BITSIGHT

E-BOOK

# 5 bewährte Strategien zur Maximierung des Angebots Cyber-Risiken in der Lieferkette Management

# Inhaltsverzeichnis

# 01

# Die Notwendigkeit eines integrierten TPRM zum Schutz der Lieferke

# 01 Die Notwendigkeit eines integrierten Third-Party-Risikomanagements zum Schutz der Lieferkette

**Tim Grieveson**
Leitender Vizepräsident—
Globaler Cyber-Risikoberater, Bitsight

Vereinfachen, integrieren, konsolidieren … CISOs stehen unter dem Druck von oben, ihre Betriebs- und Sicherheitsprogramme sowie Tools und Ressourcen zu optimieren und deren Wert unter Beweis zu stellen. Sie werden oft aufgefordert, Kosten zu senken, Anbieter zu konsolidieren oder mehr zu erreichen, ohne Personal oder Budget zu erhöhen – während gleichzeitig die hohen Erwartungen an den Schutz ihres Unternehmens vor Cyberbedrohungen bestehen.

## Vier Gründe, warum dadurch mehr Druck entsteht als je zuvor:

- **Die digitale Lieferkette boomt,** doch die vorhandenen Tools und Prozesse zur Bewertung und Reduzierung von Lieferantenrisiken lassen sich oft nicht so schnell skalieren. Dies wird durch die zunehmende Abhängigkeit von bekannten und unbekannten SaaS-Anwendungen verstärkt – wobei Schatten-IT zusätzliche Schwachstellen schafft.

- **Sicherheitsverletzungen durch Dritte nehmen zu** und verursachen hohe Kosten. Die Zero-Day-Sicherheitslücken von SolarWinds, Kaseya und MOVEit waren ein Weckruf und haben uns daran erinnert, dass Kriminelle nichts lieber tun, als sich über einen anfälligen Anbieter Zugang zu Ihrem Netzwerk zu verschaffen.

- **Vorschriften erhöhen die Erwartungen – von** den SEC-Anforderungen in den USA bis hin zu den DORA- und NIS2-Rahmenwerken in der EU wird die Compliance-Landschaft immer strenger von Minute zu Minute. Verantwortliche im Bereich Cybersicherheit müssen zunehmend zur Verantwortung gezogen werden, Kunden verlangen Vertrauen und Vorstände und Aufsichtsbehörden greifen härter gegen die Widerstandsfähigkeit der Lieferketten vor.

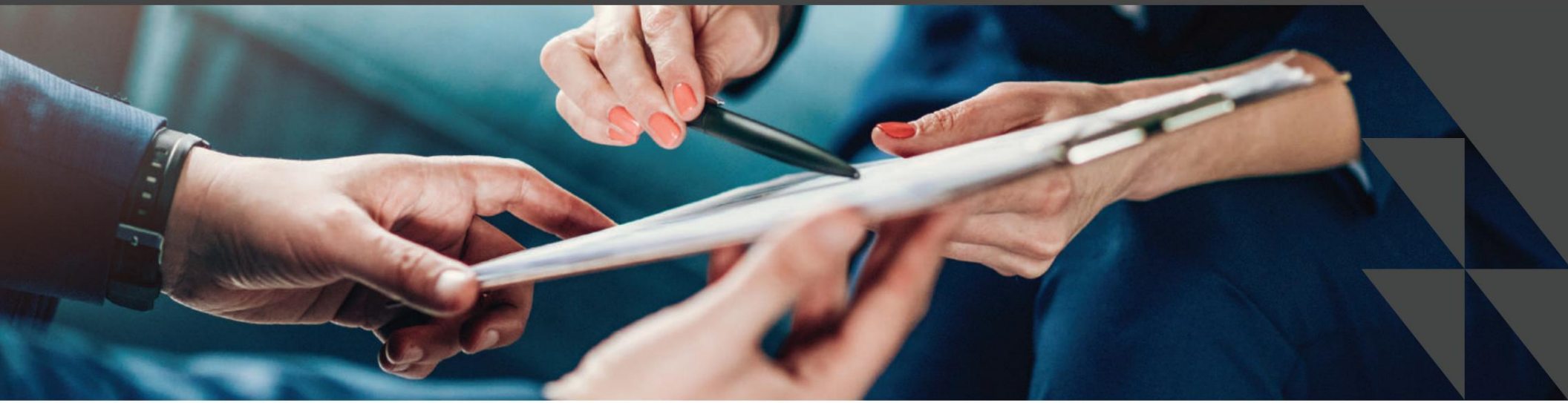
- **Die Nutzung von KI und ML nimmt weiter zu und** fördert den Einsatz von Technologien für sinnvolle Zwecke – beispielsweise zur KI-gestützten Bedrohungssuche –, birgt aber auch das Risiko, dass Bedrohungsakteure sie für Zwecke wie Ransomware-as-a-Service-Kampagnen einsetzen. Bei zunehmend automatisierten und komplexeren Anwendungsfällen besteht die Gefahr, dass Angriffsflächen durch nicht genehmigte und hinsichtlich Qualität und Sicherheitseignung nicht geprüfte Anwendungen unbeabsichtigt vergrößert werden. Es sollte sorgfältig überlegt werden, wie Technologielösungen einfacher entwickelt und für alle ohne spezielle IT-Entwicklungs- oder Sicherheitserfahrung verfügbar gemacht werden können.

