

HOWDEN

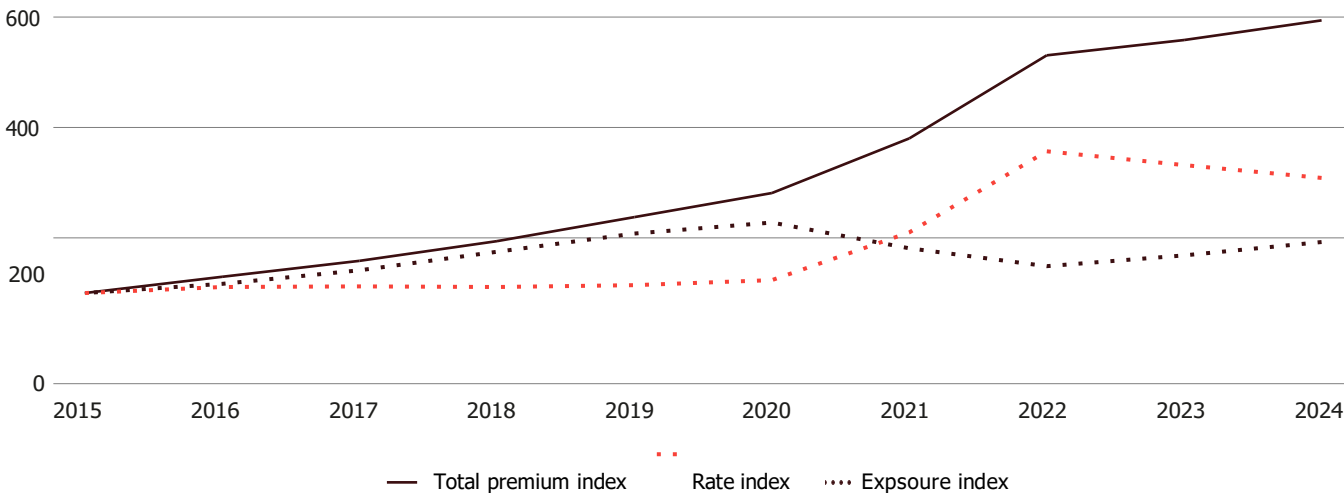
Siber Sigortaları

Büyümeye Yeniden İvme Kazandırmak

Temel Noktalar

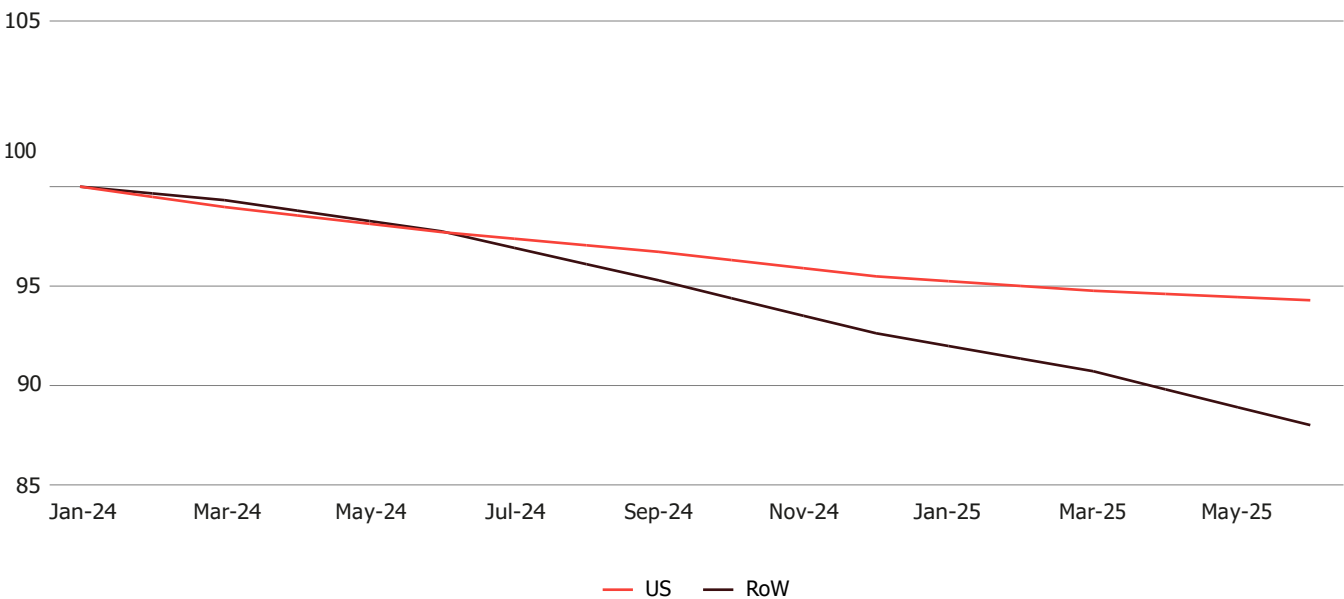
Siber sigorta pazarı bir kırılma noktasında; prim artışı, düşen fiyatlar ve durağan risk maruziyetleri nedeniyle ivme kaybediyor. Bir sonraki büyüme döngüsü, özellikle yeterince hizmet almayan bölgelerde penetrasyonun artırılması yoluyla yeni risk havuzlarının açığa çıkarılmasına odaklanacak. Bu da sigorta alıcıları ve (re)sigortacılar için yeni fırsatlar yaratacak.

Plateauing global premium growth since 2022



Elverişli piyasa koşulları, sigorta alıcılarının, sıkı piyasa döneminden önceki seviyelerdeki şartlar ve fiyatlarla teminat sağlamalarına olanak tanıyor. Bu sırada sigortacılar, yüksek potansiyel ile kanıtlanmış kârlılığı bir araya getiren bu branşa olan bağlılıklarını daha da derinleştiriyor.

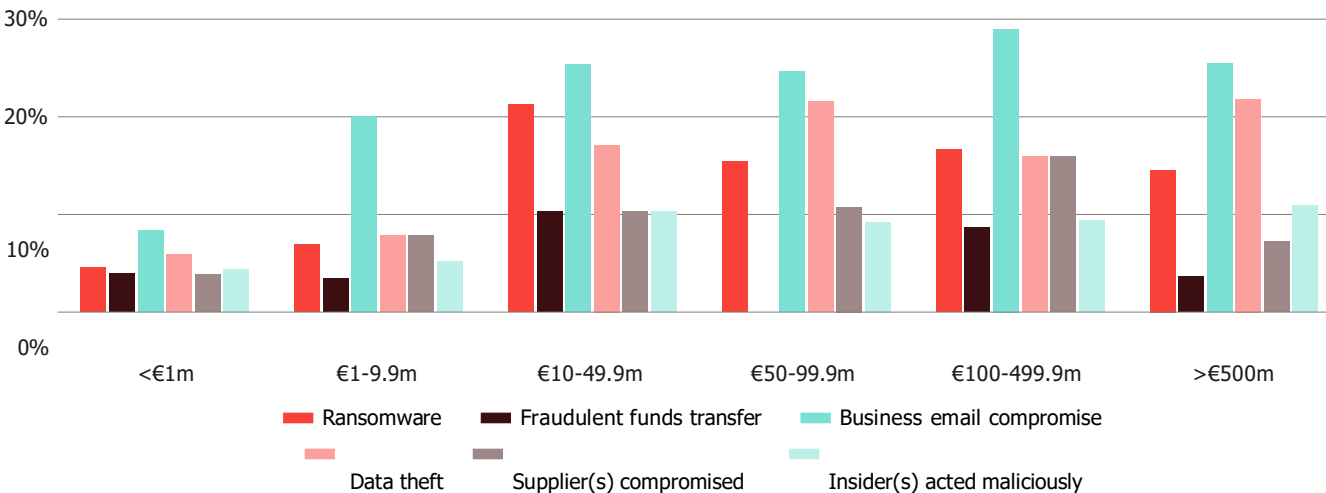
Softening rate environment in international markets in particular



Gelecekteki büyüme, yeni iş alanlarının güvence altına alınmasına bağlı ve bu raporun odağında Avrupa yer alıyor.

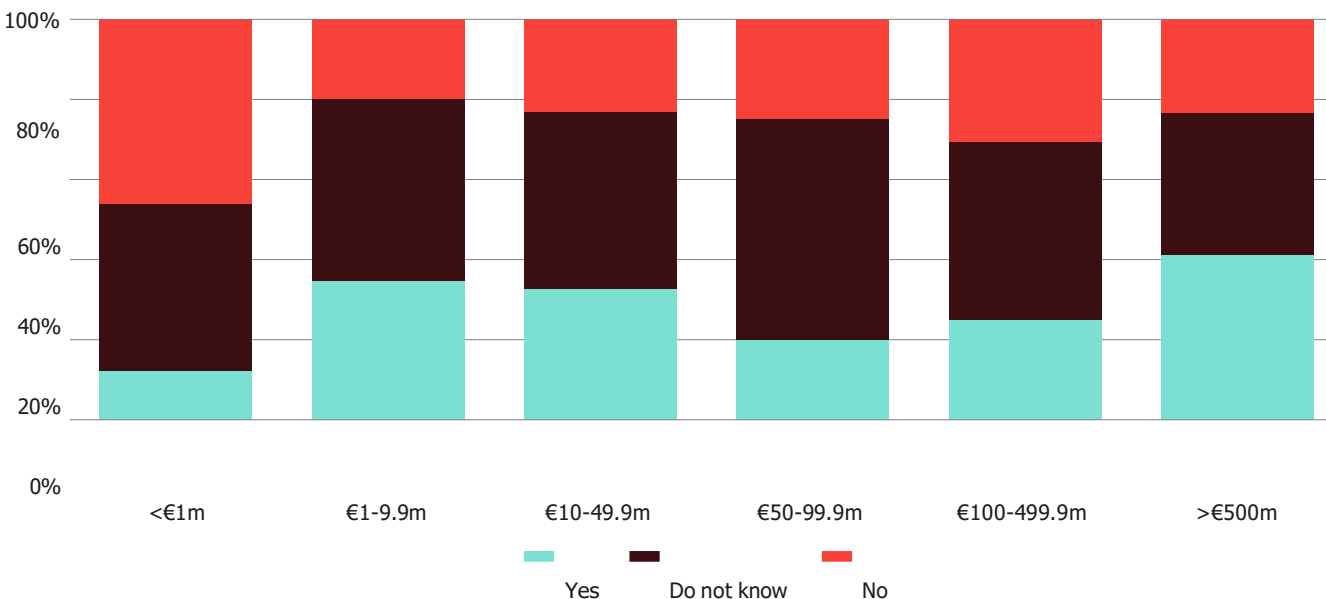
Son beş yılda Fransa, Almanya, İtalya ve İspanya'da siber saldırıların yol açtığı yaklaşık 300 milyar avroluk ekonomik etki, tehdidin büyüklüğünü ve etkin risk transferine duyulan acil ihtiyacı açıkça ortaya koyuyor.

Frequency of cyber-attacks by revenue band for surveyed companies



Bu rapor, siber sigortanın güçlü değer önerisini ortaya koyuyor; analizimiz, %19'luk bir yatırım getirisi sağladığını gösteriyor. Artık gizli kalmış talebin açığa çıkarılması konusunda sorumluluk brokerlar ve sigorta şirketlerine düşüyor — bu da, toparlanma sürecini hızlandırarak ve finansal kayıpları azaltarak kurumsal dayanıklılığın güçlendirilmesini mümkün kılıyor.

Future cyber insurance purchase intentions for non-buyer survey respondents



Özet

Siber sigorta, son on yılın öne çıkan başarı hikâyelerinden biri olmuştur.

Dünya genelinde işletmelere her yıl milyarlarca dolara mal olan karmaşık ve dalgalı bir tehdit ortamıyla karşı karşıya kalan sektör, geleneksel zarar teminatını proaktif risk yönetimi hizmetleriyle birleştirerek güçlü bir büyüme ve kârlılık motorunun kilidini açmıştır.

Kırılma Noktası

Ancak ilk kez, bu büyüme hikayesi rüzgara karşı ilerlemeye başladı.

Global fiyatlar düşmeye devam ediyor; 2022 ortasındaki zirveye kıyasla %22 oranında gerilemiş durumda ve pazarın risk maruziyet tabanı bu kaybı telafi edecek hızda genişlemiyor.

Performans hala güçlü seyretse de – global birleşik rasyolar ortalama %70 seviyesinde ve 2022-2024 arasında yaklaşık 9 milyar ABD doları tutarında sigortacılık karı yaratıldı – global brut prim üretimi aynı dönemde yıllık bileşik %6 büyümeye geriledi. Bu, 2020 -2022 arasında fiyatların yüksek çift haneli oranlarla arttığı dönemde görülen yaklaşık %40'lık CAGR'a kıyasla keskin bir düşüşü temsil ediyor.

En temkinli prim hedeflerine ulaşmak bile, hizmet alınmayan bölgelerde korumanın yaygınlaştırılması için kararlı bir çaba gerektirecektir.

Mevcut fiyat trendlerinin devam etmesi durumunda, analizimiz siber sigortacıların önümüzdeki yıllarda risk maruziyetlerini yıllık yaklaşık %15 oranında artırmaları gerektiğini gösteriyor. Bu büyümenin büyük kısmı, mevcut limitlerin yükseltilmesinden ziyade yeni işlerden kaynaklanacaktır.

Mevcut piyasa koşulları, özellikle uluslararası piyasalarda, yeni alıcılar için elverişli bir giriş noktası sunuyor. Burada fiyatlar, 2024 başından buyana %12 düşerken, ABD'deki düşüş oranı yalnızca %6 seviyesinde kaldı.

€307^{bn}

2020-2025 yılları arasında Almanya, Fransa, İtalya ve İspanya'da siber saldırıların tahmini ekonomik maliyeti.

%19

Yıllık 500 milyon € gelir elde eden işletmeler için siber sigortanın yatırım getirisi.

%41

İlk kez siber sigorta satın almayı önümüzdeki beş yıl içinde planlayan büyük ölçekli işletmeler (>500 milyon € gelir).

Avrupa'daki Fırsatı Daha İyi Anlamak İçin

Howden, yakın zamanda Almanya, Fransa, İtalya ve İspanya'daki geniş bir iş kesimini kapsayan bir anket gerçekleştirdi. Sonuçlar, kapsamlı bir teminat ihtiyacının, risk yönetimi ve sigortadan güçlü bir yatırım getirisinin ve ilk kez sigorta alacakları kapsayan hazır bir alıcı kitlesinin varlığını ortaya koyuyor.

Ankete katılan işletmelerin yarısı, 2020-2025 yılları arasında siber saldırıya maruz kaldı ve bu durum dört ekonomide toplamda yaklaşık 307 milyar avroluk ekonomik maliyete yol açtı. Beklendiği üzere, katılımcıların %69'u, liderlik kadrolarının siber riski önemli bir tehdit olarak doğru şekilde değerlendirdiğine inanıyor.

Siber sigorta hem riski azaltmada hem de transfer etmede oldukça etkili olduğunu kanıtlıyor. Hasar ödemelerinin yanı sıra, sağlam risk kontrolü uygulamalarının benimsenmesini teşvik ediyor ve kriz yönetimi hizmetlerine standart erişim sağlıyor; bu hizmetlere şu anda sigorta yaptırmayanların sadece %20'si sahip.

Toplamda, yıllık 500 milyon avro gelir elde eden bir işletme için siber sigorta satın almak, 10 yıllık dönemde siber saldırı kaynaklı yaklaşık 16 milyon avro tasarruf sağlayabilir. Bu da %19'luk bir yatırım getirisine karşılık geliyor; teminat maliyetini fazlasıyla karşılayan ve finansal getiriye net şekilde gösteren etkileyici bir sonuç.

Değer önerisi net. Pazar, önümüzdeki beş yıl içinde siber sigorta satın alma niyetini belirten şirketler için açık kapı niteliğinde; bunların arasında 500 milyon avro üzeri gelire sahip olanların %41'i yer alıyor. Kararsız olan yüksek oranlardaki sigorta yaptırmayanlar göz önüne alındığında, fırsat çok daha büyük olabilir. Bu durum, pazarın ilgiyi benimsemeye, bilgilendirmeye ve satın almaya dönüştürmeye yönelik net bir çağrısıdır.

Howden, uzun süredir risk yönetimini, teminatları ve satın alma deneyimini geliştirerek siber sigortayı savunmaktadır. Bu araştırmayı, yeni kitlelerle etkileşim kurmak ve karar alma süreçlerini desteklemek amacıyla.

