırakabilir. Ancak bu posta kutusunu sadece kutunun sahibi ve dolayısıyla kutuyu açacak anahtarı olan kişi açarak mektupları alabilir (Şeker, 2008).

Bilginin erişilebilirliği ise, bir bilgiye ihtiyaç duyulduğu anda erişilip erişilemediğidir. Bu konuda son zamanlarda en çok yaşanan sıkıntı kurumlara yapılan DoS (Denial of Service) saldırılarıdır.

Bilginin kurtarılabiliriliği ise bilginin kaybedilmesi durumunda tekrar elde edilebilmesi anlamına gelmektedir. Örnek olarak bir şirketin muhasebe

kayıtlarının bulunduğu yerde yangın çıktığını düşünelim. Eğer şirket sahip olduğu verilerini bir başka yerde daha yedekliyorsa, yangında odada bulunan bütün veriler kaybolsa bile alınan yedekler sayesinde, veri kaybı önlenmiş olacaktır.

Diğer önemli bir konu ise kurumların sahip olduğu iş süreçlerinde sürekliliğin sağlanmasıdır. Bunun için günümüzde en yaygın olarak kullanılan yöntemlerden bir tanesi Kümeleme (Clustering) yöntemidir ve yüksek erişilebilirlik sağlamak için bir numaralı bir çözümdür. Kümeleme yöntemi, belirli bir amaç için, belirli bir konfigurasyon yapılarak bir araya getirilmiş, kümelenmiş, belli sayıda bilgisayarın, aynı görevi birlikte ya da yedekli çalışmasını sağlayan bir servistir. Kümeleme farklı amaçlar için oluşturulsa da, son kullanıcı tarafından her zaman tek bir bilgisayar gibi gözükecektir. Bir küme oluşturmak için en az iki tane sunucuya ihtiyaç vardır ve bir küme içindeki her bir sunucu "node" olarak adlandırılır. Çeşitli sayıdaki "node"lar bir araya gelerek kümeleri oluştururlar. Kümelerin içerisindeki node sayısı kurumların ihtiyaçlarına göre değişiklik gösterebilmektedir.

Genel olarak baktığımızda, kümeleme işleminin iki temel amacı vardır. Bunların başında süreklilik (continuity) gelmektedir. Burada sürekliliğin anlamı sistemin her türlü felaket ve arızalara karşı her zaman çalışır durumda kalmasını sağlamaktır. Kümeleme yapılarını geliştirmenin temel amacı kullanıcılara kesintisiz bir hizmet vermektir. Diğer bir amacı ise yük dengelemedir (Load Balancing). Kümelemenin anahtar teknolojisi olarak adlandırılır. Burdaki amaç eldeki bilgisayarlardan olabildiğince yararlanmak, işlerin daha hızlı yapılabilmesini sağlamak için gelen yüklerin küme içindeki bilgisayarlara eşit oranda dağıtılmasını sağlamaktır.

Kümeleme yöntemi kendi içinde Yüksek Performanslı Kümeler ve Ağ Yükü Dengeleme Kümeleri olarak ikiye ayrılmaktadır. Yüksek Performanslı kümelemede en önemli özellik erişilebilirliği artırmaktır. Burda tek bir

sunucunun görevini, herhangi bir yazılım ya da donanım problemi meydana geldiğinde diğer bir sunucunun otomatik olarak devralması söz konusudur. Bu yöntemle özellikle veritabanı ya da web servisleri gibi kritik önem taşıyan servislerde kesintisiz ya da minimum kesinti süresiyle hizmet verilmeye devam edilecektir. Küme içindeki arızalı sunucuya müdehale sırasında hizmetin kesintisiz olarak devam etmesi durumuna "failover" denilmektedir. Kümeleme ortamında ne kadar çok node olursa sağlanılan serviste kesinti ihtimali bir o kadar düşecektir. Bir kümeleme yönteminde en yaygın olan konfigurasyon iki node ile oluşturulan konfigurasyondur. Bu konfigurasyon Aktif-Aktif ya da Aktif-Pasif şekilde çalışmaktadır. Yani bu durumda bir sunucu sürekli olarak hizmet sağlarken, diğer sunucu pasif bir şekilde brinci sunucuda oluşabilecek olası bir soruna karşı arka planda beklemektedir.

Ağ Yükü Dengeleme Kümelerinde ise, kendisine gelen istekler otomatik olarak müsait olan sunucular arasında dağıtılır. Herhangi bir olağan üstü durumda bir node çöktüğünde, gelen istekleri otomatik olarak en başta hazırda bekleyen ya da müsait olan bir sunucuya yönlendirir. Burada sunuculardan birinin devre dışı kalması son kullanıcılar tarafından farkedilmeyecektir. Böylece kullanıcıların zarar görmesi engellenerek iş sürekliliği sağlanmış olacaktır.

