ECONOMIST IMPACT

Risiko-Reset: Verlagerung des Schwerpunkts von Reaktion auf Antizipation

Gefördert durch

IRON MOUNTAIN®

Inhalt

Über diese Forschung und Danksagungen

Risiko-Reset: Verlagerung des Schwerpunkts von Reaktion auf Antizipation ist ein von Economist Impact durchgeführtes und von Iron Mountain in Auftrag gegebenes Forschungsprogramm, das die wichtigsten internen und externen Faktoren untersucht, die den Umgang eines Unternehmens mit Risiken prägen, sowie die Rolle, die Führungskräfte, Technologie und das institutionelle Umfeld beim Risikomanagement spielen. Economist Impact nutzte Daten aus Interviews mit Expert*innen und einer speziell durchgeführten Befragung von 656 Führungskräften aus Schlüsselindustrien in Australien, Brasilien, Kanada, Frankreich, Deutschland, Hongkong, Indien, Mexiko, Neuseeland, Singapur, dem Vereinigten Königreich und den USA.

Wir möchten uns bei den folgenden Expert*innen für ihre Zeit und Erkenntnisse bedanken:

- Simeon Fishman, Executive Vice President und CRO bei The Clearing House
- Sophie Heading, Global Risks Lead beim Weltwirtschaftsforum
- Dr. Witold J. Henisz, Vice Dean und Faculty Director der Initiative für Umwelt, Soziales und Governance der Wharton School

Das Briefing Paper wurde von einem Team von Forscher*innen, Redakteur*innen und Designer*innen von Economist Impact erstellt. Beteiligt waren unter anderem:

- Monica Ballesteros – Project Director
- Durukhshan Esmati – Project Manager
- Kathleen Harrington – Analyst
- Alasdair Ross – Writer
- Amanda Simms – Editor
- EMC Design Ltd – Designer

Economist Impact trägt die alleinige Verantwortung für den Inhalt dieses Berichts. Die hierin geäußerten Erkenntnisse und Ansichten spiegeln nicht unbedingt die Ansichten unseres Auftraggebers, unserer Partner*innen oder der interviewten Expert*innen wider.

Vorwort von Iron Mountain

In den vergangenen drei Jahren haben viele Unternehmen als Reaktion auf neu auftretende Bedrohungen und globale Umwälzungen erhebliche Umstrukturierungen vorgenommen. Diese Entwicklung erfordert von uns allen, widerstandsfähiger zu werden und von reaktiven Maßnahmen zu proaktiver Antizipation überzugehen. Indem sie sich gegen potenzielle künftige Bedrohungen wappnen, anstatt nur auf bekannte Bedrohungen zu reagieren, sind Unternehmen in der Lage, sich auf unvorhergesehene Risiken einzustellen und sich bietende Chancen zu nutzen.

Seit über 70 Jahren unterstützt Iron Mountain Kunden auf der ganzen Welt dabei, Risiken für ihre Marke, ihren Ruf und ihre Finanzlage zu mindern und ihre Fähigkeit, Kunden, Patienten oder Bürger effektiv zu bedienen, zu verbessern. Vor diesem Hintergrund freuen wir uns, die jüngste Studie von Economist Impact sponsern zu können, die sich mit der veränderten Wahrnehmung des Risikomanagements in Unternehmen befasst.

Wie Sie in diesem Bericht erfahren werden, legen mehr als 90 % der Unternehmen aufgrund der jüngsten globalen und wirtschaftlichen Störungen mehr Wert auf das Risikomanagement. Im Hinblick auf neu auftretende Risiken hebt der Bericht die anhaltenden Bedenken hinsichtlich der Cybersicherheit hervor. Ein weiterer Faktor ist die Verbreitung neuer Technologien, beispielsweise durch generative künstliche Intelligenz, die neue Risiken schafft und gleichzeitig die Fähigkeit von Risikomanagern erweitert, diese Bedrohungen zu erkennen. Während der Schutz physischer Vermögenswerte für unser Unternehmen nach wie vor von entscheidender Bedeutung ist, sind wir uns bewusst, dass jeder heute anfälliger für Cyber-Bedrohungen ist, und haben uns dem Markt angepasst, um Kundendaten im digitalen Raum zu schützen.

