kyndryl

Umfrageergebnisse

Was IT-Entscheidungsträger über den aktuellen Stand der IT-Risiken mitteilen

IT-Risiken werden mittlerweile auf Vorstandsebene diskutiert.

In einer Welt, in der Unternehmen auf komplexe, geografisch verteilte und hybride IT-Systeme angewiesen sind, kann ein Netzwerkausfall, ein Malware-Angriff oder eine andere Systemstörung verheerende Auswirkungen auf die Produktivität, den Ruf und das Endergebnis einer Marke haben.

Folglich drängen viele Unternehmensvorstände ihre Managementteams dazu, ihre Vorbereitungen auf ein solches Ereignis zu erläutern.

Angesichts der hohen Risiken haben wir versucht, die Wahrnehmung des IT-Risikos und die Maßnahmen der Unternehmen zur Gewährleistung der Cyberresilienz zu bewerten. Wir haben eine weltweite Gruppe von IT-Entscheidungsträgern sowie Risiko- und Compliance-Fachkräften befragt, um herauszufinden, mit welchen Schwierigkeiten sie konfrontiert sind. Außerdem wollten wir wissen, welche IT-Risiken sie am meisten beunruhigen und was ihre Unternehmen tun, um diese Risiken zu antizipieren, sich davor zu schützen, ihnen zu widerstehen und sich von ihnen zu erholen.

Die Ergebnisse dieser Umfrage werden in den IT-Risikobericht für das Jahr 2023 aufgenommen.

Unsere Ergebnisse bestätigen, dass die IT-Systeme der Unternehmen in der Tat gestört werden. Wir haben die häufigsten Hindernisse für Maßnahmen zur Minderung von Störungen ermittelt. Überrascht hat uns auch diese Feststellung: Die Befragten haben großes Vertrauen in die IT-Verantwortlichen in ihren Unternehmen und in deren Fähigkeit, IT-Störungen zu bewältigen und das Unternehmen wieder in Gang zu bringen.

Wir laden Sie ein, die Ergebnisse als Benchmark für Ihre eigene IT-Risikominderungsstrategie zu nutzen. Zusätzlich zu den Ergebnissen der Umfrage schlagen wir neun Schritte vor, um einen erfolgreichen Pfad zu finden, wie Unternehmen Cyberresilienz erreichen können.

In der Sendung The Progress Report, diskutierte ich die Ergebnisse auch mit Ricardo Morales, CISO von Banorte, einer der größten mexikanischen Geschäftsbanken.

Herkunft der Daten

Wir haben ein externes Forschungsunternehmen beauftragt, eine Online-Umfrage unter 300 IT-Entscheidern aus Großunternehmen (mehr als 1.000 Beschäftigte) durchzuführen. Die Antworten wurden in der Zeitspanne von März bis April 2023 erfasst.

Respondent locations:

→ 65% Nordamerika
→ 19% im Vereinigten Königreich
→ 16% in Indien

Branchenspezifische Aufgliederung:

→ 18% Finanzwesen
→ 17% Regierung
→ 17% Fertigung
→ 14% Telekommunikation
→ 14% Medien
→ 20% sonstige Branchen

Über den Autor

Kris Lovejoy ist Kyndryl's Global Practice Leader für Sicherheit und Resilienz.

Unternehmen verlassen sich beim Betrieb kritischer Geschäftsprozesse auf die IT.

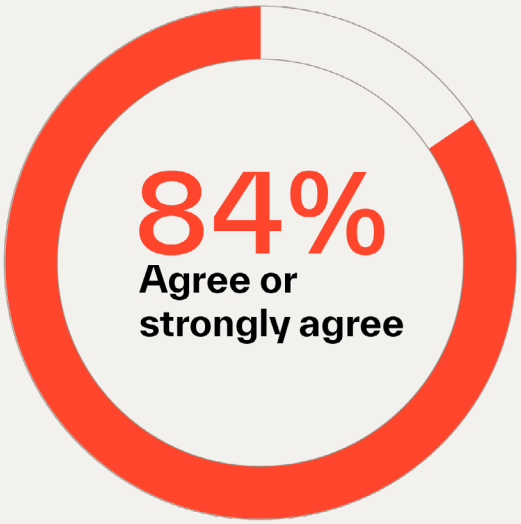
Um die Diskussion über die IT-Risiken zu verankern, haben wir die Befragten gebeten, anzugeben, in welchem Umfang sie in ihrem Tagesgeschäft von der IT abhängig sind.

