



BİLİŞİM RİSKLERİ SİGORTASI

Bilgisayar Saldırısı nedir?

- Bilgisayar saldırısı aynı zamanda Bilişim Saldırısı olarak da bilinir; bu saldırıyı tanımlamak için aşağıdaki tanımlardan biri kullanılabilir:
- Yetkisiz bir kullanıcının sigortalı bilgisayar sistemine giriş yapması,
- Bir virüs veya kötü amaçlı bir yazılımın saldırısı,
- Hizmeti engelleme saldırısı.

BİLİŞİM RİSKLERİ SİGORTASI / Kapsam & Faydaları

Kapsam & Faydaları

Ana Teminatlar

Sigortalıya «Police döneminde gerçekleşen» ve sigorta kapsamına giren (*sorumluluktan doğan şikayet maliyetleri ve harcamalar da dahil olmak üzere*) hasarı karşılar.

«Police döneminde gerçekleşen» Hasar tipi poliçelerde iki ana unsur bulunmaktadır. Police dönemine ait iki tip hasar tarihi tanımı yapılabilir: Police vadesi içinde gerçekleşen Hasar tarihi ve «Geriye Dönük» kapsam tarihi içinde meydana gelen hasar. Bu iki tarihten hangisi önce ise,

- 1) Meydana gelen Bilişim Suçu oluş tarihi itibariyle hali hazırda mevcut poliçede teminat altındadır.
- 2) Söz konusu hasarın «bildirimi» sizin veya sigortalınızın bu suçu ilk kaydettiği veya ilk defa haberdar olduğunda yapılır.

BİLİŞİM RİSKLERİ SİGORTASI / Kapsam & Faydaları

Kapsam & Faydaları

Ana Teminatlar

- Satın aldığınız bu poliçe «**Masraf Dahil**» temelli bir poliçedir.
- Poliçenin Tazminat limiti **Senelik Toplam Limit** olarak belirlenir.
- Verilen teminat dahilindeki suçlar için mevcut çalışanlar, işe alınma aşamasında olanlar, eski çalışanlar (*yönetici, ofis çalışanları, ortak ve şirket yetkilileri dahil olmak üzere*) herhangi bir alt yüklenici veya yasal olarak alt yüklenici ve / veya sigortalının sorumluluğunda olan çalışan sıfatına haiz herhangi biri tarafından gerçekleştirilen bilişim suçları teminat kapsamındadır.

BİLİŞİM RİSKLERİ SİGORTASI / Kapsam & Faydaları

Veri Sorumluluk Vakaları (Üçüncü Şahıs Teminatı)

Sigortalıya karşı yapılan İlk Hasar Talebi Zararları karşılanır. Veri Sorumluluk Vakalarında;

- Kamuya açık olmayan verilerin zararları (fiziki olmayan değerler)
- Gizlilik Haklarının ihlali

Gizlilik Hakları 1998 Veri Koruma Anlaşması, 2003 Gizlilik ve Elektronik İletişim Düzenlemeleri olmak üzere ülkemizde ise 2007 tarihli 5651 kanunla koruma altına alınmıştır.

Ağ Güvenliği Vakaları (Üçüncü Şahıs Teminatı)

Sigortalıya karşı yapılan İlk Hasar Talebi Zararları karşılanır. Ağ Güvenliği Vakalarında;

- Üçüncü Şahıslara kasıtsız ve ihmal sonucu iletilen kötü amaçlı yazılım (iletişim ağını veya sistemini silici kod barındıran, girişi engelleyen, çökerten, zarar veren, bozan veya iletişim ağı güvenliğini aşan yazılımlar.
- İzinsiz Giriş (Sigortalının teminat altındaki bilgisayar sistemini veya iletişim ağını kullanan ve bunu yapmaya yetkisi olmayan kişi / çalışanın eylemidir).

İyileştirme Masrafları (Lehtar Teminatı)

Sigortalının gerçek veya olası bir Veri Sorumluluk veya Ağ Güvenliği vakalarından kaynaklı masraflardır. İyileştirme Masrafları şunları içerir:

- Kredi İzleme Masrafları;
- Bilişim Gasp Masrafları;
- Kurtarılan Veri Yapılandırma Masrafları;
- Adli Masraflar;
- Savunma Masrafları;
- Tebligat Masrafları; ve
- Halkla İlişkiler Masrafları.

