Cost of a Data Breach Report 2025

Die Lücke bei der KI-Aufsicht

Zusammenfassung

think report

IBM

Zusammenfassung

Willkommen zum jährlichen Cost of a Data Breach Report von IBM. Mit dieser Ausgabe feiern wir 20 Jahre Forschung zu Datenschutzverletzungen. In diesem Jahr haben wir den grundlegendsten technologischen Wandel seit einer Generation im Visier: die Einführung von KI.

Mit dem Bericht 2025 beginnen wir mit der Chronifizierung und Quantifizierung der mit der KI verbundenen Risiken. Was wir herausgefunden haben, ist besorgniserregend: Unternehmen übergehen Sicherheit und Governance für KI zugunsten einer sofortigen Einführung von KI. Bei diesen unkontrollierten Systemen ist es wahrscheinlicher, dass eine Sicherheitslücke entsteht – und es ist kostspieliger, wenn dies der Fall ist.
Das überrascht uns nicht.

Seit 2005 hat dieser Bericht die sich ständig erweiternde Technologielandschaft und die daraus resultierenden Bedrohungen verfolgt. Unsere Forschungspartner vom Ponemon Institute haben nicht nur das Auftauchen neuer Bedrohungen und Angriffsflächen dokumentiert, sondern diese Bedrohungen auch in finanzieller Hinsicht quantifiziert, so dass Sicherheits- und Unternehmensleiter sie verstehen und entsprechend handeln können. Insgesamt haben die Forscher mehr als 6.485 Sicherheitsverletzungen untersucht und über 34.652 Führungskräfte aus den Bereichen Technologie, Sicherheit und Wirtschaft befragt, die an der Reaktion ihres Unternehmens auf die Sicherheitsverletzung beteiligt waren.

Natürlich haben sich die Sicherheitsbedrohungen im Laufe der Jahre verändert. Vor zwei Jahrzehnten wurde fast die Hälfte aller Datenschutzverletzungen (45 %) durch ein verlorenes oder gestohlenes Computergerät, wie z. B. einen Laptop oder einen USB-Stick, verursacht, während nur 10 % der Datenschutzverletzungen auf „gehackte elektronische Systeme“ zurückzuführen waren. Heutzutage werden die meisten Sicherheitsverletzungen durch eine Reihe von bösartigen Aktivitäten verursacht, von Phishing bis hin zu Insider-Bedrohungen.

Vor zehn Jahren waren Sicherheitsverletzungen aufgrund von Fehlkonfigurationen in der Cloud noch nicht einmal eine kategorisierte Bedrohung. Heute sind die Cloud und die darin befindlichen Daten ein Hauptziel. Und der Anstieg von Ransomware begann erst während der COVID-19-Lockdowns im Jahr 2020. Ein Jahr später beliefen sich die Kosten für diese Angriffe auf durchschnittlich 4,62 Mio. USD, im diesjährigen Bericht waren es 5,08 Mio. USD.

Eine Konstante ist jedoch die Arbeit von Ponemon. Die diesjährige Studie, die vom Ponemon Institute unabhängig durchgeführt und von IBM gesponsert, analysiert und veröffentlicht wurde, untersuchte 600 Unternehmen, die zwischen März 2024 und Februar 2025 von Datenschutzverletzungen betroffen waren. Wir haben Unternehmen aus 17 Branchen in 16 Ländern und Regionen untersucht, bei denen zwischen 2.960 und 113.620 Datensätze kompromittiert wurden.
Um Erkenntnisse vor Ort zu gewinnen, befragten die Ponemon-Forscher 3.470 Führungskräfte aus dem Sicherheitsbereich und der Geschäftsleitung, die aus erster Hand über die Datenschutzverletzungen in ihren Unternehmen informiert waren. Zu diesen Führungskräften gehörten CEOs, Betriebsleiter, Controller oder Finanzleiter, IT-Fachleute, Leiter von Geschäftseinheiten und Geschäftsführer sowie Fachleute für Risikomanagement und Cybersicherheit.

Das Ergebnis ist ein Benchmark-Bericht, den Unternehmens-, Technologie- und Sicherheitsverantwortliche nutzen können, um ihre Verteidigung zu stärken, die Ressourcenzuweisung zu informieren und Innovationen voranzutreiben, insbesondere im Hinblick auf die Sicherung und Steuerung ihrer KI-Initiativen.