Die Ergebnisse des Berichts zeigen ebenfalls, dass die Führungskräfte Umweltrisiken mehr Aufmerksamkeit schenken als in den vergangenen Jahren. Was die Nachhaltigkeit betrifft, so konzentriert sich unser Weg zu „Netto-Null“ auf die Verringerung des Energieverbrauchs, die Elektrifizierung unserer Systeme und Fahrzeuge, die Installation von Systemen für erneuerbare Energien und die Beschaffung von Ökostrom, um das Risiko steigender Preise für fossile Brennstoffe und lokaler Emissionsvorschriften zu verringern. Indem wir unsere eigenen Ziele in den Bereichen Umwelt, Soziales und Unternehmensführung verfolgen und unsere Kunden bei der Verwirklichung ihrer Ziele unterstützen, mindern wir nicht nur die Risiken, die mit der Entwicklung von Vorschriften, dem Klimawandel und sozialer Ungleichheit verbunden sind, sondern erschließen auch neue Chancen.

Die Ergebnisse der Befragung, die zeigen, dass Führungskräfte proaktiver mit Risiken umgehen und ihre Widerstandsfähigkeit verbessern, stimmen uns zuversichtlich. Dies selbst ist der Kern unseres Auftrags. Die datengestützten Erkenntnisse in diesem Bericht geben uns Aufschluss darüber, wie wir uns und unsere Kunden besser auf die Zukunft vorbereiten können.

Larry Jarvis
SVP und Chief Information Security Officer
bei Iron Mountain

Zusammenfassung

Das Risikomanagement wird immer mehr Teil der Unternehmensstruktur und ist auf höheren Unternehmensebenen präsent. Risikomanager*innen sammeln Daten über potenzielle Bedrohungen und koordinieren die Reaktion ihres Unternehmens darauf. Da sich diese Bedrohungen jedoch immer schneller entwickeln, ist es von entscheidender Bedeutung, die Risiken zu antizipieren, die noch nicht auf dem Radar des Unternehmens sind, anstatt einfach auf Ereignisse zu reagieren, wenn sie eintreten.

Economist Impact hat mit Unterstützung von Iron Mountain eine Primärstudie durchgeführt, um herauszufinden, wie Führungskräfte die wichtigsten internen und externen Faktoren wahrnehmen, die das Risikomanagement eines Unternehmens beeinflussen, und welche Rolle Führungskräfte, Technologie und die institutionelle Struktur beim Risikomanagement spielen. Economist Impact nutzte Daten aus Interviews mit Expert*innen und einer speziell durchgeführten Befragung von 656 Führungskräften aus Schlüsselindustrien (Finanzdienstleistungen, Gesundheitswesen und Biowissenschaften, Energie und der öffentliche Sektor) in Australien, Brasilien, Kanada, Frankreich, Deutschland, Hongkong, Indien, Mexiko, Neuseeland, Singapur, dem Vereinigten Königreich und den USA.

Risikomanager*innen setzen immer mehr auf ein tieferes Verständnis dafür, wie sich Risiken kaskadenartig auf das Unternehmen auswirken – zum Beispiel, wie sich ein Ausfall oder eine Sicherheitsverletzung bei einem wichtigen Lieferanten auf Betrieb, Umsatz und Ruf des Unternehmens auswirken könnte. Das Bewusstsein für Eventualrisiken nimmt zu, doch es gibt noch Raum für Verbesserungen.

Ein ganzheitliches und vorausschauendes Risikomanagement, das auf neu auftretende Bedrohungen reagiert, muss von der Unternehmensführung durchgesetzt werden, mit einer systematisch koordinierten Risikoreaktion, die von allen Mitarbeiter*innen angenommen und getragen wird. Auch im Unternehmensumfeld – bei Partner*innen, Lieferant*innen und Vertriebshändler*innen – sollte dieses Risikobewusstsein verinnerlicht werden.

Neue digitale Technologien, wie maschinelles Lernen und künstliche Intelligenz (KI), versprechen eine Erweiterung des Instrumentariums der Risikomanager*innen und das Erkennen von Mustern in Daten, die menschlichen Analyst*innen möglicherweise entgehen. Allerdings haben auch Angreifer*innen Zugang zu diesen Technologien und können sie dazu nutzen, Schwachstellen zu finden oder noch effektivere Phishing-Angriffe durchzuführen. Diese aufkommenden Technologien müssen sorgfältig überwacht werden, während sich ihre wahren Auswirkungen immer deutlicher herauskristallisieren.