İş Durması Kaybı (Lehtar Teminatı)

Sigortalının Bilişim İşinin Kesilmesinden kaynaklı masraflardır. İş Durması Kaybı aşağıdaki başlıkları içerir;

- Brüt Gelir veya Brüt Kâr seçenekleri
- Artan Çalışma Masrafları Teminatı
- Zararı Azaltma Teminatı.

Sigortalının sistem kesintisi etkilerini veya ağ kesintilerini kaçınma veya azaltma amaçlı yaptığı keşif veya böyle bir kesintinin etkilerini en aza indirme veya ağın işlev yitimi kayıplarını ispatı veya delilleri muhafazası gereklidir.

Sivil Cezalar & Para Cezaları

Sivil Cezalar & Para Cezaları yasal olarak sigorta tarafından teminat altına alınamaz hükümde olmadığı durumlarda mahkeme tarafından ödenmesi kararlaştırılan cezaları teminat altına alır.

Sivil cezalar oluşan zararın telafi edilmesi amacıyla kesilen parasal cezalardır. Cürüm sonucu kesilen para cezalardan farklı olmasının sebebi nakdi cezayı ödemeye mahkum edilen kişinin cezalandırılması değildir. Aslında zarar gören diğer tarafın zarar veren tarafından tazmin edilmesidir. Sivil cezalar aynı zamanda sivil para cezaları olarak da adlandırılır, sadece parasal cezalardır.

Bazı durumlarda sivil para cezaları başka bir idari yasaklama veya cürüm cezalarıyla beraber yürütülür. Böyle bir cürüm cezası alan kişi için verilen para cezası miktarı hakim tarafından belirlenmektedir.

Cürüm'e bağlı ceza ve para cezalarının sorumluluğunu sigortalamak mümkün değildir.

İstisnalar

Sigortalının ameli, konu hakkında bilgi sahibi olması veya davranış şekli bir başka sigortalı için uygulanacak istisnalara örnek teşkil etmez. Bu sayede bir tarafın amel, bilgi ve davranışı sonucu oluşan istisnaların masum olan ve aksi durumda poliçe teminat kapsamına alınabilecek diğer taraflara uygulanma zorunluluğunu ortadan kaldırılmasını sağlar.

İş bu poliçe kapsamındaki istisnaların büyük bir bölümü başka özel riskler poliçeleri dahilinde teminat altına alınabilir.

