www.pwc.de

PwC Commercial Cyber-Insurance Advisory 2023

Marktumfeld, Herausforderungen und Handlungshinweise bei steigender Bedrohungslage

pwc

Inhalt

1. Zielsetzung und Überblick

Die Identifizierung und Einschätzung von Cyber-Risiken ist eine komplexe und herausfordernde Aufgabe auf dem Cyber-Versicherungsmarkt. Im Gegensatz zu traditionellen Versicherungszweigen, bei denen historische Daten und statistische Modelle zur Risikobewertung herangezogen werden können, fehlt es bei Cyber-Versicherungen oft an ausreichender Datengrundlage.

Wie Unternehmen ihre IT-Systeme und Daten schützen können unterliegt ständigen Veränderungen. Neue Angriffsvektoren und Schwachstellen werden von Angreifern kontinuierlich ausgenutzt, während gleichzeitig innovative Sicherheitslösungen entwickelt werden. Eine präzise Einschätzung des individuellen Risikos und der damit verbundenen Prämienkalkulation wird damit erschwert.

Darüber hinaus variieren Deckungsumfänge von Cyber-Versicherungen je nach Versicherer und Police erheblich. Ohne einheitliche Standards oder etablierte Normen haben Unternehmen Schwierigkeiten, den genauen Umfang des benötigten Versicherungsschutzes zu verstehen und zu bewerten. Die Komplexität der Cyber-Bedrohungen und die sich ständig verändernde Risikolandschaft erschweren es den Versicherungsgesellschaften, klare und umfassende Deckungsumfänge anzubieten und zu bepreisen.

Trotz dieser Herausforderungen ist die zentrale Bedeutung des Schutzes durch eine Cyber-Versicherung für Unternehmen unerlässlich und unbestreitbar. Denn die finanziellen Auswirkungen eines Cyber-Angriffs können existenzbedrohend sein. Eine umfassende Versicherungspolice kann vor diesen finanziellen Verlusten schützen, indem sie beispielsweise die Kosten für Datenschutzverletzungen, Wiederherstellung der IT-Infrastruktur, Rechtsstreitigkeiten und den Imageverlust abdeckt.

Diese Broschüre stellt daher Herausforderungen bei der Beschaffung des Versicherungsschutzes mit Handlungsempfehlungen zum Erwerb des bestmöglichen Versicherungsprodukts in Zusammenhang. Die Empfehlungen können auch als Leitfaden verstanden werden, um einen angemessenen Cyber-Versicherungsschutz zu erlangen und damit die Cyber-Resilienz zu stärken.

2. Bedeutung der Cyber-Versicherung

1) Hintergrund und Marktumfeld

Eine Cyber-Versicherung soll zunächst Unternehmen gegen finanzielle Verluste infolge von Cyberangriffen und den damit verbundenen Risiken wie beispielweise Betriebsunterbrechungen absichern. Die Policen können daher verschiedene Formen annehmen und von einer rein finanziellen Absicherung bis hin zur präventiven oder reaktiven Bewältigung der Folgen eines Cyber-Angriffs reichen. Im Gegensatz zu klassischen Domänen der Versicherung fehlt es im Cyber-Versicherungsmarkt jedoch an einheitlichen Produkten und Tarifen, was mitunter an den sich stets wandelnden Cyber-Risiken liegt.

Die zunehmende Digitalisierung und Vernetzung von Unternehmen führen gleichzeitig zu einer erhöhten Anfälligkeit. Neben den eingangs erwähnten Betriebsunterbrechungen können Kosten für die Wiederherstellung von Daten und Systemen, forensische Untersuchungen, rechtliche Auseinandersetzungen und auch Imageschäden und Haftungsansprüche von Kunden oder anderen betroffenen Parteien entstehen.