Come and talk to us.

Kırılma Noktası

Siber sigorta, gelişiminde kritik bir dönemeçte bulunuyor. Özel bir branş olarak benzersiz bir yol izledi; başlangıçta temkinli adımlar, güçlü sonuçlarla artan güven, piyasayı etkileyen zarar dönemleri ve kapasite çekilmesi... Şimdi ise rekabet artarken ve fiyatlar düşerken siber sigorta pazarı bir kırılma noktasına ulaşmış durumda.



Mevcut piyasa koşullarının (büyük bir zarar yaşanmadığı sürece) yakın gelecekte de devam etmesi muhtemel olduğundan, gelecekteki büyüme, KOBİ'ler ve uluslararası bölgeler gibi yeterince hizmet almayan pazarlarda penetrasyonun artırılmasına bağlıdır.

Siber sigortanın değeri (ve gerekliliği) her zamankinden daha güçlüdür. Yüksek profilli fidye yazılımı saldırılarının hedefi olan İngiltere ve ABD şirketlerinin yanı sıra daha geniş çaplı saldırıların yol açtığı etkilerin görüldüğü, ayrıca ayrı bir kötü niyet taşımayan BT kesintisinin yaşandığı yüksek tehditli 18 aylık dönemde, siber sigorta etkilenen firmaların ve daha geniş ekonomilerin dayanıklılığında kritik bir rol oynamıştır.

Hasar ödemelerinin ötesinde, teminat aynı zamanda sigortalılara uzman olay müdahale hizmetlerine anında erişim sağlar; bu sayede tehditlerin kontrol altına alınması, iyileşme sürecinin hızlanması ve zararların sınırlandırılması mümkün olur. Özellikle KOBİ'ler, poliçeleri kapsamında sunulan dış uzman hizmetlerden önemli ölçüde faydalanmıştır.

Yaygın Bir Tehdit

Güçlendirilmiş siber dayanıklılık, zorlu risk ortamında sigortalılar (ve sigortacılar) için olumlu sonuçlar doğuruyor.

Fidye yazılımı, 2022'den bu yana her yıl bir öncekinden daha fazla küresel olay yaşanmasıyla (Şekil 1'de NCC verileriyle gösterildiği gibi) en önemli tehdit olmaya devam ediyor.

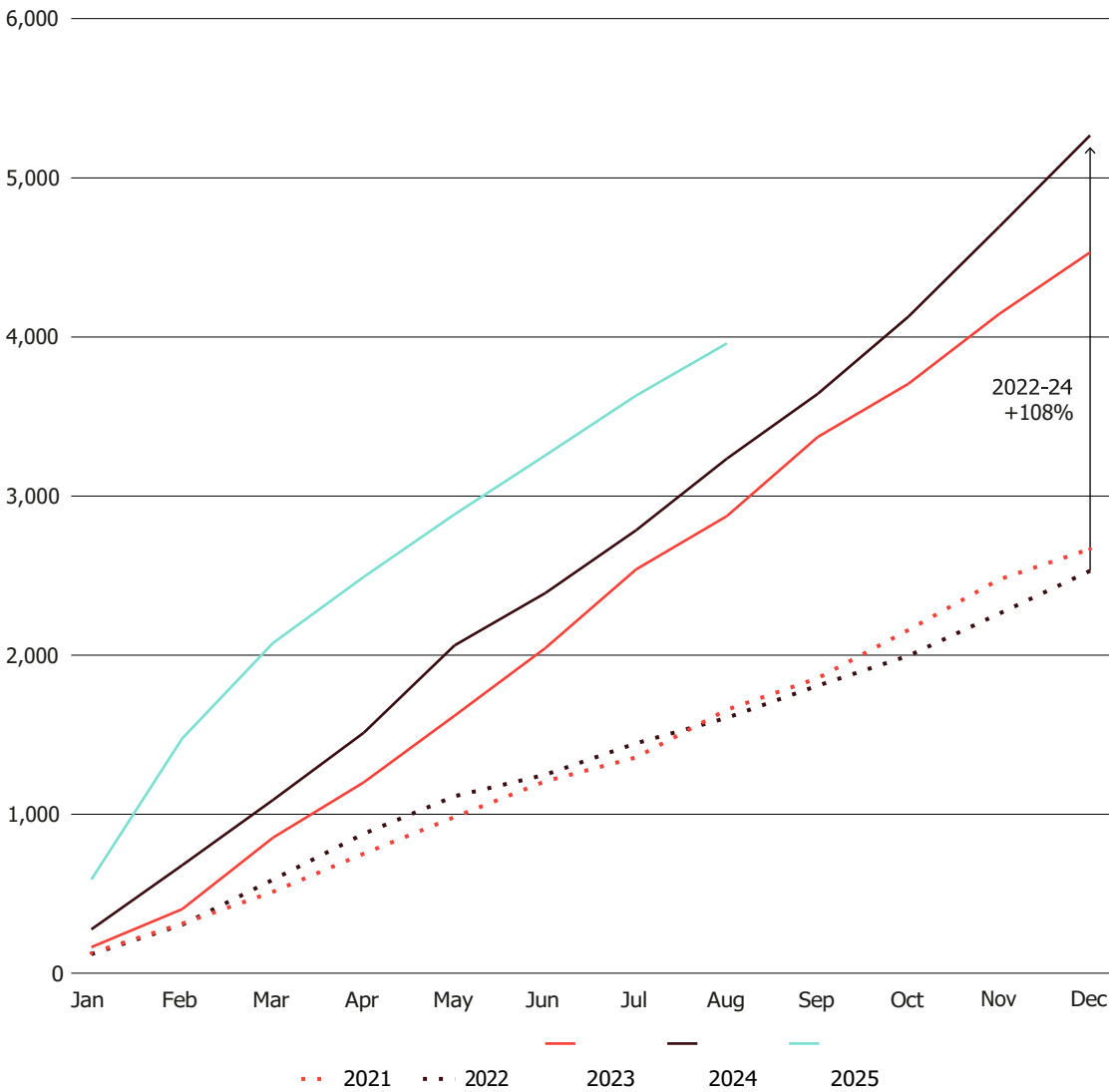
Hâlâ yüksek seyreden sigortacılık kâr marjları, artan küçük hasar talepleri ve devam eden büyük çaplı saldırılar nedeniyle daralmaya başladı.

Microsoft, yakın zamanda devlet destekli bilgisayar korsanlarının SharePoint sunucularındaki bir güvenlik açığını kullandığını doğruladı; bu durum en az 400 şirketi etkiledi.

Ayrıca, Salesloft Drift ile ilgili ayrı bir güvenlik ihlali de 700'den fazla firmayı etkiledi.

Figure 1: Cumulative global ransomware activity – 2021 to 3Q25¹

(Source: Howden analysis based on NCC data)



¹ NCC Group tracks ransomware groups operating the hack and leak double extortion tactic by monitoring leak sites and scraping victims' details as they are released.



Aynı zamanda, ABD’de farklı bir risk türü giderek artıyor; biyometrik veri ihlalleri ve piksel takibi davalarındaki artış nedeniyle gizlilikle ilgili talepler yükseliyor.

Sistemik tehditlerden kaynaklanan risk birikimi endişesiyle birleşen bu durum, siber sigorta pazarının artık küçük hasar talepleri, büyük çaplı olaylar ve uzun vadeli risklerle karakterize edilen benzersiz bir zarar ortamında yol aldığı anlamına geliyor.

Artan jeopolitik gerilimler ve hızlı teknolojik değişimlerle daha da belirsizleşen değişken tehdit ortamına rağmen, siber sigorta, sigortacılık sektörünün en iyi performans gösteren alanlarından biri olmaya devam ediyor ve yeni iş fırsatları ile yeniliklerin odak noktası olarak öne çıkıyor. İşletmeler, elverişli piyasa koşullarından faydalanırken, güçlü sonuçlar ve özellikle ABD dışındaki büyük, henüz keşfedilmemiş risk havuzlarının cazibesi, reasürörlerden artan taahhütler almayı sağlıyor.

Tüm bunlar, günümüzde hem sigorta alıcılarına hem de kapasite sağlayıcılarına siber sigortanın sunduğu cazip değeri açıkça ortaya koymaktadır. Devam eden analiz, karmaşık bir hasar ortamının hâlâ kabul edilebilir seviyelerde seyrettiğini, fiyatlarda bir yumuşama olduğunu ancak ABD ile diğer bölgeler arasında hızlanan bir ayrışma yaşandığını ve siber sigortanın sigortacılık sektörünün en hızlı büyüyen alanlarından biri olarak konumunu yeniden kazanmasının, yeni iş hacminin güçlendirilmesine bağlı büyük bir büyüme fırsatı sunduğunu göstermektedir.

Fidye Yazılımını Kontrol Altına Almak

Fidye yazılımı, bu yıl yaşanan birçok yıkıcı saldırı ve tehdit aktörlerinin artık sadece düşmanca devletlerle sınırlı kalmamasıyla siber zarar ortamında hakimiyetini sürdürüyor.

Üçüncü taraf tedarikçileri hedef alan ve sıklıkla İngilizce ana dilini kullanan kişilerin sosyal mühendislik teknikleriyle yardım masalarını kandırarak erişim sağladığı ihlallerin öne çıkması, 2025 yılında dikkat çeken önemli bir gelişme olmuştur.

Global fidye yazılımı saldırılarındaki artış, büyük ölçüde ilk çeyrekte fidye yazılımı grubu ClOp tarafından gerçekleştirilen geniş çaplı bir istismar kampanyasından ve ikinci ile üçüncü çeyrekte İngiltere ve ABD’de çok sayıda firmaya yönelik Scattered Spider saldırı serisinden kaynaklanan gecikmeli bir yükselişi yansıtmaktadır.

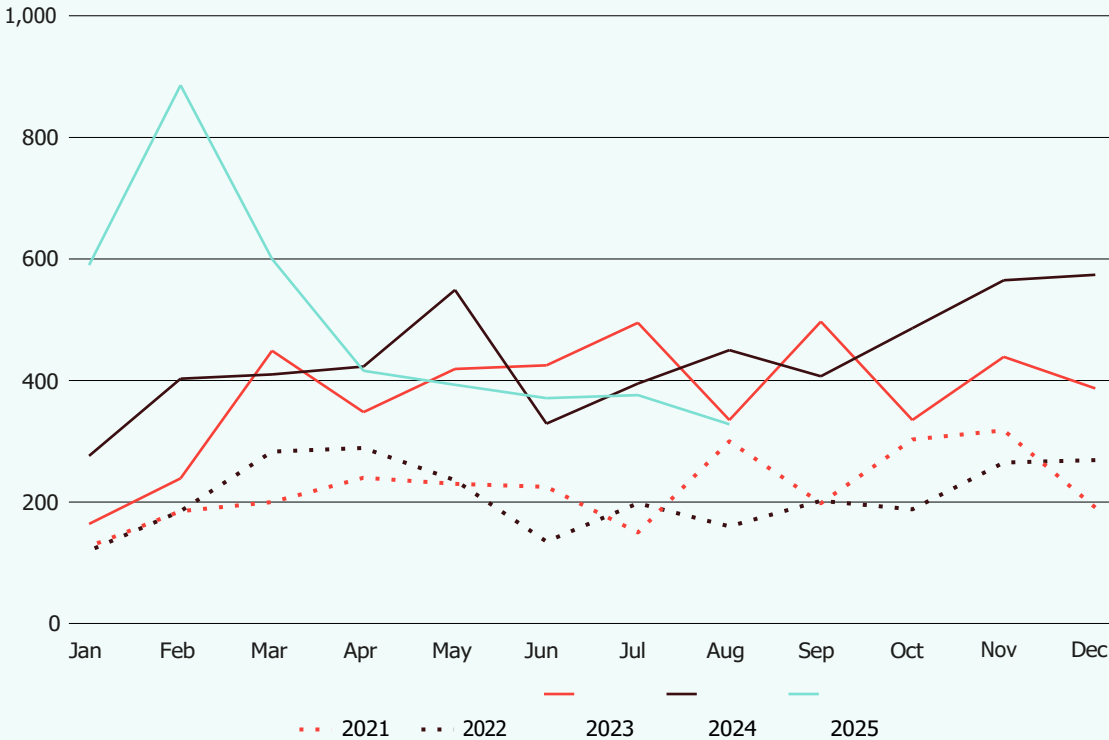
Bu durum, işletmeler için devam eden tehditin göstergesidir.

Howden Re’nin yakın zamanda yayımladığı Cyber Watch tehdit raporundaki analiz, 2025’in ilk yarısında fidye yazılımı mağdurlarının %9’unun, firmamızın özel sektör maruziyet veri tabanındaki sigortalı kuruluşlarla eşleştiğini göstermektedir (2024 yılı tamamı için bu oran %8 idi).

Bu mağdurların çoğunluğunu 50 milyon ABD dolarının altında gelire sahip küçük ölçekli şirketler oluşturmakta olup, bu durum fırsatçı saldırı kampanyalarının KOBİ’ler üzerindeki etkisini ve sigorta kapsamının savunmasız işletmelere nasıl yayıldığını ortaya koymaktadır.

Figure 2: Monthly breakdown of global ransomware activity – 2021 to 3Q25

(Source: Howden analysis based on NCC data)



² Howden Re, *Cyber Watch report: strategic threat review*, August 2025.

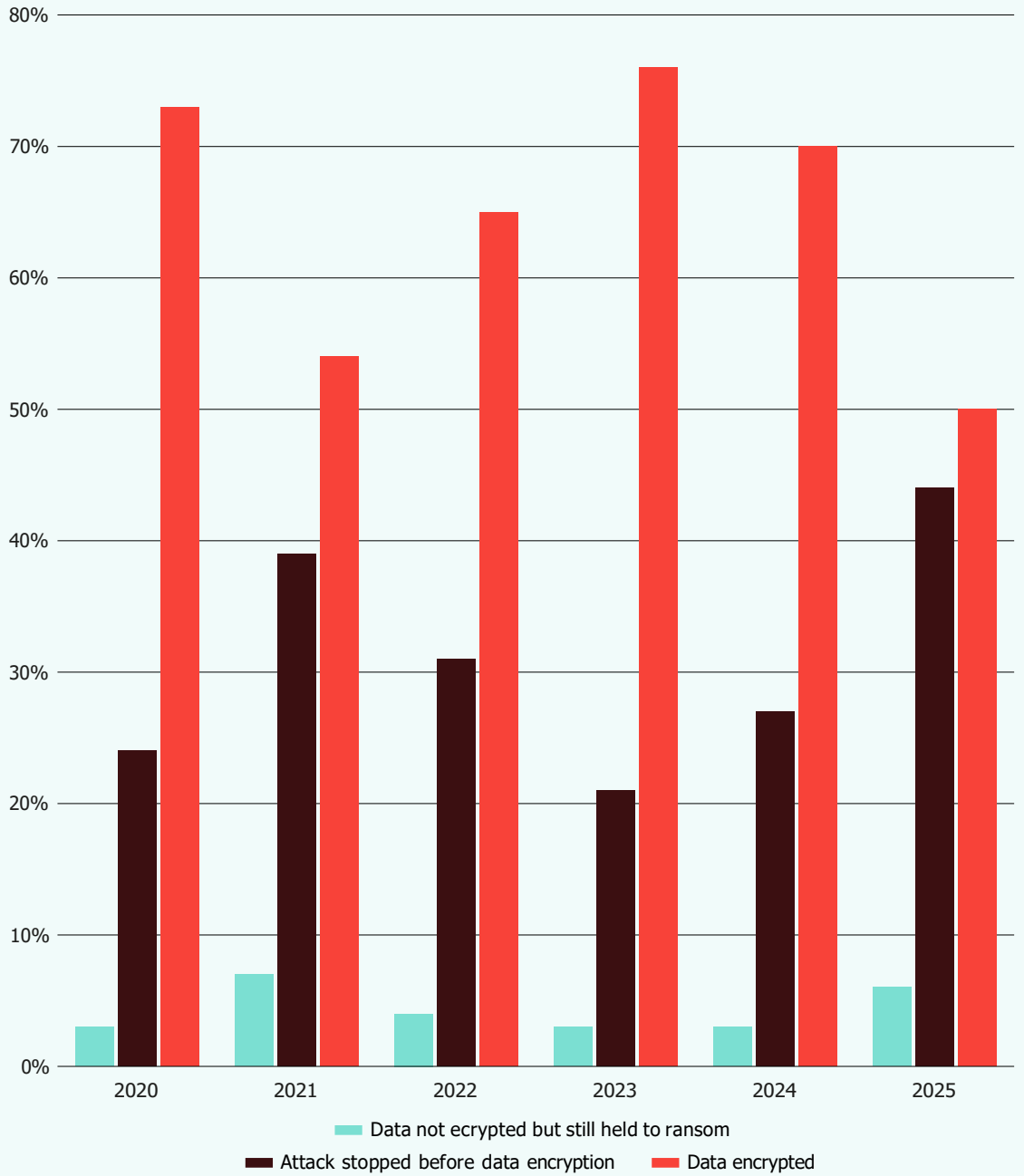
2025 yılında fidye yazılımı zararları mikro düzeyde alarm verici boyutlara ulaşmıştır; birçok yüksek profilli saldırı, milyonlarca dolarlık maddi hasara yol açmış ve kurumsal sistemlerin kritik güvenlik açıklarını ortaya çıkarmıştır.

