# Yeni dijital güven çağı

## Siber güvenliğin ötesine uzanarak toplumun dijital geleceğe hazırlanmasını sağlamak

BSI Dijital Güven Danışmanlık Hizmetleri Genel Müdürü Mark Brown ile bir tartışma

bsi.

# İçindekiler



# Özet

**Yazar: Mark Brown**

**BSI Dijital Güven Danışmanlık Hizmetleri Genel Müdürü**

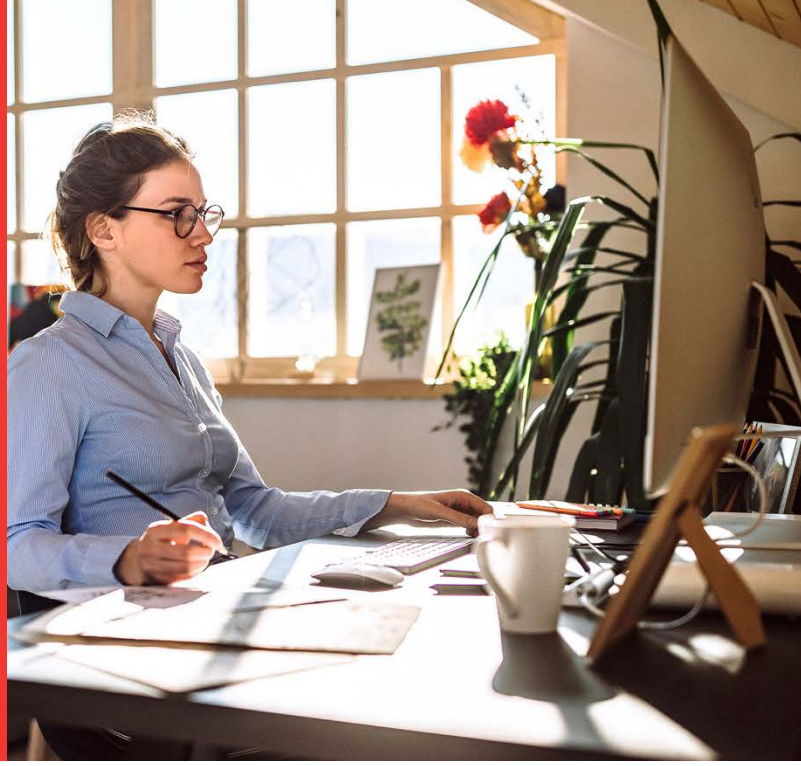
Mark Brown siber güvenlik, veri gizliliği ve iş dayanıklılığı danışmanlığı alanlarında 30 yılı aşkın deneyime sahiptir. Daha önce Wipro Ltd. ve Ernst & Young gibi şirketlerde görev almıştır. Nesnelerin İnterneti (IoT) ve genişleyen siber güvenlik pazarı alanında kapsamlı bir bilgi birikimine sahip olan Mark Brown siber güvenliğin stratejik etkinleştirme ve risk koruma bileşenlerine odaklı çalışmalar yürütmüştür.

Yaşamımızın gün geçtikçe artan bir şekilde Internet'e bağlı hale gelmesi nedeniyle, yanlış bilgilendirme, dijital dolandırıcılık ve kişisel ve dijital güvenlik arasındaki çizgilerin bulanıklaşması gibi yeni ortaya çıkan riskler kuruluşların ve toplumun dijital sistemlere ve teknolojilere duyduğu güveni zedeleyerek tehdit etmektedir.

Mark Brown bu yazısında aşağıdaki konuları tartışarak ele almaktadır:

- hızlandırılmış dijital dönüşümün kuruluşlar ve toplum açısından getirdiği sonuçlar;
- toplumun teknolojik ve siber risklere yönelik geleneksel yaklaşımlardan ziyade daha yaygın iş ve operasyon risklerini ele alan bir yaklaşıma doğru yaptığı geçiş
- dağıtılmış dijital tedarik zincirlerinin eşlenmesi ve yönetilmesi ile ilişkili zorluklar
- dijital güveni inşa etmenin ve yerleştirmenin, dijital dünyada faaliyet gösteren kuruluşların başarıya ve dayanıklılığa ulaşmasını sağlamada oynadığı kritik rol