Kurumlarda bir diğer önemli nokta ise sahip oldukları önemli verilerin korunmasıdır. Bunun için verileri yedekleme teknikleri vardır ve böylece bir felaket esnasında yedekleme sayesinde kurumun verileri korunmuş olacaktır. Yedekleme, bir bilgisayar sistemi üzerinde çalıştırılan yazılımların ve depolanan verilerin arıza, hata, hasar ya da herhangi bir felaket durumunda çalışmaların kesintiye uğramasını ve verilerin geri döndürülemez bir biçimde kaybolmasını engellemek amacıyla birden fazla kopya halinde bulundurulmasını sağlayan işlemler bütünüdür. Yedekleme, felaket durumlarında verinin hazır halde bulunmasının sağlandığı önemli yöntemlerden biridir.

Buna ek olarak yedekleme yapılsa dahi yedekleme ünitelerinde yaşanabilecek disk bozulmaları da bilişim sistemleri için ayrı bir risk konusu teşkil etmektedir. Bu tip risklere karşı geliştirilmiş çözüm yolları da bulunmaktadır. Günümüzde en çok kullanılan teknik ise RAID (Reduced Array Inexpensive Disks) teknolojisidir. RAID teknolojisi, veri saklama ortamlarından kaynaklanabilecek hatalar ve dolayısıyla felaket durumlarının en aza indirilmesini sağlamak için yapılmış bir veri saklama ve erişim teknolojisidir. RAID, diskler arasında veri kopyalama ya da veri paylaşımı için birden fazla sabit disk kullanılarak yapılan veri depolama stratejisidir. RAID kullanımının tek disk kullanımına göre yararı, veri bütünlüğünü, hata toleransını ve toplam disk kapasitesini artırmış olmasıdır.

5. FELAKET KURTARMA PLANININ KURUMLAR ÜZERİNDEKİ FAYDALARI

Kurumlarda felaketten kurtarma planlarının başarılı bir şekilde uygulanabilmesi için, işletme yönetimi bu planın başarılı ya da başarısız sonuçlanması ihtimaline karşı sorumluluk alabilme özelliğine sahip olmalıdır. Bu planının oluşturulması ve uygulanmasında üst yönetim, bütün işletme seviyelerinde etkin bir iletişim ağı oluşturmalıdır.

İşletmeler için iyi bir felaketten kurtarma planının faydaları kısaca şunlardır (Carlson ve diğ, 1998):

- İşletme varlıklarının ve kayıtlarının korunması,
- İşletme faaliyetlerine yeniden başlanması,
- İşletme personelinin korunması,
- İşletme yönetiminin sürekliliğinin sağlanmasıdır.

Felaketten kurtarma planı hazırlamanın sağladığı faydalar doğrultusunda, işletmeler; faaliyetlerinde kesinti yaşanmasını engelleyerek gerekli önlemler alabilmekte ve herhangi bir felaketle karşılaşıldığı anda çöken bilgi sistemlerini düzeltici süreçleri devreye sokabilmektedirler.

Ülkemizde Felaket Kurtarma Planlarını düzenli bir şekilde uygulayan ve bu konuda olumlu sonuçlar elde eden firmalar bulunmaktadır. Ford Otosan "Felaket Kurtarma" ve "İş Sürekliliği Projesini" gerçekleştirmek için önceden bir plana sahip olan ve bu konuda büyük başarı gösteren kurumlardan bir tanesidir. Uygulanan projede öncelikle kurumun sahip olduğu yetkili satıcı ağı, yan sanayi ağı ve Türkiye'nin 4 farklı yerleşiminde (Acıbadem, Kartal, Eskişehir, Kocaeli) yer alan fabrika ve operasyon merkezi ile büyük bir veri ağına sahip olan Ford Otosan'ın, dağınık yapıda yer alan verilerinin konsolide edilmesi, tek merkezden yönetilmesi, güvenliğinin ve sürekliliğinin sağlanması amacı ile "Felaket Kurtarma" ve "İş Sürekliliği" projesini başlatmışlardır (İş Sürekliliğinde Başarılı Örnek: 'Ford Otosan', 2004).

Proje kapsamında yapılan çalışmalar ise:

- İş modelinin oluşturulması
- İş modeli kapsamında istenenler ve ihtiyaçların belirlenmesi
- Bu ihtiyaçlara paralel olarak kriz senaryolarının oluşturulması
- Genel teknolojik araştırma ve altyapı tasarımı
- Sektörde yer alan ürünler ve bu ürünlerin getirdiği yeniliklerin araştırılması
- Çalışmada Felaket Kurtarma ve İş Sürekliliği Planından yola çıkılarak hareket edilmiştir

Verilerin ve uygulamaların senkron yedeklenmesinin yanı sıra,

- Geniş Alan Ağlarını, Yerel Alan Ağlarını ve Sistem odalarını yedeklediler. Bu yedekleme, merkezi bir yedekleme çözümü olan Depolama Alan Ağı üzerinden yapılmıştır. Böylece yerel alan ve geniş alan ağındaki tüm sunucular var olan depolama alan ağına bağlanırlar ve ordanda bu ağa bağlı olan yedekleme kütüphanesine aktarılırlar.