84 % stimmten zu bzw. stimmten nachdrücklich zu, dass ihr Unternehmen in hohem Maße auf IT-Ressourcen angewiesen ist, um kritische Geschäftsprozesse durchführen zu können.

Angesichts der Tatsache, dass die digitale Transformation allgegenwärtig ist und täglich kommentiert wird, überrascht das Ergebnis nicht.

Erstaunlicher ist nur, dass die Antworten nicht noch emphatischer ausfielen.

F: Wie sehr stimmen Sie zu oder nicht zu: "Mein Unternehmen ist in hohem Maße auf IT-Ressourcen angewiesen, um kritische Geschäftsprozesse zu betreiben."



Die meisten Unternehmen erlebten Störungen ihrer IT-Systeme.

Wir haben nicht nur die Kritikalität der IT-Systeme bestätigt. Wir haben auch festgestellt, dass Störungen zum Alltag gehören. 92 % der Befragten gaben an, dass in ihrem Unternehmen in den letzten zwei Jahren ein unerwünschtes Ereignis aufgetreten ist, das die IT-Systeme beeinträchtigt oder gestört hat. Wer also ein Unternehmen betreibt, geht ein IT-Risiko ein.

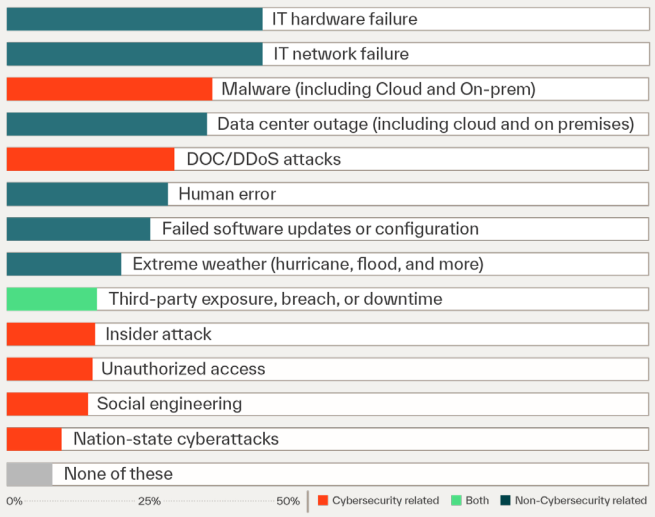
Die meisten Befragten gaben an, drei oder vier verschiedene Arten von Störungen erlebt zu haben. Obwohl Cyberangriffe in der Regel die Schlagzeilen beherrschen, zeigen die Ergebnisse, dass bei der Diskussion und Behandlung von IT-Risiken eine viel breitere Perspektive erforderlich ist.

Während 71 % der Befragten angaben, ein Ereignis im Zusammenhang mit der Cybersicherheit erlebt zu haben, gaben 88 % an, ein unerwünschtes Ereignis erlebt zu haben, das nicht mit der Cybersicherheit zusammenhing. (Diese Gruppierungen entsprechen nicht entweder/oder.) Drei der fünf häufigsten unerwünschten Ereignisse standen nicht im Zusammenhang mit der Cybersicherheit:

- → IT-Hardwarefehler
- → IT-Netzausfall
- → Ausfall des Rechenzentrums

Menschliches Versagen ist nach wie vor eine der Hauptursachen für Störungen. Es steht an sechster Stelle der 13 spezifischen Störungen, nach denen wir gefragt haben, und gehört bei den Befragten aus dem Finanzdienstleistungssektor konstant zu den drei am häufigsten genannten Störungen.

F: Wurden Ihre IT-Systeme/Daten in den letzten 24 Monaten durch eines der folgenden unerwünschten Ereignisse beeinträchtigt oder gestört?



Störungen in den IT-Systemen führen zu Schäden an der Marke, zu Bußgeldern und vielem mehr.