In diesem Paper betrachten wir vier Bereiche, in denen sich die Risikomanagementlandschaft durch neue Praktiken verändert:

Entwicklung des Arbeitsplatzes: Das Personal eines Unternehmens ist sowohl sein größtes Kapital als auch seine größte Schwachstelle. Dies spiegelt sich in den Anstrengungen und Ressourcen wider, die Unternehmen für die Einstellung, Bindung und Schulung von Mitarbeiter*innen aufwenden. Durch die Digitalisierung sind die Mitarbeiter*innen enger mit den kritischen Prozessen verbunden, was das Risiko und die Geschwindigkeit, mit der es sich manifestiert, erhöht. Inzwischen hat die Verlagerung hin zu Fernarbeitsmodellen die digitalen Unternehmensgrenzen durchlässiger gemacht. Auch die Gewinnung und Bindung von Mitarbeiter*innen wird immer schwieriger, da junge Generationen eine werteorientierte Einstellung zur Arbeit haben. Aus unserer Befragung geht hervor, dass Risikomanager*innen mit diesen aufkommenden Trends Schritt halten. 96 % der Befragten gaben an, dass ihr Unternehmen neue Richtlinien und Verfahren für das Personalmanagement entwickelt hat, die beispielsweise auch hybride Arbeitsmodelle umfassen.

Cybersicherheit und Data Governance: Die digitale Datenverarbeitung hat nicht nur eine neue Welle von Produktivitätssteigerungen ermöglicht, sondern auch neue Risikoquellen geschaffen. Informationen fließen schneller und umfassender als je zuvor und vor allem schneller als der Mensch reagieren kann. Da die Risiken durch das Aufkommen großer, dezentraler und multinationaler Unternehmen weiter zunehmen, ist der Schutz der digitalen Präsenz eines Unternehmens vor versehentlichem oder böswilligem Schaden zu einer Überlebensfrage geworden. Die Einführung offener generativer KI-Modelle hat ein seit langem erwartetes Risiko plötzlich präsent werden lassen und in das Bewusstsein der Vorstandsetage gebracht, wobei die Auswirkungen dieser aufkommenden Technologie noch immer schwer abzusehen sind. Manager*innen können am besten auf dieses sich verändernde Umfeld reagieren, indem sie sich intensiv auf drei große Datenrisikobereiche konzentrieren: Governance, Sicherheit und Datenschutz.

Nachhaltigkeit: Der Klimawandel bedroht unsere Zukunft und seine Auswirkungen sind bereits spürbar. Extreme Wetterereignisse nehmen an Intensität und Häufigkeit zu, während die biologische Vielfalt zunehmend gefährdet ist. Dies führt auch zu katastrophalen Auswirkungen auf den Handel und die Infrastruktur. Daher konzentrieren sich Unternehmen heute auf die Aufrechterhaltung vielfältiger und flexibler Lieferketten. Während die Widerstandsfähigkeit für Unternehmen ein zentraler Aspekt ist, werden sie auch von den Stakeholder*innen unter Druck gesetzt, zur Lösung der zugrundeliegenden Probleme beizutragen: Erschöpfung der Ressourcen, Umweltzerstörung und schädliche

Emissionen. Werden diese Bereiche ignoriert, können schwerwiegende Konsequenzen die Folge sein. Dies wird von der überwiegenden Mehrheit der Teilnehmer*innen an unserer Befragung anerkannt, wobei 80 % die Bedeutung von Kennzahlen für das Reputationsrisiko hervorheben.

Operative Effizienz: Während die Unternehmen mit immer neuen Risiken konfrontiert sind, die jenseits ihrer Grenzen entstehen, müssen sich die Risikomanager*innen weiterhin auf unmittelbarere Bedrohungen konzentrieren, unabhängig davon, ob die Quelle Menschen, Prozesse oder gesetzliche Anforderungen sind. Unternehmen sind in die Falle getappt, die Risikofunktion als eine Kostenstelle zu betrachten, die die Umsatzgenerierung bremst. Risikomanager*innen sind immer besser in der Lage, dem Management Kennzahlen zur Verfügung zu stellen, die ein Gleichgewicht zwischen den Kosten für die Aufrechterhaltung solider Risikopraktiken und den potenziellen Verlusten durch Sicherheitsvorfälle herstellen. Wie sich das operative Risiko manifestiert, ist von Unternehmen zu Unternehmen und von Branche zu Branche sehr unterschiedlich. Unsere Befragung zeigt jedoch, dass Risikomanager*innen unabhängig von ihrem Hintergrund die Bedeutung von Investitionen in diesem Bereich erkennen.

Obwohl sich das Risikomanagement im Einklang mit der sich verändernden Bedrohungslandschaft weiterentwickelt, steht es weiterhin vor großen Herausforderungen. Dazu gehören:

Messung: Die Kosten für die Einführung eines Risikomanagementsystems sind klar, doch sein Nutzen lässt sich nicht so einfach messen. Ein Teil der Aufgabe dieser Funktion besteht darin, dafür zu sorgen, dass potenzielle Bedrohungen nicht eintreten, doch die Bewertung der Kosten von etwas, das nicht eingetreten ist, gestaltet sich problematisch. Und während die Investition unmittelbar erfolgt, kann der Nutzen über Jahre hinweg anfallen, was die Messung zusätzlich erschwert. Der Schlüssel liegt in der Entwicklung von Kennzahlen, die Risiken mit messbaren Unternehmenszielen verknüpfen.