Die diesjährige Schlagzeile: Die weltweiten Kosten für Datenschutzverletzungen sind zum ersten Mal seit fünf Jahren gesunken, und zwar auf 4,44 Mio. USD, was auf eine durch KI-gestützte Abwehrmaßnahmen erreichte schnellere Eindämmung von Datenschutzverletzungen zurückzuführen ist. Aber so wie die Verteidiger immer besser und schneller agieren, so werden auch die Angreifer immer schlauer. 16 % der Sicherheitsverletzungen wurden von Angreifern begangen, die KI verwenden, die häufig bei Phishing- und Deepfake-Angriffen eingesetzt wird. Während dieses ausufernde KI-Wettrüsten den Unternehmen zugute kommt, indem es die Kosten für Sicherheitsverletzungen weltweit senkt, stemmen sich die USA gegen den Trend. Dort sind die Kosten für Sicherheitsverletzungen auf über 10 Mio. USD gestiegen, was auf strengere gesetzliche Strafen und steigende Entdeckungskosten zurückzuführen ist.

Wir haben auch festgestellt, dass die Einführung von KI schneller voranschreitet als die Überwachung. Wir haben festgestellt, dass 97 % der Sicherheitsverstöße im Zusammenhang mit KI Systeme betrafen, die keine angemessenen Zugangskontrollen hatten.
Und die meisten der betroffenen Unternehmen gaben an, dass sie keine Governance-Richtlinien haben, um KI zu verwalten oder Schatten-KI, d. h. den Einsatz von KI ohne Genehmigung des Arbeitgebers oder ohne Aufsicht, zu verhindern. Sowohl der verdeckte Einsatz von Schatten-KI als auch das Fehlen von Governance treiben die Kosten für Sicherheitsverletzungen in die Höhe.

Neuerungen im Bericht 2025

Wie immer spiegelt der Data Breach Kostenreport neue Technologien, neue Taktiken und aktuelle Ereignisse wider. In der diesjährigen Studie wird zum ersten Mal untersucht:

- Stand der Sicherheit und Governance für KI
- Prävalenz und Risikoprofil von Schatten-KI
- Art der Daten, die bei Sicherheitsvorfällen mit KI ins Visier genommen werden
- Dauer der Unterbrechungen von Sicherheitsverletzungen in Unternehmen
- Kosteneinsparungen durch den Einsatz von Quantum-Sicherheitstools
- Kosten für Sicherheitsverletzungen im Zusammenhang mit KI-gestützten Angriffen
- Höhe der an die Kunden weitergegebenen Kosten für Sicherheitsverletzungen

Wesentliche Feststellungen

Die im Folgenden dargestellten Ergebnisse basieren auf der unabhängigen Analyse von Forschungsdaten des Ponemon Institute durch IBM.

4,44 Mio. USD

Die weltweiten Durchschnittskosten einer Datenschutzverletzung

Die weltweiten durchschnittlichen Kosten für Sicherheitsverletzungen sanken von 4,88 Mio. USD im Jahr 2024 auf 4,44 Mio. USD, was einem Rückgang von 9 % und einer Rückkehr zum Kostenniveau von 2023 entspricht. Die schnellere Identifizierung und Eindämmung von Sicherheitsverletzungen – ein Großteil davon von den eigenen Sicherheits- und Sicherheitsdienstteams der Unternehmen mit Hilfe von KI und Automatisierung – hat zu diesem Rückgang geführt. Der weltweite Durchschnitt wäre niedriger, wenn man die Vereinigten Staaten nicht berücksichtigen würde, wo die durchschnittlichen Kosten um 9 % auf 10,22 Mio. USD gestiegen sind. Dies ist ein Allzeithoch für alle Regionen. Höhere behördliche Bußgelder und höhere Kosten für die Erkennung und Eskalation in den Vereinigten Staaten trugen zu diesem Anstieg bei.