In den letzten Jahren ist das Bewusstsein über die Bedeutung einer Absicherung gegen Cyber-Gefahren daher gestiegen, wie auch der 24. Annual CEO Survey unserer PwC-KollegInnen aus Großbritannien zeigt: Inzwischen sehen 91% der befragten CEOs Cyber-Gefahren als eine der Top-Prioritäten. Die Bedeutung der Cyber-Versicherung lässt sich daneben auch an verschiedenen Faktoren und Leistungen erkennen:

1

Kostendeckung: Eine Cyber-Versicherung soll die finanziellen Kosten abdecken, die mit einem Cyberangriff verbunden sind. Dies umfasst beispielsweise Ausgaben für forensische Untersuchungen, Wiederherstellung von Daten und Systemen, Benachrichtigung von Kunden, Rechtskosten, Krisenkommunikation und mögliche Schadenersatz-forderungen.

2

Haftungsabsicherung: Eine Cyber-Versicherung kann Schutz vor Haftungsansprüchen bieten, die aus Datenschutz-verletzungen oder Verlust von Kundendaten resultieren können. Dies kann die finanzielle Stabilität und den Ruf einer Organisation schützen.

3

Risikomanagement: Die Cyber-Versicherung unterstützt Unternehmen bei der Bewertung und Verbesserung ihrer Cyber-Sicherheitspraktiken. Versicherer bieten oft Richtlinien und Ressourcen zur Risikominderung an, um die Wahrscheinlichkeit von Vorfällen zu verringern.

4

Image-Schaden: Ein Cyberangriff kann erhebliche rufschädigende Auswirkungen haben. Eine Cyber-Versicherung kann bei der Kommunikation und der Wiederherstellung des Vertrauens der Kunden unterstützen.

Trotz dieser zentralen Bedeutung der Cyber-Deckung zeichnet sich ein äußerst komplexes Bild des Marktumfelds ab.

Neben des verstärkten Einsatzes von digitalen Technologien nimmt die Gefahr von Cyber-Risiken auch durch zunehmende Cyber-Kriminalität stark zu. Hacker nutzen inzwischen beispielsweise künstliche Intelligenz (AI), um ihre Angriffe zu automatisieren und zu optimieren. Ungeschultes Personal sowie veraltete IT-Systeme erhöhen zusätzlich die Anfälligkeit.

Cyber-Attacken sind damit heute unvermeidlich und kein Unternehmen ist vollständig vor den Auswirkungen geschützt.

Angesichts dieser Bedrohungslage bietet sich ein immenses Geschäftspotenzial für die Versicherungsindustrie. Um diesen Markt erfolgreich zu erschließen, müssen Versicherer jedoch einige wichtige Maßnahmen ergreifen:

a. Zusammenarbeit und Standardisierung:

Versicherer kooperieren heute noch nicht mit anderen Häusern, Branchenexperten und Regulierungsbehörden, um prozessuale Standards zu entwickeln und den Zugang zu Versicherungsprodukten zu erleichtern. Die Entwicklung standardisierter Baseline-Fragebögen kann aber beispielsweise helfen, die Vertriebsprozesse effizienter zu gestalten.

b. Maßgeschneiderte Produkte:

Die Versicherungsindustrie bietet noch keine Produkte, die auf die unterschiedlichen Bedürfnisse und Anforderungen bestimmter Kundengruppen, wie KMUs zugeschnitten sind. Dies würde es Unternehmen ermöglichen, den Schutz zu erhalten, der den individuellen Risiken gerecht wird.

c. Wissen und gemeinsame Sprache:

Die Versicherer sollten vor dem Hintergrund fehlender historischer Daten ihr Wissen über Cyber-Schadenfälle teilen und eine gemeinsame Sprache entwickeln, um den Schadenmanagement-Prozess zu optimieren und den Versicherungsnehmern eine transparente und effektive Abwicklung zu bieten.

d. Transparenz der Deckungen:

Der Cyber-Versicherungsindustrie mangelt es an Klarheit bei der Frage, welche Arten von Schäden durch eine Cyber-Versicherung abgedeckt sind und welche nicht. Hierzu gehören auch die viel diskutierten systemischen Risiken und Cyber-Kriege. Die Branche könnte hier in Zusammenarbeit mit staatlichen Behörden zu einer Lösung und so zu mehr Transparenz kommen.