**"Günümüzde hem işletmeler hem de bir bütün olarak toplum, sürekli gelişen bilgi teknolojisi dünyasında faaliyet gösterirken daha fazla çevikliğe ve hızlı uyum sağlama kabiliyetine ihtiyaç duymaktadır."**



# Statüko değişimi

Son yirmi yıl içinde dijital sistemlere artan bağlılık tüm dünya genelindeki toplumların davranış kalıplarında ve işleyişinde köklü değişiklikleri de beraberinde getirdi. Birçok sektörü hızlandırılmış bir dijital dönüşümden geçmek durumunda bırakan, çalışanların uzaktan veya hibrit çalışma modellerine geçiş yapmasını gerektiren ve bu değişimde kolaylaştırıcı rol oynayan platform, sistem ve cihazların sayısının katlanarak arttığı COVID-19 pandemisi de bu eğilimi daha belirgin bir şekilde ortaya koydu. Toplumların bu yeni dijital dünyaya geçişi hız kesmeden devam ediyor olsa da, siber suç tehditleri her zamankinden daha fazla görünüyor ve tüm dünya genelinde işletmelere tonlarca veya hatta yüzlerce milyon dolar maliyet yüklüyor.

Son yıllarda kötü amaçlı yazılım saldırılarının üç kat, fidye yazılımı saldırılarının ise dört kat artış göstermesiyle birlikte artık hem daha sık cereyan eden hem de daha gelişmiş siber güvenlik tehditleriyle karşı karşıya kalıyoruz. Üstelik bu saldırıların olumsuz etkileri maddi kayıp ve marka saygınlığının zedelenmesi gibi organizasyonel sonuçlarla sınırlı kalmıyor. Bu tür güvenlik olayları ulaşım altyapısı ile bilgi ve iletişim sistemlerine zarar vererek toplumsal bütünleşmeyi ve bireysel zihinsel sağlığını tehlikeye atabilir.

Büyük siber saldırılar halihazırda kuruluşların ve toplumların saldırıları etkin bir şekilde önleme ya da saldırılara yanıt verme kabiliyetini aşıyor. Doğrusu, kuruluşlar bu siber suç tsunamisi karşısında büyük çaba gösterse bile ancak yerinde sayabiliyor.

Bu durum çok önemli bir statüko değişimini tetikledi. Geçmişte kuruluşlar genel olarak esasen tehditlerin yönetimine ve iş ortamlarını korumaya odaklı bir siber güvenlik ve risk yönetim programı uyguluyordu. (bu genellikle iş operasyonlarını yavaşlatabilen, inovasyonu ve değişikliklere uyum sağlama kabiliyetini kısıtlayan, çok yoğun çaba gerektiren bir yaklaşımdı)

"Ancak, günümüzde hem işletmeler hem de bir bütün olarak toplum, sürekli gelişen bilgi teknolojisi dünyasında faaliyet gösterirken daha fazla çevikliğe ve hızlı uyum sağlama kabiliyetine ihtiyaç duymaktadır." Siber güvenlik programlarının ortamınızı hedefleyen her saldırıyı önlemeye odaklı bir şekilde tasarlanmaması, bunun yerine kritik iş fonksiyonlarının yürütülmesini mümkün kılmak ve desteklemek için algılama ve yanıt verme kabiliyetlerini geliştirebilecek ve operasyonların devamlılığını güvence altına alabilecek bir şekilde yapılandırılması önemlidir. Kısacası, siber saldırıların doğurabileceği etkileri, normal iş operasyonlarını sürdürebilme kabiliyeti ile dengeleyebilecek bir yaklaşım geliştirilmesi gerekmektedir.

**"Yeni dijital toplumlarda, teknolojinin başarısız kalması halinde en çok etkilenen alan operasyonlardır. Operasyonlar aksadığında ise neredeyse anında maddi gelir kaybı yaşanmaktadır."**

## Teknoloji odaklı bir tartışmadan operasyonel bir tartışmaya geçiş yapmak

Salt olarak teknolojinin sonuçlarına odaklanmak yerine durumu iş ve operasyonlar açısından daha geniş bir perspektiften ele alabilmek için kuruluşların (kullanıcıların) buna neden ihtiyaç duyulduğu konusunda eğitilmesi gerekir.