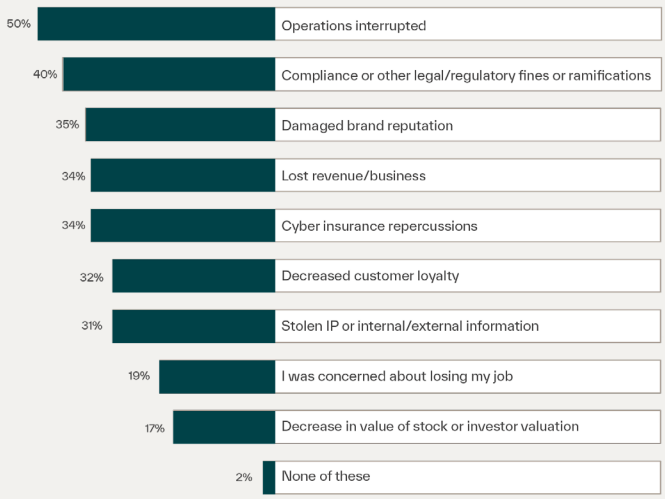
Ausgehend von der Bedeutung der IT für Routineabläufe, nannten die Befragten Betriebsunterbrechungen als häufigste Auswirkung, die sie als Folge von negativen IT-Ereignissen erlebt haben.

Als zweithäufigste Auswirkung wurden Bußgelder oder andere gesetzliche oder regulatorische Einhaltung von Vorschriften genannt. Dies trifft insbesondere für Befragte aus den Bereichen Finanzwesen, Behörden und Medien zu.

Betriebsunterbrechungen und Probleme mit der gesetzlichen oder regulatorischen Einhaltung von Vorschriften traten nicht nur am häufigsten auf. Sie wurden von den Befragten auch als die beiden Kategorien eingestuft, die am meisten Anlass zur Sorge bereiten, wenn IT-Ressourcen in Zukunft nicht mehr zur Verfügung stehen oder gefährdet sind. Denial-of-Service-Störungen und Datenlecks können beispielsweise zu hohen Geldstrafen führen.

35 % der Befragten gaben an, dass der Ruf der Marke ihres Unternehmens durch IT-Störungen geschädigt wurde. Für die Befragten aus den Bereichen der Medien, von denen 63 % eine solchen Auswirkung feststellen, trifft dieses Ergebnis in besonderem Maße zu. Jedes negative Ereignis ist heute durch den ständigen Nachrichtenfluss und die Aktivität der Kunden in den sozialen Medien sichtbarer als je zuvor.

F: Welche der folgenden Auswirkungen hatten unerwünschte Ereignisse [in den letzten 24 Monaten] für Ihr Unternehmen?



Was macht es IT-Entscheidungsträgern schwer, IT-Risiken rechtzeitig zu erkennen?

Wir hatten damit gerechnet, dass der weltweite Mangel an IT-Fachkräften eine wichtige Rolle unter den beeinträchtigenden Faktoren spielen würde, aber er stand nicht ganz oben auf der Liste. Die fehlende Möglichkeit, Systeme und Daten aus einem verschlüsselten, bereinigten Backup wiederherzustellen, wurde von den Befragten am häufigsten als größte Herausforderung bei der Bewältigung der Auswirkungen von Zwischenfällen genannt. Das stellen wir auch immer wieder fest, wenn Unternehmen uns nach unseren Services fragen. Wir ermutigen sie wie folgt:

- → Investieren Sie in die Automatisierung und Orchestrierung von Wiederherstellungsprozessen
- → Ermitteln und bewerten Sie, wie menschliches Versagen bei der Wiederherstellung von Backups am besten reduziert werden kann
- → Testen Sie die Behebung von Störungen wiederholt und häufig

Als die drei größten Herausforderungen bei der Risikominderung nannten die Befragten die ständig wachsende IT-Landschaft und die Unfähigkeit, mit neuen Bedrohungen Schritt zu halten. Der Mangel an IT-Fachkräften steht an vierter Stelle.

F: Was sind die drei größten Herausforderungen, denen Sie sich bei der Bewältigung der Auswirkungen von unerwünschten Ereignissen stellen müssen?

