MARSH | TÜSİAD

2020 Türkiye Siber Risk Algı Araştırması

ARAŞTIRMA | 2020

2020 Türkiye Siber Risk Algı Araştırması

İÇİNDEKİLER

Giriş

2020 Türkiye Siber Risk Algı Araştırması, Türkiye'deki şirket ve kurumların siber risklere ve bilgi güvenliğine yönelik farkındalıklarını, tedbir alma reflekslerini görmek, bu alandaki yatırımlarını, ihtiyaçlarını ve beklentilerini anlamak üzere gerçekleştirilmiştir.

COVID-19 salgını öncesinde gerçekleştirilen bu çalışma kapsamında kurumların siber risk yönetim sürecinden sorumlu üst ve orta kademe yöneticileri ve uzmanlarının değerlendirmeleri alınmıştır.

Ayrıca üretim, enerji, havacılık, gıda gibi sektörlerde faaliyet gösteren Türkiye'nin önde gelen şirketlerinin üst yöneticileri ile görüşmeler gerçekleştirilmiştir.

Türkiye'de siber risklere yönelik algıyı; risk yönetim yaklaşımı, yeni teknolojiler ve kamu politikaları gibi çeşitli perspektiflerden değerlendirmesi açısından bir ilk olan araştırmamızın okuyucularımıza kendi şirketlerinin nerede olduklarını görmeleri açısından fikir vereceğini umuyoruz.

Anket ve mülakatlara katılarak görüş ve tecrübelerini paylaşan değerli katılımcılarımıza ve içerik konusunda destek veren TÜSİAD Bilgi İletişim Teknolojileri Çalışma Grubuna ve danışma kurulumuza teşekkür ederiz.

"Siber güvenliğe yönelik farkındalık ve yatırım büyük ölçüde siber saldırı deneyimi ve regülasyonlarla tetiklenmektedir."

Temel Bulgular

Siber Risk Farkındalığı ve Algısı

Siber risk şirketler için gün geçtikçe önem kazanan bir gündem konusudur.

- Türkiye'de siber güvenlik, reel sektörün son dönemde daha fazla odaklandığı ve daha sık gündemlerine giren bir alandır.
- Kurumların siber riskleri diğer risk başlıkları gibi önemsemeleri ve yönetmeleri gerektiğine yönelik farkındalık seviyesi artan bir trend göstermektedir.
- Türkiye'de risk yönetimi ve/veya bilgi teknolojilerinden sorumlu çalışanların %9'u kurumunun karşı karşıya olduğu en büyük riski siber tehdit olarak görmektedir. 2019 yılında benzer bir katılımcı kitlesi ile gerçekleştirilen Global Siber Risk Algı Araştırması'nda bu oran %22 düzeyindedir ve raporda siber risklerin her geçen gün daha da önem kazandığı ifade edilmektedir. Bu sonuçlar Türkiye'nin siber risk farkındalığı açısından henüz global şirketlerin oranını yakalayamadığını göstermektedir.

Siber güvenliğe yönelik farkındalık ve yatırım büyük ölçüde siber saldırı deneyimi ve regülasyonlarla tetiklenmektedir.

- Kurumların bu konudaki genel eğilimi 'bekle-gör' davranışı üzerinden şekillenmektedir.
- Kurumların kendileri ya da tanıdıkları/bildikleri bir kuruma yönelik bir problem/tehdit ile karşılaşmadan siber riski fark etme ve aksiyona geçme pratiğine sahip olmadıkları gözlemlenmektedir. Bir başka deyişle riskin varlığının kabul edilmesi ve önlem alınması için temel tetikleyici riskin gerçekleşmesi gerekmektedir (%78).
- Siber atakların bugüne kadar, işlerin yavaşlamasına-durmasına ve/veya finansal zarara sebebiyet verebilecek bir vaka yaşatmamış olması, siber güvenlik konusunun gündemde gerilerde kalmasının ardındaki temel nedendir.
- Siber güvenlik yönetimine yatırım yapan kurumların %77'si regülasyonların teşvik edici etkisi olduğunu belirtmektedir.
- Havacılık, finans, bilgi teknolojileri, enerji ve üretim sektörlerinde yer alan kurumların siber riskin yönetimi konusunda nispeten daha hassas ve bilgili davrandıkları görülmektedir. Buna, söz konusu sektörlerin doğası gereği risk ile karşılaşma olasılığının yüksekliği de eklendiğinde içselleştirme artmaktadır.
- Devletin yasa ile çerçevesini çizdiği ve takip ettiği konular kurumlar tarafından hem daha çok dikkate alınmakta hem daha çabuk içselleştirilmekte ve prosedürlere geçirilmektedir. Bu bağlamda KVKK, GDPR, ISO ve dünya/Avrupa standartları; EPDK, BDDK gibi sektör denetleme kurumları ile halka açılma süreçlerinden geçen/geçmiş kurumların SPK tarafından belirlenen mecburiyetleri siber risk konusunda harekete geçmeyi etkileyebilmekte ve yol göstermektedir.

COVID-19 ve son hızla devam eden dijital dönüşüm hem siber risk farkındalığını hem de risk olasılığını artırmaktadır.

- Kurumların teknolojiyi kullanma kapasitesi arttıkça ve dijitalleşme sürecinde ilerledikçe siber risklerin varlığına yönelik farkındalık da artmaktadır.
  - COVID-19 salgınının etkisiyle her alanda hızlanan dijital dönüşümün hem farkındalığı artıracağı hem de kurumları siber risk yönetimine yönelik daha fazla aksiyon almaya teşvik edeceği görülmektedir.
  - Nitekim, bu süreçte birçok kurumun tam olarak hazır olmadan hayli hızlı biçimde dijitalleşmesinin, atak/saldırı olasılıklarını yükseltmesi beklenmektedir.

Siber Risk Yönetimi

Siber risk yönetiminde yetkin ve yeterli insan kaynağı açığı en önemli konu olarak karşımıza çıkmaktadır.

Kurumlarda siber risk konusundaki sorumluluk genellikle IT/BT ekiplerinin üzerindedir (%77).

- Siber risk bu ekiplerin ana işi değildir. Bu nedenle de siber risk yönetimi açısından temel beklentinin atak ya da risk oluştuğunda önlem almak ya da aksiyon almak olarak çerçevelendiği görülmektedir. Risk potansiyelinin ölçümlenmesi, etki analizi, modelleme ve önlem stratejileri gibi konular daha geri planda kalabilmektedir.
- Kurumların büyüklüğü ve sektörel yapısına göre siber güvenlik sorumluluğu CTO/CIO/CSO/CICO pozisyonlarından biri ile paylaşılmakta, bir başka deyişle süreci C seviyesi yönetmektedir (%75). Özellikle bu seviyedeki yöneticilerin konuya yaklaşımları kurumun farkındalığını ve stratejisini doğrudan etkilemektedir.
- Yatırım kararı için en önemli dayanak noktası yine sektörden örnekler, dünyada/Türkiye'de benzer kurumların yaşadığı olumsuz deneyimlerdir. Büyük ölçekli kurumlar doğru bir strateji kurabilmek için tarafsız bir kurumdan danışmanlık alabilmektedir (%56).

Şirketler riskin tespiti ve yönetiminden çok azaltılmasına odaklanmaktadır.

- Şirketlerin risk yönetimi konusundaki öncelikli refleksi riski azaltıcı uygulamaları hayata geçirmektir (%78).
- En çok cihazların güvenliğini artırmaya, sisteme/ağlara hem şirket içinden hem de dışından erişimi daha güvenli hale getirmeye yönelik yatırımlar yapılmaktadır.
- Siber riski ölçme, yönetme ve önleme süreçleri belirgin yatırımlar istemektedir. Bunların başında altyapı, organizasyon ve insan kaynakları gelmektedir.
- Şirket yönetimleri bu yatırımları yapma konusunda daha çekimser davranabilmekte; bu aşamalarda daha çok penetrasyon, zafiyet analizleri ile yetinmektedir(%50).

Yeni Teknolojiler ve Siber Riskler

Temel Bilişim Teknolojileri hem çok cazip hem de çok riskli bulunmaktadır.

- Temel bilişim teknolojileri şirketlerin operasyonlarında önemli bir yere sahiptir. (%77).
- Şirketlerin büyük bölümü yeni teknolojileri kullanma kararı aldıktan sonra risk değerlendirmelerini keşif ya da başlangıç aşamasında yapmaya başlamaktadır. Ancak risk tespiti konusunda refleksleri gelişmemiş kurumlarda (%33) bu değerlendirme daha sonraki aşamalara bırakılabilmekte ve bu nedenle etkin sonuçlar alınamamaktadır.

Tedarik Zincirinde Siber Risk Yönetimi

Siber güvenlik açısından tedarikçiler önemli risk kaynağı olarak görünmektedir.

- Kurumların %70'i tedarikçilerin siber güvenlik açısından risk taşıdığını düşünmekte, %36'sı ise bu risk düzeyini yüksek bulmaktadır.
- Özellikle dış kaynaklı hizmet sağlayıcıları ve geçici çalışanlar/ danışmanlar bu açıdan kurumların yumuşak karnı olarak tanımlanmaktadır.

Siber Risk Sigortası

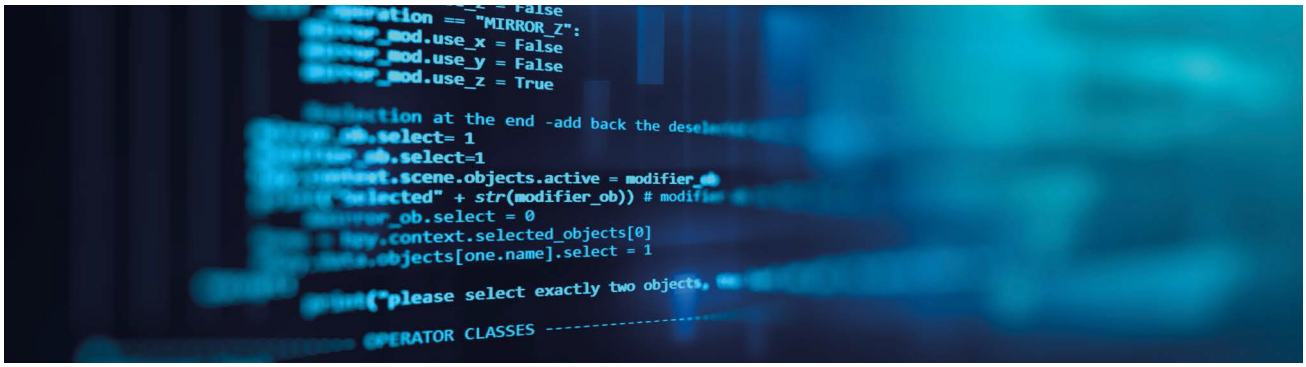
- Siber riski yönetimi konusunda adım atmaya başlamış olan kurumların, kısa ve orta vadeli planlarının içine siber yönetim stratejilerinin alınabilmesi önemli bir gelişme olacaktır.
- Bu gelişmenin önemli bir adımı siber risk sigortasıdır. Şirketlerin siber güvenlik alanındaki olgunlukları, siber risk sigortasına yatkınlıklarını olumlu yönde etkileyecektir.
- Kurumların büyük çoğunluğu siber risk sigortası hakkında yeterli bilgiye sahip değildir. Bu durum; sigortanın kapsamına güvenilmemesi ile birlikte siber risk sigortası alınmasının önündeki en önemli bariyerlerdendir.
- Siber risk sigortası sahiplerinin %86'sı sigortanın kendilerini koruyacağına güven duymaktadır, bu oran sigorta sahibi olmayanlarda %34 düzeyindedir.

Siber risk sigortası sunan kurumların da poliçe alımı süreçlerini şirkete özel tasarlaması, primlerin hesap sistemini şeffaflaştırması, kurumun ihtiyaçları ile ürün detayları arasında belirgin bağ ve referanslar oluşturması önemlidir. Bu durum siber risk sigortası ihtiyacının üst yönetime detaylı anlatılması ve yöneticilerin ikna edilmesi konularında siber güvenlikten sorumlu ekip ve yöneticilerin işini kolaylaştıracaktır.

Kamu Etkisi

Kamunun farkındalığı artırma ve yatırıma teşvik etme gücü önemlidir ancak beklenti bununla sınırlı değildir.

- Yasa ve yönetmeliklerin kurumların siber risk farkındalıkları üzerinde 'mecburi' bir etki gücü bulunmaktadır.
- Sektör temsilcilerinin kanun koyucular ile bir araya gelip görüş bildirmeleri, kuralların sektörler özelinde detaylı tasarım süreçlerine dahil olmaları beklenmektedir.
- Kamunun özellikle dış ülkelerden kaynaklanabilecek siber tehditler konusunda daha aktif bir rol üstlenmesi de beklenmektedir.



