



2026 YILINDA ŞİRKETLERİ BEKLEYEN BÜYÜK

RİSKLER RAPORU

Şirketlerin yalnızca ekonomik baskılarla değil; dijital tehditler, operasyonel kırılganlıklar ve hukuki yükümlülüklerle aynı anda sınandığı bir dönem olacaktır. Bu rapor, işletmelerin karşılaşılabileceği en kritik riskleri ortaya koyarak kurumların geleceğini korumak için ihtiyaç duyacağı stratejik çerçeveyi sunmaktadır.

İÇİNDEKİLER

- 1. 2026 İş Dünyası Risk Görünümü**
- 2. Şirketleri Tehdit Eden Temel Risk Alanları**
- 3. Operasyonel ve Finansal Kırılganlıklar**
- 4. Dijitalleşme, Siber Riskler ve Veri Güvenliği**
- 5. İnsan Kaynakları ve Hukuki Yükümlülükler**
- 6. Yönetici Sorumluluğu ve Karar Riskleri**
- 7. 2026 İçin Kritik Uyarı Trendleri – Tablo ve Mini Analizler**
- 8. Başınıza Gelebilecek En Ağır Hasar Örnekleri (12 Vaka)**
- 9. 2026 İçin Kurumsal Dayanıklılık Yaklaşımı**
- 10. Sonuç**

1. 2026 İş Dünyası Risk Görünümü

2026, işletmelerin yalnızca ekonomik koşullarla değil; dijital güvenlik açıkları, insan kaynaklı riskler, operasyonel kırılganlıklar ve yönetsel sorumluluklarla şekillenen çok katmanlı bir risk haritasıyla karşılaşacağı bir yıl olacaktır. Şirketler için en belirgin değişim, risklerin artık birbirinden bağımsız değil; zincirleme etkiler yaratan karma bir yapı hâline dönüşmesidir. Özellikle siber risklerin yaygınlaşması, klasik risk yönetimi anlayışının ötesine geçilmesi gerektiğini göstermektedir.

2. Şirketleri Tehdit Eden Temel Risk Alanları

Aşağıdaki grafik, 2026'da işletmeler üzerinde baskı kurması beklenen başlıca risk alanlarını özetlemektedir:

Risk Alanı	Yoğunluk Seviyesi	Görsel Gösterim
Siber Saldırıları	Çok Yüksek	
Operasyon Kesintileri	Yüksek	
Veri İhlalleri / KVKK	Çok Yüksek	
Çalışan Davaları	Orta-Yüksek	
Tedarik Zinciri Aksamaları	Orta	
Yönetimsel Hata Sorumluluğu	Yüksek	

Bu grafik, şirketlerin özellikle dijital altyapılarını güçlendirmede süreci operasyonel istikrarlarını korumakta zorlanabileceğini açıkça göstermektedir.

3. Operasyonel ve Finansal Kırılganlıklar

Bir işletmenin değer zinciri çoğu zaman görünmez risklerle çevrilidir. Üretimin beklenmedik şekilde durması, tedarik zincirindeki aksamalar, enerji dalgalanmaları, lojistik hataları ve sistemsel çökmeler, şirketlerin finansal performansını doğrudan etkileyebilir.

Örnek bir tabloyla bu risklerin zincirleme etkisi özetledik;

Operasyonel Aksaklık Zinciri – 2026

Olay / Aksaklık	Zincirleme Etki	Sonuç
Üretim hattında arıza	Teslim gecikmesi ↑	Müşteri kaybı
ERP sisteminin çökmesi	Fatura/tedarik sürecinin durması	Nakit akışı bozulur
Lojistik gecikme	Sözleşmesel yaptırımlar	Ek maliyet
Enerji kesintileri	Verimlilik kaybı	Operasyon durması

Bu tablo, tek bir teknik aksaklığın bile bir şirketi finansal açıdan savunmasız bırakabileceğini göstermektedir.

4. Dijitalleşme, Siber Riskler ve Veri Güvenliği

Siber riskler bu dönemde tüm işletmeler için en kritik risk türü hâline gelmiştir. Fidyeye yazılımlar, sosyal mühendislik saldırıları, kimlik bilgisi hırsızlığı, kötü amaçlı eklentiler, tedarik zinciri üzerinden gelen zararlı yazılımlar ve bulut bilişim açıkları, şirketleri hem hukuki hem operasyonel açıdan baskılayan en önemli tehditlerdir.

Şirketler sadece dış saldırılarla değil, iç kaynaklı hatalarla da dijital risklere açık hâle gelir. Yanlış yapılandırılmış bir bulut sunucusu, yanlış kişiye gönderilmiş bir dosya veya zayıf bir parola politikası bile veri ihlali için yeterlidir.

Siber Risk Gerçekleri

- Saldırıları artık tamamen otomasyon ve yapay zekâ ile yürütülüyor.
- Fidyeye yazılımları “çift yönlü” hâle geldi: Hem veriyi kilitliyor hem çalıyor.
- Küçük işletmeler büyük şirketler kadar hedef oluyor, çünkü savunmaları daha zayıf.
- Bir sistem çökmesi sadece IT’yi değil, üretimi, muhasebeyi ve müşteri ilişkilerini aynı anda durdurabiliyor.

5. İnsan Kaynakları ve Hukuki Yükümlülükler

Çalışan kaynaklı süreçler, 2026’da şirketlerin karşılaştığı en yoğun hukuki risk alanlarından biridir. Performans tartışmaları, mobbing iddiaları, ücret uyuşmazlıkları, eksik evrak, uygunsuz fesih sebepleri, kariyer eşitliği şikâyetleri gibi konular, işletmeleri hem maliyet hem de itibar anlamında zorlayabilir.