Ressourcen: Unternehmen neigen dazu, die Risikofunktion so zu finanzieren, dass sie die Bedrohungslandschaft der Vergangenheit widerspiegelt, anstatt sie für die Zukunft zu rüsten. In einer Zeit, in der neue Risiken aufkommen und alte sich weiterentwickeln, führt dies dazu, dass das Risikomanagement unterfinanziert, unterbesetzt und möglicherweise auch unterqualifiziert ist.

Koordinierung: Eine vorausschauende, effiziente und widerstandsfähige Risikofunktion erfordert ein einzigartiges Bewusstsein und eine Koordinierung in der gesamten Unternehmensstruktur, nicht nur in den traditionellen, isolierten Funktionen. Sie erfordert sowohl eine Top-down-Führung als auch eine Bottom-up-Zusammenarbeit und -Ausführung und sollte über die Unternehmensgrenzen hinausgehen, um Partner*innen, Lieferant*innen und andere Stakeholder*innen einzubeziehen.

Einführung

Die Geschäftstätigkeit von Unternehmen kennt keine Gewissheiten. Die Möglichkeit, dass in jedem Unternehmen und an jedem Punkt seiner Wertschöpfungskette ein Problem auftritt, ist allgegenwärtig. Von einem Abschwung auf wichtigen Märkten über die Unterbrechung kritischer Lieferungen bis hin zu den schädlichen Handlungen eines/einer verärgerten Mitarbeiters/Mitarbeiterin – Risiken, die sich nur schwer vorhersehen oder vermeiden lassen, belasten die Ergebnisse und Ziele eines Unternehmens. Der Schaden kann von geringfügigen Widrigkeiten bis zu Konkursen und Gefängnisstrafen in extremen Fällen reichen.

Die Abwehr dieser Bedrohungen ist eine anspruchsvolle und schnelllebige Aufgabe. Erschwerend kommt hinzu, dass sich Risiken im Laufe der Zeit in Intensität, Art und Umfang verändern. Während und unmittelbar nach dem Finanzcrash von 2008–2009 war das Risiko, keine Kredite zu erhalten, eine der Hauptsorgen. Während der COVID-19-Pandemie lag der Schwerpunkt auf der Aufrechterhaltung des Geschäftsbetriebs, da Unternehmen aufgrund von Einschränkungen gezwungen waren, ihre Standorte zu schließen. Als russische Panzer 2022 in die Ukraine einrückten, trieben die Beschränkungen der weltweiten Lebensmittel- und Kraftstofflieferungen die Preise in die Höhe und störten die Lieferketten.

Das Aufkommen immer fortschrittlicherer und leichter zugänglicher Technologien in Verbindung mit der zunehmenden Verbreitung und Verankerung der Fernarbeit hat eine völlig neue Risikoebene geschaffen. Die geografischen Grenzen von Unternehmen haben sich von speziell eingerichteten und zentralisierten Büros auf Dachböden, Arbeitszimmer und Gartenzimmer von Privathäusern erweitert, die oft viele Kilometer vom Hauptsitz entfernt und nicht selten sogar in einem anderen Land liegen. Die Sicherung von Prozessen und geschützten Daten in einer solchen dezentralen Umgebung ist eine doppelte Herausforderung, da jede*r Mitarbeiter* ein*e potenzielle*r Angreifer*in oder Saboteur*in ist.

Economist Impact hat mit Unterstützung von Iron Mountain eine Primärstudie durchgeführt, um herauszufinden, wie Führungskräfte die wichtigsten internen und externen Faktoren wahrnehmen, die das Risikomanagement eines Unternehmens beeinflussen, und welche Rolle Führungskräfte, Technologie und die institutionelle Struktur beim Risikomanagement spielen. Economist Impact nutzte Daten aus Interviews mit Expert*innen und einer speziell durchgeführten Befragung von 656 Führungskräften aus Schlüsselindustrien in Australien, Brasilien, Kanada, Frankreich, Deutschland, Hongkong, Indien, Mexiko, Neuseeland, Singapur, dem Vereinigten Königreich und den USA.