Siber Risk Yönetimine Bakış

Şirketler İçin En Önemli Risk Faktörleri

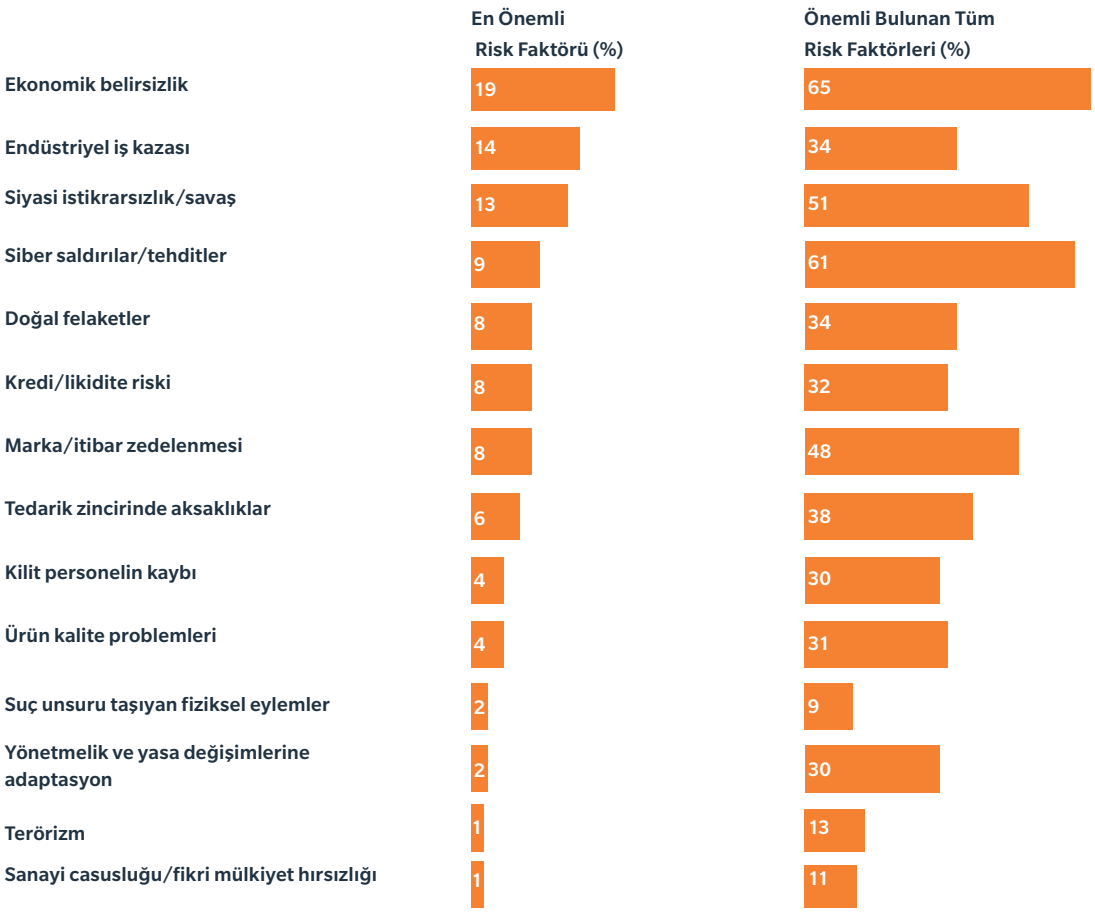
Ülkemizde özel sektörde risk yönetimi, Finans ve Enerji gibi sektörler içerisinde bu alana yönelik yatırımların ve organizasyonel yapıların kurulması ile başlamıştır. Risk yönetimi tarihinin ülkemizdeki son 10 yılına baktığımızda, farkındalık seviyesinin Perakende, Üretim, Havacılık gibi farklı sektörlerde de önemli ölçüde arttığını görüyoruz. Şirketlerde Risk Yönetimi birimlerinin kurulması, bu alanda yetişmiş insan kaynağının istihdam edilmesi ve finansal kaynak ayrılması gibi ölçütler önem derecesinin ve olgunluk seviyesinin artışını göstermektedir. Bu çerçevede baktığımızda araştırmamızın ilk bölümünde kurumların siber risklere bakış açısını ve kurumsal risk yönetimi içerisinde siber riskleri nasıl ele aldıklarına ilişkin içgörü kazanmak hedeflenmiştir.Araştırmanın tamamlandığı tarihte COVID-19 salgını henüz Türkiye'de görülmemiştir. Salgının siber risk algısı üzerindeki etkilerine ilişkin değerlendirmelere çalışmanın ilerleyen bölümlerinde yer verilmiştir.

Katılmcılarımızın şirketleri için en önemli gördükleri 5 risk başlığına ilişkin yaptıkları değerlendirmede, %61'i siber saldırılar ve tehditler faktörüne ilk 5 içerisinde yer vermiştir. Araştırmaya katılan çalışanların %19'u firmaları için en önemli risk faktörünü ekonomik belirsizlik olarak tanımlamış olup, %9'u siber saldırılar ve tehditleri ilk sıraya koymuştur. Marsh ve Microsoft tarafından 2019 yılında gerçekleştirilen Global Siber Risk Algı araştırmasında benzer profildeki katılımcıların %22'si siber saldırıları ve tehditleri en önemli risk faktörü olarak değerlendirmiştir. Bu oranın Türkiye'de %9 düzeyinde olması ülkemizde siber risk yönetimi konusunun öncelik seviyesinin diğer ülkelere kıyasla henüz düşük olduğunu göstermektedir.

ŞEKİL 1

10 kurumdan 6'sı için siber risk en önemli ilk 5 risk faktörü arasında yer almaktadır.

S: Şirketiniz için en önemli bulduğunuz 5 risk başlığını önem sırasına göre belirtiniz.

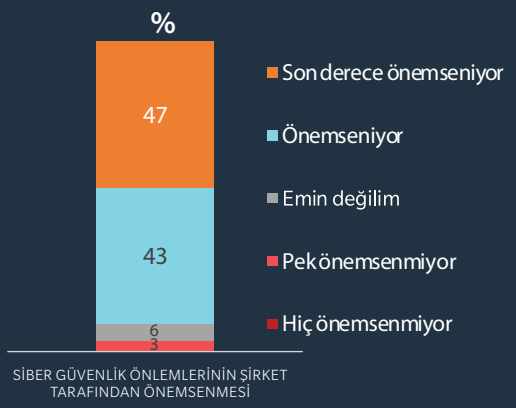


Siber Risk Yönetimine Yaklaşım

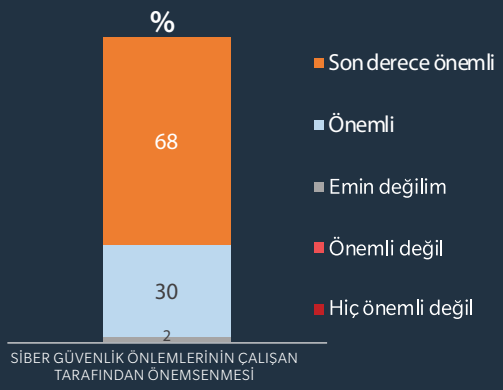
ŞEKİL 2

Çalışanlar siber güvenlik önlemlerine şirketlerinden daha fazla önem vermektedir.

S: Siber riskler ve bu risklere yönelik alınan siber güvenlik önlemleri genel olarak şirketinizde ne kadar önemseniyor?



S3. Siz ne kadar önemli buluyorsunuz?



Genel risk algısından siber risk yönetimine yaklaşıma doğru gittiğimizde anket katılımcıları siber risklerin önemsenme oranını bireysel ve kurumsal açıdan değerlendirdiler.

Hem kurumsal hem de bireysel düzeyde siber risk konusu son derece önemli bulunmaktadır. Ancak çalışanlar, bu konuyu şirket yönetimine kıyasla daha çok önemsediklerinin altını da ayrıca çizmiştir. Bu fark büyük ölçüde araştırmaya katılanların çoğunluğunun Bilgi Sistemleri ve Güvenliği ekibinde yer almasından ve siber risk sahipliğinin bu birimler üzerinde olmasından kaynaklanmaktadır. Nitekim, siber risk yönetiminin sahipliği ve sorumluluğu hangi birimdedir sorusunda katılımcılar öncelikli olarak Bilgi Teknolojileri ve Bilgi Güvenliği birimlerini adreslemektedir.

"Ben çok önemsiyorum ancak çalıştığım şirket benim kadar önemsemiyor."

Siber Güvenlik İle İlgilenen Birimler Ve Özellikleri

Siber güvenlik yönetimi, kurumlar tarafından sadece risk değerlendirmenin bir parçası değil aynı zamanda özel uzmanlık isteyen bir konu olarak değerlendirilmekte ve bu nedenle de özellikle Bilgi Teknolojileri departmanının öncelikli alanına dahil edilmektedir. Siber güvenlik yönetim sürecini yürüten ekiplerin büyük bölümü doğrudan üst yönetime raporlamaktadır. Bu şekilde ele alındığında kurumların %75'inde siber güvenlik yönetimi, takibi, risk azaltıcı aksiyonların alınması gibi konuların doğrudan (%10) ya da dolaylı olarak (%65) Üst Yönetim ve Yönetim Kurulu seviyesinde ele alındığı görülmektedir.

Kurum içi siber güvenlik yönetiminin sahibiyeti açısından Türkiye'deki kurumlar, dünya geneli ile benzer bir yapılanma içindedir. Katılımcılardan son 1 yıl içerisinde katıldıkları yönetim toplantılarında kaç defa siber risk konusunun gündem maddesi olduğunu değerlendirmelerini istediğimizde, %73'ü en az birkaç kez siber risklere ilişkin görüştüklerini belirtmektedirler. Siber güvenlik konusunun gündeme taşınma sıklığı ile üst yönetimin bu konuyla ilgilenim düzeyi arasında önemli bir paralellik bulunmaktadır. Üst Yönetim seviyesinde siber risk farkındalığı ve sahipliği arttıkça, bu konu şirket gündemlerinin daha önemli bir parçası haline gelecektir. Siber güvenlikten sorumlu olan birimler içerisindeki çalışan sayısı ortalama 4 kişiden oluşmakta olup, olgunluk seviyesi en yüksek sektörlerden olan finans sektöründe bu rakam 2 katına çıkmaktadır. İçinde bulunulan sektörün siber ataklar açısından cazip olması, siber olayların yaratacağı finansal zarar ve itibar kaybı ile sektörde daha önce siber atakların yaşanmış olması şirketlere daha fazla personel istihdamı ve diğer yatırımların yapılması açısından itici güç olmaktadır.

Siber güvenlik konusuyla hangi birim ilgileniyor?	İlgili departman hangi birime rapor ediyor?
%77 Bilgi Teknolojileri / Bilgi Güvenliği	%65 Üst Yönetim / Yönetim Kurulu
%10 Üst Yönetim / Yönetim Kurulu	%21 Bilgi Teknolojileri / Bilgi Güvenliği
%3 Risk Yönetimi	%4 Finans

ŞEKİL 3

Firmaların %87'si son 1 yıl içinde yönetim toplantılarında siber güvenlik konusunu en az 1 kez tartışmış. Her 10 firmadan 3'ünün ise gündeminin önemli bir konusu olarak yer alıyor.

S: Geçtiğimiz 1 yıl içinde herhangi bir yönetim toplantısında siber güvenlik konusu gündeme geldi mi?

Gündeme hiç gelmedi	**%13**
Bir kez konuştuk	**%13**
Birkaç kez gündeme geldi	**%46**
Çoğu kez gündemimizde yer aldı	**%24**
Bütün toplantılarda gündemimizde yer aldı	**%3**

Siber Risk Yönetiminde Şirketlerin Yaşadığı Zorluklar

Siber risk yönetimini içinde bulunulan sektörün dinamiklerine, şirketin ihtiyaçlarına ve faaliyet alanına uygun bir şekilde kurgulamak için şirketlerin farklı açılardan ele alması gereken konular bulunmaktadır. Bilgi Sistemlerinin karmaşıklığı, üçüncü taraflara bağımlılık, bu alana ayrılan kaynak, çalışan farkındalığı gibi farklı konu başlıklarını aynı anda ve doğru bir şekilde yönetmek her zaman mümkün olmamaktadır. Araştırmaya katılanlardan bu bakış açısıyla siber risk yönetiminde yaşadıkları en büyük zorlukları değerlendirmelerini istediğimizde en zayıf halkanın "insan" faktörü olduğu görülmektedir. Siber güvenlikten sorumlu olan personelin birden fazla alanda sorumluluğu olması nedeniyle siber güvenlik alanına yeterince zaman ayıramaması şirketler için en büyük zorluk olarak karşımıza çıkmaktadır. Bununla ilişkili olarak ayrı bir siber güvenlik ekibinin olmaması siber güvenlik yönetiminde şirketlerin yaşadığı zorluklar sıralamasında üçüncü sırada yer almaktadır. Şirketler nitelikli siber güvenlik çalışanlarının işe alınması ve devamlılıklarının sağlanması konusunda problem yaşamaktadır. Ülkemizde akademik ve akademik olmayan alanlara yapılan yatırımlar artmakta olup; üniversitelerde ilgili bölümlerin açılması ve genç girişimcilerin yönelimi artışa ivme kazandırmaktadır. Farkındalık ve yönetişim yapısı, "insan" faktöründen sonra şirketlerin yaşadığı diğer önemli zorluklar arasında olup; standart, güncel, ölçülebilir ve izlenebilir bir siber risk yönetimi yapısının kurulmasının ve tüm çalışanların anlayabileceği ve sahiplenebileceği seviyede tutulabilmesinin önemini göstermektedir.

Her yıl Dünya Ekonomik Forumu'nda sunulan ve Marsh'ın ana partnerlerinden biri olduğu Küresel Riskler Raporu'nun COVID-19 salgınına özel olarak 2020 yılında güncellenmiş versiyonunda ilk 3 en önemli risk başlığı içerisinde çalışma modelindeki değişimden dolayı siber saldırı ve veri sahtekarlığında artış olması yer almaktadır. Dolayısıyla siber risk yönetiminde şirketlerin karşılaştığı zorlukları destekler nitelikte yetişmiş insan, farkındalık ve doğru kurgulanmış bir risk yönetimi metodolojisi salgın sonrası iş dünyasında da önemini koruyacaktır.

ŞEKİL 4

Siber risk yönetimine odaklanan ve bu konuda uzmanlaşmış insan kaynağı ihtiyacı her geçen gün daha fazla artmaktadır.

S: Siber risk yönetimi açısından şirketinizin yaşadığı en büyük zorluklar nelerdir?

Siber Risklerin Tespiti, Değerlendirilmesi ve Ölçülmesi

Siber Risk Yönetimi Uygulamalarına Yönelik Güven Algısı

Risk yönetimi uygulamaları risklerin tespiti, değerlendirilmesi ve önlem alınması temeline dayanmaktadır. Bu anlamda siber risk yönetiminde etkin bir yapı kurulması şirketlerin siber riskleri proaktif veya reaktif bir yaklaşımla ele alınması ile yakından ilişkilidir.

Proaktif bir risk yönetimi yapısı bütünleşik ve güncel bir metodoloji kullanılarak risklerin önceliklendirilmesi ve aksiyonların takip edilmesi yoluyla gerçekleşir. Bunun için farklı yöntemler kullanılabilir, önemli olan yöntemin şirketin faaliyet alanına, kültürüne ve sektörüne uygun olmasıdır. Reaktif bir yaklaşımda bir olay yaşanması durumunda söz konusu olay çerçevesinde tespit edilen risklere yönelik aksiyon alınması ve uygulanması söz konusudur. Her iki durumda da şirketler aksiyon alamayacakları veya almalarının maliyetli olacağı riskleri Siber Sigorta yoluyla transfer etmeyi tercih edebilirler.

Siber risk yönetiminin alt kırılımlarına ilişkin katılımcılarımızdan bir değerlendirme yapmalarını istediğimizde, önemli bir çoğunluğunun siber risk yönetimine ilişkin şirketlerinin uygulamaları konusunda bilgi ve fikir sahibi olduğu görülmektedir. Siber tehditlerin değerlendirilmesi, ölçülmesi, önlenmesi ve müdahale edilmesi açısından çalışılan kuruma güven duyulmaktadır.