> Insgesamt bietet das komplexe Marktumfeld für Cyber-Versicherungen sowohl Herausforderungen als auch Chancen. Die Versicherungsindustrie kann jedoch durch Kollaboration, Standardisierung und Transparenz den steigenden Anforderungen gerecht werden und Unternehmen dabei unterstützen, sich angemessen vor den zunehmenden Cyber-Bedrohungen zu schützen.“

Simon Dia,
Director, Financial Services Consulting,
Industrie- und Rückversicherungsexperte bei PwC Deutschland

2) Herausforderungen bei der Beschaffung des Versicherungsschutzes

Vor dem Hintergrund des komplexen Marktumfelds, stellt die Beschaffung einer Cyber-Versicherung Unternehmen vor diverse Herausforderungen. Die Branche ist jung und befindet sich in einer Entwicklungsphase. Die Versicherungsprodukte sind noch nicht ausdifferenziert, sodass Unternehmen mit einer Vielzahl von Angeboten und Policen konfrontiert werden, die sich in ihren Bedingungen und Leistungen stark unterscheiden. Eine Vergleichbarkeit und die Auswahl des richtigen Produkts sind damit erheblich schwerer als in traditionellen Versicherungszweigen.

Versicherer passen zudem ihre Bedingungen und Verträge für Cyber-Versicherungen regelmäßig an, um den sich ständig verändernden Cyber-Bedrohungen gerecht zu werden. Diese Änderungen können sowohl neue Anforderungen als auch Einschränkungen beinhalten. Kunden müssen daher regelmäßig ihre Versicherungsverträge überprüfen, um sicherzustellen, dass sie angemessen geschützt sind und die aktuellen Bedingungen verstehen.

Insbesondere die Prüfung des angemessenen Schutzes stellt viele Unternehmen vor immense Schwierigkeiten: Vor allem KMUs ohne eigenes Risikomanagement, geschweige denn Cyber-Abteilungen müssen ihre spezifischen Risiken und Schwachstellen verstehen, um die richtige Versicherungsdeckung zu wählen. Wie jedoch eine umfassende und angemessene Risikoanalyse beziehungsweise Bewertung von Gefahren für IT-Infrastruktur und Prozesse vorgenommen werden kann, um einen passenden Versicherungsschutz auszuwählen, ist bei vielen Unternehmen mit Unsicherheiten verbunden.

Die Verflechtung und Komplexität dieser Faktoren tragen letztendlich dazu bei, dass Unternehmen bei der Beschaffung eines passenden Schutzes schlichtweg überfordert sind oder gar falsche Annahmen treffen und der so ausgewählte Versicherungsschutz unangemessen ist.

3) Aktuelle Entwicklungen: Mutual „MIRIS“

Die Unsicherheiten und Herausforderungen bei der Beschaffung eines Versicherungsschutzes vor Cyber-Risiken betreffen Unternehmen aller Branchen und Größen. Die Mutual Insurance and Reinsurance for Information Systems (MIRIS) stellt hierbei eine interessante Initiative dar, bei der Industrieunternehmen gegen diese Herausforderungen gemeinsam anzukämpfen versuchen.

Es handelt sich zunächst um einen Versicherungsverein auf Gegenseitigkeit mit dem Ziel, die Mitglieder mit Versicherungskapazitäten zu unterstützen. Der Verein wurde vordergründig gegründet, weil auf dem herkömmlichen Versicherungsmarkt eine Deckung nicht oder in den letzten Jahren nur noch erschwert verfügbar war. So wurden beispielsweise Preise drastisch erhöht, Versicherungssummen reduziert und strengere Auflagen und Voraussetzungen definiert, denen die Industrieunternehmen heute gerecht werden müssen.

MIRIS reagiert auf diese Marktsituation, indem seinen Mitgliedern durch die Bereitstellung von Cyber-Versicherungskapazitäten von bis zu 25 Mio. Euro ein alternativer Zugang zur Absicherung ermöglicht wird. Zudem haben sich die Industrieunternehmen darauf verständigt, sich langfristig beim Aufbau von Fähigkeiten und notwendiger Expertise im Risiko- und Krisenmanagement zu unterstützen.