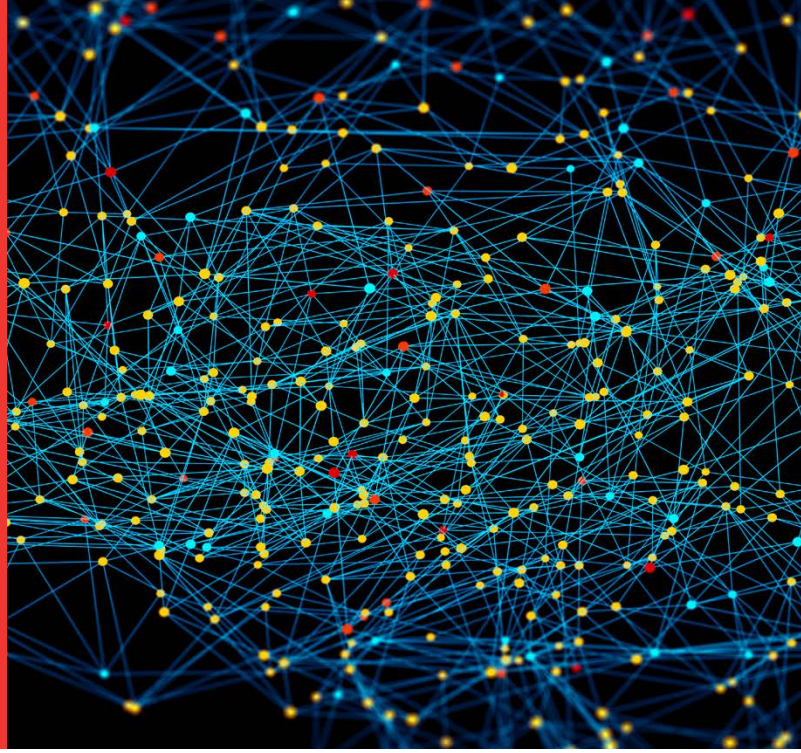
Birçok kuruluş Dijital Dönüşüm Direktörü [Chief Digital Officer (CDO)] veya Veriden Sorumlu Genel Müdür Yardımcısı [Chief Data Officer (CDO)] rollerinin öneminden bahsediyor fakat bu roller zaten uzun yıllardır işletmelerin sistematik bir parçası. Kuruluşlar "Elektrikten Sorumlu Genel Müdür" gibi bir rolden bahsetmiyor çünkü elektrik toplumun sistematik bir parçası ve herkeste zaten var.

BSI olarak, muhtemelen beş yıl sonra kimsenin artık Dijital Dönüşüm Direktörü [Chief Digital Officer (CDO)] veya Veriden Sorumlu Genel Müdür Yardımcısı [Chief Data Officer (CDO)] rollerinden bahsetmeyeceğini, zira bu rollerin zaten sistemin bir parçası haline geleceğini ve kuruluşlarda normal şekilde kendilerine yer bulacağını tahmin ediyoruz.

Burada önemli olan teknolojinin mistik yönlerini ortadan kaldırmak, teknolojiyi kuruluşun her kademesinden çalışanlarca tüketilebilir ve anlaşılabilir kılmaktır. Bilişim Kurulu Başkanı [Chief Information Officer (CIO) veya Baş Bilgi Güvenliği Yöneticisi [Chief Information Security Officer (CISO)]rolü gelecekte de çok önemli olacak fakat Operasyon Genel Müdür Yardımcısı [Chief Operations Officer (COO)] rolü ise ana karar vericilerden biri haline gelen, gelişen bir rol olarak karşımıza çıkıyor.