13 %

Anteil an KI-bezogenen Sicherheitsvorfällen

Sicherheitsvorfälle, an denen die KI eines Unternehmens beteiligt ist, bleiben begrenzt – vorerst. Im Durchschnitt meldeten 13 % der Unternehmen Verstöße, die ihre KI-Modelle oder -Anwendungen betrafen. Bei denjenigen, bei denen dies der Fall war, fehlte es jedoch fast allen (97 %) an angemessenen KI-Zugriffskontrollen. Die meisten dieser Sicherheitsvorfälle ereigneten sich in der KI-Lieferkette, durch kompromittierte Apps, APIs oder Plug-ins. Diese Vorfälle hatten einen Dominoeffekt: Sie führten zu einer weitreichenden Datenkompromittierung (60 %) und Betriebsunterbrechungen (31 %). Die Ergebnisse deuten darauf hin, dass sich KI zu einem hochwertigen Ziel entwickelt.

4,92 Mio. USD

Durchschnittliche Kosten für böswillige Insider-Angriffe

Im zweiten Jahr in Folge verursachten Angriffe durch böswillige Insider die höchsten durchschnittlichen Kosten unter den ursprünglichen Bedrohungsvektoren: 4,92 Millionen USD. Die Kompromittierung von Drittanbietern und der Lieferkette folgte dicht dahinter mit 4,91 Millionen USD. Weitere teure Angriffsvektoren waren die Ausnutzung von Schwachstellen und Phishing. Der häufigste Angriffsvektor auf Unternehmen war jedoch mit 16 % Phishing, das im Durchschnitt 4,8 Millionen USD kostete.

200.000 USD

Zusätzliche Kosten für eine Sicherheitsverletzung mit Schatten-KI

Von den in diesem Jahr untersuchten Unternehmen gaben 20 % an, dass sie aufgrund von Sicherheitsvorfällen im Zusammenhang mit Schatten-KI eine Datenschutzverletzung erlitten haben. Diese Verstöße erhöhten den durchschnittlichen Preis für eine Sicherheitsverletzung um USD 200.321. Diese Vorfälle führten auch dazu, dass mehr persönliche Daten (65 %) und geistiges Eigentum (40 %) kompromittiert wurden. Und diese Daten wurden meist in mehreren Umgebungen gespeichert, was zeigt, dass ein einziges nicht überwachtes KI-System eine weitreichende Gefährdung darstellen kann. Der rasche Anstieg der Schatten-KI hat den Mangel an Sicherheitskompetenzen als einen der drei wichtigsten Faktoren für kostspielige Sicherheitsverletzungen abgelöst, die in diesem Bericht untersucht wurden.

1,9 Mio. USD

Kosteneinsparungen durch umfassenden KI-Einsatz in der Sicherheit

Sicherheitsteams, die KI und Automatisierung einsetzen, verkürzten die Dauer eines Verstoßes um 80 Tage und senkten die durchschnittlichen Kosten für einen Einbruch um 1,9 Millionen USD im Vergleich zu Unternehmen, die diese Lösungen nicht einsetzten. Fast ein Drittel der Unternehmen gab an, dass sie diese Tools über den gesamten Sicherheitslebenszyklus hinweg ausgiebig nutzen – zur Prävention, Erkennung, Untersuchung und Reaktion. Allerdings ist diese Zahl im Vergleich zum Vorjahr nur leicht gestiegen, was darauf hindeutet, dass die Einführung von KI ins Stocken geraten sein könnte. Die Studie zeigt auch, dass die Mehrheit der Unternehmen noch immer keine KI und Automatisierung einsetzt und daher die Kostenvorteile nicht sieht.

63 %

Anteil der Unternehmen, die sich geweigert haben, Ransomware-Angreifer zu bezahlen

Im Jahr 2025 (63 %) weigerten sich mehr Ransomware-Opfer, ein Lösegeld zu zahlen, als im Jahr 2024 (59 %). Die durchschnittlichen Kosten eines Erpressungs- oder Ransomware-Vorfalls sind jedoch nach wie vor hoch, vor allem, wenn er von einem Angreifer aufgedeckt wird (5,08 Mio. USD). Gleichzeitig gaben weniger Ransomware-Opfer an, die Strafverfolgungsbehörden eingeschaltet zu haben – 40 % der Unternehmen in diesem Jahr gegenüber 53 % im letzten Jahr.

49 %

Anteil der Unternehmen, die nach einer Sicherheitsverletzung in die Sicherheit investieren

Die Zahl der Unternehmen, die nach einer Sicherheitsverletzung Investitionen in die Sicherheit planen, ist deutlich gesunken: 49 % in diesem Jahr gegenüber 63 % im letzten Jahr. Weniger als die Hälfte derjenigen, die in Sicherheit investieren wollen, planen, sich auf KI-gesteuerte Sicherheitslösungen oder -dienste zu konzentrieren, wie z. B. die Erkennung von und Reaktion auf Bedrohungen, die Planung und das Testen von Incident Response (IR) sowie Tools für die Datensicherheit oder den Datenschutz.