Risikomanagement – Trends und Wahrnehmung

Das Risikomanagement hat sich als Disziplin weiterentwickelt, um den aufkommenden Bedrohungen zu begegnen. Es wurde allmählich tiefer und höher in die Unternehmensstruktur integriert und hat mehr (wenn auch angeblich nie genug) Mitarbeiter*innen und Ressourcen auf höheren Ebenen einbezogen. Die Verantwortung für Risiken liegt häufig auf Vorstandsebene, wobei die Chief Risk Officers (CROs) direkt dem CFO oder CEO unterstellt sind. Gleichzeitig werden Risikomanager*innen weniger als Leiter*innen einer bestimmten Abteilung gesehen, sondern eher als Koordinator*innen von Aktivitäten, die über alle Unternehmensbereiche verteilt sind. Die Risikoverantwortung und die Zuständigkeit für die Berichterstattung liegen häufig bei den Abteilungsleiter*innen, wobei die Risikofunktion Leitlinien bereitstellt, Daten sammelt und der Geschäftsleitung Abhilfemaßnahmen empfiehlt.

Es war ein langer Weg vom Risiko als kaum beachtetem Nebenschauplatz bis zur heutigen unternehmensweiten Risikoarchitektur. Das Bewusstsein für das Risiko als existenzielles organisatorisches Problem entstand in der zweiten Hälfte des letzten Jahrhunderts, doch die ersten CROs wurden erst in den 1980er Jahren ernannt und erst Anfang dieses Jahrhunderts wurde diese Funktion weithin als Reaktion auf Risiken gewürdigt. Heute ist das Risikomanagement eine anerkannte Schlüsselkompetenz des Managements. Mehr als vier von fünf Unternehmen, die an unserer Befragung teilgenommen haben, geben an, dass sie in unternehmensweite Teams für das Risikomanagement investieren, die Teil ihres taktischen Ansatzes in diesem Bereich sind.

Unsere Untersuchungen deuten darauf hin, dass diese Entwicklung noch nicht abgeschlossen ist, auch wenn das Verständnis für diese Disziplin bei den leitenden Risikomanager*innen immer besser wird. Zum Beispiel verlagert sich die Aufmerksamkeit von der Reaktion auf Risiken, wenn sie entstehen, hin zu ihrer Antizipation und dem Aufbau von Widerstandsfähigkeit im Unternehmen, bevor ein Schaden entsteht. Für mehr als 90 % der Befragten hat seit 2020 die Risikoerkennung und für fast ebenso viele die prädiktive Risikomodellierung an Bedeutung gewonnen. Der Schwerpunkt auf der Antizipation erstreckt sich auch auf die Umgestaltung der Unternehmen zu diesem Zweck. 28 % gaben an, dass sie die Fähigkeit zur Erkennung und Antizipation von Bedrohungen verbessern möchten, während 41 % angaben, dass sie Risiken durch die Überwachung aufkommender Bedrohungen und die Ermittlung von Prozessanomalien antizipieren. Diese Verlagerung des Schwerpunkts ist kaum überraschend, wenn man bedenkt, dass die Manager*innen von Unternehmen in den letzten Jahrzehnten von einer Reihe von Schocks überrascht wurden.

Risiko-Reset: Verlagerung des Schwerpunkts von Reaktion auf Antizipation

Unternehmen müssen sich darüber hinaus mit der Verflechtung von Risiken beschäftigen. Eine ungünstige Entwicklung in einem Teil des Unternehmens oder der Welt kann sich auf unzählige Weisen auf den gesamten Betrieb auswirken. Wenn ein wichtiger Lieferant durch eine Naturkatastrophe ausfällt, kann dies zu Produktionsverzögerungen, erhöhten Kosten bei der Suche nach alternativen Bezugsquellen, Umsatzeinbußen durch verspätete oder nicht ausgeführte Aufträge und zu einer Schädigung der Marke und des Rufs des Unternehmens führen, wenn sich die Nachricht von der Störung verbreitet. Ausgehend von einem einzigen Drittrisiko wird das gesamte Unternehmen in das Krisenmanagement einbezogen. Die Antizipation dieser möglichen Bedrohungen ist ein Schlüsselelement des modernen Risikomanagements.

Auch hier machen die Unternehmen Fortschritte, doch es gibt noch Raum für Verbesserungen. Sophie Heading, Global Risks Lead beim Weltwirtschaftsforum, erklärt, dass „die Zusammenhänge zwischen den Risiken inzwischen besser verstanden werden, dieser Bereich jedoch noch immer in der Entwicklung ist. Mit ein wenig Fantasie kann man die Auswirkungen von Ereignissen auf der einen Seite der Welt nutzen, um ein potenzielles Risiko auf der anderen Seite zu antizipieren. Das Fehlen einer solchen Sichtweise kann ein Unternehmen anfällig für Risiken machen, die sich aus diesen Ereignissen ergeben."