Yeni dijital toplumlarda, teknolojinin başarısız kalması halinde en çok etkilenen alan operasyonlardır. Operasyonlar aksadığında ise neredeyse anında maddi gelir kaybı yaşanmaktadır ve büyük bir şirkette bu kayıplar saatte onlarca milyon dolara tekabül edebilir. Dolayısıyla, dijital tehditlere yönelik bir yaklaşımın olmazsa olmazı iş risklerinin ve iş operasyonlarının sürecin bir parçası olarak ele alınmasıdır ve kuruluşların da bu yönde önemli bir değişikliğe gittiğini görüyoruz.

**"Aslında bilgi güvenliği süreci diye bir şey yoktur. BT süreci diye bir şey yoktur. Süreç, BT tarafından mümkün kılınan ve bilgi güvenliği tarafından korunan bir iş sürecidir."**



# Kullanıcı deneyimi üst düzey yöneticilerine yönelik tavsiyeler

Son yirmi ila otuz yıldır kuruluşların genel olarak BT ve siber güvenlik faaliyetlerini stratejik bir varlık yerine maliyet merkezi olarak değerlendirmiş olması, teknolojinin ve teknolojiyi yöneten teknologların hak ettiği değeri göremediği bir kültürün ortaya çıkmasına neden olmuştur.

BT'ye bu gözle bakılması nedeniyle, liderlik ekipleri genellikle paradan tasarruf etmek için BT faaliyetlerinin bir dış kaynaktan tedarik edilebileceğini ve böylece şirket içi bir BT departmanına sahip olmakla aynı faydaların elde edilebileceğini düşünmektedir. Ancak, bu durumda teknologlar çözümlerin işletmeye nasıl yardımcı olabileceğini gerçekten anlamak zorunda olmadan işletmeye teknik çözümler sunan sıradan çalışanlar olarak görülmesi nedeniyle işletme ve BT arasında bir kopukluk meydana gelmektedir.

Diğer taraftan da BT, yöneticiler ve yönetim kurulu üyeleri açısından herhangi bir anlam taşımayan süreçlere boğularak faaliyet gösterir. Gerçek dünyada, BT süreci veya siber güvenlik süreci diye bir şey yoktur. Sadece bir iş süreci vardır ve bu sürecin BT veya siber güvenlik ile mümkün kılınması gerekir.

Örneğin, yeni çalışanlar kuruluşlarının verilerine erişmeye gerek duyar ve yüksek pozisyonlara terfi ettiklerinde ya da şirketten ayrıldıklarında erişim izni düzeylerinin de buna uygun şekilde değişmesi gerekir. Ancak bu tür bir değişim BT olmadan meydana gelmez.

Kendim de Fortune 10'daki bir küresel şirkette CISO olarak görev yaptığım için Operasyon Genel Müdür Yardımcısı (Chief Operations Officer) rolünün ne anlama geldiğini yakından öğrenme fırsatını buldum. İşletmenin nasıl faaliyet gösterdiğini öğrendim. İşletmenin temelde nasıl işlediğini öğrendim.

CISO'lara tavsiyem: Sadece teknolojiye odaklanırsanız, yalnızca Bilgi Güvenliğinden Sorumlu Başkan (CIO) rolüne göre hareket ederseniz bu dönüşümü işletmenin bütününe yansıtabilecek misiniz?

" Burada önemli olan işletmenizin gerçekte ne yaptığını anlamanızdır. Kuruluşunuzun ana var olma amacı nedir? Her zaman şunu derim: "Aslında bilgi güvenliği süreci diye bir şey yoktur. BT süreci diye bir şey yoktur. Süreç, bilgi güvenliği tarafından mümkün kılınan ve korunan bir iş sürecidir."

Benim için CISO'nun temel rolü de budur. Desteklediğiniz iş süreçlerini iyice kavrayın, bu iş süreçlerinin başarısız olması durumunda nelerin ters gidebileceğini öğrenin ve CEO ve liderlik ekibi ile rolünüzü ve nasıl destek sağlayabileceğinizi konuşun ve iş üzerindeki etkilerinize odaklanın.