Wie effektiv der Verein bei der Bewältigung von Cyber-Risiken tatsächlich ist, bleibt jedoch noch zu beobachten. Festzuhalten bleibt aber in jedem Falle, dass diese Lösung zwar keine vollständige finanzielle Deckung erlaubt, jedoch als Initiative erhebliche Entlastung für Industrieunternehmen mit starker Cyber-Exponierung bieten kann.

3. Handlungsempfehlungen

Wie Unternehmen und potenzielle Versicherungsnehmer auf die Problematik des Erwerbs eines angemessenen Cyber-Versicherungsschutzes reagieren können, soll anhand der folgenden Handlungsempfehlungen dargestellt werden. Diese Empfehlungen sind jedoch keineswegs vollumfänglich. Vielmehr zielen sie darauf ab, einen Überblick darüber zu geben, wie eine fundierte Strategie von der Quantifizierung der eigenen Risiken zum gezielten Erwerb des passenden Schutzes entwickelt und so die Widerstandsfähigkeit eines Unternehmens gestärkt werden kann.

1) Risiko-Assessment als Fundament

Obwohl die Bedrohung durch Cyber-Risiken stetig zunimmt, besitzen nur wenige Unternehmen einen passenden Schutz - trotz eines steigenden Bewusstseins über die Gefahren. In Deutschland besitzen bis zu 80% der KMUs keine Absicherung in Form von Versicherungspolicen gegen Cyber-Risiken und auch größere Firmen haben Schwierigkeiten bei der Identifizierung, Bewertung und Abwehr ihrer Exponierung.

Um diese Risiken angemessen zu bewältigen, müssen Strategie und geeignete Maßnahmen zunächst auf ein fundiertes Risiko-Assessment fußen, welches die individuellen Risikotoleranzen und Geschäftsziele des Unternehmens berücksichtigt. PwC empfiehlt Unternehmen, dieses Assessment regelmäßig durchzuführen, zu aktualisieren und anzupassen, um auch auf sich ändernde Bedrohungen und Technologien zu reagieren.

Der entscheidende Unterschied zum passiven Umgang mit Cyber-Risiken besteht damit in der bewussten Wahrnehmung und Bewertung des Impacts von potenziellen Attacken, bevor Strategien, Geschäftsaktivitäten und Prozesse entwickelt und angepasst werden.

Ein wesentliches Instrument für eine solche Risikobewertung ist die Business Impact Analyse (BIA) für Cyber-Risken von PwC. Mithilfe dieser Analyse kann eine erste detaillierte Quantifizierung der möglichen Auswirkungen von Cyber-Angriffen auf ein Unternehmen vorgenommen werden. Sie hilft auch dabei, die kritischen und damit am stärksten gefährdeten Geschäftsprozesse und -systeme zu identifizieren. Auf diese Weise wird zudem eine gezielte Priorisierung von Schutzmaßnahmen ermöglicht.

Indem die BIA die potenziellen finanziellen Auswirkungen eines Cyber-Angriffs auf ein Unternehmen bewertet, kann ferner eine realistische Einschätzung der Deckungssummen kalkuliert werden, die für eine adäquate Absicherung benötigt wird. Die BIA wird damit das Fundament für eine gezielte Suche nach Versicherungsprodukten, die den individuellen Anforderungen eines Unternehmens entsprechen.