Ancak makro düzeyde ilerleme işaretleri de görülmektedir.

Veri şifrelemesi gerçekleşmeden saldırıyı durdurabilen fidye yazılımı mağdurlarının oranı, 2024'te %27'den 2025'te %44'e yükselmiştir (Şekil 3'te gösterildiği gibi). Bu durum, izleme ve hızlı müdahale yeteneklerindeki anlamlı gelişmeleri ve daha geniş anlamda artan kurumsal dayanıklılığı yansıtmaktadır.

Figure 3: Data encryption rate in ransomware attacks – 2020 to 2025

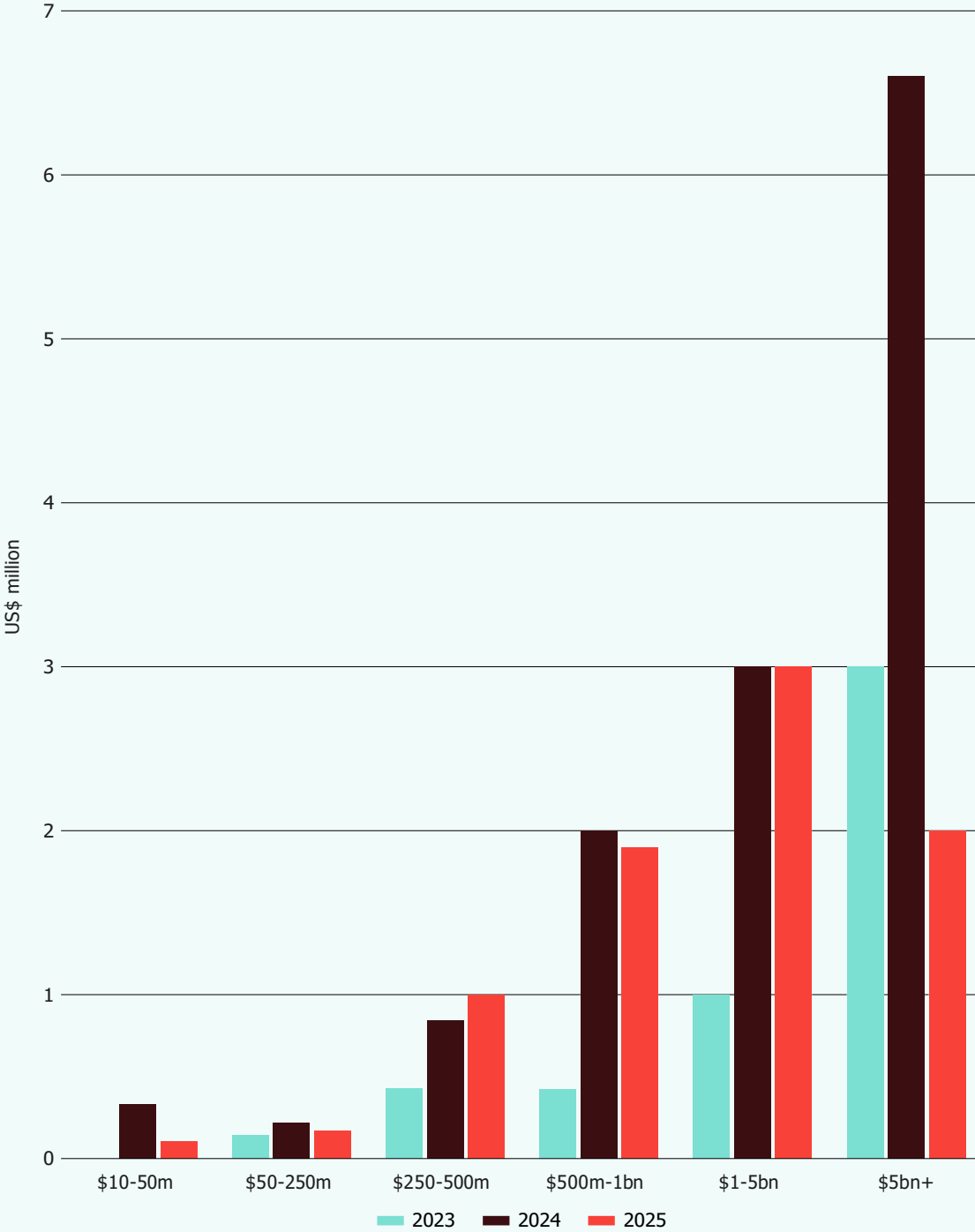
(Source: Howden analysis based on Sophos data)



Şekil 4, ortanca fidye ödemelerinin çoğu gelir grubunda sabit kaldığını veya arttığını göstermektedir; yalnızca 5 milyar ABD doları üzeri gelir grubunda dalgalanma görülmektedir ki bu da büyük ölçekli şirketlerin saldırıya uğrayıp uğramamasına bağlı olarak değişkenlik göstermektedir. Fidye tutarları şirket büyüklüğüyle yakından ilişkili olduğundan, yıllık ortalama ödeme tutarındaki değişimler, ödemelerin miktarından çok mağdurların gelir profiline bağlı olarak şekillenmektedir.

Figure 4: Median ransom payment by revenue band – 2023 to 2025

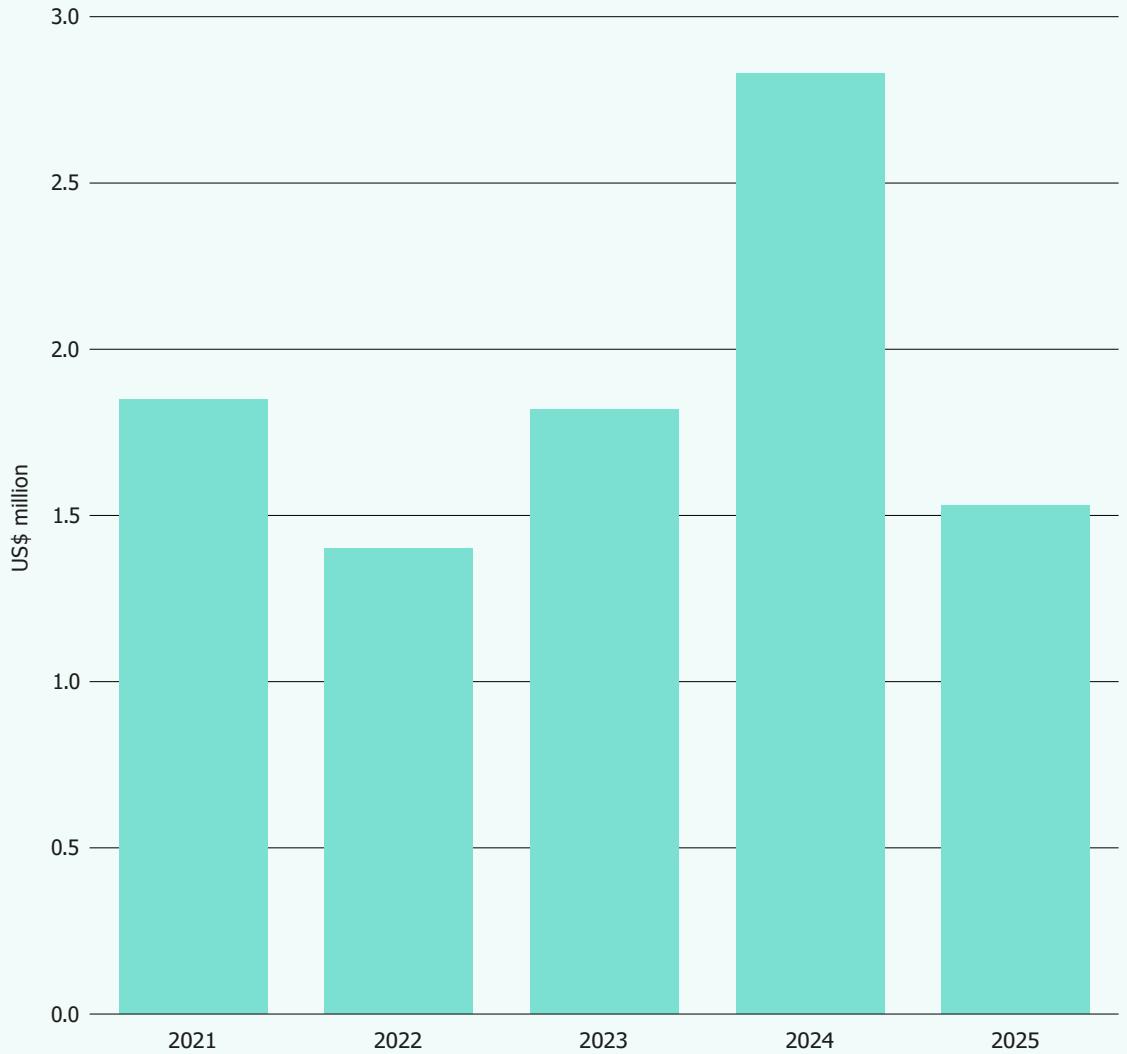
(Source: Howden analysis based on Sophos data)



Kurtarma maliyetleri, genellikle fidye ödemelerinin ötesine geçen ek bir yük olarak işletmelerin üzerinde ciddi bir baskı oluşturmaktadır. Her ne kadar Şekil 5, 2025 yılında ortalama maliyetlerde %45'lik bir düşüş olduğunu gösterse de, fidye ödemelerine ek olarak ortaya çıkan 1,5 milyon ABD doları tutarındaki gider, çoğu kuruluş için ciddi sonuçlar doğurabilecek anlamlı bir maliyet olmaya devam etmektedir.

Figure 5: Mean recovery costs from ransomware attacks – 2021 to 2025³

(Source: Howden analysis based on Sophos data)



Yılın fidye yazılımı cephesinde hareketli başlamasına rağmen, siber güvenlikteki iyileşmeler, kuruluşların genel dayanıklılığını artırmada son derece etkili olduğunu kanıtlamaktadır. Siber sigortanın değeri ise açıkça ortadadır — yalnızca finansal bir güvence sağlamakla kalmaz, aynı zamanda siber hijyenin iyileştirilmesi, olay müdahalesi ve operasyonel dayanıklılığın güçlendirilmesinde de önemli bir rol oynar.

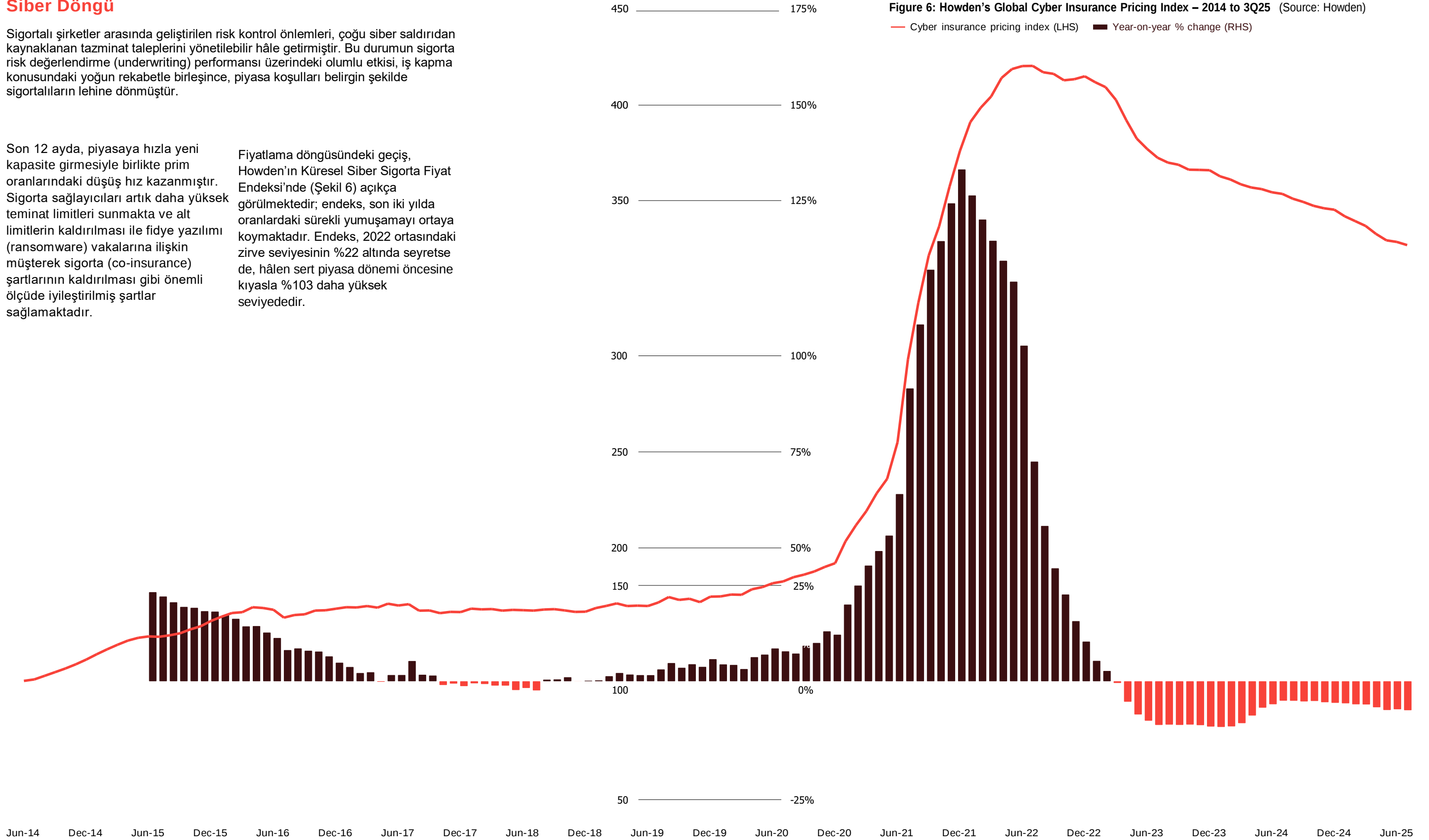
³ Recovery costs include downtime, people time, device costs, network costs, lost opportunities and exclude ransom payments.

Siber Döngü

Sigortalı şirketler arasında geliştirilen risk kontrol önlemleri, çoğu siber saldırıdan kaynaklanan tazminat taleplerini yönetilebilir hâle getirmiştir. Bu durumun sigorta risk değerlendirme (underwriting) performansı üzerindeki olumlu etkisi, iş kapma konusundaki yoğun rekabetle birleşince, piyasa koşulları belirgin şekilde sigortalıların lehine dönmüştür.

Son 12 ayda, piyasaya hızla yeni kapasite girmesiyle birlikte prim oranlarındaki düşüş hız kazanmıştır. Sigorta sağlayıcıları artık daha yüksek teminat limitleri sunmakta ve alt limitlerin kaldırılması ile fidye yazılımı (ransomware) vakalarına ilişkin müşterek sigorta (co-insurance) şartlarının kaldırılması gibi önemli ölçüde iyileştirilmiş şartlar sağlamaktadır.