Wie können Sie also Ihre Einfallsreichtum steigern, wenn Sie ein erstklassiges Cyber-Risikomanagementprogramm aufrechterhalten und gleichzeitig die Geschäftserwartungen weiterhin erfüllen möchten?

Dies ist Ihr Leitfaden zum Aufbau effizienter, skalierbarer und wiederholbarer Workflows für das Lieferantenrisikomanagement (VRM) als Teil Ihres ganzheitlichen Third-Party Risk Management (TPRM)-Programms – eines integrierten Programms, das Lieferantenrisiken kontinuierlich erkennt, überwacht und minimiert. Wir gehen über anfängliche Bewertungen hinaus und entwickeln uns hin zu einer proaktiven, kontinuierlichen Überwachung der Lieferantenintegrität, der Validierung von Ja/Nein-Fragen anhand objektiver Daten und einem kollaborativen Ansatz zur Beschleunigung von Reaktions- und Korrekturmaßnahmen – unerlässlich für neue Vorschriften – und sprechen dabei die universelle Sprache positiver Geschäftsergebnisse.

Die Strategien in diesem E-Book ermöglichen Ihnen die Konsolidierung von Lösungen, damit Ihr Programm mit dem Unternehmen wachsen kann – und Hunderte oder sogar Tausende von Lieferanten genauso effektiv verwaltet wie zehn. Wenn Sie es mit der Cybersicherheit ernst meinen, ist dies Ihre Chance, den entscheidenden Schritt hin zu einem durchgängigen Drittanbieter-Risikomanagement zu gehen und Ihre Lieferkettenprogramme zu beschleunigen, um die Anforderungen von Vorschriften wie SEC, NIS2 oder DORA zu erfüllen.



02

# Erweiterung von TPRM zur Aktivierung Geschäftsergebnisse

# 02 Erweiterung des TPRM zur Ermöglichung von Geschäftsergebnissen

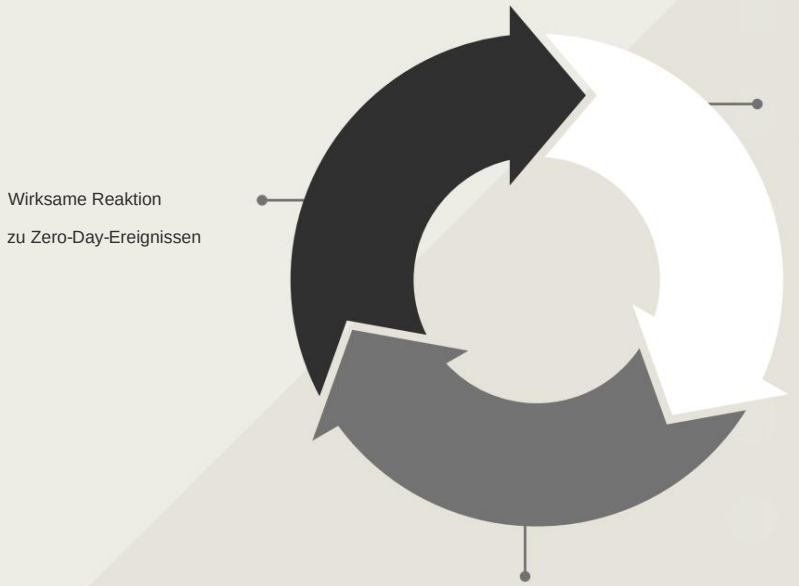
Cybersicherheitsexperten werden ständig mit einer sich ständig weiterentwickelnden Risiko- und Regulierungslandschaft bombardiert. Das Finden und Festhalten an funktionierenden Tools und Prozessen hilft Sicherheitsverantwortlichen, konsequent zu bleiben.

Die Einführung eines ganzheitlichen, integrierten Ansatzes für das Third-Party Risk Management (TPRM) ist eine Strategie, von der Ihr Unternehmen im Laufe Ihrer Geschäftsbeziehungen mit Ihren Lieferanten nur profitieren wird, wenn Sie ein Programm entwickeln, das seinen Wert und seine Geschäftsergebnisse unter Beweis stellt.

Durch die Zentralisierung und Kombination des Lieferanten-Onboardings mit einer einzigen, umfassenderen Ansicht Ihres Risikoportfolios und der Fähigkeit, neu auftretende Sicherheitsereignisse und Zero-Day-Angriffe schnell zu erkennen und darauf zu reagieren, wird das Risiko durch bessere, systematische Arbeitsabläufe verringert.