Simeon Fishman, Executive Vice President und CRO bei The Clearing House, ist der Ansicht, dass man sich zunehmend auf neu entstehende Risiken konzentriert, d. h. Risiken, die weniger klar umrissen und offensichtlich sind. Er erklärt, dass „es für Unternehmen heute wichtiger ist, einen schärferen Blick über den Tellerrand hinauszuwerfen und zu versuchen, diese Risiken besser zu verstehen. Ein wichtiger Bereich entstehender Risiken ist die Rolle des Technologierisikos, die sich ständig weiterentwickelt. So bieten beispielsweise nur wenige Anbieter Cloud-Dienste an, was potenziell zu einer Konzentration der Clouds führen kann. Dies führt wiederum dazu, dass sich technikorientierte Unternehmen durch die Software, die sie verwenden oder entwickeln, unfreiwillig auf einen oder nur wenige Anbieter verlassen."

Die Manager*innen werden bei diesem Übergang vom reaktiven zum proaktiven Risikomanagement durch eine Reihe neuer digitaler Tools unterstützt, wie die Antworten auf unsere Befragung zeigen, in der 43 % der Führungskräfte angaben, kognitive Technologien und KI für das Risikomanagement zu nutzen. Veränderungen sind zwar das Handwerkszeug von Risikomanager*innen, aber das Tempo, das wir bei der künstlichen Intelligenz beobachten, bringt eigene Herausforderungen mit sich. Es liegt auf der Hand, dass maschinelles Lernen eine neue Möglichkeit bietet, Daten zu untersuchen, die in großen Unternehmen hinein- und hinausfließen, und menschliche Analyst*innen zu unterstützen, indem es Muster erkennt, die dem menschlichen Auge vielleicht verborgen bleiben. Es kann sich aber auch als Vektor für Cyberangriffe erweisen, da Hacker*innen und

Technologie kann nur begrenzte Vorteile bringen, wenn Sie innerhalb Ihrer Systeme nicht über das richtige Design, die richtige Risikoarchitektur oder die richtigen Daten verfügen. Es ist außerdem wichtig, zu verstehen, wie Prozesse und Daten miteinander verbunden sind. Sobald die Bereiche Daten und Design stehen, können Big Data, Analysen und Datenabfragetools genutzt werden, ein umfassenderes Verständnis der Risiken in einem Unternehmen zu entwickeln.

Simeon Fishman, Executive Vice President und Chief Risk Officer bei The Clearing House

Betrüger*innen diese Technologie nutzen, um ihre Programmierung zu optimieren. Es ist noch zu früh, um zu sagen, wie sich diese Technologie entwickeln wird und welche Auswirkungen sie auf das Risikomanagement haben wird.

Die Notwendigkeit, in einer Zeit des raschen technologischen Wandels Risiken und deren Auswirkungen im gesamten Unternehmen zu antizipieren, unterstreicht die Bedeutung eines ganzheitlichen Ansatzes für das Risikomanagement. Wenn man sich darauf verlässt, auf Bedrohungen zu reagieren, sobald sie eintreten, werden Unternehmen auf dem falschen Fuß erwischt und haben Mühe, diesen Situationen Herr zu werden. Die getrennte Betrachtung der einzelnen Tätigkeitsbereiche setzt Unternehmen ungewissen Risiken aus. Die Antwort liegt jedoch nicht einfach darin, auf innovative Technologien zu setzen. Wer sich blindlings auf Innovationen einlässt, setzt sich neuen und unvorhergesehenen Bedrohungen aus. Frau Heading gibt zu bedenken, dass „Technologie das Risikomanagement unterstützt. Es muss jedoch mit dem menschlichen Element verknüpft werden."

Der ganzheitliche Ansatz des Risikomanagements erfordert eine Führung von oben und eine Koordinierung nach unten und über die gesamte Unternehmensstruktur hinweg, damit alle verfügbaren Informationen denjenigen zur Kenntnis gebracht werden, die am besten in der Lage sind, sie zu interpretieren und entsprechend zu handeln. Dr. Witold J. Henisz, Vice Dean und Faculty Director der Environment, Social and Governance Initiative der Wharton School, stimmt dem zu und ergänzt, dass „es entscheidend ist, Daten verständlich, transparent und leicht nachvollziehbar zu machen, wenn man sie Menschen mit unterschiedlichen Datenkenntnissen und funktionalem Hintergrund vorlegt."