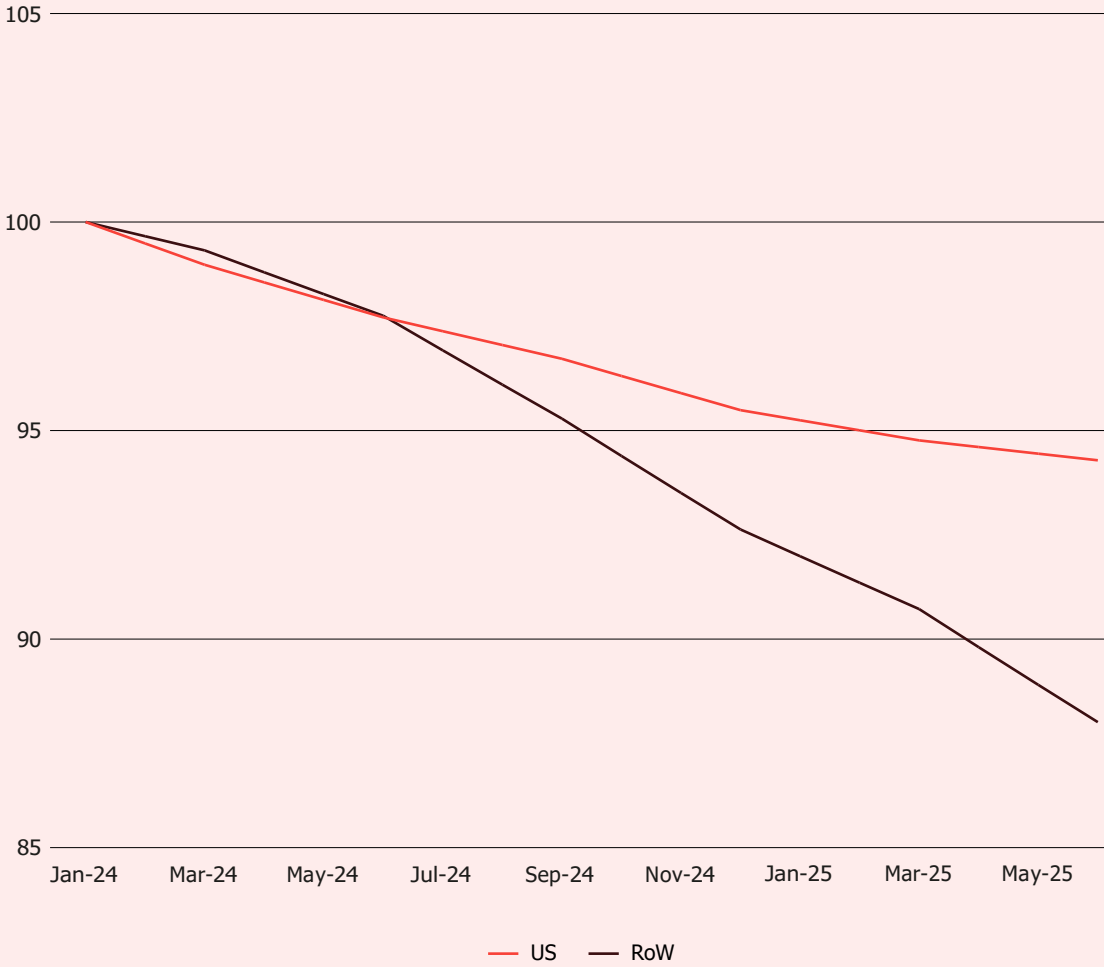
Fiyatlama döngüsündeki geçiş, Howden'ın Küresel Siber Sigorta Fiyat Endeksi'nde (Şekil 6) açıkça görülmektedir; endeks, son iki yılda oranlardaki sürekli yumuşamayı ortaya koymaktadır. Endeks, 2022 ortasındaki zirve seviyesinin %22 altında seyretse de, hâlen sert piyasa dönemi öncesine kıyasla %103 daha yüksek seviyededir.



Şekil 7’de görüldüğü üzere, ABD ve uluslararası piyasalar arasındaki fiyatlamaya eğilimleri farklılaşmaya başlamıştır. Uluslararası piyasalarda, alıcılar lehine devam eden olumlu koşullar, yönetilebilir zarar deneyimi ve güçlü büyüme potansiyeli, prim oranlarında düşük ila orta düzeyde çift haneli düşüşlere yol açarken; ABD piyasası ise, kendi düzenleyici ve dava ortamına özgü gizlilikle ilgili taleplerle başa çıkmaya çalışırken fiyatlarda istikrar sinyalleri vermeye başlamıştır.

Figure 7: Cyber insurance pricing indices for US vs rest of the world – 2024 to 1H25

(Source: Howden)

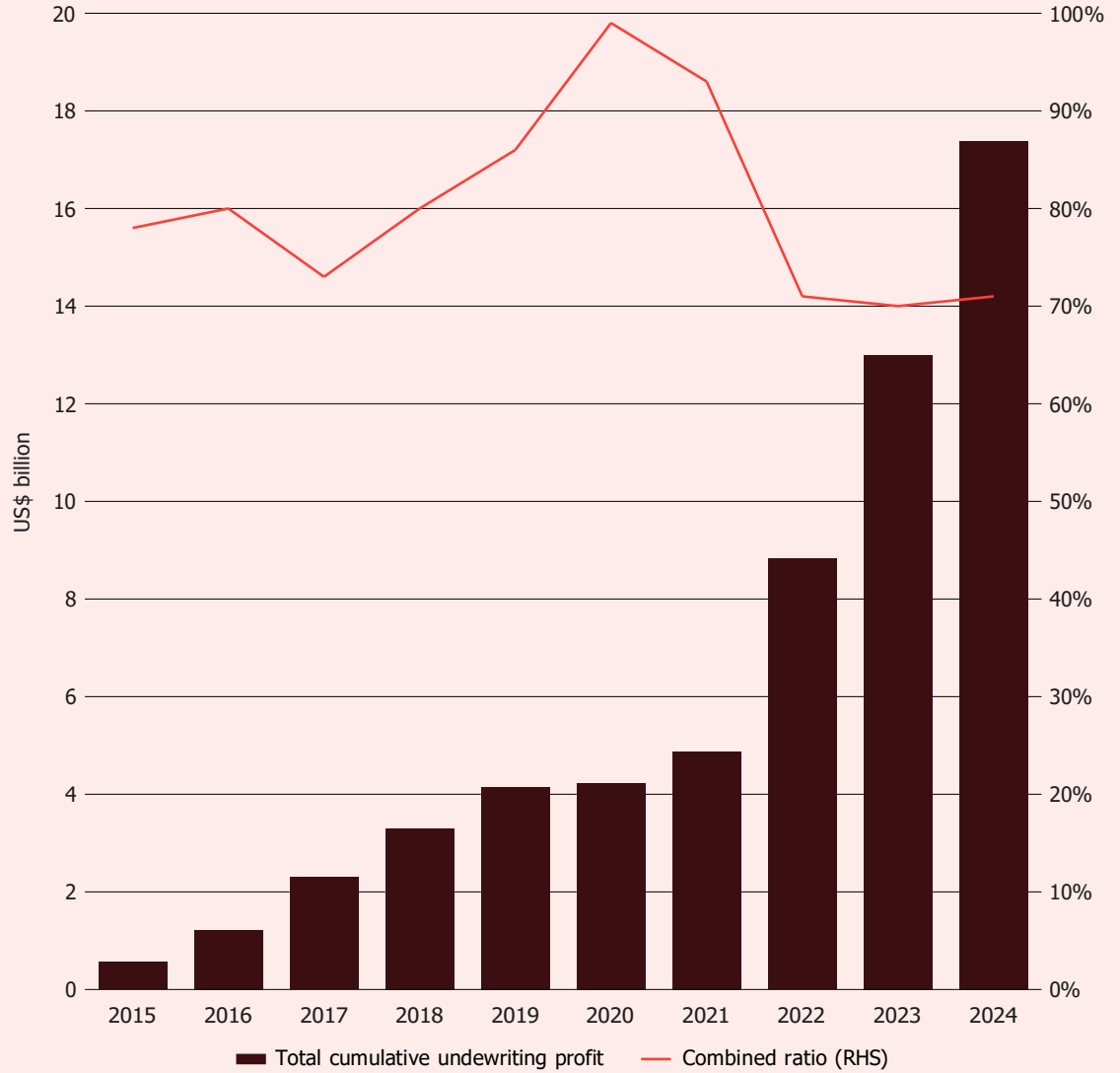


Note: RoW excludes Canada

Siber risklerin fiyatlandırılmasındaki piyasa olgunluğu ile 2025/26 için belirlenen iddialı büyüme hedefleri, prim oranlarındaki yumuşamaya rağmen önemli bir kâr tamponunun mevcut olduğunu göstermektedir. Howden’in sigorta risk değerlendirme (underwriting) performansına ilişkin analizi de bu görüşü desteklemekte olup, Şekil 8’de 2015’ten bu yana küresel siber sigorta pazarındaki kümülatif kârlılık grafiklendirilmiştir.

2021’e kadar yıllık ortalama 0,7 milyar ABD doları artışla pozitif ancak istikrarlı underwriting kazançları kaydedilirken, sonraki yıllarda kârlılık belirgin şekilde iyileşmiştir. 2022-2024 döneminde, daha yüksek prim oranları ve daha düşük birleşik oranların (combined ratio) uygulandığı, önemli ölçüde genişlemiş prim tabanı sayesinde ortalama underwriting kârları yıllık 4,3 milyar ABD doları artmış; bu da piyasanın hızla değişen zarar ortamının önünde kalma kapasitesini ortaya koymuştur.

Figure 8: Cumulative underwriting profit for global cyber insurance market – 2015 to 2024⁴
(Source: Howden)



Arz tarafındaki bu gelişmeler, siber risk konusundaki farkındalığın artması ve koruma talebinin yükselmesiyle aynı döneme denk gelmiştir. Bu durum, sadece yeni alıcılar arasında (genişleyen Hasar ve Kayıp – P&C – piyasasının yumuşamasıyla başka alanlarda sağlanan prim tasarruflarını yeniden yatırıma yönlendiren artan sayıda şirket dahil) değil, aynı zamanda mevcut müşterilerin de kapsam ihtiyaçlarını yeniden değerlendirmesiyle kendini göstermektedir.

2024'te yaşanan zararlar dizisi ve 2025'teki yüksek profilli siber saldırılar, birçok işletim için ek bir uyarı niteliği taşımış; firmaları, teminat limitlerinin yeterliliğini ve olay müdahale planlarının sağlamlığını yeniden değerlendirmeye sevk etmiştir. Tüm bunlar, giderek daha alıcı bir piyasa ortamında gerçekleşmektedir.

⁴ Global market based on premium and loss ratio data from Howden and third parties, including NAIC, Lloyd's and Beazley.

Büyümeye Yeniden İvme Kazandırmak

Mevcut piyasa koşulları, iki yönlü bir fırsat sunmaktadır: Alıcılar için, uygun fiyatlar ve şartlarla koruma sağlama imkânı; sigortacılar için ise, önemli (risk temelli) büyüme potansiyeli ve etkileyici bir kârlılık geçmişini sergileyen bir sektöre daha fazla yatırım yapabilme fırsatı.

Şekil 9, ABD siber sigortacıların büyüme ve underwriting performansını son on yılda ABD genelinde Hasar ve Kaza (P&C) piyasasıyla karşılaştırmaktadır. Analizi üç ayrı döneme ayırarak yapılan değerlendirme, hem büyüme hem de underwriting alanlarında siber sigortanın üstün performansını doğrulamakla birlikte, 2022-2024 arasındaki sert piyasa dönemlerinde büyümenin önemli ölçüde durakladığını göstermektedir.

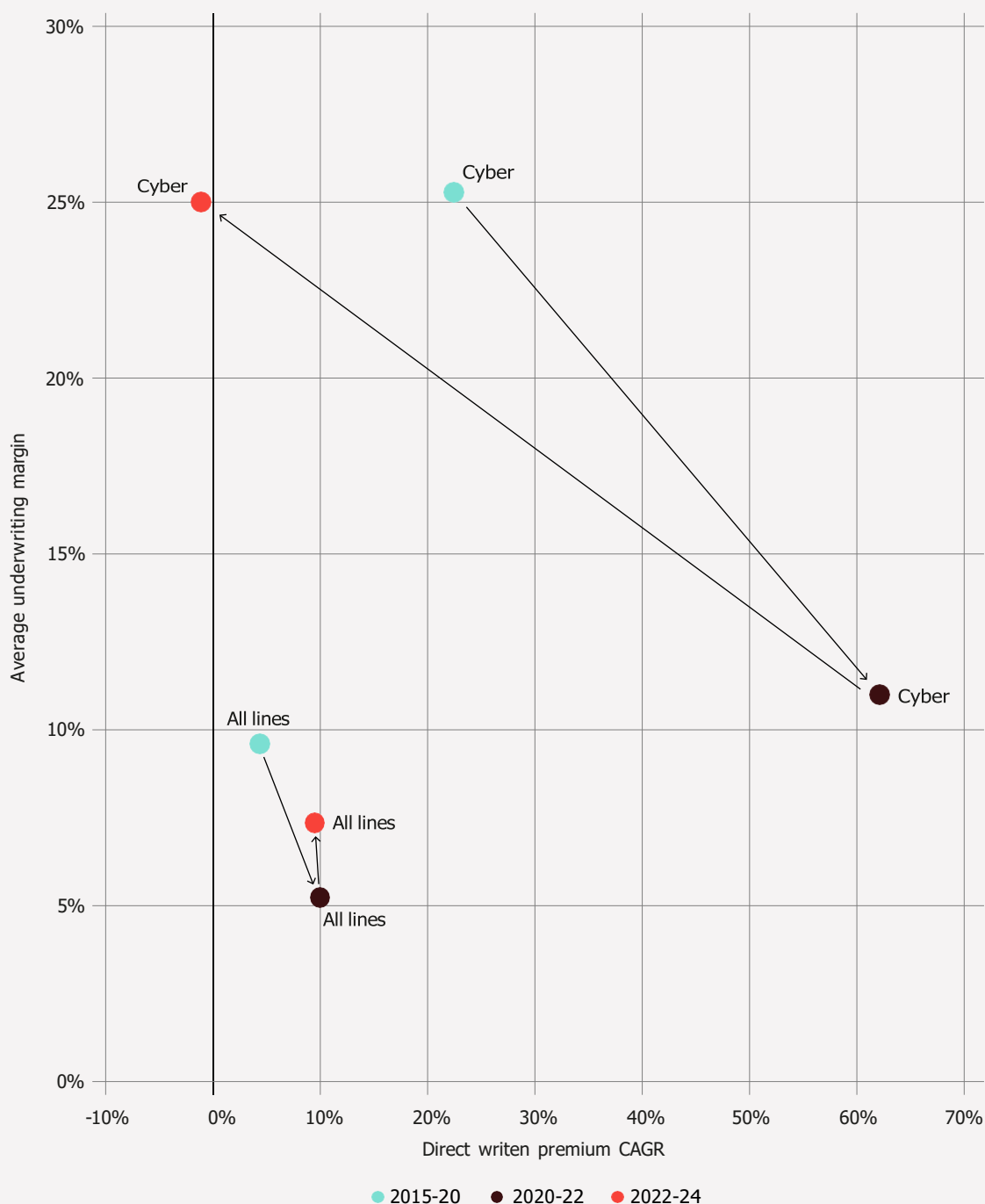
Bu analiz ABD'ye özgü verilere dayansa da (ABD dışındaki siber piyasalar için karşılaştırılabilir kalite ve şeffaflık halen gelişme aşamasındadır), baskın eğilimler uluslararası alanda da geçerlidir. Örneğin, Fransız piyasasında primler 2024 yılında hafifçe daralırken, kayıp oranı %17 olarak gerçekleşmiştir.

“

Mevcut piyasa koşulları, yeni alıcılar için avantajlı bir giriş noktası sunmaktadır.

⁵ Cyber premiums in France fell from €328 million in 2023 to €317 million in 2024, according to AMRAE.