Siber sigortaya ise daha şüpheli yaklaşılmaktadır. Araştırmaya katılanların %20'si siber risklerin sigortalanmasına ilişkin şirket içindeki uygulamalardan haberdar değildir, haberdar olanlarda ise güven seviyesi %53 düzeyiyle diğer uygulamalara kıyasla çok daha geride kalmaktadır. Sonuç olarak, siber sigorta poliçesinin kapsamı ve hasarları karşılamasına ilişkin güven seviyesinin henüz düşük olduğu gözlemlenmektedir.

Ülkemizde Telekom, Finans, E-Ticaret gibi sektörler dışında henüz yaygın olmayan siber sigorta ile ilgili bilgi ve farkındalık düzeyinin düşük olmasının güven seviyesine yansıdığı görülmektedir.

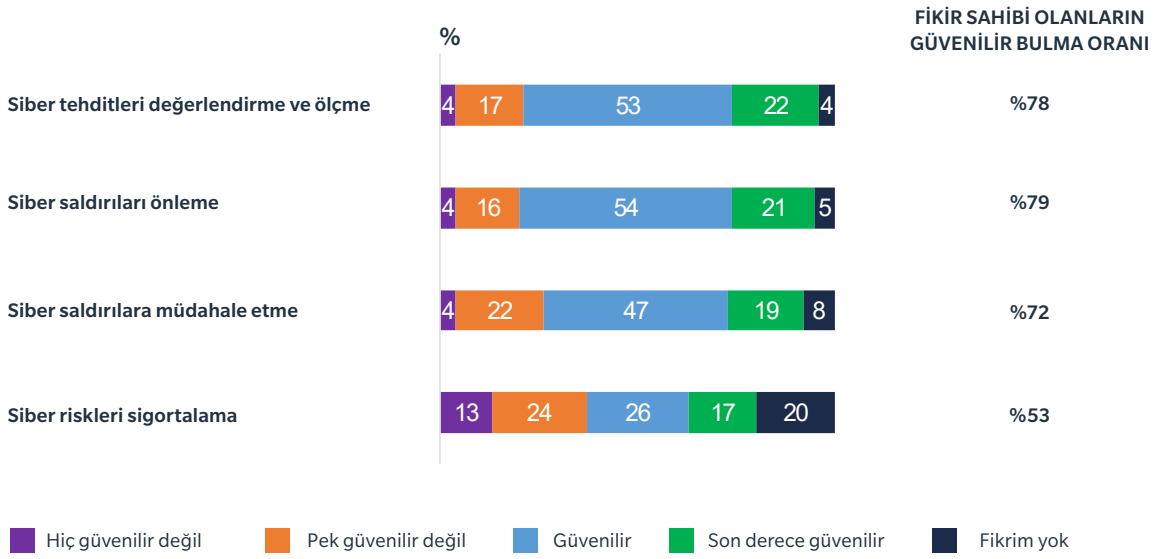
Tüm alanlar için şirketlerin uygulamalarını çok güvenilir seçen katılımcılar %8 oranındadır. Marsh & Microsoft tarafından 2019 yılında gerçekleştirilen Global Siber Risk Algı Araştırması'nda bu sonuç %11 olarak görülmektedir. Çalışanların şirketlerinin siber güvenlik konusunda yaptıkları yatırımların yetersiz olduğuna inanmaları, siber dayanıklılığa ilişkin güven seviyesinin düşük olmasında kısmen rol oynamaktadır.
Bu ürün ve hizmetler daha çok siber riskleri önleme veya azaltma amacına hizmet ederken, siber dayanıklılığın sağlanmasına katkıda bulunmamaktadır. 2019 yılında siber güvenlik ürünlerine ilişkin pazarın 124 milyon dolar seviyesinde olduğu öngörülmüştür. Buna karşılık siber suçların şirketlere yarattığı maliyet 1 trilyon dolar olarak tahmin edilmektedir.

"Yönetim Kurulu üyelerinin siber saldırıları önleme ve müdahale uygulamalarına güveni düşük seviyededir."

ŞEKİL 5

Siber risk yönetiminin bir parçası olarak sigorta en az bilinen ve güven duyulan uygulamadır.

S: Siber risk yönetimi ile ilgili olarak aşağıdaki konularda şirketinizin uygulamalarını nasıl buluyorsunuz?



Aşağıda yer alan tabloya göre; siber sigortası olan şirketler genel olarak bütün uygulamalar konusunda kendilerini daha güvende hissetmektedir. Öte yandan siber sigorta algısı iki grup arasında en çok farklılaşan konu olarak görülmektedir.

Siber sigortası olmayan şirketlerin, bu hizmete olan güvenlerinin son derece düşük olması, siber sigorta tercihinde önemli bariyerlerden birinin güven olduğunu ortaya koyuyor.

ŞEKİL 6

Siber sigorta tercihinde önemli bariyerlerden birinin güven olduğunu görüyoruz.

S: Siber risk yönetimi ile ilgili olarak aşağıdaki konularda şirketinizin uygulamalarını nasıl buluyorsunuz?

	Siber Sigortası Olanların Güvenilir Bulma Oranı	Siber Sigortası Olmayanların Güvenilir Bulma Oranı
Siber tehditleri değerlendirme ve ölçme	%88	%78
Siber saldırıları önleme	%91	%77
Siber saldırılara müdahale etme	%77	%76
Siber riskleri sigortalama	%86	%34
	n:34	n:69

Siber Risk Belirleme ve Ölçümleme

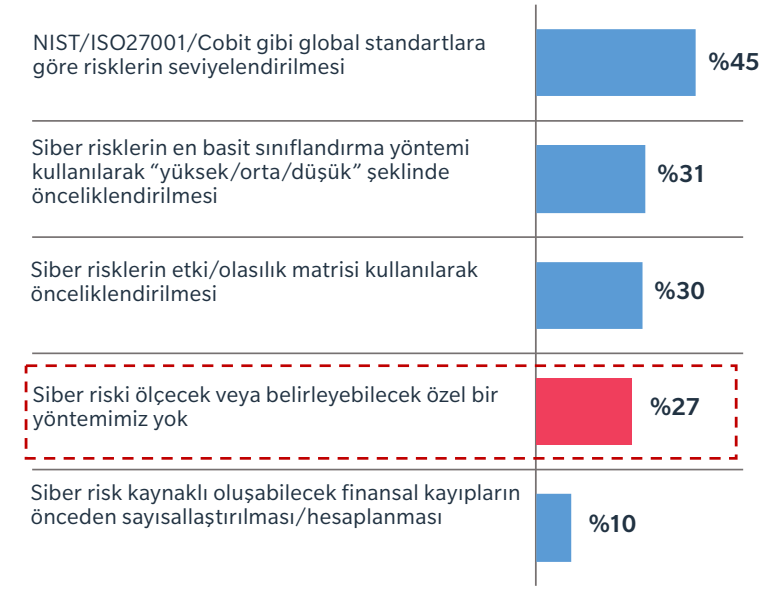
Siber risklerin tespiti ve değerlendirilmesinde faaliyet alanı, sektörün beklentileri, olgunluk seviyesi, üst yönetimin sahipliği gibi farklı etmenler rol oynamaktadır. Ülkemizde risk yönetimi organizasyonlar içerisinde kendisine daha fazla yer bulurken, siber riskler çoğunlukla ayrı bir kategori olarak değerlendirilmiştir. Bu durum yalnızca yönetişim ve organizasyon içerisindeki sahipliğine değil, kullanılan metodolojilere de yansımıştır.

Araştırmaya katılan her 4 kişiden 1'i siber riski ölçecek veya belirleyecek bir metodolojileri bulunmadığını söylemiştir. Buna şirketlerin iş sağlığı ve güvenliği, sigorta yönetimi ve kurumsal risk yönetimi gibi farklı başlıklar altında riskin tespit edilmesi ve ölçülmesi konusunda belirlenmiş bir yaklaşımları olmasına rağmen bunu siber riskler alanında uygulamaya geçirememeleri kısmen bir neden olabilir. Bunun dışındaki şirketlerin çoğunlukla bu alana özel NIST ve ISO standartlarını takip ettiği görülmektedir. Siber risklerin sayısallaştırılması konusunda şirketlerin yalnızca %10'unda çalışmalar yapılması, siber risklerin finansal etkisinin öngörülerek buna uygun bir risk yönetimi ve transferi mekanizmasının oluşturulması tarafının da gelişmeye açık olduklarını göstermektedir. Bu amaçla siber senaryolar yaratılması, yaşanabilecek kayıpların analiz edilerek sayısallaştırılması riskin finansal boyutunun üst yönetim seviyesinde anlaşılmasına katkıda bulunarak yapılacak yatırımlarda ve siber risk sigortasına ilişkin değerlendirmelerde şirketlere kılavuzluk edebilecektir.

ŞEKİL 7

Siber risk belirleme ve ölçümlemelerde global standartların kullanımı oldukça yaygındır. Herhangi bir yöntemle risk ölçümü yapan firmalar bazında bakıldığında global standartların kullanımı %62 düzeyine çıkmaktadır.

S: Şirketinizde siber riskleri belirlemek ya da ölçmek için hangi yöntemleri kullanıyorsunuz?



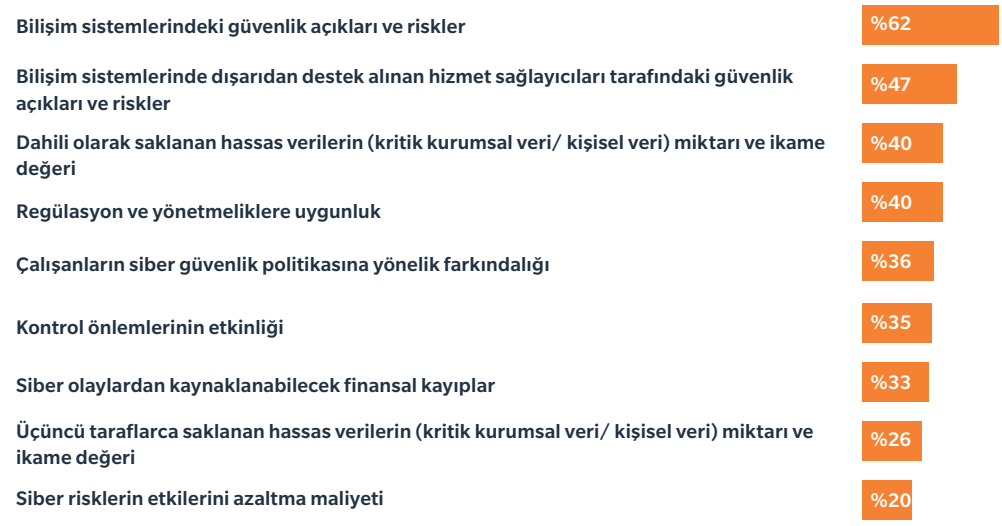
Toplam Baz (n): 108 - Yönetimi Bilenler

Siber risklerin tespit edilmesi ve ölçülmesi sürecinde şirketlerin önceliklerinin değiştiği görülmektedir. Bu öncelikler, tutulan veri tipi, bilgi sistemlerinin karmaşıklığı ve üçüncü taraflara bağımlılığı, düzenleyici kurumlardan gelen siber güvenliğe ilişkin ek önlemler (BDDK, EPDK gibi kurumlar), ulusal düzenlemeler gibi değişkenlere göre farklılaşabilmektedir. Son iki yıldır Kişisel Verilerin Korunması Kanunu'na uyum sürecinin başlaması ile birlikte şirketlerin mevcut bilgi güvenliği yönetimi sistemlerini kanuna uyumlu hale getirmek için çalışmalarını hızlandırdığını ve bu alandaki uzmanlarla daha fazla çalıştıkları görülmektedir. Özellikle dünya çapındaki atakların, regülasyonlardaki majör değişikliklerin ve Bilgi Sistemlerinde dış kaynak kullanımının yaygınlaşması şirketler için siber risklerini değerlendirme konusunda önemli bir motivasyon kaynağı olmaktadır. Araştırmamıza katılan çalışanların %62'si bilgi sistemlerindeki olası zaafiyetlerinden dolayı riske maruziyetlerinin fazla olduğunu ve bu nedenle siber risklerin belirlenmesi ve ölçülmesine yönelik çalışmalar yaptıklarını belirtmiştir. Bilgi sistemleri konusunda dışarıdan destek alınması kurumlar için bilinmezliği arttırması açısından ikinci sırada yer almaktadır. Birlikte çalıştıkları tarafların siber riskler konusundaki önlemlerinin seviyesi ve şirketin yaklaşımı ile tutarlılığı riske maruziyet konusunda şirketlerin endişelerini arttırmasını, siber risklerin belirlenmesi konusunda itici bir güç olmaktadır. Şirketin veritabanlarında tuttuğu ticari ve kişisel verilerin dışarı sızması, bozulması ve kaybolmasına ilişkin endişeler siber risklerin tespit edilmesi ve değerlendirilmesinde dikkate alınan 3. önemli başlık olarak karşımıza çıkmaktadır.Tutulan verilerin kritikliği nedeniyle yaşanabilecek bir siber olayın; operasyonların durması, itibar kaybı, finansal kayıp, düzenleyici kurumlardan gelecek cezalar gibi konuları tetikleyecek olması bu değerlendirmede belirleyici olmuştur.

ŞEKİL 8

Siber risk tespit ve ölçümlemede bilişim sistemindeki güvenlik açıkları ve riskler en öncelikli konudur.

S: Şirketiniz siber risklerin tespit edilmesinde ve ölçülmesinde aşağıdakilerden hangilerini dikkate alıyor?



Yöntemleri bilenler (n): 108

%38 risk belirlemede siber senaryoların finansal etkilerinin sayısallaştırılması ve maliyetlerinin hesaplanması gibi sayısal değerlendirme yöntemlerini kullanmadıkları görülmektedir.

Kantitatif/Sayısal Yöntemleri Tercih Etmeme Nedenleri

Ölçümle ilgili maliyet ve çabayı gerektiren bir riske sahip olunmaması	%34
Sayısal/nicel olmayan diğer yöntemlerin yeterli olması	%22
Bütçe/finansman yetersizliği	%13
Kuruluşun sayısal/nicel modelleme yapacak becerilere veya uzmanlığa sahip olmaması	%9
Risk modellerinin, siber tehditlerin hızlı gelişimine ayak uyduramaması	%9
Etkili bir ölçüm ve modelleme için verilerin yetersiz olması	%9

Yöntemleri bilenler (n): 42

Riski Tespit / Azaltma ve Yönetme Eylemleri

Son 1 yıl içinde şirketler tarafından siber risk tepiti, yönetimi ve riskin azaltılmasına ilişkin pek çok önlem alınmıştır ancak şirketlerin öncelikli odağı büyük ölçüde riski azaltıcı faaliyetler olmuştur.