Wie die Bezeichnung „ganzheitlich" schon andeutet, wird das Risikomanagement zur Aufgabe des gesamten Unternehmens (und seiner Lieferant*innen, Partner*innen und Vertriebshändler*innen). Die Risikomanager*innen setzen das System um und koordinieren es, aber anders als Marketingdirektor*innen oder

Betriebsleiter*innen sind sie für diese Aufgabe nicht allein zuständig. Das Risikomanagement hat sich von einem wenig beachteten Eintrag im Organigramm zu einem integralen Bestandteil der Unternehmenskultur entwickelt, das auf einer Ebene mit der Marke, dem Leitbild oder dem Ansatz zur Entwicklung und Bindung von Humankapital steht. Dazu gehören unternehmensweite Verpflichtungen wie eine Erklärung zur Risikobereitschaft, ein immer häufigeres Merkmal moderner Unternehmen, in der die Höhe des akzeptablen Risikos und die allgemeine Risikobereitschaft festgelegt werden.

Im Mittelpunkt dieses Konzepts steht die Koordinierung zwischen den verschiedenen Abteilungen der Unternehmen, ihrer erweiterten Lieferkette und ihren wichtigsten Stakeholder*innen. Unsere Befragung zeigt, dass viele leitende Risikomanager*innen Verfechter*innen dieses Ansatzes in ihren Unternehmen sind. Von den Befragten stimmten 77 % zu, dass das Risikomanagement alle Teile des Unternehmens berücksichtigen muss, während 46 % angaben, in unternehmensweite Teams für das Risikomanagement zu investieren. Weitere 36 % gaben an, dass die Integration des Risikomanagements in die allgemeine Unternehmensstrategie und die Entscheidungsfindung eine Priorität darstellt.

Dies erfordert „strukturelle Veränderungen, die je nach Art und Größe eines Unternehmens variieren", so Fishman. „Die Kommunikation von der obersten Führungsebene und dem/der CEO bis hinunter zu allen Mitarbeiter*innen wird immer wichtiger, um sicherzustellen, dass das Risikomanagement Teil der DNA des gesamten Unternehmens ist und nicht nur eine abgegrenzte Funktion, die sich speziell mit dem Vorantreiben des Risikomanagements beschäftigt."

Die Führungskräfte sind jedoch noch immer auf der Suche nach dem Optimum. Siebenundfünfzig Prozent gaben an, dass ihr Unternehmen die funktionsübergreifende Zusammenarbeit verbessern muss. Nur 4 % der befragten Führungskräfte gaben an, über einen Ausschuss für das Risikomanagement zu verfügen, der direkt für das Risikomanagement verantwortlich ist, während 27 % angaben, dass ihr*e CEO/Präsident*in/Partner direkt dafür verantwortlich ist. Über 60 % der Befragten waren der Ansicht, dass ihr Unternehmen das Engagement der Mitarbeiter*innen und den Informationsaustausch zwischen Funktionen, Teams und externen Partner*innen verbessern muss.

Risikomanagement in den vier Säulen

Es liegt in der Natur der Sache, dass Risiko diffus ist. Selbst wenn seine Quellen klar sind (was selten vorkommt), ist der Weg, den das Risiko nimmt – wo es in ein Unternehmen eintritt und wie es sich darin bewegt – schwer vorherzusagen. In diesem Abschnitt werden wir vier verschiedene Erscheinungsformen des Unternehmensrisikos betrachten, ihre Auswirkungen nachverfolgen und untersuchen, wie Manager*innen mit ihnen umgehen. Die vier Säulen sind:

- Entwicklung des Arbeitsplatzes
- Cybersicherheit und Data Governance
- Nachhaltigkeit
- Operative Effizienz

Entwicklung des Arbeitsplatzes

Ein Unternehmen ist nicht viel mehr als die Gruppe von Personen, die es zusammenbringt, um seine Mission zu erfüllen. Deren unterschiedliche Talente tragen dazu bei, Inputs in höherwertige Outputs zu verwandeln. Zu Recht schätzen viele Unternehmen ihr Humankapital als höchstes Gut und investieren Geld und Mühe in die Einstellung, Schulung und Bindung von Mitarbeiter*innen. Neben ihren Fähigkeiten und ihrer Energie sind Menschen jedoch auch unberechenbar und neigen dazu, Fehler zu machen. Die menschlichen Risiken gehören aus drei Gründen zu den am schwierigsten zu handhabenden Risiken. Erstens sind sie Teil jedes Prozesses, den ein Unternehmen mit oder ohne Technologie durchführt, sodass sich diese Risiken überall manifestieren. Zweitens sind sie von menschlichen Motivatoren abhängig, was im Vergleich zu einer Maschine zu einer unvorhersehbaren Leistung führt. Drittens entwickeln sich die Beziehungen zwischen Unternehmen und ihren Mitarbeiter*innen weiter und die Fernarbeit wird immer alltäglicher, sodass die Situation, die heute vorherrschend ist, bereits morgen anders sein kann.