# Dijital tedarik zinciri riski

Bugün tanık olduğumuz açık bulut ve hızlandırılmış dijital dönüşüm ortamında, dijital tedarik zincirleriyle ilişkili riskler inanılmaz boyutlara ulaşmıştır. Yaklaşık 20 yıl önce bir kuruluş yürüttüğü operasyonların koşullarını ve ortamını çok kolay bir şekilde tespit edip anlayabiliyordu. Dijital ortamlarını büyük bir güvenlik duvarıyla çevirip bu güvenlik duvarının etrafında olup bitenlere odaklanabiliyorlardı.

Ancak, artık söz konusu perimetrenin ortadan kaldırıldığı yeni bir çağdayız. Her kuruluşun hem fiziksel hem de dijital bir tedarik zinciri bulunuyor. Dijital tedarik zincirindeki sorun, uygulanacak denetimlere ve güvenliğin nasıl konumlandırılacağına kendiniz karar verebileceğiniz şirket içi BT ortamlarının aksine, dijital tedarik zincirinde birlikte çalıştığınız üçüncü tarafın doğru seçimleri yapmasına bel bağlamış olacak olmanızdır.

BSI, 195 ülkede 77.500 müşteriye hizmet veriyor ve müşterilerimiz bize dijital tedarik zincirinin temel siber güvenlik risklerinden biri olduğunu söylüyor. Yakın zaman önce 150'den fazla müşteriyle görüşülerek yapılan bir araştırmada, kuruluşların %73'ü CISO ve COO'larının gündeminin ilk sırasında bu risklerin yer aldığını belirtmiştir. Konuştuğumuz kuruluşlardan biri bile bu alanda tam kontrole sahip olduğunu düşünmüyordu.

.BSI'ın siber güvenlik ile ilgili en iyi uygulamalar geliştiren lider bir kuruluş olması nedeniyle, bu durum bize şirketlerin risklerin yapısını ve riskleri nasıl yönetebileceklerini anlamasına yardımcı olabilmek ve kuruluşların ve toplumların dijital tedarik zinciri risklerinin etkilerini anlamasına ve ele almasına yardımcı olacak çözümler geliştirebilmek için söz konusu alanı tam anlamıyla kavramamız gerektiğini gösteren kritik bir işaretti.

**“Çözümlerinizin haritasını çıkararak, ortamınızın dışındaki tedarikçileri belirleyerek ve bu tedarikçilerin değer zincirleri ve iş süreci içindeki konumunu tespit ederek kritik kritik riskleri belirleyebilirsiniz.”**

## Süreç haritası çıkarmak

Dijital tedarik zinciri çevresindeki boşlukların tanımlanması çok zor olabilir. Dikkat etmeniz gereken taraflar sadece sözleşme yaptığınız taraflardan ibaret değildir.

Üçüncü taraf, dördüncü taraf ve beşinci taraf riskleri bulunur

Üretime dönük riskler, ara riskler ve tüketiciye dönük riskler bulunur.

Bağlantı noktalarının anlaşılabilmesi için iş sürecinin haritalanması gerekir.

Birçok kuruluş teknoloji cephesine bakarken sadece sahip oldukları teknoloji çözümlerini ele almaktadır. Bunları iş süreciyle eşleştirmemektedir.

Çözümlerinizin haritasını çıkararak, ortamınızın dışındaki tedarikçileri belirleyerek ve bu tedarikçilerin değer zincirleri ve iş süreci içindeki konumunu tespit ederek kritik risklerin haritasını çıkarabilirsiniz.

Sadece sözleşmenin büyüklüğüne bakmanız yeterli değildir, bu birçok kuruluşun yaptığı yaygın bir hatadır. Bir kuruluşa milyonlarca ödeme yapıyor olmanız bu kuruluşun kritik bir risk teşkil ettiği anlamına gelmez.

Yıllık faaliyet raporunuzu hazırlatmak için hizmet aldığınız bir şirket bu bağlamda uygun bir örnek olacaktır. Özellikle borsaya kote bir kuruluşsanız, kuruluşunuzun en hassas verilerinden bazılarını faaliyet raporunuz yayınlanmadan üç ila dört hafta önce bu gibi bir şirketle paylaşırsınız. Ancak bu şirketle yaptığınız sözleşme, kuruluşunuzun yıl içinde imzaladığı en düşük tutarlı sözleşmelerden biri olabilir ve bu tür düşük tutarlı sözleşmeler genellikle siber güvenlik perspektifinden dikkate alınmamaktadır.