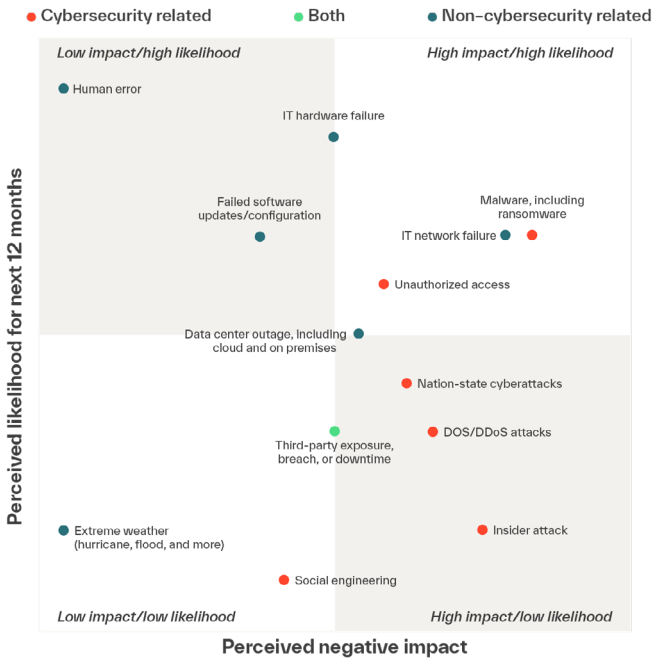
Mit Blick auf die nächsten 12 Monate werden Malware-Ereignisse als das höchste IT-Risiko in Bezug auf die Wahrscheinlichkeit und die negativsten Auswirkungen eingeschätzt.

Wir baten die Befragten, uns die unerwünschten Ereignisse zu nennen, mit denen sie in den nächsten 12 Monaten am meisten rechnen. Außerdem sollten sie angeben, wie stark sich diese Ereignisse auf ihr Unternehmen auswirken würden, falls sie eintreten sollten.

Menschliches Versagen wurde als das wahrscheinlichste Ereignis erachtet. Die erwarteten Auswirkungen wurden jedoch geringer eingeschätzt als bei den meisten anderen Ereignissen. Malware hingegen wurde als das am meisten erwartete und bedrohlichste IT-Risiko eingestuft.

Da Malware, insbesondere von Ransomware, zunimmt, ist das Ergebnis nicht überraschend. Angesichts der oben genannten Herausforderungen bei der Wiederherstellung von Daten aus verschlüsselten, bereinigten Backups, ist auch dies ein Grund für erhöhte Aufmerksamkeit. Unabhängig davon, ob Ihr Unternehmen mit Backup-Problemen zu kämpfen hat oder nicht, kommt erschwerend hinzu, dass Ransomware-Angreifer zunehmend auf Backups abzielen. Nicht nur, dass Unternehmen in solchen Fällen - wenn Backups kompromittiert wurden - ihre Systeme nicht wiederherstellen können. Sie können sie auch nicht auf Malware überprüfen. Dadurch steigen das Risiko und die potenziellen Auswirkungen drastisch.

Ein weiteres, mit Spannung erwartetes und potenziell folgenschweres Risiko ist der unbefugte Zugang, der ebenfalls erhebliche negative Auswirkungen haben kann. Zero-Trust-Prinzipien werden eine immer wichtigere Rolle spielen, um unbefugten Zugriff zu kontrollieren. Diese Prinzipien empfehlen, dass Unternehmen ihre wertvollsten Assets identifizieren, den privilegierten Zugriff festlegen und Technologien wie die Multi-Faktor-Authentifizierung zur Validierung einsetzen.