Figure 9: Growth vs profitability for US cyber and broader P&C market – 2015 to 2024
 (Source: Howden analysis based on NAIC data)

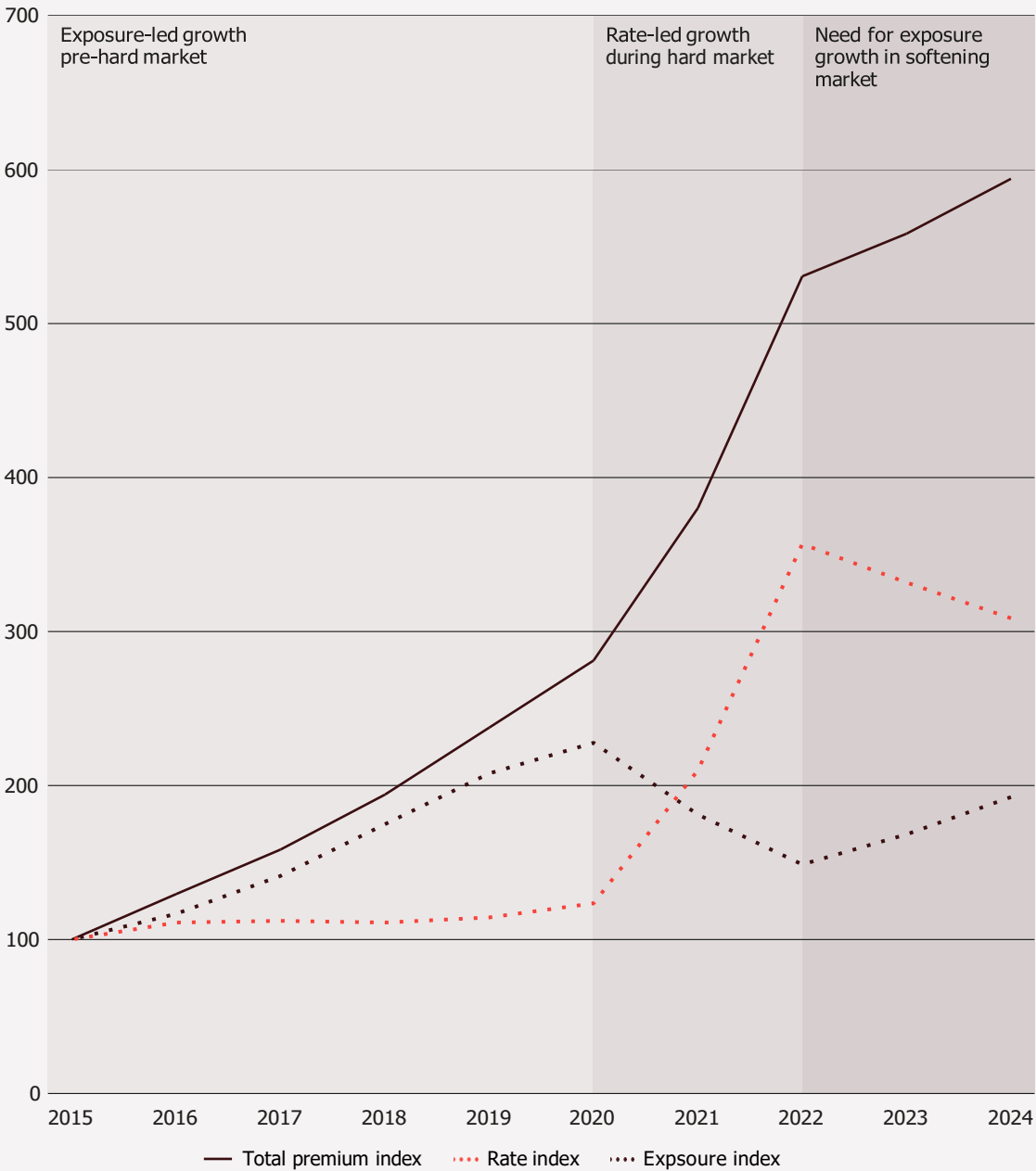


Note: underwriting margin = 100 minus average loss ratio and 30% for expense ratio
 Analysis excludes alien E&S business

Şekil 10, primin iki ana unsurunu — fiyat ve risk hacmi — ayrıştırarak analizi derinleştirmektedir. 2020'ye kadar büyüme büyük ölçüde risk hacmi kaynaklı olup, fiyatlar genel olarak istikrarlı kalmıştır. Ancak, fiyatlandırma ortamı 2021/22 yıllarında belirgin bir değişime yol açmış; yüksek çift haneli yıllık fiyat artışları, underwriting tedbirleri ve buna bağlı olarak risk hacmindeki daralmayı fazlasıyla telafi etmiştir.

2023/24 yıllarında risk hacmi artış göstermesine rağmen, piyasanın risk tabanı sert piyasa öncesi seviyelerin altında kalmaya devam etmekte olup, bu durum daha olgunlaşmış olan piyasada büyüme için önemli bir potansiyel (ve piyasa yumuşamasının temel nedenlerinden biri) olduğunu ortaya koymaktadır.

Figure 10: Premium growth of global cyber insurance market broken down by rate and exposure – 2015 to 2024 (Source: Howden)

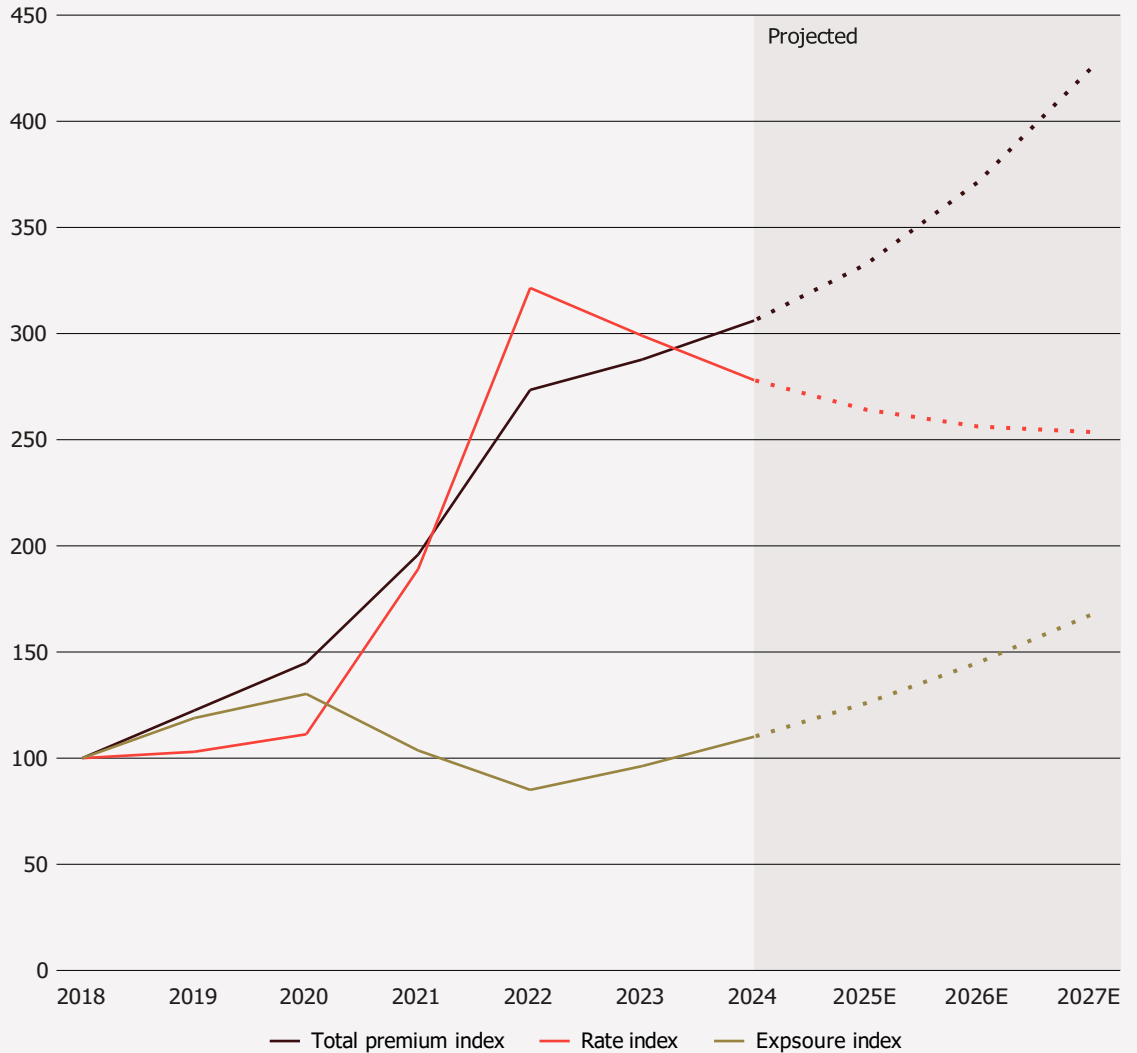


Bu analiz, önümüzdeki yıllarda siber piyasasının karşı karşıya olduğu temel zorluğun özünü yansıtmaktadır. Fiyatlama rüzgarları artık tersine döndüğüne göre, büyümeyi hızlandırmak için özellikle hizmet verilmeyen bölgeler ve şirket segmentlerinde penetrasyonu artırarak yeni risk havuzlarının açılması kritik önem taşımaktadır.

Şekil 11, önümüzdeki birkaç yıl boyunca fiyatların stabil kalacağı varsayımına dayanarak bu görevi gözler önüne sermektedir. 2027 yılına kadar piyasa genelinde yaklaşık 20 milyar ABD doları (aşağı yönlü revize edilmiş) prim hedefine ulaşmak için, siber sigortacıların sert piyasa öncesi büyüme hızına benzer bir tempoda risk hacmini genişleten yeni bir disiplinli büyüme dönemine başlamaları gerekmektedir. Bu yenilenmiş büyüme döngüsünü desteklemek üzere hem geleneksel hem de alternatif olmak üzere geniş bir reasürans kapasitesi mevcuttur.

Figure 11: Projected premium growth of global cyber insurance market up to 2027

(Source: Howden, Munich Re, Swiss Re, Beazley)



Siber sigorta penetrasyonunun artırılması, kurumsal dayanıklılığın güçlendirilmesi ve piyasanın uzun vadeli öneminin korunması açısından kritik öneme sahiptir. Artık sağlam ve kârlı bir temel üzerine oturan piyasa, risk hacmi odaklı büyümeye yeniden yönelmek için elverişli bir konumdadır.

Avrupa: Keşfedilmemiş Potansiyel

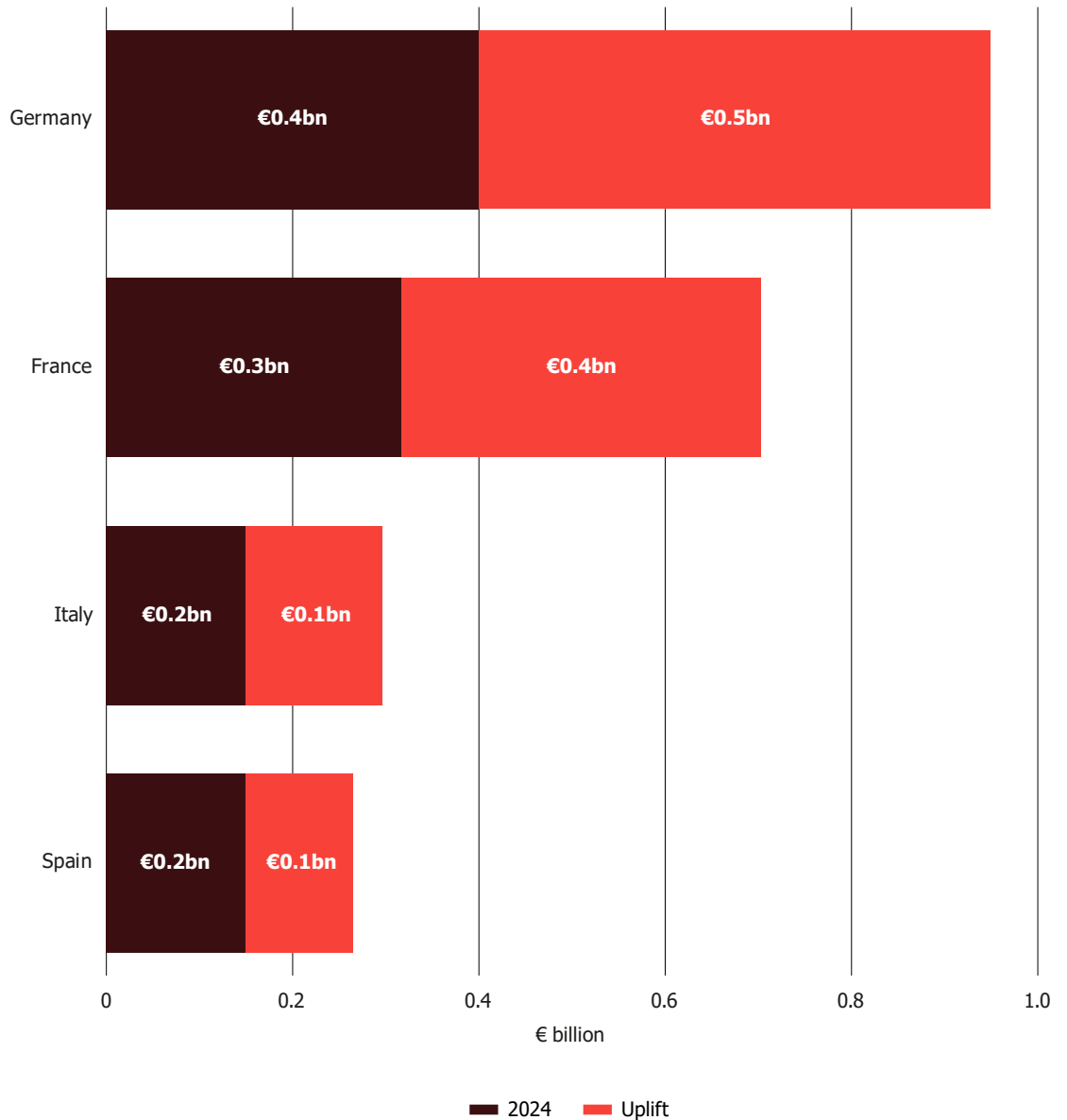
Raporun giriş kısmı, mevcut yumuşayan piyasa döngüsünde siber prim havuzunun genişletilmesinin aciliyetine dikkat çekmektedir.

Bu bölüm, “nasıl” sorusuna odaklanarak Avrupa’nın öne çıkan büyüme potansiyelini ve Fransa, Almanya, İtalya ile İspanya’daki işletmelerin siber savunmaları güçlendirmek ve zararları azaltmak amacıyla risk yönetimi ve risk transferi konularında benimsedikleri yaklaşımları incelemektedir.

Olgunlaşmış ABD pazarı siber sigortada büyümenin temel itici gücü olmaya devam edecek olsa da, kıta Avrupası'nın en büyük dört Hasar ve Kaza (P&C) pazarı, düşük penetrasyon oranları nedeniyle çok daha yüksek büyüme potansiyeli sunmaktadır. Şekil 12'de gösterildiği gibi, mevcut ABD siber penetrasyon seviyelerine ulaşılması, bu pazarlarda yaklaşık 1,2 milyar € tutarında ek prim yaratabilir.

Figure 12: Major European cyber insurance markets premium growth potential

(Source: Howden analysis based on data from SNL, Swiss Re, Lloyd's and AMRAE)



Note: uplift represents premiums at US level of penetration rate in terms of cyber / total non-life GWP
Total uplift of €1.2 billion is shown as €1.1 billion in the chart due to rounding

Potansiyelin Açığa Çıkarılması

Bu potansiyelin hayata geçirilmesi, Avrupa'daki iş liderlerinin siber riski nasıl algıladığını, karşılaştıkları saldırıların sıklık ve şiddetini, etkileri azaltmadaki risk yönetimi araçlarının (özellikle sigortanın) etkinliğini ve sigortacıların ile brokerların piyasa penetrasyonunu artırmak ve koruma boşluklarını kapatmak için atması gereken adımları anlamaya bağlıdır.

Bu soruları yanıtlamaya yardımcı olmak amacıyla Howden, Fransa, Almanya, İtalya ve İspanya'daki çeşitli özel sektör işletmelerinde görev yapan 1.200 üst düzey BT karar vericisi ile bir anket gerçekleştirmiştir. Bu çalışma, Howden'in Birleşik Krallık'ta yürüttüğü benzer araştırmalar üzerine inşa edilerek kıyaslama için değerli bir referans sağlamaktadır.

Elde edilen bulgular siber sigorta pazarı için cesaret vericidir: İş liderleri, siber riski operasyonları için başlıca (hatta en önemli) risk olarak görmektedir. Ayrıca, siber hijyen ile saldırı sıklığı ve maliyetler arasında güçlü bir bağlantı olduğunu teyit etmişlerdir; bu durum sigortalanabilirliği artırmakta ve önemli ekonomik faydalar sağlamaktadır. Siber sigorta satın almayanların büyük çoğunluğunun ürünü almaya açık olması, ürünün değerini etkili şekilde iletişim kurmaya yönelik yoğun çabaların yeni talepte önemli bir artışa yol açacağını göstermektedir.