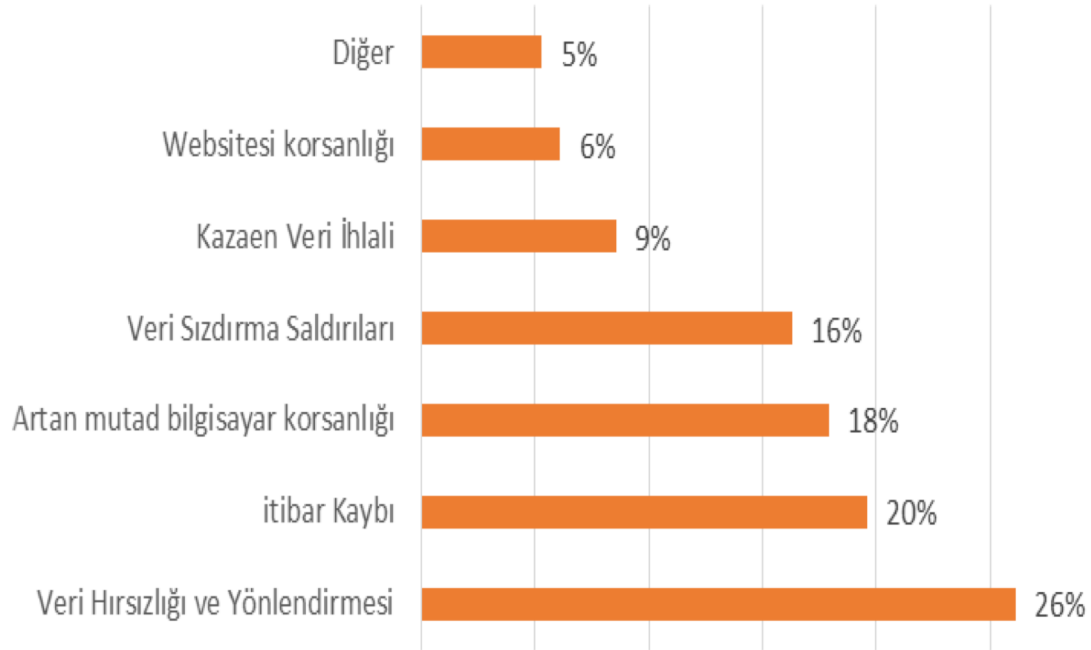
İstisnalar

- ✓ Başka bir Sigortalının faydasına olan Asbestos, nükleer, Kirlilik & Elektromanyetizma kaynaklı hasarlar
- ✓ Bedensel Yaralanmalar
- ✓ Sözleşme gereği anlaşmalardan ve temin edilen ürünlerden doğan zararlar
- ✓ Yönetici & Çalışanların sebep olduğu zararlar
- ✓ Görevlendirme Uygulama Sorumlulukları
- ✓ Dış Hizmetlerden Kaynaklı Zararlar
- ✓ Dolandırıcılık veya Emniyeti Suiistimal
- ✓ Fikri Mülkiyet Hakları
- ✓ Ödeme aczi
- ✓ Para
- ✓ Ürün Hataları ve geri çağırma
- ✓ Mesleki Sorumluluk
- ✓ Geriye dönük işlerlik tarihi
- ✓ Menkuller
- ✓ Terörizm (Her türlü Bilişim İş Durması Zararları için)
- ✓ Savaş
- ✓ Finansal veya Ticari yasaklardan kaynaklı zararlar