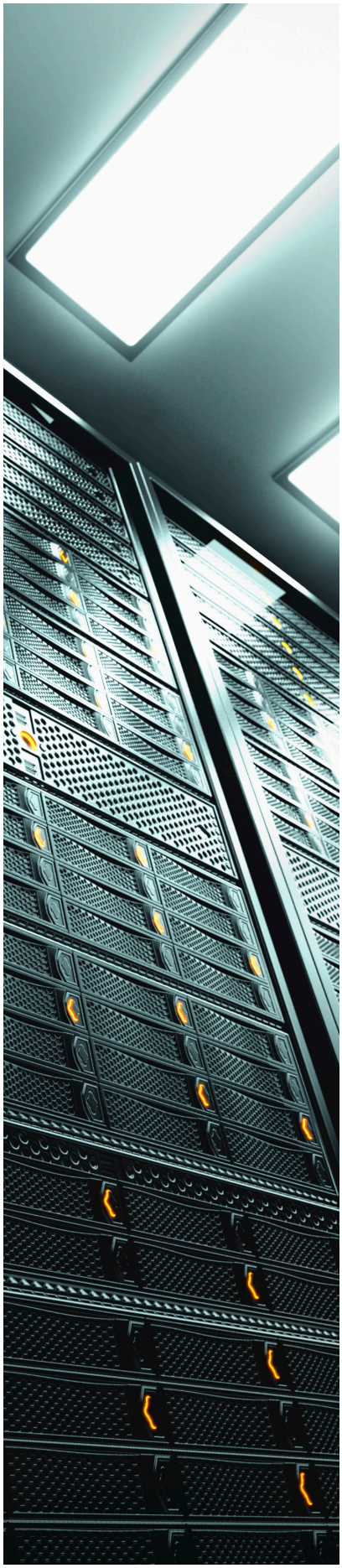
Sistemlere erişim, cihaz ve bağlantı güvenliğini sağlamak şirketlerin öncelikli risk azaltma önlemleri arasındadır. Bu amaçla şirketler siber güvenlik ürünlerine daha fazla yatırım yapmakta ve danışmanlık hizmetleri almaktadır. Riskin yönetimi tarafında dikkat çekici olan siber sigorta yapılandırması konusunda şirketlerin önceliklendirme yapmaması olmuştur. Bu durum kısmen siber risk sigortası yaptıran şirket sayısının az olmasından kaynaklanabilir. Her yıl değişen ve gelişen siber saldırı tipleri düşünüldüğünde her yıl sigorta kapsamının bu gözle yeniden değerlendirilmesi önemlidir. İçinden geçtiğimiz COVID-19 sürecinde olduğu gibi yalnızca siber saldırılar değil, çalışma şeklimizde ve iş modelimizde yapacağımız değişikliklerin de siber sigorta kapsamına yansıtılması gerekmektedir.

Sektörel olarak göze çarpan bir bulgu üretim sektörünün siber risk konusunda farkındalığının artması ve son 1 yıl içerisinde her üç alanda da en fazla çalışma yapan sektör olmasıdır. Finans sektörü diğer taraflara kıyasla üçüncü tarafların siber risk değerlendirmesi konusunda daha yoğun çalışmaktadır. Dış kaynaklara bağımlılık ve tutulan verinin kritikliği göz önünde bulundurulduğunda bu sonuç şaşırtıcı olmamıştır.

GEÇTİĞİMİZ 1 YIL İÇİNDE GERÇEKLEŞTİRİLEN UYGULAMALAR

Risk Tespiti	**%65**
Teknik siber risk değerlendirmesi (Penetrasyon testi, zafiyet analizi gibi)	%50
Kurumsal risk yönetimi kapsamında siber risk değerlendirmesi	%40
Üçüncü taraflar için siber risk değerlendirmesi	%26
Potansiyel siber kayıp senaryoları modellemesi	%16
Riski Azaltma	**%78**
Bilgisayarlarımızın ve mobil cihazlarımızın güvenliğini arttırma	%67
Sistemlerimize erişim güvenliğini arttırma	%67
Sistemlerimize ve ağımıza dışarıdan bağlantıyı daha güvenli hale getirme	%65
Veri sızıntısı olasılığını azaltma	%51
Penetrasyon (sızma) testi bulgularına ilişkin yatırım yapma	%36
Risk Yönetimi	**%71**
Bilgi güvenliği yönetimin sisteminin iyileştirilmesi	%56
Siber güvenlik farkındalık eğitimlerinin gerçekleştirilmesi	%44
Siber olaylara müdahale planımızı test etme ve iyileştirme	%32
Bilgi güvenliği yönetimin sisteminin kurulması	%31
Siber güvenlik operasyon merkezinin kurulması ya da hizmetinin alınması	%17
Üst düzey yönetim için masa başı kriz egzersizleri ve/veya farkındalık eğitimi düzenleme	%15
Yeni siber risk çalışanı / siber güvenlik lideri işe alınması	%12
Siber sigorta kapsamımızı yeniden yapılandırma	%7
Fikrim yok	%10
Yukarıdakilerin hiçbiri	%10

Şirketler söz konusu risk belirleme, azaltma ve yönetme eylemlerine her yıl önemli bir kaynak ayırmaktadır. Harcanan efor, zaman ve bütçe düşünüldüğünde bu çalışmaların karşılığını nasıl değerlendirdiklerini sorduğumuzda katılımcılarımız etkinlik seviyesinin yüksek olduğunu belirtmişlerdir. Burada Bilgi Güvenliği kalite yönetim sisteminin kurulması, sızma testi yatırımı ve teknik siber risk değerlendirmesi yapılması ön plana çıksa da genel olarak riskin anlaşılması ve yönetilmesi konusunda alınan tüm aksiyonlar takdir edilmiş, önemli bulunmuş ve şirkete geri dönüş sağladığı belirtilmiştir. Dolayısıyla şirketler siber risk yönetiminde küçük bir önlemden büyük bir yatırıma kadar tüm opsiyonları değerlendirmeli ve şirkete sağlayacağı faydayı göz ardı etmemelidir.



ŞEKİL 9

Siber risklerin tespit edilmesi, ölçülmesi ve yönetilmesi için şirketler çok çeşitli yöntemleri aynı anda kullanmakta ve başta riski azaltmaya yönelik olanlar olmak üzere genel olarak hepsini etkin bulmaktadır.

S. Son 1 yıl içinde yapmış olduğunuz her bir eylem sizce ne kadar etkili oldu?

Siber Risk Sigortası

Siber Risk Sigortası Sahipliği

Şirketlerin IT sistemlerine bağımlı hale gelmesi, verinin şirketlerin en önemli varlıklarından biri haline gelmesi, kişisel verileri korumanın öneminin her geçen gün artması ve yasalarla da desteklenmesi, IT sistemlerinin erişilebilirliğinin iş sürekliliğine etkisi, kötü niyetli ataklardaki artış ve firmalarda sebep olduğu katastrofik zararlarla birlikte siber risklere karşı bir sigorta ihtiyacı doğmuştur. Bu ihtiyaca yönelik olarak, sigorta şirketleri de geniş teminatlı siber risk sigortası poliçelerini dizayn etmeye ve şirketlere teminat sağlamaya başlamışlardır.

Ülkemizde de siber risk algısının değişmesi ve gelişmesi ile birlikte siber risk sigortasına yönelik farkındalık da artmaya başlamış ancak, halen bu tamamlayıcı çözüm yöntemiyle ilgili fikir sahibi olmayan ya da sigortanın riskleri minimize etme noktasında bir rolü olmadığını düşünen kurumlar da mevcuttur.

Katılımcılara, kurumlarının siber risk sigortasına sahip olup olmadıkları sorulmuştur. Siber risk belirleme ve yönetimi konusunda kurumlarındaki uygulamalardan haberdar olan çalışanların %25'i kurumun siber risk sigortası olup olmadığını bilmemektedir. Bu konuda bilgi sahibi olan çalışanlar bazında bakıldığında ise, %43'ünün çalıştığı kurumun halihazırda siber risk sigortasına sahip olduğu görülmektedir.

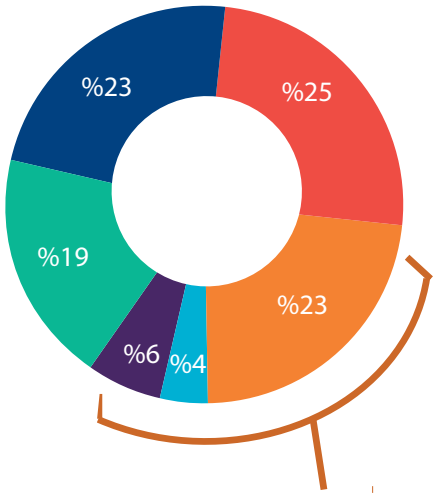
500+ çalışanı bulunan ve finans sektöründe faaliyet gösteren şirketlerde, siber risk sigortasına sahip olan ve mevcut poliçelerini yenilemeyi düşünenler çoğunluktadır.

ŞEKİL 10

Siber risk sigortası hakkında farkındalığı gelişmiş olan ancak henüz poliçe satın almamış olan kurumların %45'i önümüzdeki 1 yıl içerisinde siber risk sigortası yaptırmayı planlamaktadırlar.

S: Şirketinizin siber risk sigortası ile ilgili olarak mevcut durumu nedir?

- Şu anda bir sigorta poliçemiz var ve mevcut kapsamı yenilemeyi planlıyoruz.
- Şu anda bir sigorta poliçemiz var ve kapsamını / limitini veya her ikisini birden genişletmeyi planlıyoruz.
- Şu anda bir sigorta poliçemiz var fakat yenilemeyi planlamıyoruz.
- Siber risk sigortamız yok fakat önümüzdeki 12 ay içinde satın almayı planlıyoruz.
- Siber risk sigortamız yok ve önümüzdeki 12 ay içinde satın almayı planlamıyoruz.
- Bilmiyorum / Fikrim yok



Siber Risk Sigortası Sahipliği %33

Siber risk belirleme/ölçmede kullanılan yöntemlerden haberdar olanlar (n): 108

Siber risk sigortası sahipleri içerisinde,mevcut sigorta sahiplik durumunu bilenler %43

Siber Sigorta Ve Poliçe Kapsamı Değerlendirme

Siber risklerin özellikle iş hayatında büyük bir yer kaplamasından sonra siber risk sigortası global olarak önem kazanan bir sigorta ürünü haline gelmiştir. Türkiye'de de siber risk poliçesi satın alan kurumların sayısı arttıkça ve poliçelerin siber olaylar karşısında tetiklendiği görüldükçe, sigorta kapsamına olan güvenin de olumlu anlamda etkilenmesi beklenmektedir.

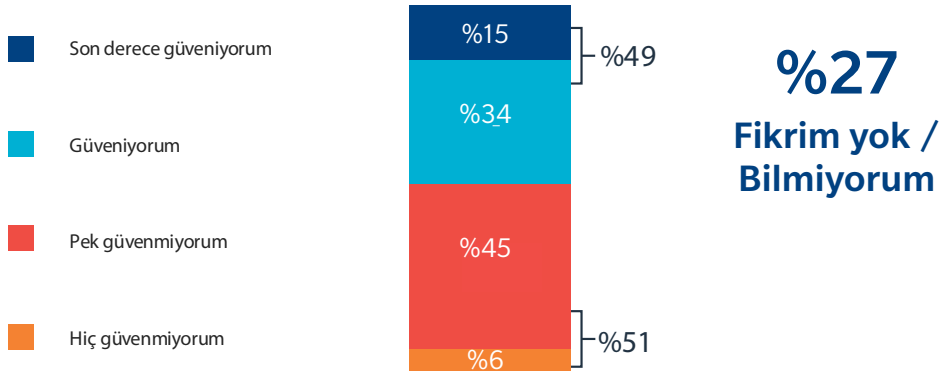
Mevcut koşullarda, Türkiye'deki firmaların siber risk sigortalarının kapsamı konusunda güvensizlik içinde olduğu gözlemlenmiştir. Araştırmaya katılan kurumların %49'u siber risk sigortasının kapsamına güven duymaktadır. Bu oran Marsh ve Microsoft tarafından 2019'da gerçekleştirilen Global Siber Risk Algı Araştırması'na göre dünyada %89 düzeyindedir.

Diğer yandan siber risk sigortasına sahip olma durumu, güven algısını da oldukça etkilemektedir. Türkiye'de özellikle siber risk poliçesine sahip olan şirketlerin %88'i sigortanın koruyuculuğuna ve kapsamına güven duymaktadır. Bu oran, siber risk sigortası sahibi olmayanlarda %17'ye düşmektedir.

ŞEKİL 11

Siber risk sigortasına sahip olan kurumların %88'i sigortanın koruyuculuğuna ve kapsamına güven duymaktadır.

S: Şirketinizdeki sigorta/ların (siber ve/veya diğer poliçelerin) mevcut kapsamının, bir siber olay durumunda şirketinizin uğradığı zararı karşılayacağına güveniyor musunuz?

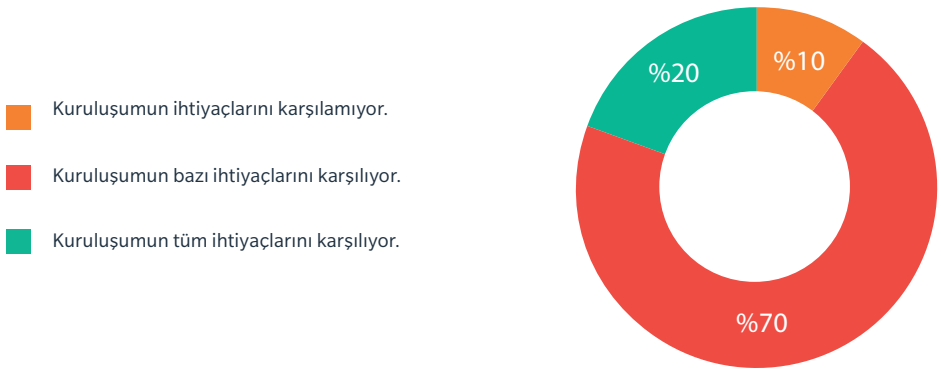


Şirketin sahip olduğu siber ya da diğer farklı sigortaların kapsamı hakkında bilgi sahibi olanlar (n): 105

ŞEKİL 12

Siber risk sigortası kapsamının daha geniş olması beklense de, her 10 kurumdan 9'u için bu kapsam genel ihtiyaca yönelik bulunmaktadır.