İş hukuku hatalarının çoğu, basit bir prosedür eksikliğinden doğar: yanlış belge, eksik tutanak, yanlış değerlendirme kriteri. Aynı zamanda çalışanların dijital ortamlarda işlem yapması, hatalı veri paylaşımı veya yanlış yönlendirilmesi, işletmeleri KVKK sorumluluklarıyla da karşı karşıya bırakabilir.

6. Yönetici Sorumluluğu ve Karar Riskleri

2026'da yöneticilerin karşı karşıya kalacağı en önemli tehditlerden biri, her kararın doğrudan kişisel sorumluluk yaratabilmesidir. Yanlış yorumlanan mali raporlar, eksik analizlerle verilen yatırımlar, sözleşme ihlalleri, ihale süreçlerindeki şeffaflık iddiaları veya kaynakların hatalı tahsisi, yönetim kadrolarını ciddi savunma süreçlerinin içine çekebilir.

Bu süreçlerde şirket değil, bizzat yöneticiler sorumlu tutulabildiğinden, karar süreçleri artık çok daha çerçeveli ve kontrollü yürütülmelidir.

7. 2026 İçin Kritik Uyarı Trendleri

Aşağıdaki tablo, 2026'da en hızlı yükseliş göstermesi beklenen risk türlerini göstermektedir:

Risk Alanı	2026 Etki Seviyesi	Neden Önemli?
Siber Saldırıları	Yüksek	Tüm iş akışını durdurabilir
Yönetim Hata Sorumluluğu	Yüksek	Kişisel varlık riskine dönüşebilir
Çalışan Davaları	Orta-Yüksek	Artan iş hukuku talepleri
Veri İhlalleri / KVKK	Yüksek	İnceleme + hukuki yükümlülük
Tedarik Zinciri Aksamaları	Orta	Operasyonel gecikme etkisi

Risklerin, ağırlıklı olarak dijital ve yönetsel alanlarda yoğunlaştığını göstermektedir.

8. Hasar Örnekleri

1. Bir üretim tesisinde yaşanan enerji dalgalanması tüm makineleri durdurur ve kritik bir müşteriye yapılacak teslimat yetiştirilemez.
2. Lojistik yazılımının fidye yazılım ile kilitlenmesi taşıma planlarının tamamını erişilemez hâle getirir.
3. Bulut sunucusunda yanlış yapılandırma sonucu müşteri verileri internete sızar ve inceleme süreci başlatılır.
4. Bir çalışan performans değerlendirmesinin ayrımcılık içerdiğini iddia ederek dava açar.
5. Yanlış yorumlanan bir teknik rapor yüzünden büyük bir altyapı yatırımı beklenen sonucu vermez ve yönetim sorumlu tutulur.
6. Tedarikçiden geç gelen kritik bir malzeme üretim hattını tamamen durdurur.
7. Phishing saldırısıyla finans biriminin erişim bilgileri ele geçirilir ve ödeme talimatları manipüle edilir.
8. Depo alanında nem kontrolü yapılmadığı için yüksek hacimli ürün kullanılamaz hale gelir.
9. Hatalı bir disiplin süreci, çalışan tarafından mobbing iddiasına dönüştürülür.
10. Yanlış yükleme nedeniyle konteyner devrilir ve tüm ihracat yükü hasar görür.
11. Bir yöneticinin sözleşme maddesini hatalı yorumlaması şirketi ağır bir hukuki ihtilafın içine sokar.
12. Dijital güvenlik açığı nedeniyle şirket içi yazışmalar sızdırılır ve marka itibarında zedelenme meydana gelir

9. 2026 Yılı İçin Kurumsal Dayanıklılık Yaklaşımı

2026 yılı, riskleri yok saymanın değil, onları kurumsal yapının doğal bir bileşeni olarak kabul etmenin yılıdır. Operasyonel süreçlerde şeffaflık, dijital altyapıda güçlü güvenlik çerçevesi, çalışan süreçlerinde hukuka uyum, yönetsel kararlarda daha dikkatli çerçeveler oluşturulması, şirketlerin dayanıklılığını artıracaktır. Riskler tamamen engellenemese de doğru yapı kurulduğunda etkileri kontrol altına alınabilir.

10. Sonuç

2026 yılı , işletmelerin hem dijital hem de operasyonel dünyada daha büyük tehditlerle karşılaşacağı bir dönem olabilir. Bu risklerin şirketlere verebileceği finansal ve yönetsel yükün hafifletilmesi ancak önceden yapılan hazırlıklarla mümkündür. Kurumlar, karşılıklarına çıkabilecek beklenmedik durumlara karşı ne kadar hazırlıklıysa, sürdürülebilir büyümeyi o kadar emin adımlarla sağlayabilir. Bir şirketin geleceğini koruyan şey, karşılaşabileceği büyük riskleri öngörmesi ve bu risklerin yaratacağı etkiyi yönetebilecek bir sigorta mekanizmasını zamanında kurabilmesidir.

Bizimle iletişime geçin.

Adres : Maslak Mahallesi, Maslak Meydan Sokak, Beybi Giz Plaza A Blok No:1 Kat:21 İç Kapı No: 79 Sarıyer / İstanbul

Telefon : +90 212 227 07 13

Fax : +90 212 227 07 15

Web : www.bigsrb.com