Anstatt zwischen Tabellenkalkulationen und Apps zu wechseln, können Sicherheitsmanager die Sichtbarkeit und Effizienz erhöhen, indem sie diese TPRM-Funktionen auf der rechten Seite konsolidieren.

**Durchgängiges Third-Party-Risikomanagement**



## Warum der typische Ansatz für TPRM schlägt fehl

Lange Zeit waren Fragebögen eine der wenigen Möglichkeiten, IT-Sicherheitsinformationen über Drittanbieter zu sammeln. Dies zwang Sicherheitsmanager dazu, ihre Entscheidungen zum Risikomanagement von Drittanbietern auf subjektive Daten und Antworten zu stützen, ohne Einblick in kritische externe Schwachstellendaten wie lokale Kontrollen, SIEMs, Firewalls, Schatten-IT, Remote-Netzwerke, Tochtergesellschaften oder Cloud-Daten zu erhalten.

Doch diese manuellen, einmaligen Tabellen mit Dutzenden oder Hunderten von Fragen, zahlreichen E-Mail-Nachfassaktionen und Kalendererinnerungen sind fehleranfällig, nicht skalierbar und tragen nicht zur Risikominderung bei. Anbieter könnten eine Frage leicht missverstehen, versehentlich das falsche Kästchen ankreuzen oder sich mit ihren Kontrollen, Richtlinien und Verfahren nicht auskennen.

Mit diesem Ansatz können laufende Risiken nicht berücksichtigt und gemindert werden. Zudem bietet er nur eine unzureichende Übersicht über die sich entwickelnde Risikolandschaft Dritter und neu auftretende Zero-Day-Schwachstellen.

> Eine Risikobewertung ist eine Momentaufnahme der Sicherheitslage eines Anbieters. Wie können Sie jedoch sicher sein, dass bis zur nächsten Neubewertung alles gleich bleibt?

Bedrohungen treten heute schneller und in größerem Umfang auf, aber es kann eine Herausforderung sein, Risiken ganzheitlich zu priorisieren und zu visualisieren. Das gesamte Ökosystem der Lieferkette. Angesichts der wachsenden Regulierungslandschaft ist es für Cybersicherheitsverantwortliche unerlässlich, Risiken an einem zentralen Ort zu erkennen und darauf zu reagieren, um sicherzustellen, dass die Ergebnisse umsetzbar sind.

### Fragen Sie sich:

- Kann Ihr aktueller Workflow skaliert werden, um das ständig wachsende Lieferantenportfolio ohne zusätzliche Ressourcen, Kosten oder Komplexität zu verwalten und so sicherzustellen, dass Sie die kritischen Aspekte Ihres Unternehmens erfassen und die Compliance-Verpflichtungen einhalten können?
- Reichen die Antworten auf die Fragebögen, Zertifikate und Selbstauskünfte der Anbieter als Beweis aus oder würden Sie von objektiven Daten profitieren, um deren Sicherheitslage im Laufe der Zeit besser zu verstehen?
- Wenn neu auftretende Risiken und Schwachstellen effektiv erkannt werden, wie einfach ist es dann, darauf zu reagieren? Wie viele Anwendungen benötigen Sie, um eine Kontaktaufnahme mit dem Anbieter zu initiieren und eine rechtzeitige Schadensbegrenzung sicherzustellen?
- Verfügen Sie über einen vollständigen Überblick über die gesamte Bedrohungslandschaft Ihrer digitalen Lieferkette, einschließlich des Risikos durch Viertanbieter, sowie über Erkenntnisse und Empfehlungen zur allgemeinen Gesundheit Ihres Ökosystems?
- Können Sie die Wirksamkeit Ihres Programms zuverlässig kommunizieren und darlegen oder Fragen Ihres Vorstands dazu beantworten, wie viel Risiko reduziert oder verhindert wurde? oder wie lässt sich dieses Risiko finanziell quantifizieren und mit tatsächlichen Sicherheitsergebnissen korrelieren?

# 03

# Strategien zur Vereinfachung, Integration und
# Konsolidieren Sie Ihren TPRM-Workflow

# 03 Strategien zur Vereinfachung, Integration und Konsolidierung Ihr TPRM-Workflow

Vendor Risk Management (VRM) ist oft der Ausgangspunkt für Third-Party Risk Management (TPRM) und optimiert den Workflow zur Bewertung, Verwaltung und Neubewertung von Lieferanten. Als logischer nächster Schritt auf dem Weg zur Reife von TPRM können Unternehmen ganzheitlichere Funktionen wie kontinuierliche Überwachung, Fourth-Party Risk Management und Schwachstellenerkennung hinzufügen, um schnell auf größere Sicherheitsereignisse zu reagieren und so eine effektive Absicherung zu gewährleisten.