S: Siber risk sigortalarının genel olarak kapsamını nasıl değerlendirirsiniz?



Siber sigorta kapsamı hakkında fikir sahibi olanlar (n): 67

Siber Güvenlik Yatırım Alanları

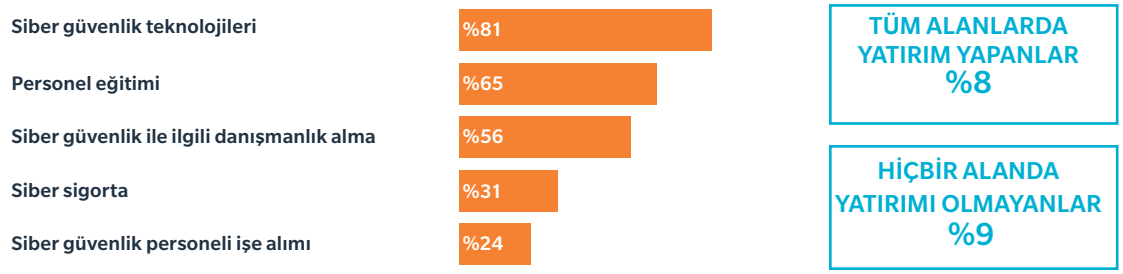
Risk Yönetimi Kapsamında Yatırım Yapılan Alanlar

2019 Global Risk Algı araştırmasıyla paralel olarak, Türkiye'deki kurumlar da siber riskleri yönetme stratejisinin temelinde daha çok teknolojik alanlara yatırım yapma eğilimindedir. Diğer taraftan bütüncül bir yaklaşımın gerektirdiği detaylı risk değerlendirmesi, risklerin sayısallaştırılması ve buna uygun olarak tasarlanmış bir sigorta programı ile risklerin transfer edilmesi çalışmalarının birçok kurum tarafından uygulanmadığı görülmektedir. Öne çıkan diğer bir nokta ise, kurumların en az yatırım yaptıkları alan siber güvenlik uzmanı işe alımı, bu sayede siber ekiplerin desteklenmesi ve büyütülmesidir. Bu durum büyük ölçüde, ülkemizde yetişmiş siber güvenlik uzman sayısının ihtiyacın çok altında olmasından ve genel anlamda finans, telekom gibi regüle edilen sektörler haricinde kalan diğer sektörler açısından siber risklerin öncelikli riskler arasında görülmemesinden kaynaklanabilmektedir.

ŞEKİL 13

Siber risk yönetimi kapsamında en çok güvenlik teknolojilerine yatırım yapılmaktadır.

S: Aşağıda yer alan siber risk yönetimi alanlarına halihazırda yatırım yapıyor musunuz?



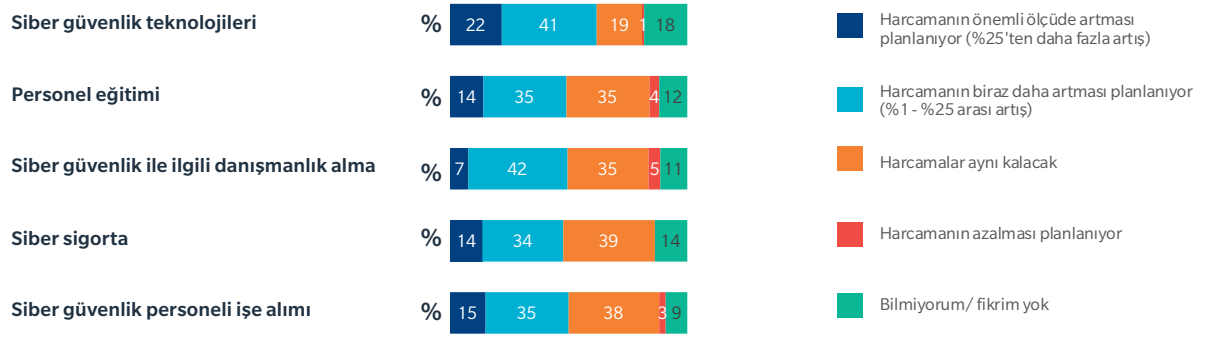
3 Yıllık Planlama – Hâlihazırda Yatırım Yapılan Alanlar

Siber risk yönetimi konusunda yatırım yapılmaya önümüzdeki dönemde de devam edilecektir. Siber güvenlik teknolojileri bugün olduğu gibi yakın gelecekte de en çok kaynak ayrılacak olan alandır. Kurumların %63'ü önümüzdeki dönemde bu alandaki harcamalarını artırarak devam edeceklerini belirtmektedir.Diğer yatırım alanlarına ilişkin öngörülere bakıldığında siber güvenlik eğitimleri, güvenlik uzmanı işe alımı ve danışmanlık temini konularında dengeli ve benzer seviyede yatırımlarını artırmayı planladıkları görülmektedir. Özellikle siber danışmanlık tarafındaki yatırımların ve bütçelerin diğer tüm alanlara kıyasla daha az büyüyeceği öngörülmektedir.

ŞEKİL 14

Kurumlar, siber güvenlik teknolojilerine yatırım yapmayı bütçelerini arttırarak sürdürmeyi planlamaktadır.

S: Aşağıdaki alanlara yatırım yaptığınızı söylediniz? Önümüzdeki 3 yıl içinde bu yatırımların şirketinizdeki payı için planlarınız nelerdir?



Toplam Baz (n): 144

Her bir kalem için yatırım yapanlar bazında

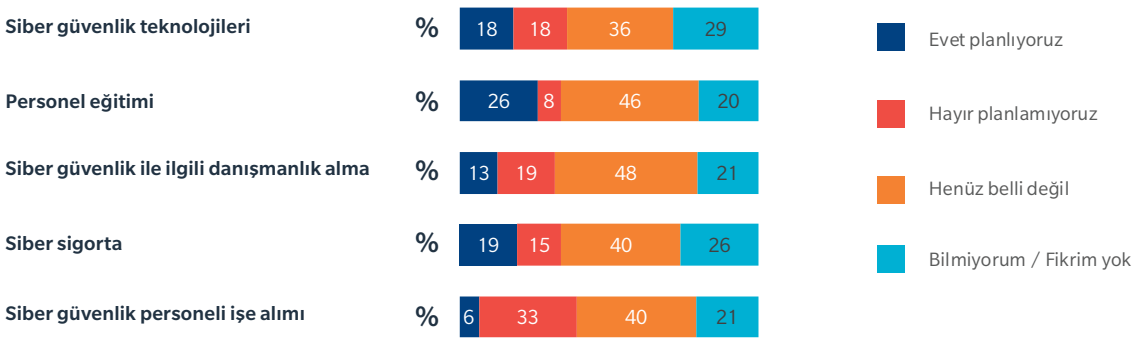
3 Yıllık Planlama – Yatırım Yapılmayan Alanlar

Kurumların siber risklerle mücadele stratejisinde yatırım yapmayı planladıkları temel alanlar sırasıyla mevcut personele siber güvenlik eğitimleri sağlamak ve teknolojik çözümlerdir. Öncelik sırasında en geride kalan alanlar ise siber güvenlik personelinin işe alımı ve siber danışmanlık hizmeti olarak karşımıza çıkmaktadır. Kurumların içinde kullanılan siber güvenlik uygulamalarını ve siber sigorta sahipliğini bilmeyen çalışanlar, kurumun bu alana yatırım yapma planlarının da uzağında kalmaktadır. Şirket içindeki sigorta sahibiyetine ilişkin bilgi sahibi olan çalışanlar nezdinde siber sigorta sahibi olmayan şirketlerin önümüzdeki dönemde sisteme dâhil potansiyeli %44 olarak görülürken, genel kitlede bu oran %19'a gerilemektedir.

ŞEKİL 15

Henüz yatırım yapılmayan alanlara yönelik planlamalar içinde en öne çıkan konu mevcut personelin eğitimidir.

S: Aşağıdaki alanlara yatırım yapmadığınızı söylediniz? Önümüzdeki 3 yıl içinde yatırım yapmayı planlıyor musunuz?



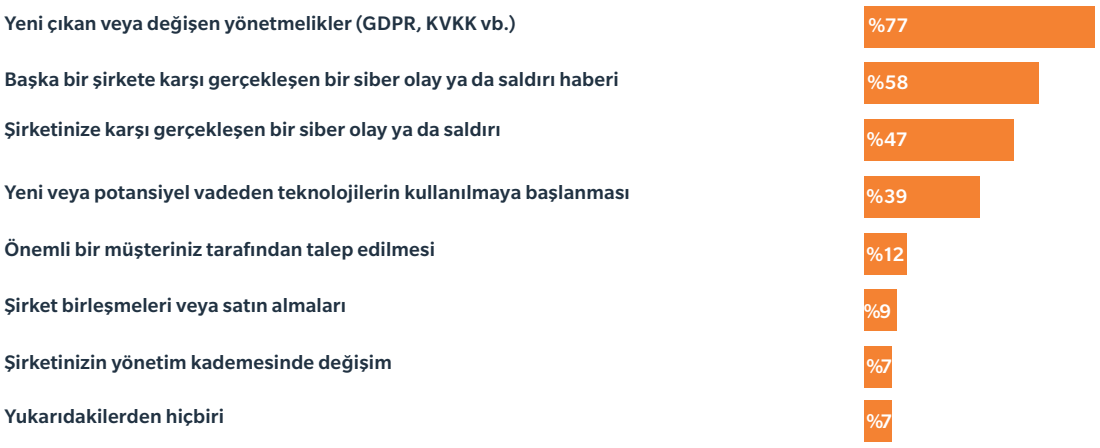
Türkiye'de siber saldırıya uğrama endişesi ve yeni çıkan ya da değişen yönetmelikler kurumları siber güvenlik konusunda yatırım yapmaya teşvik eden en önemli faktörlerdir. Yönetmeliklerin, yatırımı teşvik etme gücü diğer ülkelere göre daha yüksektir. Türkiye'de kurumların %77'si yönetmeliklerin etkisi ile siber güvenlik alanına yatırım yaparken bu oran globalde %28 düzeyinde kalmaktadır.

2019 yılında gerçekleştirilen Global Risk Araştırmasına göre firmaları siber güvenlik konusunda yatırım yapmaya yönelten en önemli konu siber saldırı riskidir (%64). Türkiye'de siber saldırı konusundaki endişenin yatırım kararına toplam etkisini anlayabilmek için kurumların hem kendilerine hem de başka şirketlere yönelik gerçekleştirilen saldırılar konusundaki hassasiyetlerine birlikte bakılarak analiz edilmiştir ve toplam etkinin %78 olduğu görülmüştür.

ŞEKİL 16

Türkiye'de siber güvenlik yönetimine yatırım yapılmasında siber saldırı endişesi kadar yönetmelikler de etkili olmaktadır.

S. Siber güvenliğe ilişkin yatırım yapma kararınızda genel olarak en etkili olan konuları işaretler misiniz?



Yeni Teknolojiler ve Siber Riskler

Kurumlar açısından teknolojilerin beraberinde getirdiği siber riskleri incelerken, teknolojiler üç farklı başlıkta ele alınmıştır. Bunlardan ilki bulut bilişim, kurumsal dijital uygulamalar ve mobil uygulamalardan oluşan temel bilişim sistemleridir. İkincisi ise daha çok enerji, kritik altyapı ve sanayi firmalarında kullanılan endüstriyel kontrol sistemleri ve akıllı bina sistemleridir. Son senelerde sıklıkla duyduğumuz Blok Zinciri, Yapay Zeka, Robotbilim süreç optimizasyonu, Nesnelerin İnterneti(IOT) ve Artırılmış Gerçeklik alanlarını içeren yeni teknolojiler ise ele alınan diğer önemli bir teknoloji alt başlığıdır.

Siber risk açısından değerlendirilen teknojiler içinde özellikle temel bilişim sistemlerinin kurumların büyük bölümü tarafından kullanıldığı gözlemlenmektedir. Operasyonel/ endüstriyel kontrol sistemlerinin kullanım tercihi kurumların faaliyet gösterdiği alana göre farklılaşmaktadır. Yeni/ potansiyel vadeden teknolojiler ise daha az bilinmekte ve kullanılmaktadır.

%77
TEMEL BİLİŞİM SİSTEMLERİ

%46
OPERASYONEL/ ENDÜSTRİYEL KONTROL SİSTEMLERİ

%38
YENİ / POTANSİYEL VADEDEN TEKNOLOJİ

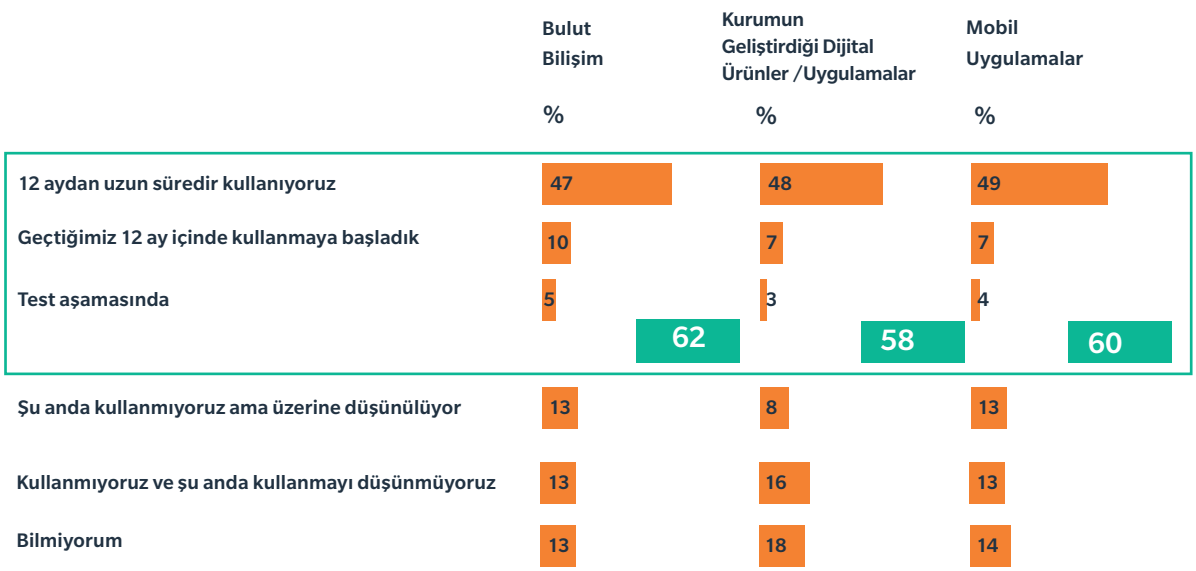
Yeni Teknolojilerin Kullanımı – Temel Bilişim Sistemleri

Temel bilişim teknolojileri uygulamaları benzer oranda tercih edilmektedir ve her biri 10 kurumdan 6'sı tarafından kullanılmaktadır.