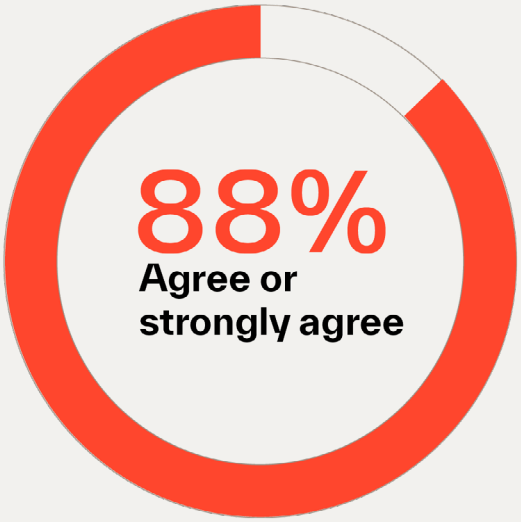


Trotz der von Ihnen wahrgenommenen Risiken bleiben die IT-Entscheidungsträger zuversichtlich..

An früherer Stelle in diesem Bericht haben wir erwähnt, dass uns die Zuversicht der IT-Entscheidungsträger angesichts der globalen Ereignisse und der bekannten Herausforderungen überrascht. Insgesamt sind 88 % der Befragten der Ansicht, dass ihr Unternehmen gut auf die Bewältigung und Wiederherstellung von widrigen Umständen, Angriffen oder Kompromittierungen vorbereitet ist, die sich auf die IT-Ressourcen ihres Unternehmens auswirken können.

Im Vergleich zu anderen Unternehmen bewerten 65 % der Befragten die Vorkehrungen ihres Unternehmens zur Bewältigung unerwünschter Ereignisse als besser als die anderer Unternehmen. Nur 8 % der Befragten sind der Ansicht, dass ihr Unternehmen in dieser Kategorie zumindest etwas schlechter abschneidet als andere Unternehmen.
Das hohe Maß an Vertrauen ist umso bemerkenswerter, da 92 % der Befragten angaben, dass es in ihrem Unternehmen zu unerwünschten Ereignissen gekommen ist. Dieser Widerspruch ist zumindest erstaunlich, wenn nicht sogar Anlass zu der Frage, ob ein solches Vertrauen gerechtfertigt ist.

F: Wie sehr stimmen Sie zu oder nicht zu: Meine Organisation ist gut darauf vorbereitet, mit widrigen Umständen, Angriffen oder Kompromittierungen, die die IT-Ressourcen meiner Organisation beeinträchtigen, umzugehen und sich davon zu erholen.



9 Schritte für IT-Führungskräfte, um einen Pfad zur Cyberresilienz zu erstellen

Wir haben diese Studie durchgeführt, um herauszufinden, wie IT-Entscheidungsträger den aktuellen Stand der IT-Risiken einschätzen. Darüber hinaus haben wir untersucht, welche Maßnahmen ihre Unternehmen ergreifen, um diese Risiken zu mindern, und zwar im Hinblick auf die vier Säulen der Cyberresilienz.

- **Antizipieren:** Maßnahmen zur Bewertung und zum Verständnis der IT-Risikosituation, um möglichen Bedrohungen besser begegnen und eventuelle Vorschriften besser einhalten zu können.
- **Schützen:** Maßnahmen zur Verstärkung des Schutzes von IT-Ressourcen, um sicherzustellen, dass sie vor negativen Ereignissen geschützt bleiben.
- **Standhalten:** Maßnahmen zur Bewältigung von Störungen und zur Verringerung ihrer Auswirkungen.
- **Wiederherstellen:** Maßnahmen zur Schadensbegrenzung nach einer jeglichen Störung und zur schnellen Wiederherstellung kritischer IT-Umgebungen.

Die Befragten bewerteten die Leistungen ihrer Unternehmen durchweg als gut, was sich in den hohen Vertrauensbewertungen widerspiegelt. Im Durchschnitt bewerteten 75 % der Befragten die Leistungen ihrer Unternehmen als sehr gut bis ausgezeichnet, und zwar über alle Aktivitäten hinweg. Eine Nuance, die uns auffiel, war, dass die Befragten, die von einer starken Unterstützung der Sicherheitsinvestitionen durch die Geschäftsleitung berichteten, sich selbst tendenziell die besten Noten für Aktivitäten im Bereich der Cyberresilienz gaben.

Um Ihnen dabei zu helfen, diese Zustimmung zu erhalten, schlagen wir Ihnen neun grundlegende Schritte vor, die Ihnen einen Pfad aufzeigen, wie Sie Cyberresilienz erreichen können.