Ganzheitliches TPRM erhöht die End-to-End-Transparenz der digitalen Lieferkette, indem es Sicherheitskontrollen von Drittanbietern misst und kontinuierlich überwacht und das Programm letztendlich an Ihre Risikotoleranz und Ihre Unternehmensziele anpasst.

| GEHEN SIE VON… | ZU… |
|---|---|
| Sicherheitsanfragen sind über mehrere Teams und Plattformen verteilt | Eine einzige, gemeinsam nutzbare Quelle der Wahrheit über Teams und Organisationen hinweg |
| Daten, die in Tabellenkalkulationen, E-Mails und manuellen Fragebögen gespeichert werden | Alle Risikodaten von Drittanbietern werden auf einer Plattform erfasst und analysiert |
| Manueller, langsamer Austausch über Wochen, wenn nicht Monate | Echtzeit-Updates, objektive Daten und kontinuierliche Überwachung der Lieferkette |
| Vertrauen auf unvollständige oder veraltete Daten bei der Entscheidungsfindung | Vertrauen auf unvollständige oder veraltete Daten bei der Entscheidungsfindung |

**Hier finden Sie eine Schritt-für-Schritt-Anleitung zum Erstellen eines nachhaltigen und skalierbaren Drittanbieter-Risikomanagementprogramms von Grund auf.**

SCHRITT 1:

## Schaffen Sie die Grundlage für die Risikobewertung und Einarbeitung von Lieferanten

Schaffen Sie die Grundlage für standardisierte Verfahren und klare Kriterien zur Bewertung des Lieferantenrisikos und sorgen Sie so für Konsistenz und Effizienz in Ihrem gesamten Unternehmen.

**Zu den typischen Anforderungen gehören:**

- Standardfragebögen wie SIG Core und Lite, Cloud Security Alliance CAIQ oder CIS Controls.
- Zertifizierungen wie SOC2-Berichte, ISO 27001, HiTrust oder Cyber Essentials.
- Nachweise wie Penetrationstests, Anwendungsscans oder Versicherungsunterlagen.
- Branchenspezifische Standards wie HIPAA für Organisationen, die Gesundheitsdaten verarbeiten, PCI DSS für Organisationen, die Kreditkartendaten verarbeiten, NERC CIP für kritische Infrastrukturen im Stromsektor oder NIST 800-53, das einen Katalog von Sicherheits- und Datenschutzkontrollen basierend auf Risiko, Kosteneffizienz und Fähigkeiten bereitstellt.
- Lokale Regulierungsstandards wie die der SEC in den USA, NIS2 und DORA in der EU, PS21/3 im Vereinigten Königreich oder Datenschutzstandards wie GDPR oder CCPA.

Die Verwaltung der Lieferantenbeziehungen muss eine Zusammenarbeit zwischen den Verantwortlichen für Lieferantenbeziehungen, der Sicherheits-, Rechts-, Beschaffungs-, Compliance-, Buchhaltungs- und anderen Abteilungen sein. Beziehen Sie bei der Entwicklung Ihres Programms die Mitglieder Ihrer Organisation ein, deren Beiträge und Beteiligung entscheidend sind, und schaffen Sie eine gemeinsam vereinbarte Grundlage. Konzentrieren Sie sich darauf, zu zeigen, wie eine relativ geringe Investition zu einer erheblichen Reduzierung der jährlichen Verlusterwartung aus Drittrisiken.

Wählen Sie abschließend die Anbieter aus, mit denen Sie Ihren Prozess aufbauen und automatisieren möchten. Nehmen Sie sich die Zeit, TPRM-Tools gründlich zu recherchieren und suchen Sie nach Anbietern, die eine End-to-End-Lösung anbieten, die über Fragebögen und Due Diligence hinausgeht und objektive Analysen und Daten umfasst, um Ihnen zu besseren Entscheidungen zu verhelfen.

SCHRITT 2:

# Richten Sie automatisierte Workflows für Neubewertungen, kontinuierliche Überwachung und Schwachstellenerkennung ein

Nutzen Sie die Automatisierung, um mit Ihrem stetig wachsenden Lieferanten-Ökosystem und der sich entwickelnden Bedrohungslandschaft Schritt zu halten. Durch kontinuierliche Überwachung und Schwachstellenerkennung können Sie Risiken proaktiv in Echtzeit identifizieren und beheben. So stärken Sie die Widerstandsfähigkeit Ihres Unternehmens gegen Cyberbedrohungen und behalten die Lieferantensicherheit stets im Blick.

Bei Zero-Day-Ereignissen müssen Sie das Ausmaß des Problems in Ihrem gesamten Ökosystem schnell erfassen und reagieren. Wie ermitteln Sie, welche Anbieter betroffen sind? Wie arbeiten Sie mit ihnen zusammen, um die Schadensbegrenzungsmaßnahmen zu priorisieren? Und was sagen Sie Ihren Vorstandsmitgliedern, wenn diese einen Sanierungsbericht anfordern?