- Hata düzeltme ve süreklilik yeteneğini artırılması sağlandı. Bunun için kurum RAID teknolojinden faydalanarak sahip olduğu diskerde meydana gelebilecek arızalara karşı önceden önlem almıştır.

- Konsolide edilmiş verinin ayrıca yedeklenmesiyle hedeflenen mimari tamamlanmış oldu.

Projenin firmaya sağladığı faydalar:

- Veritabaları konsolide edildi ve performans artırıldı.

- Dağınık veri konsolide edildi.

- Verinin senkron ve asenkron yedeklenmesi sağlandı. Burda replikasyon yöntemi ile veri senkron ve asenkron olarak farklı bir loksayona aktarılarak üretim verisinin bir başka lokasyonda bulundurulması hedeflenmiştir. Böylece firma üretim lokasyonunda oluşabilecek her hangi bir felakete karşı önlem almış bulunmaktadır.

6. SONUÇ

Günümüz çalışma ortamlarında, kurum ve kuruluşların tüm iş süreçlerinde devamlılığının sağlanması ve sahip olduğu verilerin depolanması bilişim sistemleri sayesinde olmaktadır. Böylesi çalışma ortamlarında herhangi bir felaketin sebep olacağı olumsuz durumlar, kurumlarda iş sürekliliğini ve sahip olunan verilerin güvenliğini ciddi şekilde tehdit etmektedir. Artık bir çok kurum ve kuruluş her gün karşı karşıya kaldığı riskler karşısında günlük operasyonlarını gerçekleştirdiği iş süreçlerini ve kendisi için hayati derecede

önem taşıyan verilerini güvence altına almak için İş Sürekliliği ve Felaket Kurtarma Planlarına başvurmaya başlamışlardır.

Sonuç olarak İş Sürekliliği ve Felaket Kurtarma Planlarını ciddiye alan ve bu konuda yatırım yapan kurumlar, hem verilerinin güvenliği hem de iş sürekliliklerinin sağlanması açısından olumlu faydalar elde etmişlerdir. Bunun yanında kurumların rekabetçi ortamda prestiji ve saygınlığı da alınan bu önlemler sayesinde korunmuştur.

KAYNAKLAR

Bestel, B. (2008). İş Sürekliliği Planlaması.

Brooks, C. , Bedernjak, M. , Juran, I. , Merryman, J. (2002). Disaster Recovery Strategies with Tivoli Storage Management, IBM 15.03.2010, http://www.redbooks.ibm.com/abstracts/SG246844.html

Carlson, J.S.; Parker, D.J. (1998). Disaster Recovery Planning and Accounting Information Systems, Review of Business Winter.

Demirbaş, G. (18 Kasım 2009). Şirketler 'İş Sürekliliğine' Yatırım Yapıyor. Milliyet. 26.02.2010, http://kobi.milliyet.com.tr/haber/kobi-sirketler-is-surekliligine-yatirim-yapiyor,5104,rss

Doğan, A. ; Tanç, A. ; Tanç, Ş. (2005). Felaketten Kurtarma ve Muhasebe Bilgi Sistemi. Erciyes Üniversitesi.

Ergil, A. (25.11.2009). İş Sürekliliği Nedir. 17.02.2010, http://www.issurekliligi.tr.gg/

İş Sürekliliğinde Başarılı Örnek:'Ford Otosan'. (10.03.2004). 17.04.2010, http://www.turk.internet.com/portal/yazigoster.php?yaziid=9523

Güngören, B. (2008).TMMOB Elektrik Mühendisleri Odası. Bilgi Güvenliği Nedir.
İş Sürekliliği. (14.03.2008). 20.02.2010, http://www.datateknik.com.tr/tr/content.asp?ctID=604 /a

İş Sürekliliği. (14.03.2008). 20.02.2010, http://www.datateknik.com.tr/tr/content.asp?ctID=604 /b

Özenç, C. (13.08.2009). İş Sürekliliği ve Esnekliği Hizmetleri. 22.03.2010, http://www-05.ibm.com/tr/bcrs/index2.html

Şeker, S. (2008). Açık Anahtarlı Şifreleme (Public Key Cryptography). 06.04.2010, http://www.bilgisayarkavramlari.com/2008/03/19/acik-anahtarli-sifreleme-public-key-cryptography/

Tunç, Y. (12.03.2009). Sanallaştırma ile Uygulanabilir Felaket Kurtarma Senaryoları. 16.03.2010, http://www.kocsistem.com.tr/tr/sanallastirma07.asp

Türkiye Bilişim Derneği Kamu-BİB, Kamu Bilişim Platformu XI. (2009). Felaketten Kurtarma ve Depolama. (TBD/Kamu-BDB/2009-ÇG2). Antalya.

Wilson, E.; Bob, H.; Ron, B.; Mike, N. (02.05.2004) Planning for Disaster Recovery. 25.03.2010,www.itec.suny.edu/Planning%20for%20Disaster%20Recovery,%20v5.4.ppt

Wold, G. and Shriver, R. (12.01.2008). Risk Analysis Techniques. 14.03.2010, http://www.drj.com/new2dr/w3_030.htm