ŞEKİL 17

Temel bilişim teknolojileri kurumların günlük hayatında önemli bir yere sahiptir.

S. Aşağıdaki teknolojileri şirketinizde kullanıyor musunuz?



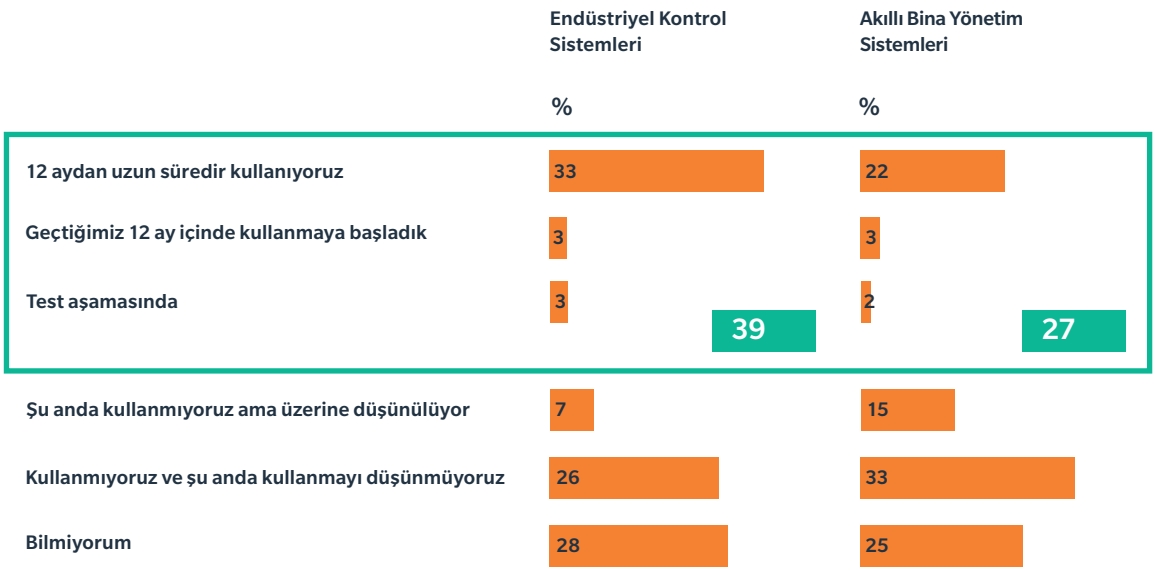
Yeni Teknolojilerin Kullanımı – Operasyonel Teknoloji

Operasyonel teknolojiler içinde endüstriyel kontrol sistemleri, akıllı bina yönetim sistemlerine kıyasla daha yaygındır. Endüstriyel kontrol sistemleri tercihinde sektör büyük önem taşımaktadır; üretim, otomotiv ve enerji sektöründe çok daha fazla kullanılmaktadır.

ŞEKİL 18

Endüstriyel kontrol sistemleri kurumların %39'unun hayatına girmiştir, bu oran akıllı bina sistemleri için %27 düzeyindedir.

S: Aşağıdaki teknolojileri şirketinizde kullanıyor musunuz?



Yeni Teknolojilerin Kullanımı – Yeni / Potansiyel Vadeden Teknoloji

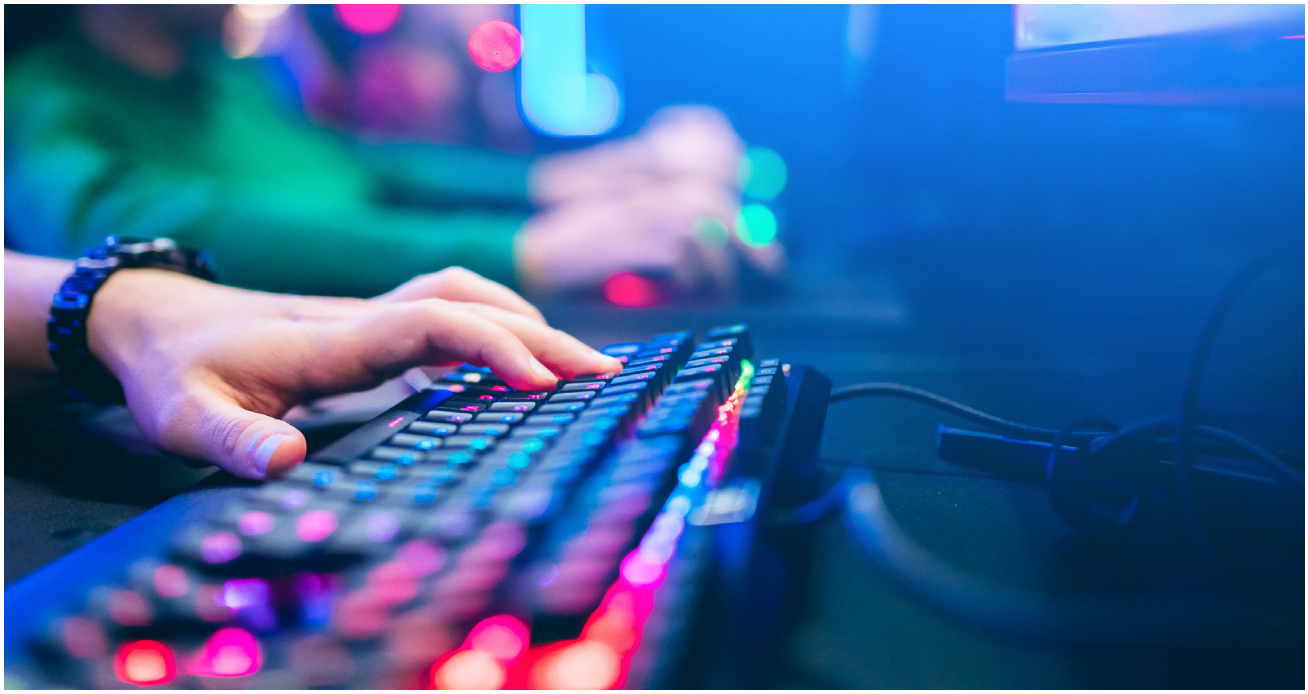
Yeni/ potansiyel vadeden teknolojilerin genel olarak kullanım düzeyi diğer teknolojilere kıyasla daha düşüktür. Diğer yandan bu alanda potansiyeli nispeten yüksek olan uygulamalar Robotbilim Süreç Optimizasyonu, Yapay Zeka, Nesnelerin Interneti'dir.

ŞEKİL 19

Robotbilim Süreç Optimizasyonu, Yapay Zeka, Nesnelerin interneti 3 kurumdan biri tarafından benimsenmeye başlamıştır.

S: Aşağıdaki teknolojileri şirketinizde kullanıyor musunuz?

	Yapay Zeka (AI) / Makine Öğrenimi %	Blok Zinciri (Blockchain) %	Robotbilim Süreç Optimizasyonu %	Nesnelerin İnterneti (IOT) %	Artırılmış Gerçeklik %
12 aydan uzun süredir kullanıyoruz	10	3	15	13	3
Geçtiğimiz 12 ay içinde kullanmaya başladık	9	1	8	7	3
Test aşamasında	10	5	11	8	6
	29	9	34	28	12
Şu anda kullanmıyoruz ama üzerine düşünülüyor	24	22	22	21	19
Kullanmıyoruz ve şu anda kullanmayı düşünmüyoruz	28	42	27	28	40
Bilmiyorum	19	26	17	23	28

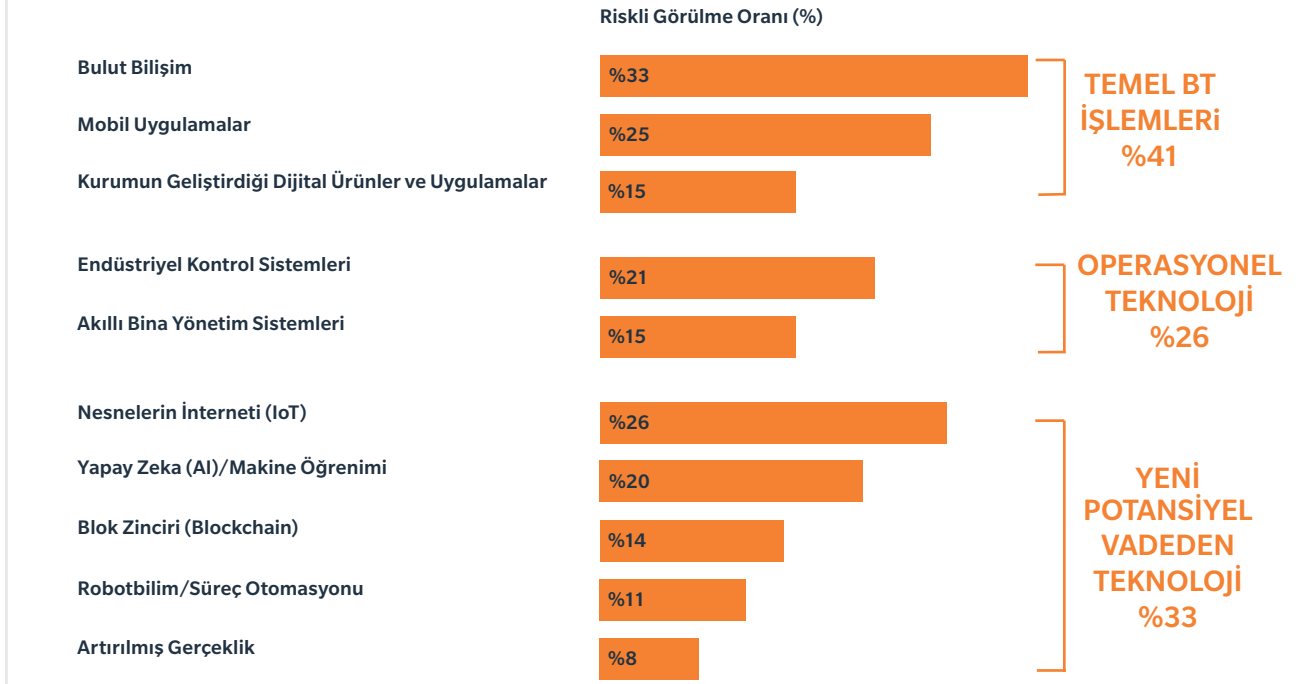


Yeni Teknolojilerin Yarattığı Riskin Değerlendirilmesi

Temel BT işlemleri en yaygın kullanılan ve hakkında en çok fikir sahibi olunan teknolojilerdir. Buna karşın en riskli görülen teknolojidir. Yeni teknolojiler arasında en çok risk yarattığı düşünülen teknoloji bulut bilişim olmuştur. Potansiyel vadeden yeni teknolojiler arasında yer alan robotbilim ve artırılmış gerçeklik en az riskli görülen uygulamalardır.

ŞEKİL 20

Bilgilerin depolanması ya da paylaşıma yönelik teknolojiler daha riskli bulunmaktadır.
S: Aşağıdaki listede yer alan her bir teknolojiyi şirketiniz için siber risk yaratması açısından nasıl değerlendirirsiniz?



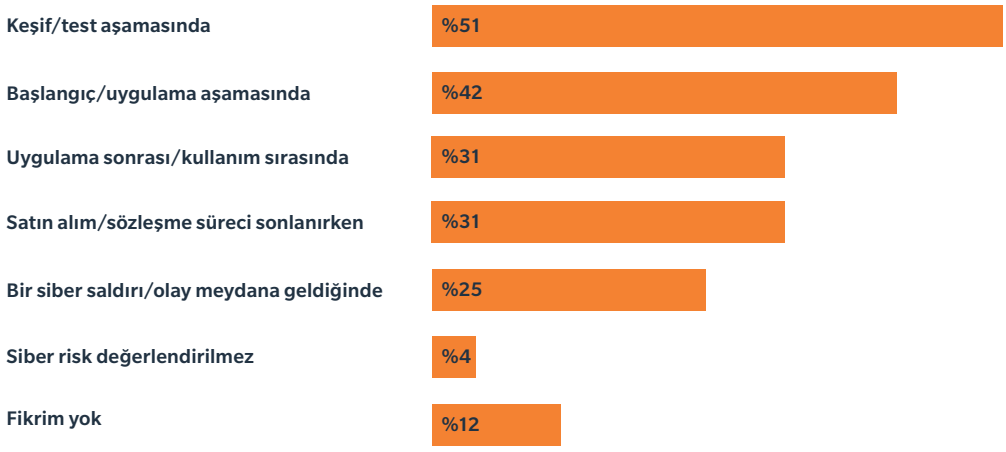
Yeni Teknolojilerin Siber Risk Değerlendirme Aşamaları

Kurumlar yeni teknolojilere ilişkin risk değerlendirmelerini pek çok aşamada gerçekleştirmektedir. Risk değerlendirmesini keşif ya da başlangıç aşamasında yapmaya başlayan kurumların oranı %67'dir. Buna göre her 3 şirketten 1'i risk değerlendirmelerini sonraki aşamalara bırakmaktadır. Bu noktada yapılan risk değerlendirmesi riskin olasılığını ve etkisini azaltmada pek etkili olamayacağı gibi geliştirilebilecek olası önleyici çözümler aşırı maliyetli olduğundan uygulanmasında büyük zorluklar söz konusu olabilmektedir. Bu nedenle risk değerlendirmelerinin önceki süreçlere entegre edilmesi önemlidir.

ŞEKİL 21

Her 3 kurumdan 2'si yeni teknolojilerine ilişkin risk değerlendirmelerini en erken aşamalarda yapmaya başlamaktadır.

S: Şirketinizde yeni teknolojiler uygulamaya alınırken siber risk genel olarak hangi aşamalarda değerlendirilir?