Ihr Prozess sollte sich auf Risikobereiche konzentrieren, die unmittelbare Auswirkungen auf Ihr Unternehmen haben könnten, beispielsweise kompromittierte Systeme oder das Vorhandensein von Schwachstellen und Bedrohungen, die in der Branche des Anbieters üblich sind.

Legen Sie basierend auf dem Risikoniveau einen regelmäßigen Neubewertungsrhythmus fest. Im Falle eines Sicherheitsvorfalls oder einer Sicherheitsverletzung, einer öffentlich gewordenen Zero-Day-Sicherheitslücke oder nachdem Sie Ihre Risikoschwellenwerte aktualisiert haben, möchten Sie möglicherweise Drittanbieter außerhalb Ihres normalen Rhythmus erneut einbeziehen.

## Beispiel für den Rhythmus der Lieferantenneubewertung

| RISIKOSTUFE | VERTRAG REZENSION | RISIKO KAT EG ORIZ AT ION | SICHERHEITSÜBERPRÜFUNG | SLA-ÜBERPRÜFUNG |
|---|---|---|---|---|
| **Stufe 1 – Hohes Risiko** | Bei Erneuerung oder wesentliche Änderungen am Umfang des bestehenden Vertrags | Jährlich oder nach einem Sicherheitsvorfall oder einer Sicherheitsverletzung; oder wesentlichen Änderungen des Umfangs des bestehenden Vertrags | Jährlich oder nach einem Sicherheitsvorfall oder einer Sicherheitsverletzung; oder wesentlichen Änderungen des Umfangs des bestehenden Vertrags | Jährlich oder nach einem Sicherheitsvorfall oder einer Sicherheitsverletzung; oder wesentlichen Änderungen des Umfangs des bestehenden Vertrags |
| **Stufe 2 – Mittleres Risiko** | Bei Erneuerung | Alle 24 Monate oder nach einem Sicherheitsvorfall oder einer Sicherheitsverletzung; oder wesentlichen Änderungen o Umfang des bestehenden Vertrages | Alle 24 Monate oder nach einer Sicherheitsüberprüfung Vorfall oder Verstoß; oder wesentliche Änderungen am Umfang des bestehenden Vertrags | Alle 24 Monate oder nach einem Sicherheitsvorfall oder einer Sicherheitsverletzung; oder wesentlichen Änderungen des Umfangs des bestehenden Vertrags |
| **Stufe 3 – Geringes Risiko** | Bei Erneuerung | Alle 36 Monate oder nach einem Sicherheitsvorfall oder einer Sicherheitsverletzung; oder wesentlichen Änderungen des Umfangs des bestehenden Vertrags | Nach einem Sicherheitsvorfall oder einer Sicherheitsverletzung; oder wesentliche Änderungen des Umfangs des bestehenden Vertrags | Nach einem Sicherheitsvorfall oder einer Sicherheitsverletzung oder wesentlichen Änderungen des Umfangs eines bestehenden Vertrags |

SCHRITT 3:

## Nutzen Sie objektive Daten und Analysen, um Sanierungsmaßnahmen zu priorisieren

Nutzen Sie datengesteuerte Erkenntnisse, um Sanierungsmaßnahmen basierend auf der Schwere des Risikos, der Wahrscheinlichkeit und den potenziellen Auswirkungen zu priorisieren.

Zusätzlich zu den Informationen, die Sie von einem Anbieter anfordern können, benötigen Sie objektive Nachweise und Daten, um dessen Antworten zu validieren und fundiertere Entscheidungen zu treffen. Sicherheitsbewertungen bieten umfassende Einblicke in die Sicherheitskontrollen von Anbietern und ergänzen Ihre Anbieter-Risikobewertungen um eine weitere Verifizierungsebene. Sie ergänzen Sicherheitsartefakte und Fragebögen um objektive Erkenntnisse zu Kategorien wie Verschlüsselung, Datenaufbewahrung, Penetrationstests und Datenschutzprotokollen.

Diese Erkenntnisse lösen nicht nur Abhilfeforderungen aus, sondern geben dem Anbieter möglicherweise auch die Möglichkeit, seine Sicherheitslage zu verbessern und so letztlich das Vertrauen in die gesamte Lieferkette zu stärken.

Qualitative und quantitative Sicherheitsbewertungen, wie sie Bitsight bereitstellt, korrelieren nachweislich direkt mit der Wahrscheinlichkeit von Datenschutzverletzungen in einem Unternehmen. Je niedriger die Bewertung, desto größer ist die Sorge, dass Ihre Daten in die Hände Dritter gelangen.

Bitsight-Metriken weisen die höchste Korrelation zu Sicherheitsverletzungen auf und Sicherheitsvorfälle.