Dolayısıyla, verilerin hassasiyetinin ve iş sürecinin önem düzeyinin anlaşılması ve ardından iş süreci ve değer zinciri haritasının çıkarılarak tedarikçilerin konumlandırılması önemli bir adımdır.

**“Dijital güven bir kuruluşun sadece iş ve teknoloji risklerinden korunmasından ibaret değildir, kuruluşun faaliyetlerini mümkün kılmak ve dijital dönüşümünü hızlandırmak için stratejik olarak nasıl bir yol izleyebileceğinin belirlenmesini içerir."**

# Yeni dijital güven çağını ele alma

Dijital güven, siber güvenliğin yeni adı değildir. Müşterilerin, kullanıcıların ve paydaşların bir işletmeye duyduğu güveni etkileyen çok daha fazla sayıda faktörü kapsar. Vizyonumuz bu dijital çağda müşterilerimize destek olmak; kanıtlar yoluyla işletmeler, insanlar ve nesneler arasında ilgi çekici, güvenli ve güvenilen etkileşimler kurulmasını sağlamak ve işletme karlılığını yükseltmektir.

BSI Group, bu yeni dijital güven çağını ele almak için danışmanlık hizmetlerini siber güvenlik alanının ötesinde dijital güvenle ilgili daha geniş bir alanı da kapsayacak şekilde genişletmiştir. Grup böylece müşterilerinin dijital tedarik zinciri risklerinden yapay zeka etiğine kadar çok farklı konuları ele almasına yardımcı olmaktadır.

BSI, 30 yıldır bilgi ve siber güvenlik dünyasıyla ilgili birçok gelişmeye öncülük etmiştir. BSI, 1995'te bugün ISO 27001 olarak bildiğimiz standardın ilk metnini kaleme almıştır. BSI olarak, müşterilerin teknolojiye ve dijital dönüşüme önemli miktarda para harcadığını ve bunu birçok farklı nedenle yaptığını tespit ettik.

COVID sonrasında dijitale duyulan ihtiyacın daha da hızla artmaya başlamasıyla birlikte, yeni bir dijital ekonomik toplumun ortaya çıktığını görüyoruz. Siber güvenlikle ilgili eski yaklaşımlara ait bazı bileşenler, risklerin olumsuz etkilerini önlemek için hâlâ gerekli olsa da müşterilerin şu gibi sorular yönelttiğini görüyoruz:

- Doğru yere yatırım yaptığımdan nasıl emin olabilirim?
- Paramın karşılığını aldığımdan nasıl emin olabilirim?
- Tedarikçilerime göre para harcadığım yerlerin gerçekten de fayda sağlayıp sağlamayacağını nereden bilebilirim?

Dolayısıyla, dijital güven bir kuruluşun sadece iş ve teknoloji risklerinden korunmasından ibaret değildir, kuruluşun faaliyetlerini mümkün kılmak ve dijital dönüşümünü hızlandırmak için stratejik olarak nasıl bir yol izleyebileceğinin belirlenmesini içerir.

Dört temel alandan yararlanmalarına yardımcı oluyoruz —

- siber güvenlik ve gizlilik
- dijital yönetişim ve risk yönetimi
- dijital tedarik zinciri
- yapay zeka etiği ve yönetişiminde veri yöneticiliği

Müşterilerimiz bu hizmetlerimizi son derece faydalı buluyor. Bu hizmetlerimiz müşterilerin teknoloji odaklı bir tartışmayı, kuruluş genelindeki daha fazla kişinin anlayabileceği yeni bir iş odaklı tartışmaya dönüştürmesine olanak sağlıyor.