63 %

Anteil der Unternehmen, die keine KI-Governance-Richtlinien haben

Die Mehrheit der betroffenen Unternehmen (63 %) hat entweder keine KI-Richtlinie oder ist noch dabei, eine zu entwickeln. Selbst wenn sie eine Richtlinie haben, verfügen weniger als die Hälfte über einen Genehmigungsprozess für den Einsatz von KI, und 62 % haben keine angemessene Zugangskontrolle für KI-Systeme. Von den Unternehmen, die über Governance-Richtlinien verfügen, führt nur eine Minderheit (34 %) regelmäßige Prüfungen auf nicht genehmigte KI durch. Dies zeigt, dass KI weitgehend unkontrolliert bleibt, da die Akzeptanz von KI sowohl die Sicherheit als auch die Governance übersteigt.

1 von 6

Anzahl der Verstöße mit KI-basierten Angriffen

Angreifer können generative KI (Gen AI) nutzen, um ihre Phishing-Kampagnen und andere Social-Engineering-Angriffe zu perfektionieren und auszuweiten. IBM hat herausgefunden, dass generative KI die Zeit, die für die Erstellung einer überzeugenden Phishing-E-Mail benötigt wird, von 16 Stunden auf nur fünf Minuten reduziert hat. Der diesjährige Bericht zeigt die Auswirkungen: Bei durchschnittlich 16 % der Datenschutzverletzungen setzten Angreifer KI ein, am häufigsten für KI-generierte Phishing-Angriffe (37 %) und Deepfake-Impersonation-Angriffe (35 %).

Empfehlungen

Um Datenschutzverletzungen vorzubeugen, sie abzumildern und die Kosten zu reduzieren sowie KI-Modelle, -Anwendungen und -Nutzung zu sichern und zu steuern, empfehlen die Experten von IBM diese fünf erfolgreichen Ansätze.

Stärken von Identitäten – Mensch und Maschine

Viele Unternehmen arbeiten mit laxen Zugriffskontrollen, Konten mit zu vielen Berechtigungen und einem geringen Überblick darüber, wer Zugriff auf wichtige Systeme hat. In vielen Fällen werden verschiedene Abteilungen und Tools für das Identitäts- und Zugriffsmanagement (IAM) verwendet. All diese Faktoren schaffen Öffnungen, die Angreifer aktiv ausnutzen, daher ist es wichtig, diese Öffnungen zu begrenzen. In der Zwischenzeit wachsen KI-Modelle und -Infrastrukturen rasant und bieten Angreifern eine neue, hochwertige Angriffsfläche.

Die Stärkung der Identitätssicherheit mit Hilfe von KI und Automatisierung kann IAM verbessern, ohne die chronisch unterbesetzten Sicherheitsteams zu überlasten. Und da KI-Agenten eine immer größere Rolle in den Abläufen eines Unternehmens spielen, müssen die Identitäten der Agenten genauso geschützt werden wie die menschlichen Identitäten. Genau wie menschliche Benutzer sind auch KI-Agenten zunehmend auf Anmeldeinformationen angewiesen, um auf Systeme zuzugreifen und Aufgaben auszuführen. Daher ist es unerlässlich, strenge Kontrollen oder Services zu implementieren, die Sie dabei unterstützen und alle Aktivitäten mit nicht-menschlichen Identitäten (NHI) zu überwachen. Unternehmen müssen in der Lage sein, zwischen NHI, die verwaltete (gesicherte) Anmeldedaten verwenden, und solchen, die nicht verwaltete Anmeldedaten verwenden, zu unterscheiden.

Sobald die Zugangsdaten verwaltet werden, ist es wichtig, sie zu schützen und eine ordnungsgemäße Lebenszyklusverwaltung und Governance durchzusetzen. Es umfasst die Bereitstellung, Rotation, Prüfung, den Schutz und die Stilllegung von Berechtigungsnachweisen sowie die Überwachung des Verhaltens von NHIs, um sicherzustellen, dass sie innerhalb der erwarteten Parameter arbeiten. Auf diese Weise können Unternehmen das Risiko des Missbrauchs von Zugangsdaten verringern und eine sichere und konforme Umgebung aufrechterhalten.