Marsh McLennan fand eine statistisch signifikante Korrelation zwischen 14 Bitsight-Analysen und Cybersicherheitsvorfällen.

Lesen Sie den Bericht →

Eine weitere Möglichkeit, die Ergebnisse Ihrer Risikobewertungen zu verbessern, ist die Nutzung von Integrationen. Beispielsweise kann Bitsight VRM Ihren automatisierten Workflow mit verschiedenen Datenfeeds integrieren, um zusätzliche Informationen über Anbieter zu gewinnen, darunter geopolitische Risiken, Offenlegung von Anmeldeinformationen, Datenschutz und finanzielle Tragfähigkeit. Darüber hinaus können Sie VRM mit Business Intelligence- oder GRC-Tools integrieren, um Ihren Prozess weiter zu optimieren und Ihre Ergebnisse zu verbessern.

SCHRITT 4:

## Programmerfolge verfolgen, verbessern, melden und kommunizieren

Ein wichtiger Weg, den Nutzen zu belegen und sowohl die Unterstützung der Geschäftsleitung als auch das Budget zu sichern, ist die Quantifizierung und Visualisierung von Cyberrisiken in finanzieller Hinsicht. Zeigen Sie, dass Ihr Third-Party Risk Management- oder Supply Chain Cybersecurity-Programm das Risiko insgesamt reduziert und unerwartete Kosten im Zusammenhang mit einem Cybervorfall reduziert oder mindert, abgestimmt auf die jährliche Schadenserwartung (ALE). Durch diese Messung von Cyberrisiken ist es oft einfacher, Unterstützung und Budget zu gewinnen, insbesondere wenn die Kosten Ihres Programms selbst geringer sind als die prognostizierte jährliche Schadenserwartung.

Sie können beispielsweise den voraussichtlichen jährlichen Verlust durch eine Datenpanne bei einem Drittanbieter berechnen, indem Sie die Wahrscheinlichkeit eines solchen Vorfalls im nächsten Jahr mit den finanziellen Auswirkungen multiplizieren, die ein solcher Vorfall für Ihr Unternehmen hätte (z. B. PR-Kosten, Betriebsunterbrechung, Rechtskosten usw.). Sollte es bei einem Drittanbieter zu einer Sicherheitsverletzung kommen, die aufgrund der Ergebnisse Ihrer Risikobewertung abgelehnt wurde, teilen Sie diese Informationen Ihrer Führungsebene mit.

**Wenn Sie bei der Gewinnung oder Beibehaltung der Zustimmung der Führungsebene auf Hindernisse stoßen, versuchen Sie es mit den folgenden Perspektiven:**

| GEMEINSAME RÜCKSCHLÄGE | ÜBERZEUGENDES ARGUMENT |
|---|---|
| Fehlendes Budget für TPRM | Die Reduzierung der jährlichen Verlusterwartung ist größer als die Kosten des Programms |
| TPRM ist eine Sicherheitspriorität, keine Geschäftspriorität | TPRM fördert das Unternehmenswachstum durch die Sicherung des Outsourcings, die Gewährleistung der Einhaltung gesetzlicher Vorschriften und den Aufbau des Kundenvertrauens |
| Manueller, langsamer Austausch über Wochen, wenn nicht Monate | Automatisierung und spezielle Tools vereinfachen TPRM will mit den gleichen Ressourcen mehr erreichen |

**SCHRITT 5:**

## Gewährleisten Sie die Einhaltung der Vorschriften in Ihrer gesamten digitalen Lieferkette

Regulierungen lenken den Fokus auf das Cyber-Risikomanagement und erkennen die entscheidende Bedeutung der Cybersicherheit für die nationale Sicherheit, die wirtschaftliche Stabilität und den Schutz des digitalen Ökosystems an. In der Europäischen Union rückt NIS2 die Verantwortlichkeit in den Mittelpunkt. Unternehmen müssen also nicht nur robuste Cybersicherheitsmaßnahmen implementieren, sondern auch Compliance nachweisen, mit Behörden zusammenarbeiten, die Sicherheit ihrer Lieferketten gewährleisten und die erforderliche Transparenz gewährleisten. In den USA verlangt die SEC von Unternehmen die Offenlegung von „Prozessen zur Überwachung und Identifizierung von Cyberrisiken im Zusammenhang mit der Nutzung von Drittanbietern“.

Das bedeutet, dass CISOs Schutzmaßnahmen und -funktionen zu Differenzierungsmerkmalen machen können, die Wachstum ermöglichen und den Umsatz sichern. Da Vorstände und Aufsichtsbehörden zunehmend in Risikodiskussionen eingebunden werden, schätzen sie quantifizierbare Kennzahlen, die die Leistung Ihres Unternehmens aufzeigen – sowohl absolut als auch relativ zu Branchenbenchmarks, insbesondere da die regulatorischen Erwartungen branchenübergreifend variieren.