1 **Das Unternehmen von Anfang an einbeziehen.**

Die IT-Abteilungen arbeiten zu oft in Silos, also getrennt von den anderen Bereichen des Unternehmens. Der sicherste Pfad für den Erfolg einer Cyberresilienzstrategie ist die Abschaffung von Silos. Laden Sie Beschäftigte außerhalb des IT-Bereichs zu Diskussionen ein und verankern Sie die Diskussionen über Cyberresilienz in Ihrem Unternehmensleitbild. Machen Sie die Einbeziehung zu einem Teil der Unternehmenskultur.

2 **Risikotoleranz anpassen.**

Der Grad der Risikotoleranz wird oft von der Branche diktiert. Das Toleranzniveau eines stark regulierten Finanzinstituts sollte beispielsweise sehr niedrig sein. Definieen Sie auf jeden Fall die Risikotoleranz, die Ihr Unternehmen anwenden sollte, und kommunizieren Sie ihre Definition mit Ihren Teams.

3 **Ihr minimal lebensfähiges Unternehmen ermitteln.**

Ein minimal lebensfähiges Unternehmen besteht aus den Teilen der Organisation, die für die Aufrechterhaltung des Betriebs und das Erreichen der Geschäftsziele entscheidend sind. Ihre Cyberresilienz-strategie sollte nicht nur die kritischen Teile identifizieren, sondern auch die Toleranzgrenzen für die Geschwindigkeit, mit der die diesen Systemen zugrunde liegenden Daten wieder online sein müssen.

4 **Bestandsaufnahme machen.**

Wie die Umfrageergebnisse zeigen, stehen viele Unternehmen vor der Herausforderung, dass ihre IT-Landschaft immer weiter wächst. Identifizieren und kartographieren Sie die IT-Ressourcen, die für Ihr Unternehmen von entscheidender Bedeutung sind. Diese Assets sind vorrangig zu schützen. Im schlimmsten Fall müssen sie nach einem unerwünschten Ereignis wiederhergestellt werden.

5 **Umstellung auf ein Zero-Trust-System.**

Wir empfehlen den Deny-by-Default-Standard (Verweigerung durch Voreinstellung), um sicherzustellen, dass nur diejenigen, die Zugriff auf die Systeme benötigen, diesen auch erhalten, während diejenigen, die ihn nicht benötigen, ihn nicht erhalten.

6 **Einen Krisenmanagementplan erstellen.**

Manchmal sind unerwünschte Ereignisse unvermeidbar. (Menschliches Versagen ist die am häufigsten erwartete Ursache für Störungen.) Durch die Festlegung von Rollen und Verantwortlichkeiten in den einzelnen Teams, die Einführung eines Kommunikationsprozesses, die Dokumentation von Abläufen und die Verbesserung der Transparenz, können die Auswirkungen von unerwünschten Ereignissen oft verringert werden.

7 **Eine Störung praktizieren.**

Allzu oft werden Pläne geschmiedet, dann aber auf Eis gelegt und nur in den seltensten Fällen in die Tat umgesetzt. Wenn ein unerwünschtes Ereignis eintritt, führt ein nicht getesteter Plan zu Unklarheit bzw. langsamen Reaktionszeiten und die Auswirkungen werden noch schwerwiegender.