**“Dijital güven bir kuruluşa güveni tesis etmek ve bu güven yoluyla çalışanlara, sistemlere ve teknolojilere güvenlik, emniyet, uyumluluk, gizlilik ve etik gereklilikleri karşılama gücünü vermektir”**

Mark Brown, BSI Dijital Güven Genel Müdürü

## BSI Hakkında

BSI olarak 1901'e dek uzanan, gururla baktığımız uzun bir geçmişe sahibiz. 1929'da, amacımızı şeffaf bir şekilde ortaya koyarak faaliyetlerimizi ve faaliyetlerimizin amacını belirleyen Kraliyet Tüzüğümüzü aldık.
1995'te dünyanın ilk bilgi güvenliği standardını geliştirdik.

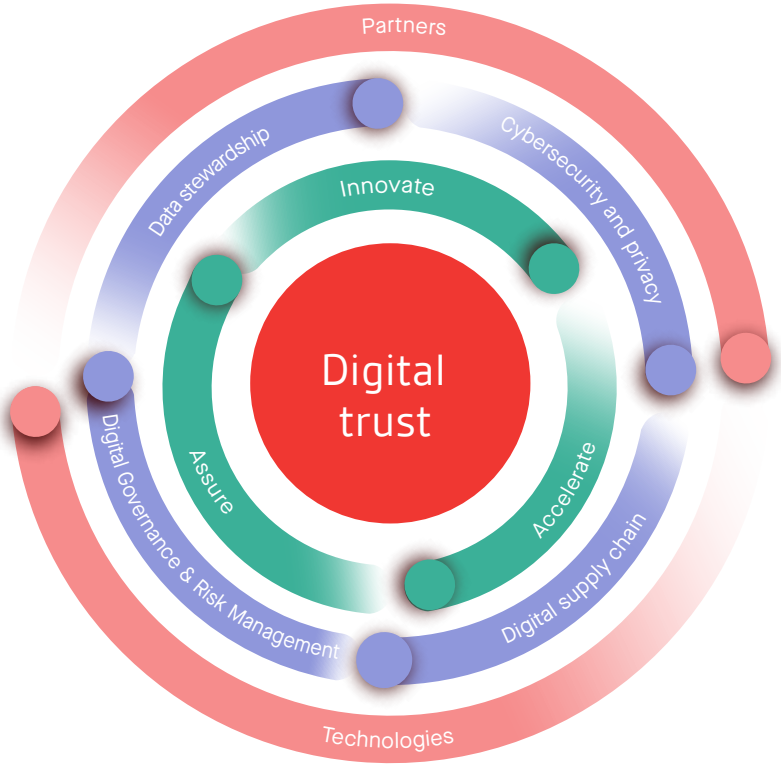
Bugün, 195 ülkeden 77.500 müşteriyle birlikte çalışarak siber güvenliği ve veri gizliliğini korumak suretiyle çalışanları, müşterileri, paydaşları ve toplulukları ile dijital güveni tesis etmelerine yardımcı oluyoruz. Her gün, yaptığımız her işte daha dayanıklı bir dünya için güven aşılamaya devam ediyoruz.

## BSI Digital güven hakkında

BSI Dijital güven olarak, global uzmanlığımız sayesinde müşterilerimizin kritik bilgi ve BT altyapılarını, çalışanlarını ve marka saygınlığını koruyarak siber dayanıklılıklarını güçlendirmesine olanak sağlıyoruz. Dijital ve siber risk danışmanlığı ve güvenlik testi hizmetleri sunarak; veri gizliliği, uyum ve yönetişim gibi alanları inceleyerek ve e-keşif ve e-delil toplama gibi niş alanları değerlendirerek entegre hizmet portföyümüzle kuruluşlara destek sağlıyoruz.

Dijital güven birbiriyle bağlantılı stratejiler, planlar ve eylemler yoluyla şu dört alt alanı bir araya getirmektedir:

1. Siber güvenlik ve gizlilik
2. BT yönetişimi ve risk iştahı
3. Veri yöneticiliği ve yapay zeka etiği
4. Dijital tedarik zinciri






**Bizimle iletişime geçin**

Telefon: +90 216 445 90 38
Email: bsi.eurasia@bsigroup.com
Ziyaret edin: bsigroup.com/tr

UK
+44 345 222 1711
digitaltrust.consulting@bsigroup.com
bsigroup.com/digital-trust

**Haber bültenimize abone olun**

**Bizi takip edin**