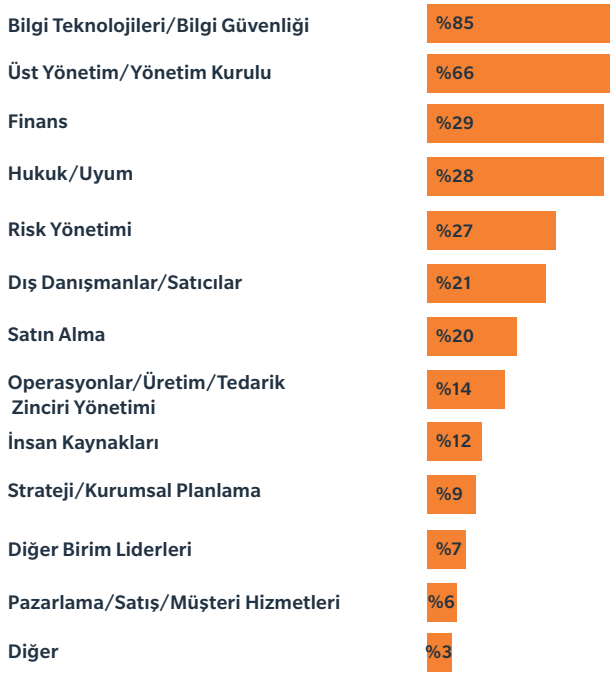


Siber Risk Değerlendirme Sürecine Dahil Olan Birimler

ŞEKİL 22

Siber risk değerlendirme süreci temelde bilgi teknolojileri birimi tarafından yöneltilse de kurumların büyük bölümünde üst yönetim tarafından da yakından takip edilmektedir.

S: Şirketinizde yeni teknolojiler uygulamaya konulurken hangi birimler değerlendirme ya da karar aşamasında siber güvenlik açısından sürece dahil oluyor?



Yeni teknolojilerin uygulamaya konulması aşamasında siber güvenlik açısından değerlendirme ve karar süreçlerine en fazla dahil olan birim %85 oranıyla Bilgi Teknolojileri/ Güvenliği olmuştur. Onun ardından %66 ile üst yönetim / yönetim kurulu siber güvenlik aşamasında sürece dahil olan birim olarak belirtilmiştir. 2019 yılında gerçekleştirilen global çalışma, dünya genelinde de benzer şekilde siber güvenlik ile sorumluluğu başta bilgi güvenliği uzmanları (%86) ve üst yönetimin (%65) üzerine aldığını ortaya koymaktadır. Dış danışmanlar ve satıcılar inşaat sektöründe daha çok devreye girmektedir.

Toplam Baz (n): 144

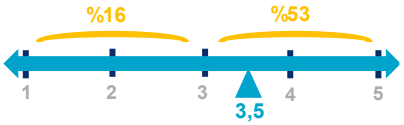
Risk Kapsamında Yeni Teknolojilere Yaklaşım

Kurumların risk kapsamında yeni teknolojilere yönelik yaklaşımlarını anlamak için aşağıda yer alan kriterlere yönelik tutumları sorgulanmıştır.

Yeni teknolojiler yarattıkları avantaj nedeniyle kurumlar için cazip görünse de, risk değerlendirmesi önemlidir. Kurumlar, yeni teknolojileri beraberinde taşıdığı riske rağmen tercih edip etmeme konusunda tereddüt yaşamaktadır. Bu noktada kurumların aldıkları önlemlere bakıldığında büyük bölümünün işi teknoloji üreticilerine bırakmadan kendi risk değerlendirmelerini yaptıkları, kendi ek güvenlik önlemlerini uyguladıkları görülmektedir.

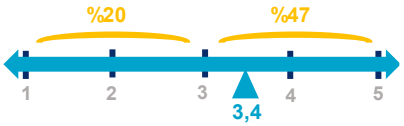
Risk yönetimine ilişkin olarak, sigorta pazarındaki mevcut ürünler yeterli güveni yaratamamaktadır; bütün riskleri kapsayacak genişlikte bir koruma düzeyinde olmadıkları ve yeterli limitleri sunamadıkları kanısı yaygındır.

Kullandığımız teknolojilerde, üretici firmanın uyguladıkları dışında güvenlik seviyesini arttırmak için herhangi bir ek güvenlik önlemi almıyoruz.



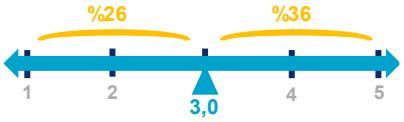
Kullanıma aldığımız teknolojilere her zaman kendi ek güvenlik önlemlerimizi uyguluyoruz.

Teknoloji ve dijital ürün üreticilerinin, tüm siber güvenlik risklerini dikkate aldığına ve yeterli güvenlik korumalarını sağladığına güveniyoruz



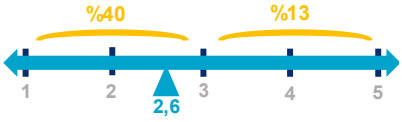
Yeni teknolojiler için tam anlamıyla güvenli olduğunu kabul etmiyoruz ve her zaman kendi risk değerlendirmemizi yapıyoruz.

Yeni teknolojilere, şirketimiz için ne kadar avantajlı olursa olsun risk faktörü nedeniyle çok ihtiyatlı yaklaşıyoruz, risk almamayı tercih ediyoruz.



Yeni teknolojilerin ve dijital ürünlerin sunduğu potansiyel fırsatlar ve avantajlar son derece faydalı olduğundan risk faktörü, neredeyse hiçbir zaman bunları benimsememize engel teşkil etmiyor.

Sigorta pazarındaki mevcut ürünler yeni teknolojiler ve dijital ürünlerle ilgili risklerin tamamını kapsama alacak genişlikte değil, yeterli limitleri sunamıyor.



Sigorta pazarındaki mevcut ürünler, yeni teknolojilerin ve dijital ürünlerin oluşturduğu bütün riskleri kapsayacak genişlikte bir koruma düzeyi ve yeterli limitleri sunuyor.

Toplam Baz (n): 144

Mean skorları verilmiştir.

Cetvelin üzerinde yer alan yüzde skorları ise sol ve sağdaki tutumların her birine katılıyorum + kesinlikle katılıyorum oranlarıdır.

Tedarik Zincirinde Siber Risk Yönetimi

Tedarik Zincirinde Risk Algısı

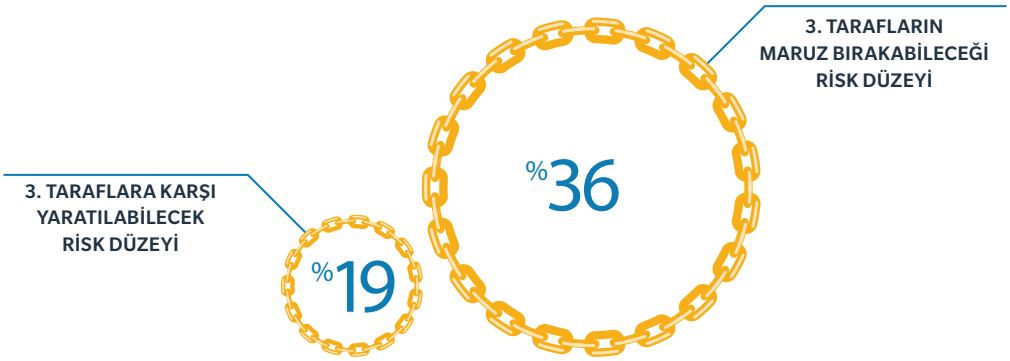
Günümüzde şirketler karmaşık bir tedarik zinciri ağı içerisinde faaliyet göstermektedir. Birlikte çalışan tarafların birbirine güven duyması zincirin sağlıklı bir şekilde işlemesi için önemlidir. Dijital tedarik zinciri yapısında organizasyonlar özellikle güvenlik ve bütünlük konusunda hassasiyet göstermektedir. Bu bakış açısıyla şirketlerden halkası oldukları değer zincirindeki rollerinin ve siber güvenlik konusundaki sorumluluklarının farkında olmaları beklenmektedir.

Bu çerçevede neredeyse her 5 katılımcıdan 2'si, üçüncü taraflardan kaynaklı siber risklerin şirketleri için önemli bir risk teşkil ettiğini belirtmiştir. Öte yandan, tam tersi bir değerlendirme yapmaları ve kendi şirketlerinin diğer tarafları maruz bıraktığı siber riskleri değerlendirmeleri istendiğinde bu oran yarıya düşmüştür. Bu sonuçlara baktığımızda şirketlerin siber güvenlik konusundaki uygulamalarına üçüncü taraflarınkine oranla daha çok güvendiği algısının olduğunu görüyoruz. 2019 Global Risk Algı Araştırması'nda çıkan sonuçlar bu oranlara birebir benzerlik göstermekte ve katılımcıların üçüncü tarafları daha riskli bulma eğilimlerinin iki kat daha fazla olduğu görülmektedir.

ŞEKİL 23

Her 3 kurumdan 1'i için 3. taraflar da kurumların önemli siber risk taşıyıcılarından biri olarak görülmektedir.

S: Şirketinizin tedarik zincirinde yer alan 3. taraflar nedeniyle maruz kalabileceği siber risk düzeyini nasıl görüyorsunuz?



Tedarikçi Kaynaklı Risklerin Önlenmesi

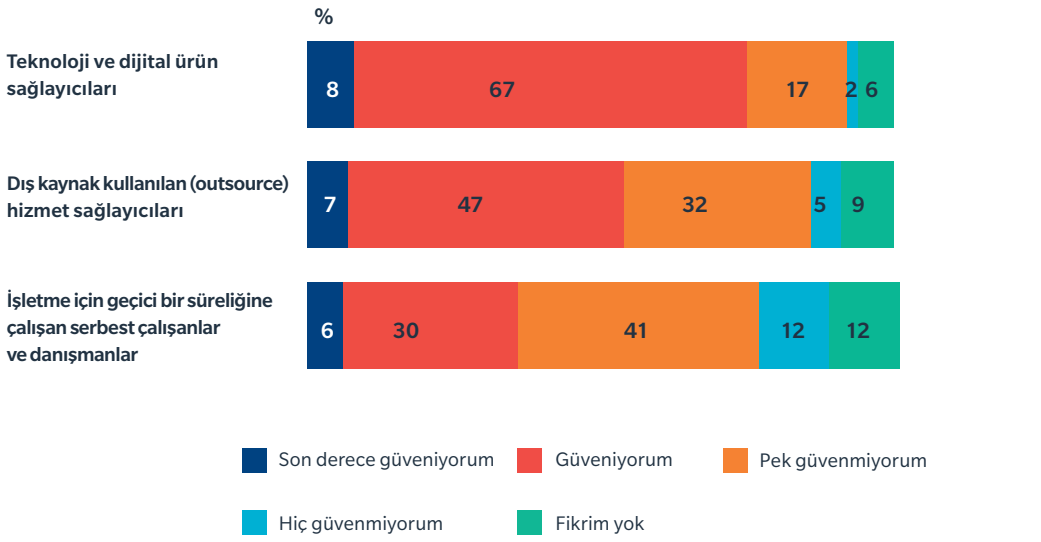
Şirketler tedarik zincirinde maruz kaldıkları risk seviyesini yüksek bulsalar da, bu riskleri minimize edebilmek için kendi önlemlerini alabilmektedirler. Şirketler arasında üçüncü taraflardan kaynaklı siber riskler konusunda kendilerini tamamen güvende hissedenlerin oranı oldukça düşüktür. Öte yandan katılımcıların büyük çoğunluğu teknoloji ve dijital ürün sağlayıcılarından kaynaklı siber risklere karşı kendilerini daha hazırlıklı hissetmektedir. Şirketlerin bu tip yatırımlar öncesinde projeye veya ürüne yönelik farklı taraflarla risk analizleri yapması, ürünleri bir süre test aşamasında kullanması ve emin olduktan sonra canlı duruma alması bu güven seviyesinin yüksek olmasında önemli bir katkı sağlamıştır.

Siber Risk Yönetimi konusunda daha önceki değerlendirmelerde değinilen "insan" faktörü bu değerlendirmede de en zayıf halka olarak karşımıza çıkmaktadır. Şirketler işletme için geçici bir süreliğine hizmet veren kişilerden kaynaklı siber risklere karşı daha savunmasızdır. Bu noktada Türkiye sonuçları 2019 Global Siber Risk Algı Raporu ile paralellik göstermektedir.

ŞEKİL 24

Danışmanlık ve geçici çalışanlardan kaynaklanabilecek siber riskler kurumların üçüncü taraflarla ilgili en kırılgan oldukları alan olarak değerlendiriliyor.

S: Şirketinizin aşağıdaki taraflardan gelebilecek siber risklere ilişkin aldığı önlemlere ne kadar güveniyorsunuz?



Toplam Baz (n): 144

Siber Risk Yönetimi ile İlgili Kurum İçi Uygulamalar ve Tedarikçiden Beklentiler

Şirketlere hizmet sağlayıcılarından kaynaklı siber risklere maruziyeti azaltmak için tedarikçilerinden hangi önlemleri almalarını beklediklerini sorduğumuzda önceliklendirmenin kendi uygulamaları ile benzerlik gösterdiğini görüyoruz.

ŞEKİL 25

Kurumların 3. taraflardan beklentileri oldukça yüksek; risk tespiti ve risk yönetiminde kendi uygulamadıkları tedbirlerin dahi alınmasını istiyorlar.

S: Tedarik zinciri iş ortaklarınızın aşağıda yer alan siber güvenlik önlemlerinden hangilerini almalarını bekliyorsunuz?