2) Cyber-Versicherung als komplementärer Bestandteil des Risikomanagements

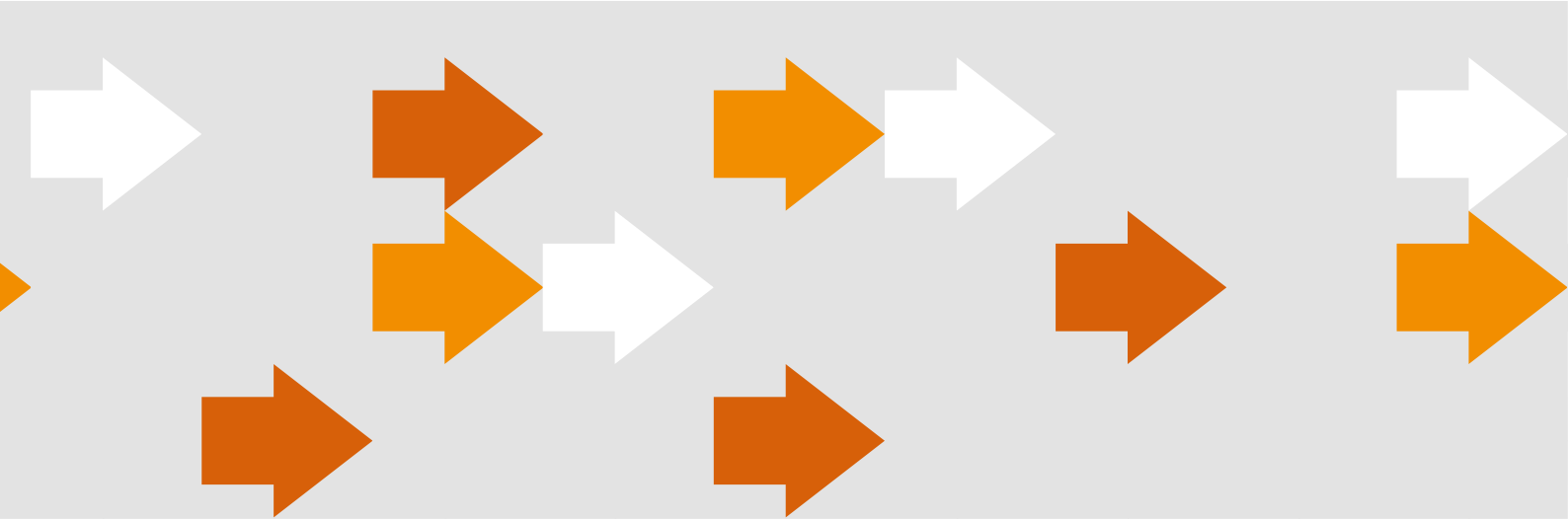
Der Erwerb einer Cyber-Versicherung kann ein wesentlicher Bestandteil eines umfassenderen Risikomanagements sein. Auch hierbei kann PwC mit den Expertenteams vor Ort und dem internationalen Netzwerk unterstützen.

Vor allem die Einführung und Überprüfung eines strukturierten Prozesses und den erforderlichen Schritten stellt sicher, dass letztendlich eine individuell angemessene Versicherungsdeckung ausgewählt wird. Die Erkenntnisse aus der idealerweise vorher durchgeführten Business Impact Analyse spielen hierbei eine zentrale Rolle. Denn mit den gewonnen Daten können Anforderungen an die passende Versicherungspolice definiert werden, die auch kosteneffektiv den Schutz bieten soll, der für das jeweilige Unternehmen angemessen ist.

Zu diesem Prozess gehört auch die Voraussetzungen für den Erwerb von Cyber-Deckungen zu definieren und zu überprüfen. Hierbei können die jeweilige IT-Infrastruktur, bestehende Sicherheitsmaßnahmen und Datenschutzrichtlinien in die Analyse einfließen, um sicherzustellen, dass die oben genannten erforderlichen Bedingungen der Versicherer erfüllt werden. Diese Analyse ist zudem ein guter Ausgangspunkt, um potenzielle Risiken frühzeitig zu identifizieren und die Weichen für geeignete Maßnahmen zur Risikominderung zu stellen.

Sobald ein deutliches Bild über Exponierung sowie Voraussetzungen und Bedarfe des Versicherungsschutzes herrscht, müssen Unternehmen die Bewertung und Auswahl von geeigneten Versicherern vornehmen, indem ein klares Verständnis der verschiedenen Policen und Deckungsarten gewonnen wird. Die Expertenteams von PwC haben hier langjährige Erfahrung und unterstützen zudem mit ihrer Expertise bei der Analyse von angemessenen Versicherungsbedingungen und -prämien.