Bauen Sie Vertrauen auf, indem Sie unabhängige, vergleichbare und konsistente Benchmarking-Daten weitergeben – eine objektive Analyse der Cybersicherheitsleistung Ihres Unternehmens auf der Grundlage quantitativer Daten.

Um den neuen gesetzlichen Anforderungen gerecht zu werden, implementieren Sie Richtlinien und Verfahren zur Minderung der Cyber-, Rechts- und Finanzrisiken im Zusammenhang mit Lieferantenbeziehungen.

Durch die proaktive Erfüllung Ihrer Compliance-Verpflichtungen können Sie den Ruf Ihres Unternehmens schützen und teure Strafen, Sanktionen, Reputationsverluste oder die Verpflichtung zusätzlicher Audit-Anforderungen vermeiden.

> Der Schlüssel zum Erfolg liegt darin, sicherzustellen, dass Ihr Programm sicherheitsorientiert und nicht complianceorientiert ist. Wenn dies an messbaren Rahmenbedingungen ausgerichtet ist, wie wie NIST, ISO27001 oder SOC2, stärkt es das Vertrauen von Führungskräften und Kunden.“
>
> **Tim Grieveson**
>
> Leitender Vizepräsident—
>
> Globaler Cyber-Risikoberater, Bitsight

# 04

# Zukunftssichere Lieferkette Cybersicherheit und Resilienz

# 04 Zukunftssichere Cybersicherheit und Widerstandsfähigkeit der Lieferkette

Zukunftssicherheit bedeutet, Entscheidungen zu treffen, die Ihre Cybersicherheit auch über den heutigen Tag hinaus sichern – von der Auswahl der richtigen Partner bis hin zur Abwägung kurzfristiger Gewinne mit langfristiger Stabilität. Dieser Weg erfordert Innovation, Planung und Auswahl der richtigen Werkzeuge.

Wenn Ihre Lösung mit Ihrer langfristigen Roadmap übereinstimmt, minimieren Sie Störungen, da sie eine natürliche Erweiterung Ihrer bestehenden Sicherheitsinfrastruktur darstellt. Diese nahtlose Integration ermöglicht einen reibungsloseren Übergang und minimiert Ausfallzeiten.

Wenn Sie Ihr TPRM-Programm zukunftssicher machen, sichern Sie schon heute Ihre Zukunft. Treffen Sie daher kluge Entscheidungen und investieren Sie strategisch.

### VEREINIGUNG

Ein einheitlicher Ansatz für das Cyber-Risikomanagement rationalisiert Ihre Bemühungen und erspart Ihnen den ständigen Aufwand für Änderungsmanagement und Schulungen. Ihr Team sollte sich auf die Minimierung von Cyberrisiken konzentrieren, nicht auf die Verwaltung eines dezentralen Toolkits.

### SKALIERBARKEIT:

Eine Funktion, die zu Ihrem langfristigen Fahrplan passt, muss Menschen, Prozesse und Technologie integrieren und sich an veränderte Anforderungen anpassen – sei es ein erweitertes Lieferantennetzwerk, erhöhte Datenmengen oder sich entwickelnde Compliance-Standards.

### VORSCHRIFTEN BEREITSCHAFT:

Sie benötigen flexible Funktionen, die sich an sich entwickelnde Anforderungen anpassen lassen – beispielsweise unabhängiges Benchmarking zur Einhaltung der Offenlegungsrichtlinien der SEC für Cyberrisiken oder die kontinuierliche Überwachung von IKT-Drittanbietern zur Einhaltung der NIS2- und DORA-Standards.

> “Beginnen Sie mit einer Vision, wohin Sie Ihr TPRM-Programm führen möchten, und finden Sie dann die Anbieter und Lösungen, die kann Sie dorthin bringen. Beachten Sie drei Schlüsselprinzipien: Vereinheitlichung, Skalierbarkeit und Regulierungsbereitschaft.“
>
> **Tim Grieveson**
>
> Leitender Vizepräsident—
> Globaler Cyber-Risikoberater, Bitsight

# Wie kann Bitsight Ihr TPRM-Programm und die Cybersicherheit Ihrer Lieferkette verbessern?

Bitsight hat maßgeblich dazu beigetragen, das Cyber-Risikomanagement zu vereinfachen und TPRM-Programmmanagern bei der Skalierung ihrer Arbeit zu helfen. Wir waren Vorreiter bei der Nutzung von Sicherheitsbewertungen zur Messung der Sicherheitslage von Unternehmen und Drittanbietern und haben Cybersicherheitsanalysen in die Arbeitsabläufe und Plattformen ihrer Wahl integriert.