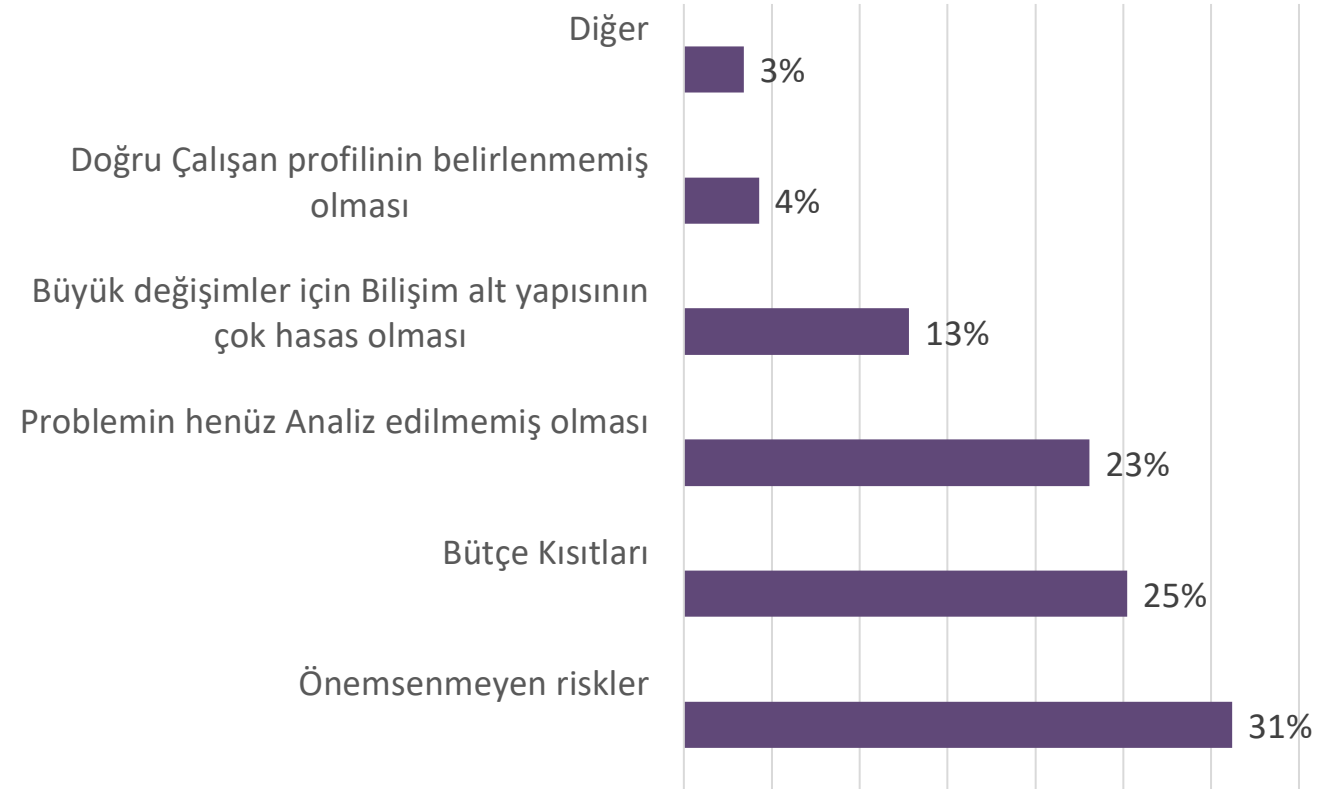
BİLİŞİM RİSKLERİ SİGORTASI



Şirketlerin en çok endişe ettikleri Bilişim Riskleri Neler?



Şirketler Bilişim Risklerine karşı nasıl korunur?



Bilişim Suçları Hasar Örnekleri

Aşağıda yer alan örnekler gerçekleşmiş hasarlar olup, ticari hayatı etkileyebilecek bazı senaryolarda ayrıca oluşturulup paylaşılmıştır;

1. Sosyal medyada paylaşılan ve rakibi yeren ifadelerin yer aldığı uzun bir iç yazışma rakip firma tarafından fark ediliyor. Bu durumun kendisine zarar verdiğini iddia ederek konuyu mahkemeye taşıyor. Mahkeme sonucunda alınan tazminat miktarı £450,000.
2. Çevrimiçi Satış yapan bir perakendeci web site sağlayıcısının hatası sonucu zarara uğradı. Sağlayıcının veri merkezindeki bilgisayar sistemi çökünce perakendecinin sipariş aldığı ve satış yaptığı web sitesi işlev göremez hale gelir. Sonuç olarak Satış ve gelir kaybı olmuştur.

Bilişim Suçları Hasar Örnekleri

3. Suçlular büyük bir firmanın yerel kablosuz ağına sızmış ve söz konusu mağazada işlem yapmakta olan müşterilerin hesap numaralarını erişimi engelleyerek kopyalamışlardır. Daha sonra erişimi kullanarak firmanın ana veri bankasına girerek milyonlarca kredi kartı ve kişisel bilgilere erişim noktası yaratmışlardır. Oluşan maliyet ile ilgili tahmin £100m üzerindedir.
4. Yemek Üreten bir fabrika üçüncü bir şahıs için hazır yemek sosu ürünü üretme anlaşması yapmıştır. Bilgisayar korsanı fabrikanın güvenlik duvarını aşarak reçeteyi çalmıştır. Reçete kopyalanmaya karşı korumalı olduğu için müşteri yemek fabrikasını kâr kaybı nedeniyle dava etmiştir.

Bilişim Suçları Hasar Örnekleri

5. Bir mali müşavirlik firması müşterileri için vergi danışma iş listesi çekmiştir. Ortaklardan birinin korumasız dizüstü bilgisayarını tüm müşterilerin detaylarının olduğu liste ve vergi kaçırma şemalarının olduğu dosyalar da dahil olmak üzere kaybolmuştur. Firma bir mücrim tarafından listenin çevrim içi yayımlanması ile tehdit edilerek £250,000 fidye ödenmesi istenmiştir.
6. Üretim yapan bir firmanın POS Yazılım Sistemi bilgisayar korsanı tarafından saldırıya uğramış ve bozulmuştur. Üretici stok yapma, siparişleri takip etme ve ürün fiyatlandırmasını yapamaz hale gelmiştir. İş durması ve kâr kaybı tazminat talebi yapılmıştır.

BİLİŞİM RİSKLERİ SİGORTASI

Bilişim Suçları Hasar Örnekleri

7. Bir firma tanıtım amaçlı olarak sosyal medya araçlarını kullanmıştır. Pazarlama departmanı Twitter, You Tube ve Facebook gibi ağlar dahil olmak üzere oldukça aktif çalışmaktadır. Aynı zamanda çalışanlarında bu sitelerden içerik yayımlamaları için teşvik etmişlerdir. Firmanın oldukça ağır bir sosyal medya politikası olmasına rağmen çalışanlardan biri çalışma saatleri dışında rakip firmayı aşağılayan bir paylaşımda bulunmuştur. Yapılan yorum firmaya karşı karalama / hakaret davası açılmasıyla sonuçlanmıştır.
8. Büyük ölçekli bir sigortalı yedekleme diskini kaybetmiştir. Maalesef söz konusu yedek içinde 500,000 müşterinin kaydı bulunmaktadır. Bunun sonucu olarak £2.3 million para cezasıyla birlikte yaklaşık 50,000 İngiliz müşterisine durumu açıklayan bildirim yazmışlardır.