Nicht zu vernachlässigen ist bei der Beschaffung einer Cyber-Versicherung in jedem Falle zuletzt die Integration der Deckung in das breitere Risikomanagement eines Unternehmens. PwC empfiehlt hierbei sicherzustellen, dass neben der korrekten Erfassung und Bewertung von Cyber-Risiken sowie des notwendigen Schutzes, die Integration einer möglichen Versicherungspolice in bestehende Richtlinien, Verfahren und Standards zu überprüfen und zu testen.



3) Aktives Risikomanagement für eine resiliente Cyber-Security

Eine Cyber-Versicherung darf jedoch nicht als zentraler oder gar alleiniger Bestandteil des Risikomanagements von Cyber-Gefahren betrachtet werden. Wie weiter oben dargestellt, sollte eine Cyber-Versicherung vielmehr als komplementäres Element einer resilienten Organisation verstanden werden. Daher müssen Unternehmen in verschiedene Bereiche ihrer Cyber-Sicherheit investieren, um präventiv, aber auch im Ernstfall effektiv und schnell zu handeln. Diese Bereiche umfassen Investitionen in:

1) die technische Infrastruktur
2) Governance und Prozesse
3) Ausbildung von MitarbeiterInnen

Die Investition in die technische Infrastruktur beinhaltet Sicherheitslösungen wie Firewalls, automatisierte Scans, wie Intrusion-Detection-Systeme und andere Tools, um Netzwerke und Systeme vor Cyber-Bedrohungen zu schützen. Eine robuste technische Infrastruktur bildet die Grundlage für eine widerstandsfähige Organisation und ermöglicht eine frühzeitige Erkennung und Abwehr von Angriffen.

Daneben sind eine effektive Governance und Prozesse von immenser Bedeutung. Unternehmen müssen Governance-Strukturen etablieren, die sicherstellen, dass Richtlinien, Standards und Verfahren für IT Service Continuity Management (ITSCM), Business Continuity Management (BCM) und Incident Management vorhanden sind. Diese Strukturen ermöglichen eine effektive Reaktion auf Cyber-Vorfälle und gewährleisten eine kontinuierliche Verbesserung der eigenen Resilienz trotz möglicher Attacken.

Wie auch für die Investitionen in die technische Infrastruktur, liefert die Business Impact Analyse von PwC das essenzielle Fundament für die Identifizierung kritischer Geschäftsprozesse und die Festlegung von Prioritäten bei der Investition in Governance und Prozesse.

Darüber hinaus müssen Investitionen im Bereich der Ausbildung und Sensibilisierung von Mitarbeitenden erfolgen. Schulungen und Trainingsprogramme tragen dazu bei, das Bewusstsein für Cyber-Sicherheit zu schärfen und Mitarbeitende zu befähigen, Bedrohungen frühzeitig zu erkennen und angemessen zu reagieren. Abhängig von der Größe sollten Unternehmen langfristig auch in die Ausbildung von Fachkräften investieren, um wichtige Skills im Bereich der Cyber-Security intern aufzubauen und so auf die steigenden Anforderungen der Cyber-Bedrohungslandschaft vorbereitet zu sein.

PwC verfügt über umfangreiche Erfahrung in allen Bereichen und hat bereits zahlreiche Unternehmen erfolgreich bei der Stärkung ihrer Cyber-Resilienz unterstützt und unterstützt diese weiterhin.

4) Risikomanagement/-minderung durch Alternativen Risikotransfer

Auch die Nutzung alternativer Risikotransfermethoden (ART) gewinnt mehr an Bedeutung angesichts der Herausforderungen auf dem traditionellen Versicherungsmarkt und den zunehmenden Cyber-Risiken. Denn wie die Gründung von MIRIS zeigt, ist der alternative Risikotransfer besonders attraktiv, wenn Risiken auf traditionellen Märkten entweder nicht oder nur zu hohen Kosten abgedeckt werden können.