Heutzutage loggen sich viele Angreifer ein, anstatt sich in das System zu hacken. Um dieses Problem zu bekämpfen, muss verhindert werden, dass Angreifer überhaupt in den Besitz dieser Anmeldedaten kommen. Eine der effektivsten Möglichkeiten, dies zu tun, besteht darin, dafür zu sorgen, dass alle menschlichen Benutzer moderne, phishing-resistente Authentifizierungsmethoden wie Passkeys verwenden. Diese Technologien wurden entwickelt, um die Schwachstellen herkömmlicher Passwörter und Einmal-Codes zu beseitigen und es Angreifern deutlich schwerer zu machen, Anmeldedaten abzufangen oder zu missbrauchen.

Verbesserung der KI-Datensicherheit

Die Unternehmen haben die Experimentierphase mit generativer KI und KI-Agenten hinter sich gelassen und sind zu praxistauglichen Innovationen übergegangen und haben die Technologie tief in die Struktur ihrer Unternehmen eingewoben. Aber die Einführung schreitet schneller voran als die Sicherheit. Der diesjährige Bericht ergab, dass 62 % der Unternehmen keine angemessenen Zugriffskontrollen auf KI-Systeme haben. Und da Daten der Treibstoff für KI sind, sind sie ein bevorzugtes Ziel für Angreifer.

Die Sicherung von KI-Daten ist nicht nur aus Gründen des Datenschutzes und der Einhaltung von Vorschriften wichtig, sondern auch, um die Datenintegrität zu gewährleisten, das Vertrauen in das Unternehmen zu erhalten und eine Gefährdung der Daten zu vermeiden. Dieser Ansatz bedeutet, über oberflächliche Kontrollen hinauszugehen und starke Datensicherheitsgrundlagen zu implementieren: Datenermittlung und -klassifizierung sowie Datenschutz wie Zugriffskontrolle, Verschlüsselung und Schlüsselverwaltung. Er kann auch den Einsatz von Daten- und KI-Sicherheitsdiensten beinhalten. Diese Maßnahmen sind nicht einzigartig für die Sicherung von KI, aber der Aufstieg von KI sowohl als Bedrohungsvektor als auch als Sicherheitsfaktor bedeutet, dass sie wichtiger sind als je zuvor.

Verbinden Sie Sicherheit für KI und Governance für KI

Sicherheit für KI und Governance für KI sind komplementäre Disziplinen. Wenn Unternehmen sie in Silos halten, erhöhen sie das Risiko, die Komplexität und die Kosten. Leider überholt die Einführung von KI die Einführung von Sicherheit und Governance: 41 % der in der diesjährigen Studie befragten Unternehmen gaben an, dass sie über keine derartigen Richtlinien verfügen, und 22 % sind noch dabei, sie zu entwickeln.

Unternehmen müssen sicherstellen, dass Chief Information Security Officers (CISOs), Chief Revenue Officers (CROs) und Chief Compliance Officers (CCOs) – und ihre Teams – regelmäßig zusammenarbeiten. Investitionen in integrierte Sicherheits- und Governance-Software und Prozesse, die diese funktionsübergreifenden Stakeholder zusammenbringen, können Unternehmen dabei helfen, Schatten-KI automatisch zu entdecken und zu steuern. Solche Investitionen können ihnen auch helfen:

- Verschaffen Sie sich einen Überblick über alle KI-Bereitstellungen.
- Identifizieren und mindern Sie Schwachstellen.
- Schützen Sie die Eingabeaufforderung und die generierten Daten vor unbeabsichtigter Verwendung.
- Verwenden Sie Observability-Tools, um die Compliance zu verbessern und Anomalien zu erkennen.

Nutzen Sie KI-Sicherheitstools und Automatisierung, um schneller voranzukommen

KI hilft Angreifern bereits, schneller zu agieren – zum Beispiel, indem sie Deepfakes mit nur wenigen Eingabeaufforderungen einfach erstellt oder die Zeit, die benötigt wird, um eine realistische Phishing-Nachricht zu erstellen, von Stunden auf Minuten verkürzt. Da Angreifer KI verwenden, um anpassungsfähigere Angriffe zu erzeugen und zu verbreiten, sollten auch Sicherheitsteams KI Technologie nutzen. Sicherheitsteams können KI nutzen, um Angriffe und deren Auswirkungen auf das Geschäft zu reduzieren oder zu verhindern, indem sie proaktiv Maßnahmen ergreifen, die die Genauigkeit der Erkennung (Bedrohungsjagd) verbessern und die Reaktionszeit verkürzen.