Bilişim Suçlarına karşı İşinizi nasıl koruyacağınızı gösteren birkaç hasar senaryosu:

I. Çalışanın hırsızlığına müteakip veri güvenliğinin ihlali

Bir iş bulma ajansı kimlik çalma şebekesi tarafından hedef seçilmiştir. Bu grup ajansın bir çalışanını isimlerin, adreslerin ve kimlik numaralarının bulunduğu dosyaları kendilerine vermesi karşılığında yanlarına alarak ödeme yapmaktadırlar. Tabii ki ajans yetkililere başvurmuştur; araştırma yapılmış ve bunun sonucuna göre ajanstan gelen verilere dayanan kişisel bilgilerin bulunduğu dokümanlara ulaşılmıştır. Vakayı çözmek için yapılan harcamalar oldukça yüküldür; çağrı merkezi çalışanlarını işe almak, etkilenen kişiler için kredi gözetleme hizmeti sunumu ve bilgilendirme yapılması, ve veri güvenlik ihlalinin boyutunu anlamak ve değerlemesi için IT soruşturması yapılması. Böyle bir durumda sigortacı ajans ile yakın bir şekilde çalışarak yasal zorunluluklardan doğan masrafları karşılar ve Halkla İlişkiler desteği ve itibarı korumak adına yapılan diğer masrafları tazmin eder.

BİLİŞİM RİSKLERİ SİGORTASI



II. Bellek Çubuğunun kaybolmasına müteakip Veri Güvenliği İhlali

Bu senaryoda şifresiz bellek çubuğu kaybolmuştur. Ayrıntılı inceleme aşamasında olan potansiyel bir satın alıcının şirket alım evraklarının içinde bulunduğu bellek çubuğu firma sahibinin el çantasından kamuya açık bir alanda çalınmıştır. Çubukta firmanın 5,000 çalışanının ev adresleri ve banka detayları gibi kişisel ve önemli verileri bulunmaktaydı. Bilişim Komisyonu (ICO) tarafından para cezasıyla birlikte önemli miktarda bir masraf ortaya çıkmıştır. Bu senaryoda sigortalı firmaya veri koruma eksperisi veya koruyucu avukat tutmasına yardımcı olabilir, ICO ile anlaşmaya varabilir ve etkilenen çalışanlara bildirim yapabilirdi.

III. Bilgisayar Korsanlığına müteakip Veri güvenliği İhlali

Yemek ve içki işinde olan büyük bir firmanın içinde 100,000 müşterisinin isim ve iletişim bilgileri bulunan IT sistemi bilgisayar korsanlığı sonucu veri tabanı kopyalanmıştır. Bu durumda sigortacı durumu Bilişim Komisyonuna bildirmeleri için destek olur ve sürecelecek olan araştırma boyunca firmaya destek olacaktır.