	TEDARİKÇİLERDEN BEKLENTİLER	ŞİRKET İÇİ UYGULAMALAR
RİSK TESPİTİ	**%81**	**%65**
Teknik siber risk değerlendirmesi (Penetrasyon testi, zafiyet analizi gibi)	%59	%50
Kurumsal risk yönetimi kapsamında siber risk değerlendirmesi	%46	%40
Üçüncü taraflar için siber risk değerlendirmesi	%44	%26
Potansiyel siber kayıp senaryoları modellemesi	%20	%16
RİSKİ AZALTMA	**%81**	**%78**
Bilgisayarlarımızın ve mobil cihazlarımızın güvenliğini arttırma	%64	%67
Sistemlerimize erişim güvenliğini arttırma	%66	%67
Sistemlerimize ve ağımıza dışarıdan bağlantıyı daha güvenli hale getirme	%53	%65
Veri sızıntısı olasılığını azaltma	%62	%51
Penetrasyon (sızma) testi bulgularına ilişkin yatırım yapma	%40	%36
RİSK YÖNETİMİ	**%80**	**%71**
Bilgi güvenliği yönetimi sisteminin iyileştirilmesi	%54	%56
Siber güvenlik farkındalık eğitimlerinin gerçekleştirilmesi	%47	%44
Siber olaylara müdahale planımızı test etme ve iyileştirme	%47	%32
Bilgi güvenliği yönetimi sisteminin kurulması	%47	%31
Siber güvenlik operasyon merkezinin kurulması ya da hizmetinin alınması	%24	%17
Üst düzey yönetim için masa başı kriz egzersizleri ve / veya farkındalık eğitimi düzenleme	%24	%15
Yeni siber risk çalışanı / siber güvenlik lideri işe alınması	%15	%12
Siber sigorta kapsamının yeniden yapılandırılması	%20	%7

Kamu Politikaları

Kamu Politikalarının Siber Güvenliğe Etkisi

Türkiye'de siber güvenlik önlemlerine yapılan yatırım üzerinde değişen yönetmeliklerin etkisinin en az siber saldırıdan duyulan endişe kadar yüksek olduğu görülmektedir. Regülasyon ve yasalar hem yatırımı teşvik etmekte hem de kurumların bu alanda kendilerini geliştirmelerine yardımcı olmaktadır.

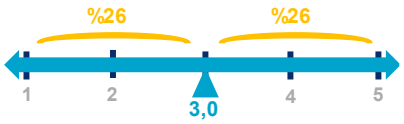
Ulusal Siber Güvenlik Kurulu belirlediği stratejiler ve yönetmelikler ile kurumlara yol göstermesi ve siber güvenliğe yönelik harekete geçmeye teşvik etmesi açısından önemlidir. Bununla birlikte yönetmeliklerin çok ayrıntılı olması kurumların sektörlerine yönelik uluslararası standart ve uygulamaları takip etmelerini zorlaştırabilmektedir. Bu kapsamda yönetmelikler ve uygulama alanları ile ilgili çerçevenin biraz daha geniş tutulması, kurumların farklılaşan ihtiyaçları doğrultusunda kendilerine özel çözümler bulabilmelerine olanak sağlayacaktır.

Siber risk belirleme ve ölçümlemede şirketlerin büyük bölümü NIST ve ISO gibi global standartları kullanmaktadır. Bu standartların şirketlerin siber güvenliğe ilişkin tutumlarının netleşmesinde ve gelişiminde etkili olduğu da düşünülmektedir. Ancak bu değerlendirme sektörel bazda farklılaşabilmektedir. Finans, profesyonel hizmetler gibi sektörlere kıyasla doğrudan risk altında bulunmayan sektörlerde bu standartların özel bir avantaj yaratmadığı düşünülebilmektedir.

Dış ülkelerden kaynaklı siber saldırı riski endişe yaratmakta ve önemsenmektedir. Bu tür saldırılardan korunmak için kamu politikaları ve düzenlemelerinin etkili olacağı düşünülmektedir. Bu nedenle de her iki şirketten biri bu noktada kamunun daha aktif bir rol üstlenmesi gerektiğine inanmaktadır.

Diğer yandan ulusal siber güvenliğin sağlanabilmesi için şirketlerin kamudan beklentileri yurtiçinde geçerli standartlar, yasalar ya da yönetmeliklerle sınırlı değildir, uluslararası düzenlemeler ve siber güvenlik yönetmelikleri ile ülkeler arasında iş birliği sağlanması istenmektedir.

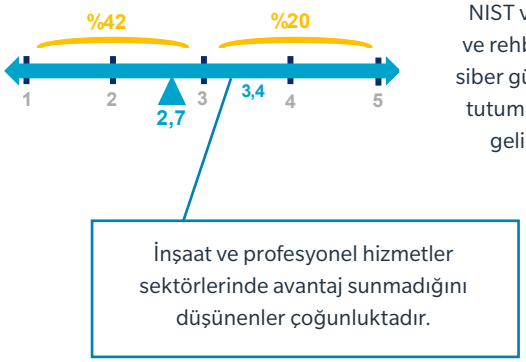
Ulusal Siber Güvenlik Kurulu'nun belirlediği stratejiler, hedefler ve politikalar, en iyi uygulamaların teşvik edilmesi ve ulusal altyapıyla özel kurumlara verilen zararları en aza indirmek açısından yeterince etkin.



Siber güvenlik konusundaki yönetmelikler fazlasıyla ayrıntıya girmektedir.

Kurumlar içinde oldukları sektörlere yönelik uluslararası standartlar ve uygulamaları tatbik etmek konusunda serbest olabilmeliler.

NIST ve ISO gibi sektör standartları ve rehberliği, siber güvenlik konusunda şirketimizin tutumunu belirlemede ve kendimizi geliştirmede çok etkili.



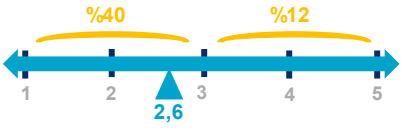
NIST ve ISO gibi sektör standartları ve rehberliğini takip ediyoruz, ancak siber güvenlik konusunda şirketimizin tutumunu belirlemede ve kendimizi geliştirmede somut bir avantaj sunmuyorlar.

Toplam Baz (n): 144

Mean skorları verilmiştir.

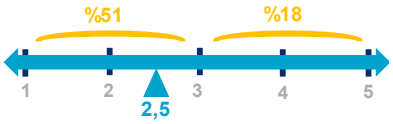
Cetvelin üzerinde yer alan yüzde skorları ise sol ve sağdaki tutumların her birine katılıyorum + kesinlikle katılıyorum oranlarıdır.

Dış ülkelerden kaynaklı siber saldırıların şirketimize verebileceği potansiyel zarar konusunda son derece endişeliyiz.



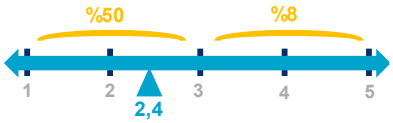
Dış ülkelerden kaynaklı siber saldırıların şirketimize zarar verebileceğini düşünmüyoruz, bu konuda hiçbir endişemiz yok.

Regülasyonlar ve yasalar siber güvenlik konusunda şirketimizin tutumunu belirlemede ve kendimizi geliştirmede çok etkili.



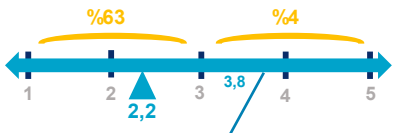
Regülasyonlar ve yasalara uygun hareket ediyoruz ancak mevcut regülasyonların ve yasaların, siber güvenlik konusunda şirketimizin tutumunu belirlemede ve kendimizi geliştirmede herhangi bir katkısı ya da etkisi olduğunu düşünmüyoruz.

Kamu politikaları ve düzenlemeleri, şirketleri dış ülkelerden kaynaklı saldırılardan korumaya yardımcı olmak için daha fazlasını yapmalı.



Kamu politikaları ve düzenlemelerinin, şirketleri dış ülkelerden kaynaklı saldırılardan korumaya yardımcı olmak için yapabileceği hiçbir şey yok.

Ülkelerin ulusal siber güvenliklerini tutarlı ve iş birliği içerisinde sağlayabilmesi için uluslararası düzenlemeler ve siber güvenlik yönetmelikleri gereklidir.



Ülkelerin ulusal siber güvenliklerini tutarlı ve iş birliği içerisinde sağlayabilmesi için ulusal düzenlemeler ve siber güvenlik yönetmelikleri gereklidir ve yeterlidir. Uluslararası yönetmeliklere gerek yoktur.

Profesyonel hizmetler sektörlerinde uluslararası yönetmeliklere gerek olmadığını düşünenler çoğunluktadır.

Toplam Baz (n): 144

Mean skorları verilmiştir.

Cetvelin üzerinde yer alan yüzde skorları ise sol ve sağdaki tutumların her birine katılıyorum + kesinlikle katılıyorum oranlarıdır.

Sonuç

Son olarak siber risk yönetim anlayışının geliştirilmesi için yapılabilecekler;

• Siber risk yönetimi konusunda bütünsel bir bakış açısı değişikliği gerekmektedir. Bunun için eğitim ve bilgilendirme şarttır. Siber risk eğitimlerinin, şirket oryantasyonların bir parçası haline getirildiği, bilinçlendirme pratiklerinin şirketlerin tüm iş birimlerine entegre edildiği yapılar kurulmalıdır.

• Siber riskin, şirketin taşıdığı diğer tüm riskler gibi konumlanması ve vizyon planlarının içine alınması önemlidir.

• Sektörlerin büyük bölümünde siber riskler konusunda bir farkındalık eksiği söz konusudur. CISO ya da şirketin temel yetki odağının tüm iş birimleriyle daha yakın temasta olup, yukarıdan aşağıya siber farkındalığı artırıcı mahiyette sürekli iletişimde bulunması gereklidir. Anlatımın yanı sıra birtakım risklerin nasıl oluşabileceğini ve etkilerini uygulamalı olarak göstermek etkili olacaktır.

• Organizasyonel değişimler ve insan kaynakları yönetimi yapılmadan etkin bir siber risk yönetimi mümkün görünmemektedir.

• Her şirkette siber risklerin gelişimi ve stratejilerine yönelik çalışacak ayrı bir Siber Güvenlik Komitesi kurulması, bu komitenin insan kaynakları, operasyon, hukuk ve diğer iş birimlerinden yetkilileri barındırması, düzenli bir toplantı takvimi ile iletişimde kalması etkili bir yönetim şekli olabilecektir.

• İş güvenliği alanındaki mevcut örnek önemlidir. İş güvenliği kamunun da yönlendirmesiyle tüm şirketlerin iç süreçlerine yerleşmiştir. Benzer adımların siber güvenlik alanında da atılması etkili olacaktır.

• Bu bağlamda özellikle siber riske yönelik stratejilerin sağlıklı biçimde kurgulanabilmesi için etkin ölçümleme metodları geliştirilmeli ve uygulanmalıdır.

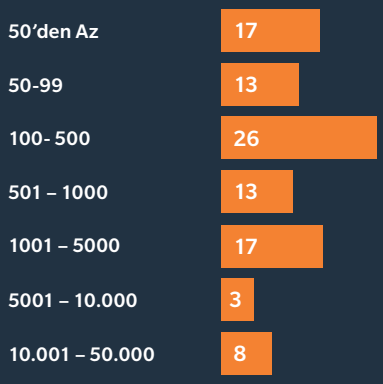
• Kamunun süreçleri daha belirgin biçimde, sektörel farklılıkları da göz önüne alarak tarif etmesi, şekillendirmesi beklenmektedir.

Anket Metodolojisi & Katılımcı Profili

Bu araştırmanın saha çalışması ve gelen bilgilerin analiz edilmesi **Sia Insight Araştırma** şirketi tarafından gerçekleştirilmiştir.

Çalışmaya 144 kişi katılmış olup, sektör, departman ve şirket büyüklüklerine ait bilgiler aşağıda özetlenmiştir.

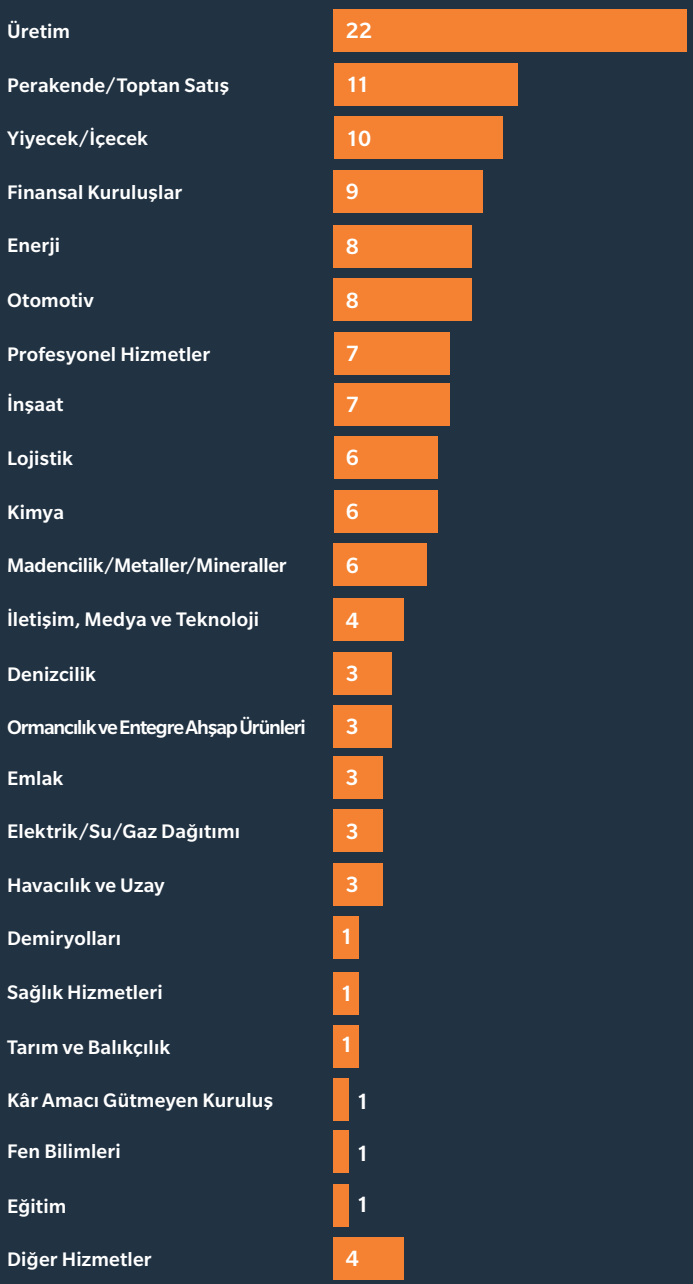
Şirket Çalışan Sayısı (%)



Ortalama: 3625

Şirketteki Görev Alanları (%)

Şirket Faaliyet Alanları (%)



Daha fazla bilgi için:

SEÇİL ÖZTÜRK
Marsh Risk Consulting Türkiye
İş Geliştirme Direktörü
secil.ozturk@marsh.com

ULVİ CEMAL BUCAK
Marsh Risk Consulting Türkiye
Siber Güvenlik ve İş Sürekliliği Direktörü
cemal.bucak@marsh.com

DİLAN GÜNGÖRDÜ
Marsh Türkiye
Finansal ve Profesyonel Sigortalar Müdürü
dilan.gungordu@marsh.com