

20 SENARYO MATRİSİ ÖRNEĞİ: Kısım 2



Risk Senaryosu:

Personelin fiziksel güvenliği tehdit altında.

İtici Etken 1:

Hükümetin özel yazışmalarımıza erişimi

İtici Etken 2:

Hükümetin üzerinde çalıştığımız konuya, yaptığımız çalışmalara karşı tutumu

	Durum 1: Demokrasi ve Destek, Bebek	Durum 2: Görünmez Örgüt Yeniden Atakta	Durum 3: Tereyağından Kıl Çeker Gibi	Durum 4: Acil Durum
Durum nasıl görünüyor?	Hükümetin özel iletişimlerimize erişimi yok ve de üstünde çalıştığımız konuyu ve yaptığımız çalışmayı onaylıyor.	Hükümetin özel iletişimlerimize erişimi yok ama yaptığımız çalışmayı onaylamıyor.	Hükümetin özel iletişimlerimize erişimi var ama yaptığımız çalışmayı onaylıyor.	Hükümetin özel iletişimlerimize erişimi var ve yaptığımız çalışmayı onaylamıyor.
Bu durum örgütümüzü nasıl etkileyecek?	Çalışmamızı uygulamaya geçirmek ve hedef grubumuzu desteklemek için geniş bir serbestliğimiz var. Personelimizle ilgili düşük bir fiziksel güvenlik riski var. Bu örgütümüz için olabilecek en iyi senaryo.	Çalışmamızı ancak "görünmez" hareket ederek sürdürebiliyoruz: web sitemiz ve halkla ilişkiler materyalimiz sansürlü ve çalışmamızın gerçek amacı görünür değil ya da güven çemberimiz dışındakilere açık yayımlanamıyor. Hükümet bazen personelimizi kamusal olaylarda taciz ediyor.	Etkin çalışabiliyoruz ama her zaman program değişikliklerimizin hükümet tarafından onaylanıp onaylanmayacağını dikkate almak zorundayız. Çalışmamız üzerinde tam bir özerkliğimiz yok. Hükümet bize sataşmıyor ama çok fazla gücü var.	Bu kritik bir durum ve de çalışmalarımızı sürdüremeyebiliriz. Hükümet etkin biçimde personelimizi taciz ediyor.
Örgütümüz bu duruma karşı nasıl hazırlanıp yanıt verebilir?	Hükümete kaynak başvurusu yaparak. Destek verebilecek hükümet yetkililerine aktif bir ağ oluşturmayı deneyerek.	Bizi destekleyebilecek insanlardan -örn., diğer sivil toplum oyuncuları, işletmeler, üniversiteler, vb.- yerel bir ağ oluşturarak. Halkla ilişkiler mesajımızı nasıl sunabileceğimizi yeniden düşünerek. Çalışmamızın ölçeğini küçültmek ya da taşımayı düşünerek.	Mümkün olan her yerde sanal özel ağ (VPN) kullanarak. Verileri çevrimdışı saklayarak. Bizi destekleyebilecek insanlardan -örn., diğer sivil toplum oyuncuları, işletmeler, üniversiteler, vb.- yerel bir ağ oluşturarak. Bize desteklerini arttırmak için yerel yönetimlerle ilişkiler kurmaya çalışarak.	Ayrıntılı bir Çıkış Stratejisi oluşturarak. Mümkün olan her yerde VPN'ler kullanarak. Verileri çevrimdışı saklayarak.
Bu durumun tekrarlanma olasılığı nedir?	Çok düşük olasılık	Ortalama olasılık	Düşük olasılık	Ortalama olasılık

Risk ve Dirençlilik

Yöntem Kartı 25 ■ ■ ■