⁶ Howden, *The cyber security gap*, January 2025.

“

**Bizim
bulgularımız, siber
sigorta pazarı
açısından umut
vericidir: İş
liderleri, siber riski
operasyonları için
öncelikli bir risk
olarak kabul
etmektedir.**



Tehdit Ortamı

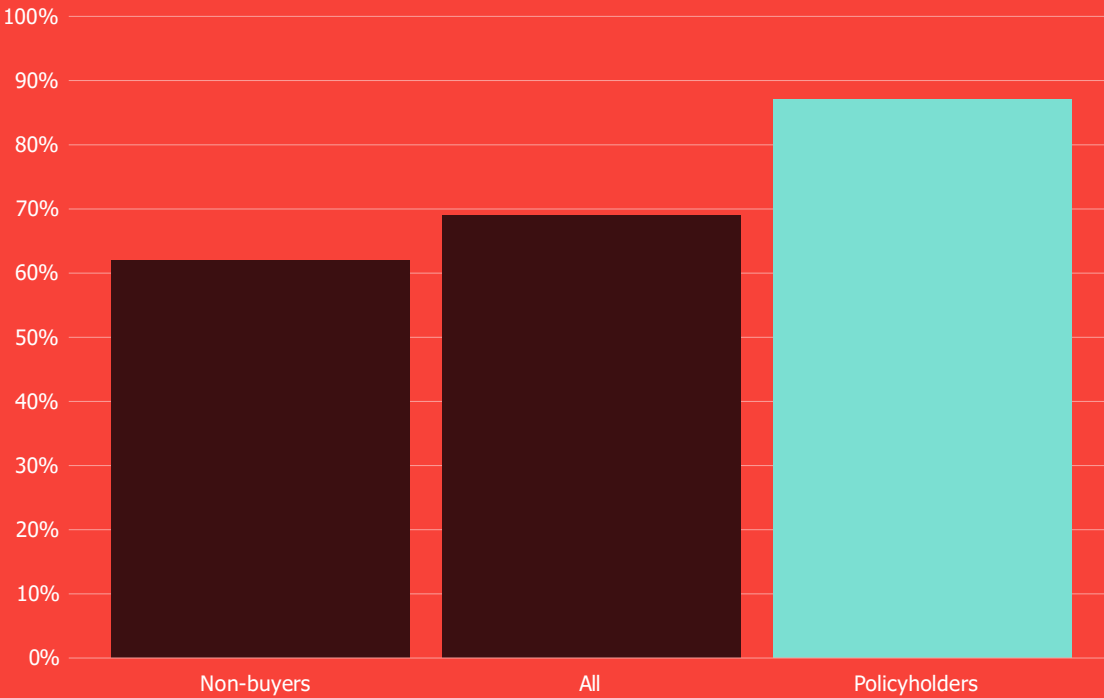
Siber tehditlerde hızlı ve karmaşık değişimlerin yaşandığı bir ortamda, iş liderleri kuruluşlarının karşı karşıya olduğu risklerin farkındadır. Tüm anket yapılan şirketlerde, katılımcıların %69'u karar vericilerin siber riski önemli bir tehdit olarak doğru değerlendirdiği görüşünde.

Siber riske hem stratejik hem de teknik bir yaklaşım benimseyen şirketlerin, üst düzey yöneticilerin daha fazla katılımından ve gelişmiş fonksiyonlar arası dayanıklılıktan daha fazla fayda sağlama olasılığı yüksektir. Beklendiği gibi, siber sigorta satın alan şirketlerde bu görüşe katılım oranı %90'a yakınken, sigorta satın almayanlarda bu oran yaklaşık %60'tır (Şekil 13'te gösterilmiştir).

Bu bulgu, piyasa uzmanlarının sıklıkla gözlemlediği bir durumu yansıtıyor: Siber riski daha iyi anlayan işletmeler, tehdit farkındalığı daha düşük olanlara kıyasla sigorta koruması satın alma olasılıkları daha yüksektir.

Figure 13: Agreement amongst respondents that their senior leadership understand and accurately assess cyber threats

(Source: Howden analysis based on survey data provided by YouGov)



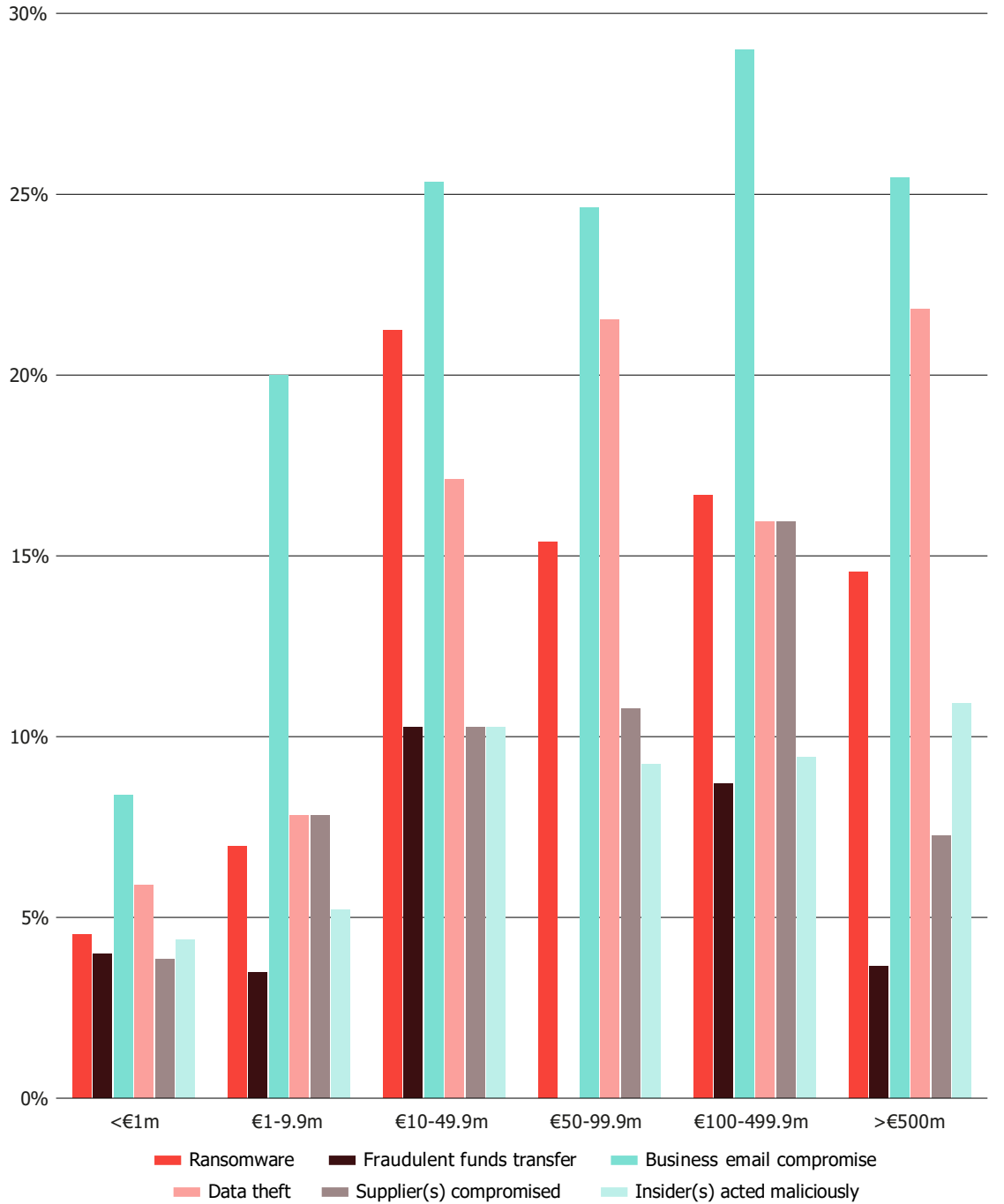
Note: agreement level = sum of strongly agree and agree

Tehdit algısı, şirket gelir grupları arasındaki saldırı sıklığı analiz edildiğinde gerçeğe uygundur. Basitçe söylemek gerekirse, birçok şirket birden fazla saldırı vektörü üzerinden hedef alınmaktadır.

Şekil 14, tüm olay türlerinde saldırı sıklığının genel olarak şirket büyüklüğü ile arttığını göstermektedir. İş e-postası dolandırıcılığı, veri hırsızlığı ve fidye yazılımı en yaygın saldırı türleridir; bu da geçen yılın sonlarında Howden tarafından Birleşik Krallık işletmeleri üzerinde yapılan analizle tutarlıdır.

Figure 14: Frequency of attacks by method and revenue band – 2020 to 2025

(Source: Howden analysis based on survey data provided by YouGov)



Anket yapılan şirketlerin %49'u 2020 ile 2025 yılları arasında en az bir siber saldırıya maruz kaldıklarını bildirmiştir; bu oran, Howden'in Birleşik Krallık araştırmasındaki %50 rakamıyla yakından örtüşmektedir. Fransa, Almanya, İtalya ve İspanya'daki tüm özel sektör şirketlerine ilişkin saldırı sıklığı ve şiddet trendleri extrapole edildiğinde, 2020-2025 döneminde doğrudan maliyetlerin (örneğin itibar kaybı hariç) tahmini ekonomik etkisi 307 milyar Euro'ya ulaşmakta, bu da sadece Birleşik Krallık için 44 milyar Sterlin olan rakama kıyasla, Avrupa'nın dört büyük ekonomisindeki finansal riskin büyüklüğünü ortaya koymaktadır.

Figure 15: Estimated economic impact of cyber attacks in France, Germany, Italy and Spain – 2020 to 2025 (Source: Howden analysis based on survey data provided by YouGov)



Frequency	Severity	Revenue	Estimated cost
%49	%2	~€30tn	= €307bn
2020 ile 2025 yılları arasında saldırıya uğrayan Almanya, Fransa, İtalya ve İspanya'daki işletmelerin oranı	En pahalı saldırının ortalama maliyeti, gelir yüzdesi olarak	Fransa, Almanya, İtalya ve İspanya'daki özel sektör tahmini gelirleri	

Note: frequency of attacks excludes 9% of respondents who did not know

“

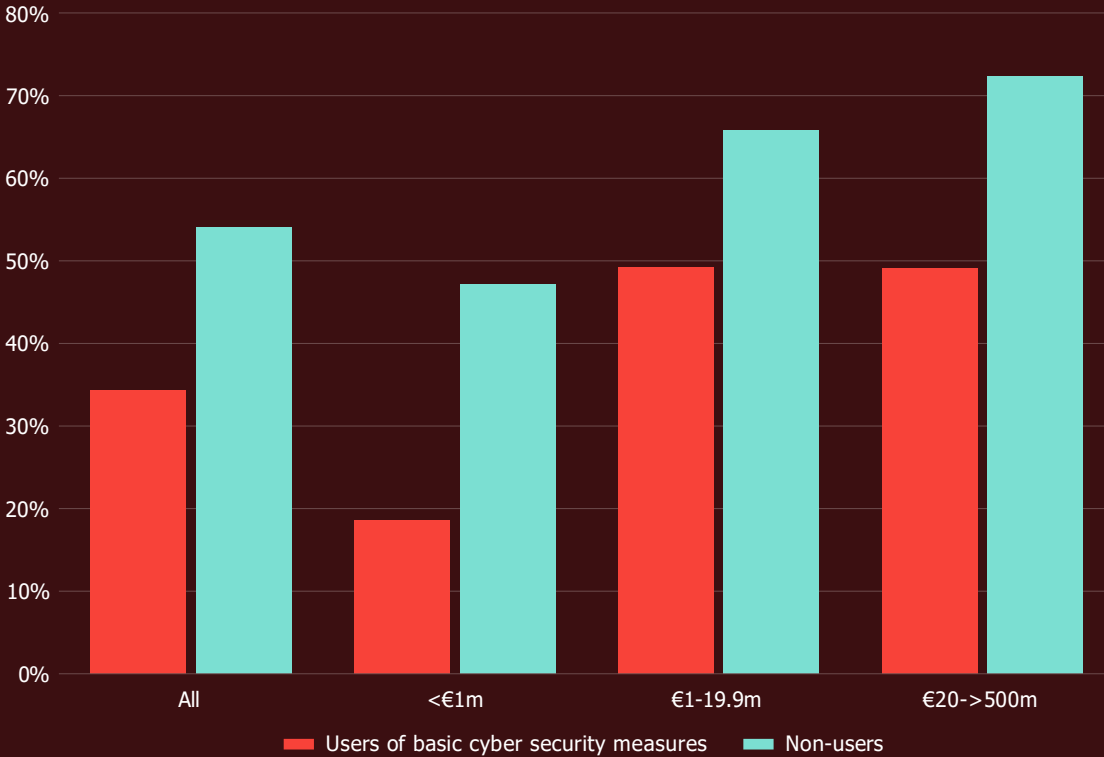
Fransa, Almanya, İtalya ve İspanya'daki tüm özel sektör şirketlerinde saldırı sıklığı ve şiddet eğilimleri, 2020-2025 dönemi için tahmini ekonomik kaybın 307 milyar Euro gelir kaybına ulaştığını göstermektedir; bu rakam, sadece Birleşik Krallık için 44 milyar Sterlin'dir.

Risk yönetimi önem taşır

Gelişmiş siber dayanıklılık, saldırıların finansal etkilerinde belirgin bir azalmaya yol açtı. Piyasa katılımcıları uzun süredir (anektodal olarak) güçlü risk kontrolleri ile daha az ve daha hafif olaylar arasında güçlü bir korelasyon olduğunu belirtse de, yaptığımız anket bu iddiaları destekleyen ampirik kanıtlar sunmaktadır.

Sonuçlar, iş kesintilerini azaltmada ve şirketlerin sigortalanabilirliğini artırmada siber risk yönetiminin kritik rolünü vurgulamaktadır. Sigorta, siber hijyen gereksinimleri ve giderek artan prim teşvikleri aracılığıyla dayanıklılığı artırarak burada önemli bir destekleyici rol oynamaktadır. Şekil 16, temel siber güvenlik önlemlerinin farklı şirket gelir gruplarında saldırı sıklığını nasıl azalttığını göstermektedir. Düzenli yazılım güncellemeleri, güçlü şifreler ve e-posta filtrelemesi gibi basit uygulamalar, anket yapılan tüm şirketlerde saldırı sıklığını üçte birden fazla azaltmaktadır. Bu etkinin, geliri 1 milyon Euro'nun altında olan firmalar için özellikle çarpıcı olduğu görülmektedir.

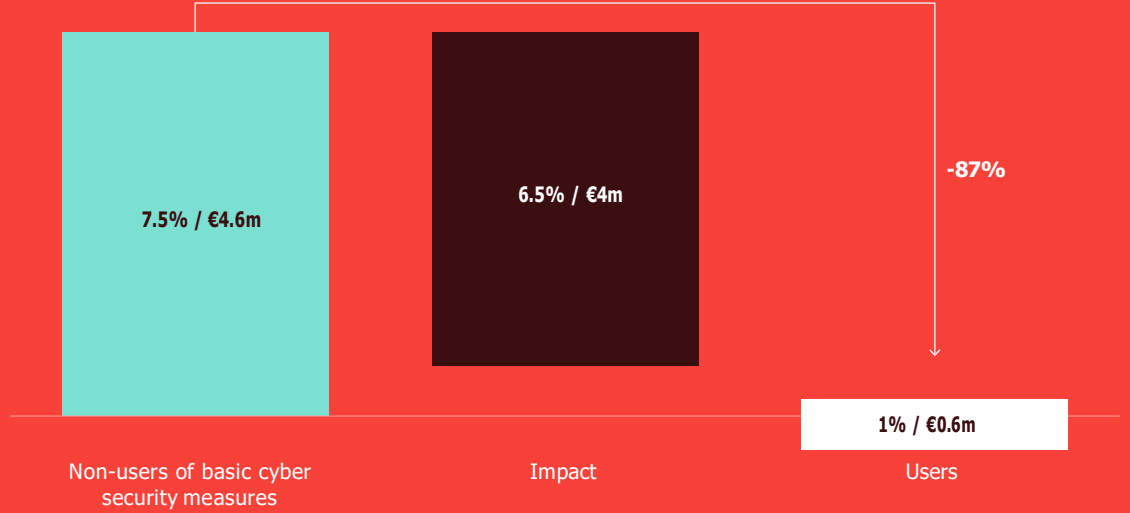
Figure 16: Impact of basic risk controls on the frequency of cyber attacks by revenue band – 2020 to 2025 (Source: Howden analysis based on survey data provided by YouGov)



Note: basics = regular software updates (patching), strong passwords and email filtering

İyi siber hijyenin etkisi, saldırı şiddeti açısından çok daha çarpıcıdır. Şekil 17, ortalama geliri 62 milyon Euro olan ve temel güvenlik önlemleri uygulayan şirketlerde siber saldırının ortalama maliyetinin %87 daha düşük olduğunu göstermektedir; bu da 2020-2025 dönemi için bu tür kontrolleri olmayanlara kıyasla 4 milyon Euro'luk bir azalmaya karşılık gelmektedir.