BİLİŞİM RİSKLERİ SİGORTASI

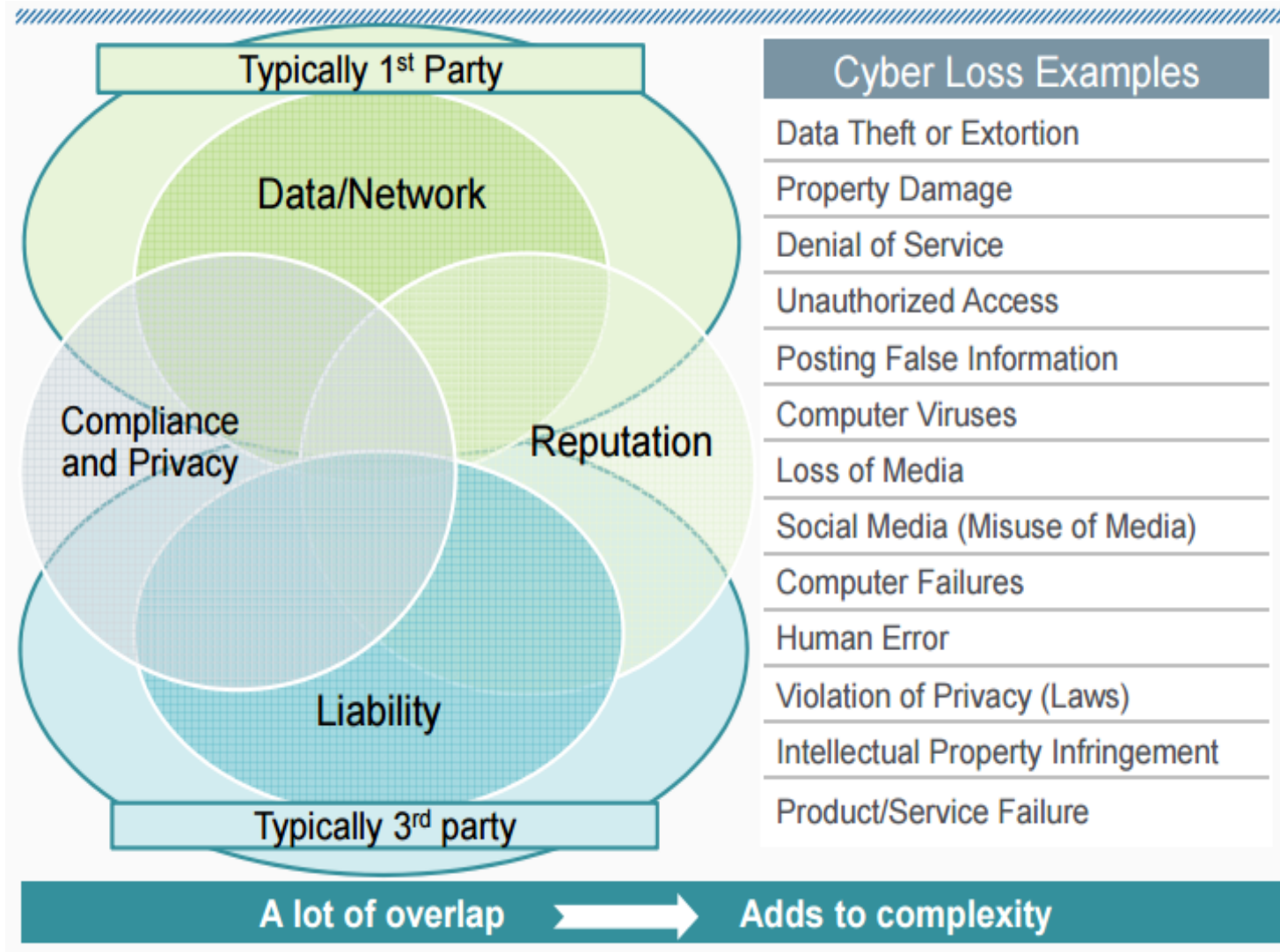
IV. Bilişim ile ilgili İşlerin Durması

Perakende işinde olan bir müşteri erişim sağlayıcı firmasının bilgisayar korsanlığı saldırısına maruz kalmasından etkilenmiştir. Bu senaryoda sigortacı perakende firmasının çevrim dışı olduğu tarih itibariyle gelir kaybını tazmin eder ve aynı korsanlık olayını takip eden üç ay boyunca gelir kaybının (itibarın zedelenmesine bağlı kayıp dahil olmak üzere) artçı darbelerine karşı teminat sağlar.

V. Hizmet Engelleme Saldırıları

Uluslararası Emlak şirketi IT sistemleriyle ilgili Hizmet engelleme saldırısı ile karşı karşıya kalmıştır; bu saldırı firmanın sadece operasyonel işlerini zarara uğratmakla kalmamış aynı zamanda ticari marka ve Pazar payına da potansiyel birkaç etkisi olmuştur. Sigortacı bu durumda sigortalının gelir kaybını teminat altına almak konusunda yardımcı olmakla kalmayıp itibar kaybının azaltılması için bir Halkla ilişkiler Uzmanı içinde ödeme yapacaktır.

BİLİŞİM RİSKLERİ SİGORTASI



BİLİŞİM RİSKLERİ SİGORTASI

Social Media/Blogging
Special Media Risk

Beyond Increased Breach Exposure.....

“Open”
Communication
Platform

Social
Media

Content Risks

Everyone is in the Publishing Business
Any person or organization, not just media companies,
can be sued for media content