Sicherheitstools und Managed Security Services, einschließlich solcher, die auf KI und Automatisierung basieren, können bereits überlastete Sicherheitsteams unterstützen. Sie können das Volumen der Warnungen erheblich reduzieren. Risikodaten zu identifizieren; Sicherheitslücken und Bedrohungen früher erkennen; Erkennung laufender Verstöße; und ermöglichen schnellere, präzisere Angriffsreaktionen.

Verbessern Sie die Resilienz

Je länger der Zeitraum, desto wahrscheinlicher sind Datenschutzverletzungen. Sie passieren trotz starker Präventionsmaßnahmen. Es ist zwar wichtig, Bedrohungen zu blockieren, aber dies kann nicht der einzige Fokus eines Unternehmens sein. Sie müssen sich auch darauf konzentrieren und planen, den Schaden zu minimieren, sobald ein Angriff durchkommt und eine Sicherheitsverletzung auftritt.

Widerstandsfähigkeit aufzubauen bedeutet, in der Lage zu sein, Probleme schnell zu erkennen, sie einzudämmen, bevor sie erhebliche Auswirkungen haben, und den Betrieb schnell und mit minimaler Störung wiederherzustellen. Ein Plan zur Stärkung der Widerstandsfähigkeit sollte regelmäßige Tests von IR-Plänen und die Wiederherstellung von Backups, die Sicherstellung klarer Rollen und Verantwortlichkeiten während der Krisenreaktion – auch für nicht-technische Führungskräfte – und die Einschränkung des Zugangs auf hoher Ebene beinhalten, um den Umfang eines potenziellen Problems zu verringern. Persönliche oder virtuelle Schulungen können entscheidend dazu beitragen, dass die Sicherheitsteams ihre Aufgaben verstehen und in einer Krise ausführen. Um ihre Fähigkeiten im Umgang mit Angriffen zu verbessern, können Unternehmen auch an Cyber-Range-Krisensimulationsübungen teilnehmen.

Über

IBM

IBM ist ein weltweit führender Anbieter von Hybrid-Cloud-, KI- und Business-Services und unterstützt Kunden in über 175 Ländern dabei, Erkenntnisse aus ihren Daten zu gewinnen, Geschäftsprozesse zu rationalisieren, Kosten zu senken und sich Wettbewerbsvorteile in ihren Branchen zu verschaffen. All dies wird durch das legendäre IBM Engagement für Vertrauen, Transparenz, Verantwortung, Inklusivität und Service unterstützt. Weitere Informationen finden Sie unter ibm.com/de-de.

Weitere Informationen zur Verbesserung Ihres Sicherheitsstatus: Besuchen Sie ibm.com/de-de/security.

Nehmen Sie am fachlichen Austausch der IBM Security Community teil.

Ponemon Institute

Das 2002 gegründete Ponemon Institute widmet sich der unabhängigen Forschung und Aufklärung zur Förderung verantwortungsvoller Praktiken im Umgang mit Daten und Datenschutz in Unternehmen und Behörden. Unsere Aufgabe ist es, hochwertige empirische Studien zu wesentlichen Themen durchzuführen, die die Verwaltung und Sicherheit sensibler Daten zu Personen und Unternehmen betreffen.

Das Ponemon Institute hält im Hinblick auf Vertraulichkeit, Datenschutz und Forschungsethik strenge Standards ein und sammelt im Rahmen seiner geschäftlichen Forschung keinerlei personenbezogene Daten von Einzelpersonen oder identifizierbare Unternehmensdaten. Darüber hinaus stellen strenge Qualitätsstandards sicher, dass Befragten keine sachfremden, irrelevanten oder unangemessenen Fragen vorgelegt werden. Bei Fragen oder Anmerkungen zu diesem Forschungsbericht, inklusive Anfragen zur Genehmigung einer Zitierung oder Vervielfältigung des Berichts, wenden Sie sich bitte per Post, Telefon oder E-Mail an:

Ponemon Institute LLC
Forschungsabteilung
1-800-887-3118
research@ponemon.org