Figure 17: Average cost of cyber attack as a proportion of revenue and estimated value, users vs non-users of basic cyber security measures – 2020 to 2025
(Source: Howden analysis based on survey data provided by YouGov)

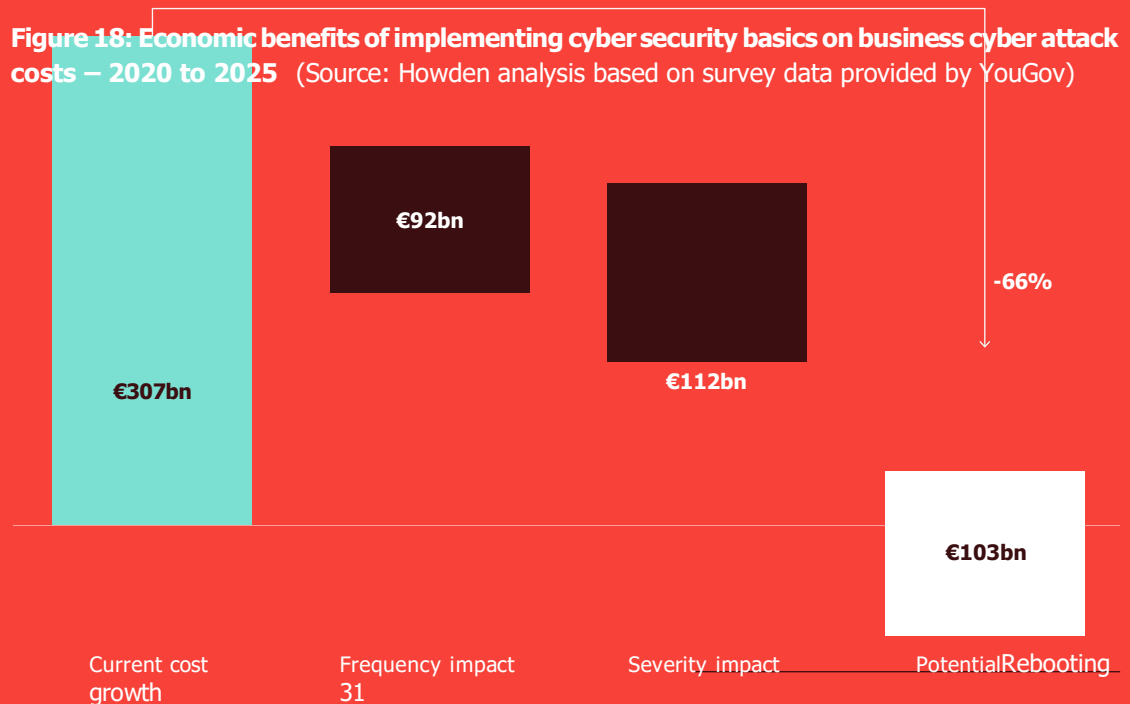


Note: basics = regular software updates (patching), strong passwords and email filtering

Gelişmiş siber dayanıklılığın sağladığı önemli ekonomik faydalar Şekil 18'de gösterilmektedir. Fransa, Almanya, İtalya ve İspanya genelinde saldırı sıklığı ve şiddetindeki azalmadan elde edilen tasarruflar extrapole edildiğinde, dört ekonomide toplam siber ilgili maliyetler %66 oranında düşmekte ve 2020-2025 döneminde 204 milyar Euro'luk bir azalma sağlamaktadır. Bu tasarrufların büyük bir kısmı şiddetin azalmasından kaynaklanmakta (€112 milyar), kalan kısmı ise sıklıktaki düşüşe (€92 milyar) atfedilmektedir.

Bu kazanımlara rağmen, dört ekonomide de önemli düzeyde kalıcı risk devam etmekte olup, bölgedeki siber sigortanın önemini vurgulamaktadır. Etkili risk yönetimi siber riski azaltabilir, ancak tamamen ortadan kaldıramaz.

Figure 18: Economic benefits of implementing cyber security basics on business cyber attack costs – 2020 to 2025
(Source: Howden analysis based on survey data provided by YouGov)





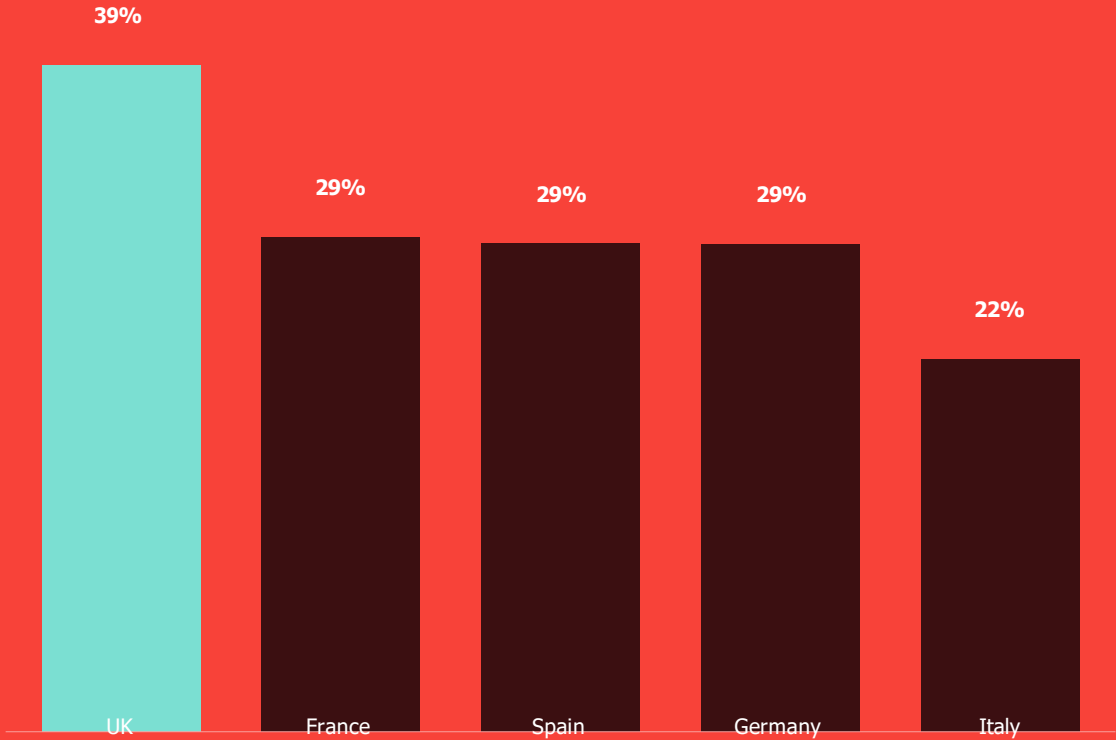
Siber Sigortası

Analizimizin son ve en önemli sonucu, siber sigortanın sağladığı önemli (ve ölçülebilir) değerdir. İşletmelerin karşılaştığı geniş çaplı siber olaylara karşı finansal koruma sağlamanın ötesinde, siber sigorta şirketlere olay müdahalesi, hukuki danışmanlık ve halkla ilişkiler rehberliği gibi uzman desteğine erişim imkânı sunar ve düzenleyici ile uyum yükümlülüklerinin yerine getirilmesinde kritik bir rol oynar.

Siber sigorta aynı zamanda daha iyi yönetişimi teşvik eder; bu da organizasyonel dayanıklılığı artırır ve bulgularımızın gösterdiği gibi, kayıpların boyutunu önemli ölçüde azaltır.

Fransa, Almanya, İtalya ve İspanya’da sigorta yaygınlığının görece düşük olması (dört ülkede de %30’un altında olup, Birleşik Krallık’ın %39 oranının oldukça gerisinde kalması – bkz. Şekil 19), siber sigortanın hem alıcılar hem de kapasite sağlayıcılar için bir fırsat olduğunu göstermektedir.

Figure 19: Cyber insurance penetration by country
(Howden analysis based on survey data provided by YouGov)

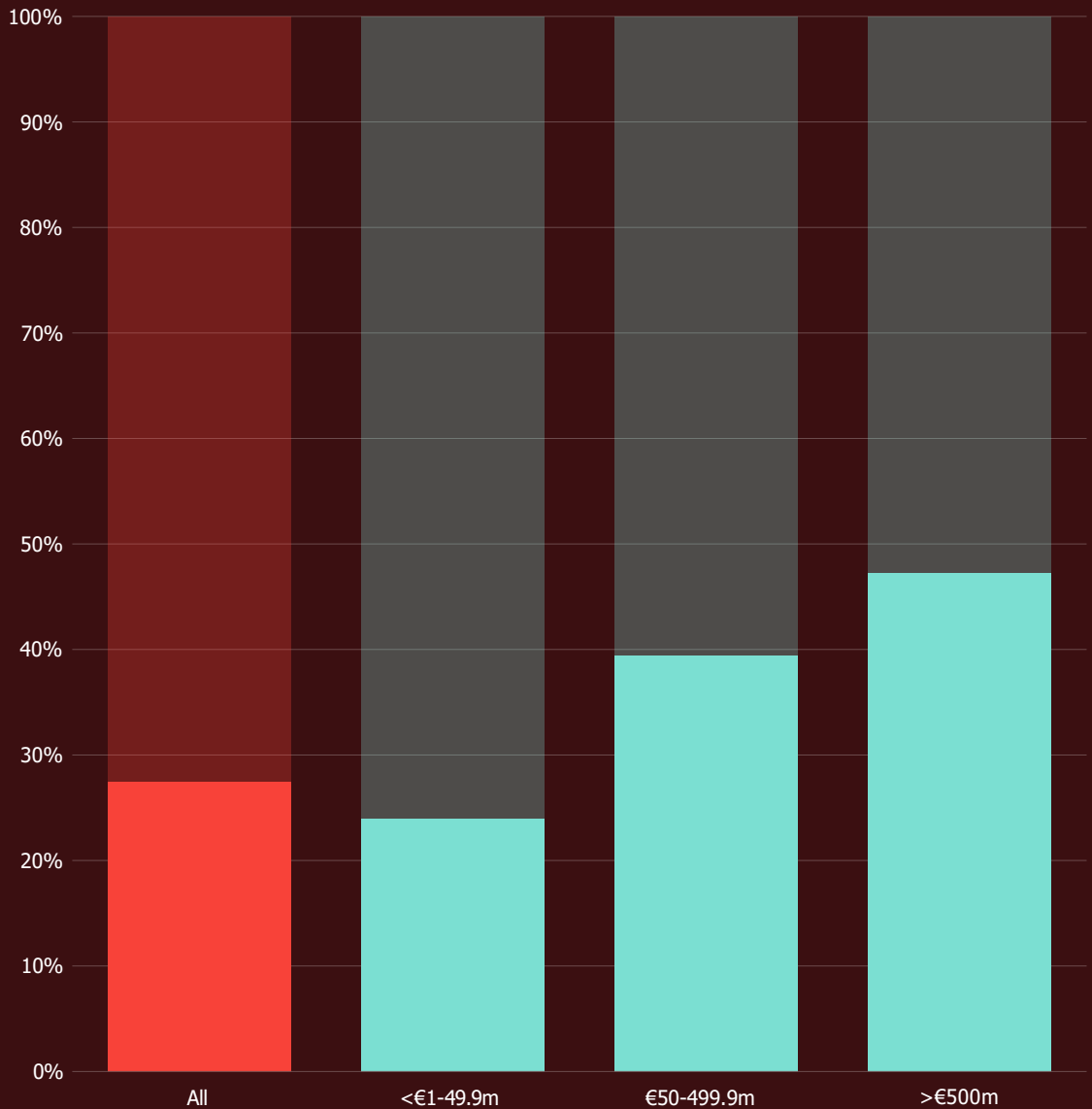


Note: UK data from Howden’s *The cyber security gap* report in 2024

Şekil 20, Avrupa’da siber sigorta kullanımının en fazla büyük ölçekli organizasyonlarda olduğunu göstermektedir; ancak burada bile yaygınlığın artırılması için önemli bir alan bulunmaktadır. Orta ve küçük ölçekli şirketlerde ise çok daha büyük bir fırsat vardır. Özellikle KOBİ’ler, genellikle bu yeteneklere kendi bünyelerinde sahip olma kaynaklarından yoksun olduklarından, olay müdahalesi gibi talep üzerine sunulan entegre hizmetlerden önemli ölçüde fayda sağlayabilirler ve bu durum işletmeler için cazip bir değer önerisi sunmaktadır.

Figure 20: Cyber insurance penetration by revenue band

(Source: Howden analysis based on survey data provided by YouGov)



Note: for France, Germany, Italy and Spain only (excludes the UK)

Şekil 21, siber sigortanın iyi uygulamaların ve güçlü yönetişimin sağlanmasındaki rolünü pekiştiriyor; sigorta satın alanlar ile almayanlar arasındaki saldırı müdahale kapasitesinde belirgin bir fark ortaya koyuyor. Ölçülen her yetkinlik alanında, sigortalı kuruluşlar, sigortasız muadillerine kıyasla bu kritik hizmetlere daha kolay erişim sağladıklarını bildiriyorlar; bu fark özellikle düşük gelirli şirketler arasında daha belirgindir.

Şekil 22, geliri 1 milyon Euro'nun altında olan poliçe sahiplerinin %36'sının, KOBİ'ler arasında saldırıları kontrol altına almak için kritik bir kaynak olan olay müdahale uzmanlığına erişimi olduğunu bildirirken, bu oran sigorta satın almayanlarda sadece %14'tür. Aslında, birçok bu yetkinliklerin bağımsız siber poliçelerde standart olarak yer alması nedeniyle bu fark daha da geniştir.