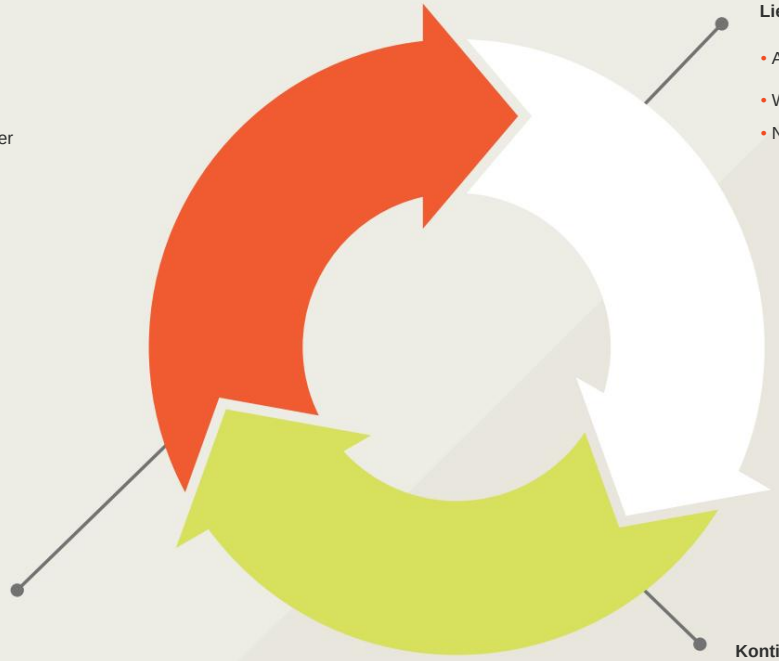
Bitsight Third-Party Risk Management ist eine End-to-End-Lösung, die den Prozess effizienter gestaltet und Unternehmen dabei unterstützt, die Sicherheitsleistung von Lieferanten zuverlässig zu bewerten, zu validieren und kontinuierlich zu überwachen. Unsere Kunden profitieren von der Effizienzsteigerung durch die Ausführung aller TPRM-Workflows auf einer Plattform.

Egal, ob Sie gerade erst anfangen oder Ihr Programm auf die nächste Ebene bringen, Bitsight hat die Werkzeuge und Dienste, die Ihnen helfen, Ihr Team führt Ihre Programme zum Risikomanagement von Drittanbietern aus.

## Bitsight Drittanbieter-Risikomanagement

**Unterstützt durch Managed Services**

- Verwaltete Lieferantenbewertungen
- Kontinuierliche Überwachung und Risikosuche
- Aufgedeckte Erkenntnisse und Berichte



**Lieferantenrisikomanagement**

- Automatisierte Bewertungen
- Wachsendes Lieferantennetzwerk
- Nachweise zur Validierung

**Exposure-Management**

- Beschleunigen Sie die Behebung von Sicherheitslücken
- Skalieren und verfolgen Sie die Bemühungen zur Anbieteransprache
- Priorisieren Sie die Eindämmung der Gefährdung

**Kontinuierliche Überwachung**

- Überprüfen Sie jederzeit die Lieferantenkontrollen
- Kontextbezogene Zusammenarbeit mit Anbietern
- Automatische Erkennung konzentrierter Viertparteienrisiko

## Die Macht des Netzwerks

Mit Bitsight Vendor Risk Management können Sie sofort auf ein schnell wachsendes Netzwerk mit über 40.000 Lieferantenprofilen zugreifen – ständig aktualisiert – und das alles in Echtzeit.
Die Effizienzgewinne sind außergewöhnlich. Das Erlebnis ist sogar noch besser.

| 40.000+ | 3-facher ROI | 90 % | 75+ % |
|---|---|---|---|
| Anbieterprofile | Innerhalb der ersten sechs Monate* | Lieferantenakzeptanzrate * | Zeitersparnis bei der Bewertung von Anbietern* |

*Wie von bestehenden Bitsight-Kunden berichtet. Die tatsächlichen Ergebnisse hängen von einer Vielzahl individueller Faktoren ab und können nicht garantiert werden.

Fordern Sie noch heute eine personalisierte Demo an und beginnen Sie mit dem Aufbau Ihres integrierten TPRM-Programms.

Starten Sie noch heute →

Bitsight ist ein führendes Unternehmen im Bereich Cyber-Risikomanagement und transformiert die Art und Weise, wie Unternehmen ihre eigene Gefährdung, Leistung und Risiken sowie die ihrer Drittparteien managen. Unternehmen vertrauen auf Bitsight, um ihre Investitionen in die Cybersicherheit zu priorisieren, das Vertrauen in ihr Ökosystem zu stärken und das Risiko finanzieller Verluste zu reduzieren. Die integrierten Lösungen basieren auf über einem Jahrzehnt technologischer Innovation und bieten Mehrwert in den Bereichen Unternehmenssicherheit, digitale Lieferketten, Cyber-Versicherung und Datenanalyse.

BOSTON (Hauptquartier) RALEIGH NEW YORK LISSABON SINGAPUR



BITSIGHT