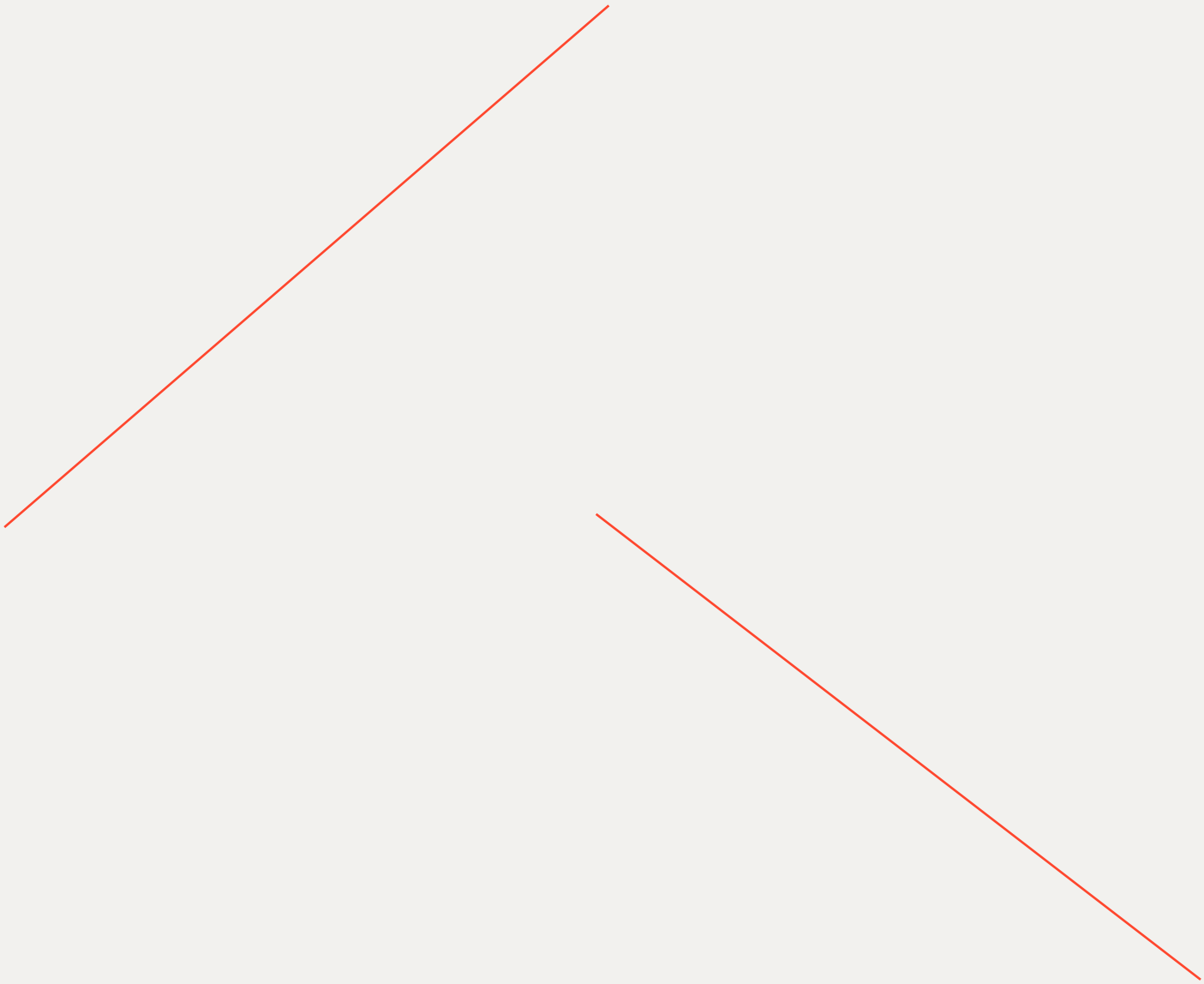
8 **Kontinuierlich Ihre Cyberresilienz-Strategie modernisieren.**

Unternehmen sind lebhafte Einheiten. Geschäftsziele ändern sich und IT-Assets werden komplexer. Externe Faktoren (z. B. Vorschriften) können Änderungen erforderlich machen. Diese Schritte müssen Teil einer kontinuierlichen Diskussion sein, um sicherzustellen, dass Ihre Cyberresilienzstrategie auch wirksam ist.

9 **Die Vorstandsebene sensibilisieren.**

Wir schließen den Bericht über die Umfrage dort, wo wir sie begonnen haben: mit der Feststellung, dass Cyberresilienz nun weltweit auf der Tagesordnung von Vorständen steht.

Wenn der Vorstand über IT-Risiken und Pläne zur Risikominderung informiert wird, kann dies dazu beitragen, die unternehmerische Top-Down-Ausrichtung zu fördern. Zudem verschafft es den nötigen Spielraum für Änderungen, die notwendig sind, um sicherzustellen, dass cybergestützte Systeme auch bei ungünstigen Ereignissen betriebsbereit bleiben.



kyndryl