Figure 21: Cyber attack response capabilities, insured firms vs uninsured peers

(Source: Howden analysis based on survey data provided by YouGov)

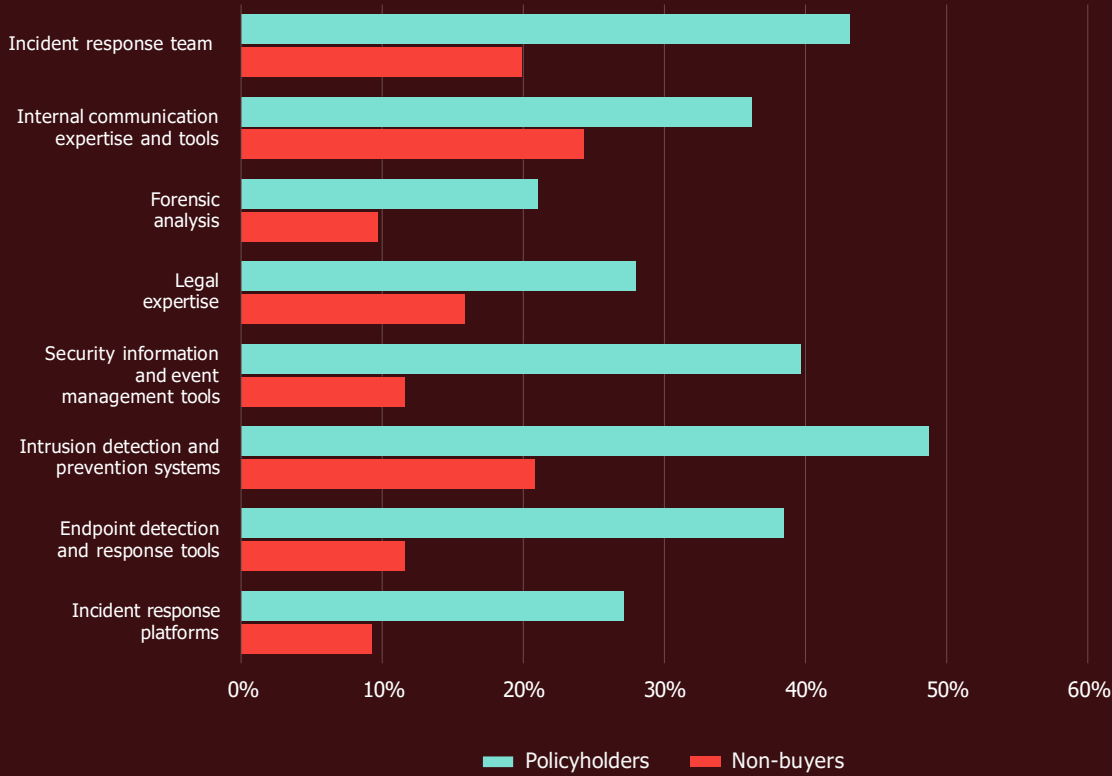
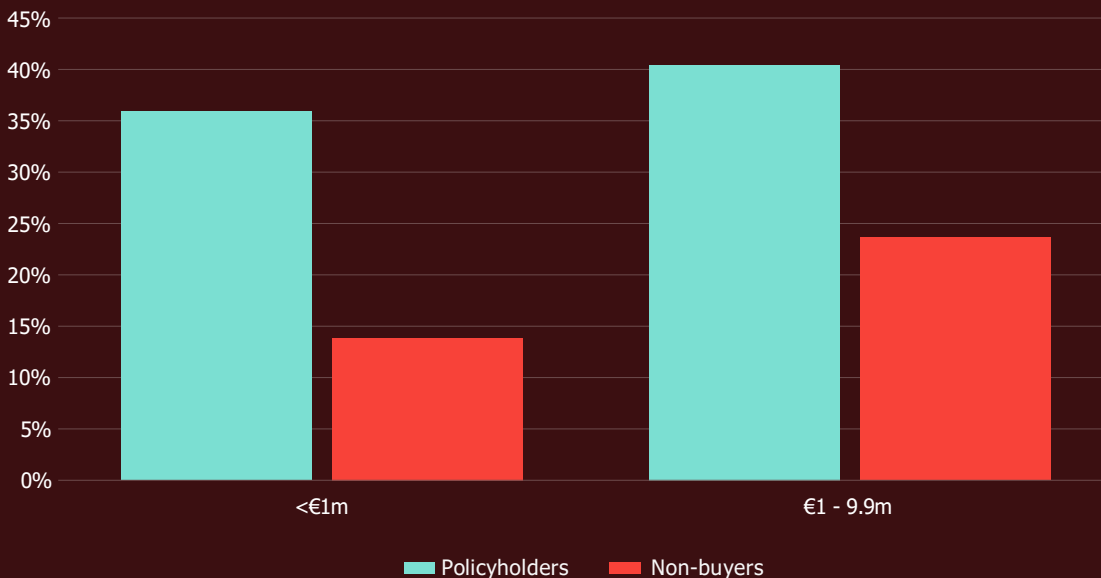


Figure 22: Firms with access to incident response capabilities by revenue band and cyber insurance holding

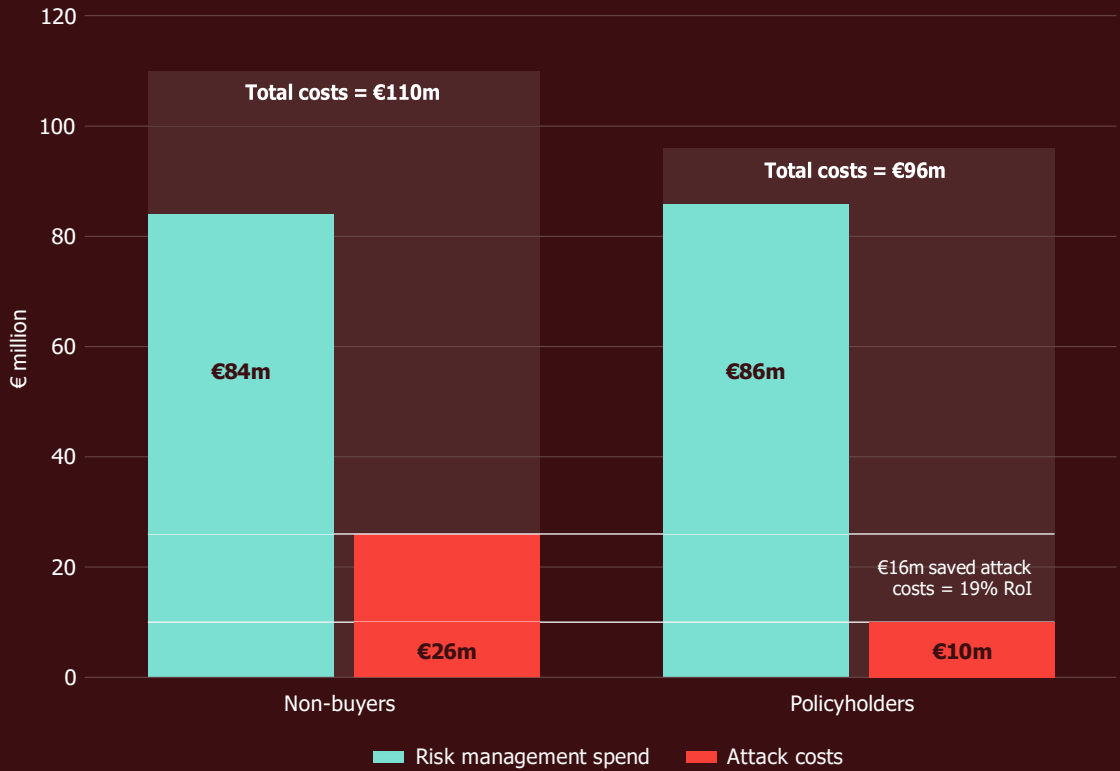
(Source: Howden analysis based on survey data provided by YouGov)



Siber sigorta, tazminat ödemeleri hesaba katılmadan önce bile, siber saldırıların finansal etkisini azaltmadaki değerini kanıtlamaktadır. Analizimiz, sigortalı şirketlerin saldırı sonrasında daha düşük maliyetlerle karşılaştığını; bunun ise risk yönetimi en iyi uygulamaları ve güçlü yönetişimden kaynaklandığını göstermektedir.

Yıllık geliri 500 milyon Euro olan bir şirket için siber sigorta poliçesi, Şekil 23'te gösterildiği gibi, on yıl içinde 16 milyon Euro tasarruf anlamına gelmektedir. Bu, satın alma maliyetlerini fazlasıyla karşılayan azalmış saldırı şiddeti sayesinde %19 yatırım getirisine denk gelmektedir. Kayba uğranması durumunda yapılan tazminat ödemeleri ise getirileri daha da artırmaktadır.

Figure 23: Estimated total cyber costs over a ten-year period for cyber insurance policyholders vs non-buyers with €500 million revenue
(Source: Howden analysis based on survey data provided by YouGov)



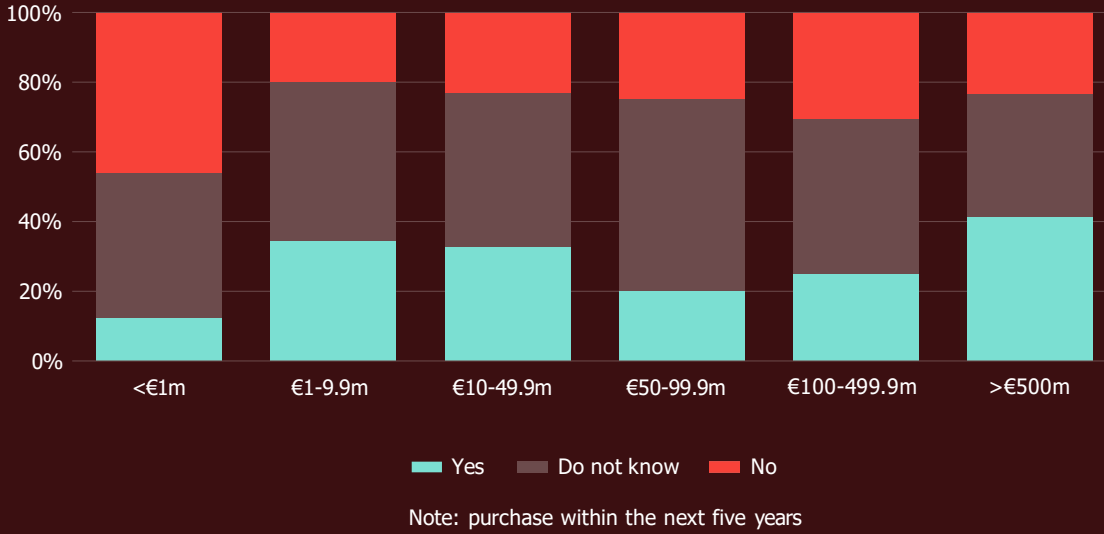
Note: risk management spend includes insurance premium for policyholders

Tüm bunlar, siber sigortanın stratejik değerini ve Avrupa'daki önemli büyüme potansiyelini bir kez daha ortaya koymaktadır. Şekil 24, tüm şirket gelir gruplarında güçlü bir gizli talep olduğunu göstermekte; mevcut sigorta satın almayanların çoğunun önümüzdeki beş yıl içinde siber sigorta satın almayı planladığını teyit etmesiyle piyasanın adeta açık kapiya doğru itildiği görülmektedir.

Bu durum, piyasanın rahatlıkla karşılayabileceği önemli bir yeni iş fırsatını temsil etmektedir. Ayrıca, şu anda siber sigorta satın alma konusunda kararsız olanların yüksek oranı göz önüne alındığında, fırsat daha da büyük olabilir. Raporun önceki bölümlerinde belirtilen büyüme projeksiyonlarının gerçekleşmesi için, sigorta aracılarının ve sağlayıcılarının bu hedef kitle ile aktif şekilde iletişim kurup onları ikna etmesi gerekmektedir.

Geliri 500 milyon Euro ve üzeri olan şirketler arasında ise yalnızca %24'ü sigorta satın alma niyetinde olmadığını belirtmektedir.

Figure 24: Future cyber insurance purchase intentions for respondents that do not currently buy by revenue band (Source: Howden analysis based on survey data provided by YouGov)

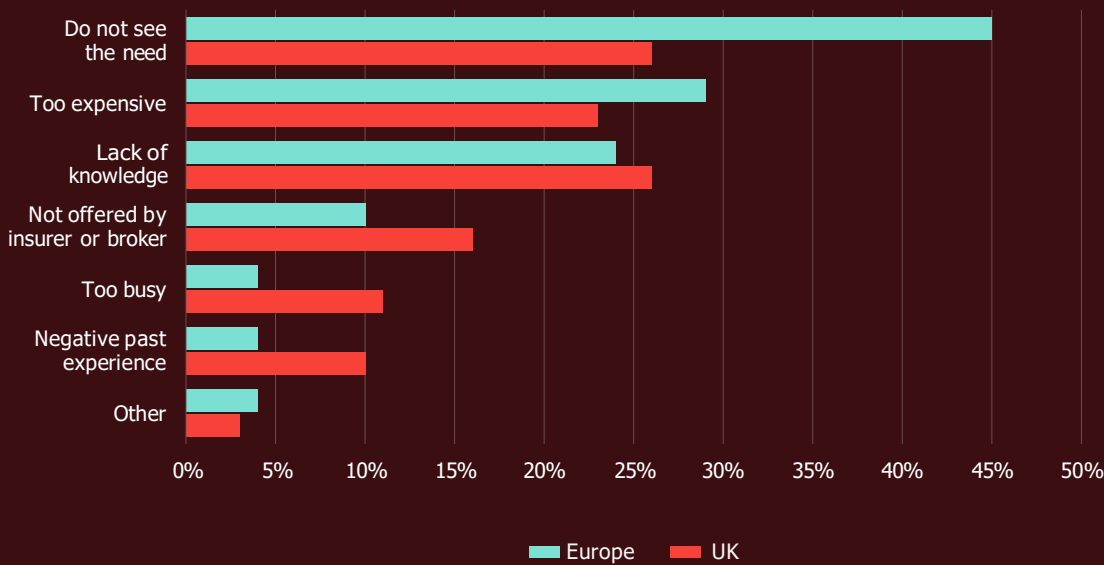


Bu talebin önündeki engeller, Şekil 25'te ve Birleşik Krallık anketimizde belirlenenlerle birlikte özetlenmiştir. Avrupa ve diğer düşük penetrasyonlu uluslararası pazarlarda bu fırsatın tam anlamıyla gerçekleştirilebilmesi için, sektörün özellikle korumanın sağladığı değer konusunda daha fazla iletişim kurması gerekmektedir. Bu değer, Şekil 23'te gösterildiği gibi, saldırı maliyetlerinden sağlanan tasarruflar sayesinde kendi kendini finanse edebilir niteliktedir.

Avrupa'daki şirketlerin %45'inin siber sigortaya ihtiyaç duymadığını düşünmesi, net bir harekete geçme çağrısıdır. Benzer bir sonuç, daha yüksek piyasa penetrasyonu nedeniyle sayıca daha az olmakla birlikte Birleşik Krallık analizimizde de ortaya çıkmış ve her dört şirketten biri aynı görüşü belirtmiştir. Yüksek maliyet algısı, çoğu uluslararası bölgede uygulanan düşük çift haneli oran indirimleriyle giderilmektedir.

Figure 25: Barriers to future cyber insurance purchase

(Source: Howden analysis based on survey data provided by YouGov)



Note: UK data from Howden's *The cyber security gap* report in 2024

“

Analizimiz, siber sigortanın günümüz işletmelerinin karşı karşıya olduğu en kritik tehditlerden birini azaltmadaki güçlü rolünü doğrulamaktadır.”

Siber sigorta sadece bir koruma aracı değil, aynı zamanda iyileşmeyi hızlandıran, risk yönetimini güçlendiren ve finansal kayıpları azaltan stratejik bir dayanıklılık sağlayıcısıdır. Penetrasyon hâlâ düşük ve talep artarken, Avrupa ve diğer uluslararası pazarlar önemli büyüme fırsatları sunmaktadır. Ancak, piyasanın bu değeri daha iyi anlatması ve tekliflerini sadeleştirilmesi gerekmektedir. Bu alanda ilerleme kaydedilmiştir: geçen yıl Cyber+’ı başlattığımızdan beri, daha küçük şirketlerin sigortaya erişimini iyileştirerek ve satın alma sürecini dönüştürerek, genel pazardan üç kat daha yüksek bir büyüme sağladık.

Bu sadece sigorta meselesi değil. Araştırmamız, Avrupa’daki siber saldırıların 2020’lerden bu yana yaklaşık 300 milyar Euro maliyeti olduğunu ortaya koydu; siber koruma açığı, acil dikkat gerektiren toplumsal bir sorundur.

Howden, müşteriler ve pazarlarla birlikte kalıcı dayanıklılık inşa etmeye kararlıdır.”

Jean Bayon de La Tour

Head of Cyber, International



Uzmanlarımızla tanışın

“

Müşterilerin ihtiyaçlarını karşılamak, derin sektör bilgisi, üçüncü taraf uzmanlarla güçlü ortaklıklar ve sigortacılar ile diğer sermaye sağlayıcılarıyla eşsiz ilişkiler gerektirir.

Howden'in siber ekibi size tüm bunları ve daha fazlasını sunmaktadır.

Yazarlar



Julian Alovise
Head of Research

julian.alovise@howdengroup.com



Peter Evans
Research Director

peter.evans@howdengroup.com

İletişim



Adam Codrington
Siber Birim Başkanı

adam.codrington@howdengroup.com



Shay Simkin
Global Siber Güvenlik Başkanı

shay@howden.co.il



Jean Bayon de La Tour
Global Siber Lideri

jean.bayon@howdengroup.com



Manuel Pérez
Siber Lideri, Güney Avrupa & Latin Amerika

manuel.perez@howdengroup.com



David Rees
Siber Lideri, İngiltere

david.rees@howdengroup.com



Sarah Neild
Siber Lideri, İngiltere

sarah.neild@howdengroup.com



**Bizimle info@howden.com.tr mail adresi
üzerinden veya [\(0212\) 290 34 44](tel:02122903444)
numarası ile iletişime geçebilirsiniz.**

www.howdengroup.com/tr-tr

Howden Group Holdings Limited is registered in England and Wales under company registration number 2937398. Registered office:
One Creechurch Place, London, EC3A 5AF. Calls may be monitored and recorded for quality assurance purposes. 09/25 13292