Unabhängig von der individuellen Risikosituation stehen eine Vielzahl von Industrieunternehmen vor ähnlichen Herausforderungen in Bezug auf die Finanzierung und Bewertung von Cyber-Gefahren. Sie müssen entscheiden, welchen Stellenwert die Risikofinanzierung für ihr Unternehmen hat, wie viel sie für Versicherungsleistungen zahlen und ob sie in der Lage sind, Schäden selbst zu tragen und zu regeln.

Ein ART kann hierbei grundsätzlich in zwei Richtungen ausgerichtet sein. Entweder wird das Risiko über den Kapitalmarkt transferiert oder es wird selbst getragen (Risikoeigentragung). Beispiele für den Risikotransfer auf dem Kapitalmarkt sind Katastrophenanleihen wie Cyber Cat Bonds. Die Risikoeigentragung dagegen kann beispielsweise über Captive-(Reinsurance)-Lösungen erfolgen, die besonders für Industrieunternehmen in Zusammenhang mit Cyber-Risiken attraktiv sein können.

Captives bieten eine Vielzahl von Vorteilen, die es Unternehmen ermöglichen, ihre Cyber-Risiken gezielt und effektiv zu managen. Durch die Nutzung von Captives können sie beispielsweise maßgeschneiderte Versicherungslösungen für das eigene Unternehmen entwickeln. Dies kann auch zu einer Effizienzsteigerung bei Schaden- und Vertragsprozessen sowie zu potenziellen Steuervorteilen führen. Darüber hinaus ermöglichen Captives ein strategisches, zentrales und umfassendes Risikomanagement, das über die rein finanzielle Absicherung von Cyber-Risiken hinausgeht. Anlageerträge auf zedierte Prämien, Kapital und Reserven bieten zusätzlich finanzielle Vorteile. Durch die Nutzung von Captives erhöhen Unternehmen zudem ihre Unabhängigkeit von Versicherern und erhalten gleichzeitig Zugang zum Rückversicherungsmarkt, was ihnen Flexibilität beim Management von Cyber-Risiken bietet.

Mit dem internationalen Netzwerk ist PwC prädestiniert bei der Überprüfung von bestehenden organisatorischen Strukturen und Prozessen, des Risikomanagements und existierenden Captives zu unterstützen, aber auch bei der Neugründung von Captive-Lösungen zur Deckung von Cyber-Risiken zu helfen.

5. Schlusswort

Vor dem Hintergrund steigender Cyber-Gefahren und des sich rasant entwickelnden Cyber-Versicherungsmarkts ist eine fundierte Strategie von einer Quantifizierung der eigenen Risiken hin zu einem gezielten Erwerb des passenden Versicherungsschutzes für Unternehmen jeder Branche und Größe wichtiger, aber auch komplexer denn je. Wir hoffen daher, dass unsere dargestellten Handlungsempfehlungen Ihnen einen Überblick darüber geben, wie die herausfordernde Problematik des angemessenen Cyber-Versicherungsschutzes bewältigt werden kann. Wir hoffen weiterhin, Sie hatten Freude bei der Lektüre und freuen uns auf einen baldigen Austausch mit Ihnen. Selbstverständlich freuen wir uns auch über Ihren Besuch auf unserer PwC-Website mit weiteren spannenden Einblicken rund um das Thema Commercial Insurance.

www.pwc.de

PwC Commercial Cyber-Insurance Advisory 2023

Ihre Ansprechpersonen

Simon Dia
Director, PwC FS Transformation
Industrie- und Rückversicherungsexperte
Tel: +49 1511 6780963
simon.dia@pwc.com

Inan Yigen
Senior Associate, PwC FS Transformation
Cyber Insurance Experte
Tel: +49 170 2272305
inan.yigen@pwc.com

Über uns

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen unseren Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expert:innennetzwerks in 152 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC Deutschland. Mehr als 13.000 engagierte Menschen an 21 Standorten. Knapp 2,61 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.