Menschen waren schon immer die größte Stärke und die größte Schwachstelle von Unternehmen, aber die jüngsten Entwicklungen haben diese Risiken noch einmal erhöht. Die digitale Transformation der letzten Jahrzehnte hat nicht nur die Produktivität im Allgemeinen gesteigert, sondern auch die Mitarbeiter*innen näher an geschäftskritische Prozesse und wertvolle Daten herangeführt. Aufgrund dieser Nähe können unvorsichtige oder böswillige Mitarbeiter*innen schneller als je zuvor mehr Schaden anrichten. In jüngster Zeit zwang die COVID-19-Pandemie zu einer tiefgreifenden und plötzlichen Veränderung vieler Arbeitsumgebungen, wodurch Unternehmen in einer kritischen Zeit zu wenig Personal hatten und Systeme für die Fernarbeit hastig einrichteten. Dies stellte die Unternehmen auch vor eine neue Herausforderung für das Management, wie Herr Fishman erklärt. „Wir verfügen nicht mehr über dasselbe Verständnis für die Rollen und Verantwortlichkeiten aller Mitarbeiter*innen – die Einsicht in die Verhaltensweisen aller Mitarbeiter*innen und in einige Risikoschwachstellen wird durch die Fernarbeit erschwert."

Mit dem Abklingen der Pandemie stellten die Unternehmen fest, dass sich die Einstellung ihrer Mitarbeiter*innen zur Arbeit verändert hat, vielleicht sogar dauerhaft. Bestehende Mitarbeiter*innen sind oft nicht erfreut, ins Büro zurückzukehren, während potenzielle neue Mitarbeiter*innen ein gewisses Maß an Heimarbeit als Standard erwarten. Die Unternehmen haben zudem einen Arbeitskräftemangel erfahren, zum Teil durch die langfristigen gesundheitlichen Auswirkungen der Pandemie, aber auch durch einen Trend, der als „große Kündigungswelle" bezeichnet wird und durch ein Zusammenspiel von Faktoren wie den Protest gegen ein toxisches Arbeitsumfeld verursacht wurde.

In Zukunft wird es aufgrund des Generationswechsels in den Einstellungen und Erwartungen der Mitarbeiter*innen, einschließlich einer zunehmenden Priorisierung von Werten wie Vielfalt, Nachhaltigkeit und soziale Gerechtigkeit, schwieriger werden, Mitarbeiter*innen zu gewinnen und zu halten. Das Gehalt allein wird als Argument nicht mehr ausreichen. Dadurch droht ein Missverhältnis zwischen den in einem

sich schnell wandelnden technologischen Umfeld erforderlichen Qualifikationen und der Verfügbarkeit und Bereitschaft von Bewerber*innen auf dem Markt. Unternehmen können sich mit einer Qualifikationslücke konfrontiert sehen, die die Produktivität beeinträchtigt und das Risiko von Fehlern und böswilligen Handlungen erhöht.

Wie in anderen Risikobereichen halten zwar viele, jedoch nicht alle Unternehmen mit den Entwicklungen Schritt. Die innovativsten Unternehmen verlagern ihre Büros, um sich an die neue, dezentralere Realität anzupassen. Unsere Befragungsergebnisse zeigen, dass 94 % der Unternehmen ihren Ansatz in Bezug auf physische Büros und Arbeitsplätze diversifiziert haben, wobei die Pandemie 45 % von ihnen in den letzten drei Jahren dazu veranlasste, dies zu tun. Entsprechend gaben 96 % der Befragten an, dass ihr Unternehmen neue Richtlinien und Verfahren für das Personalmanagement entwickelt hat, einschließlich hybride Arbeitsmodelle. Darüber hinaus prüfen Unternehmen den Talentbedarf für eine sich verändernde Arbeitswelt, zu der auch die Risikofunktion gehört. Führende Unternehmen „prüfen ihr internes Personalmodell, um sicherzustellen, dass sie über Risikomanager*innen mit den geeigneten technologischen Kompetenzen verfügen“, so Fishman. „Die Rolle von Fachexpert*innen für Technologie in den Bereichen Risiko und Wiederherstellung ist entscheidend, z. B. von Cloud- und KI-Expert*innen.“

Die Unternehmen sammeln zudem mehr Daten über personalbezogene Themen und entwickeln systematischere Verfahren für die Personalbeschaffung und -bindung. Unsere Befragung bestätigt dies: Die Hälfte der Befragten gab an, dass sie zu diesem Zweck mehr Daten nutzen, und ein paar mehr gaben an, dass sie eine Talent-Pipeline entwickelt haben.

Cybersicherheit und Data Governance

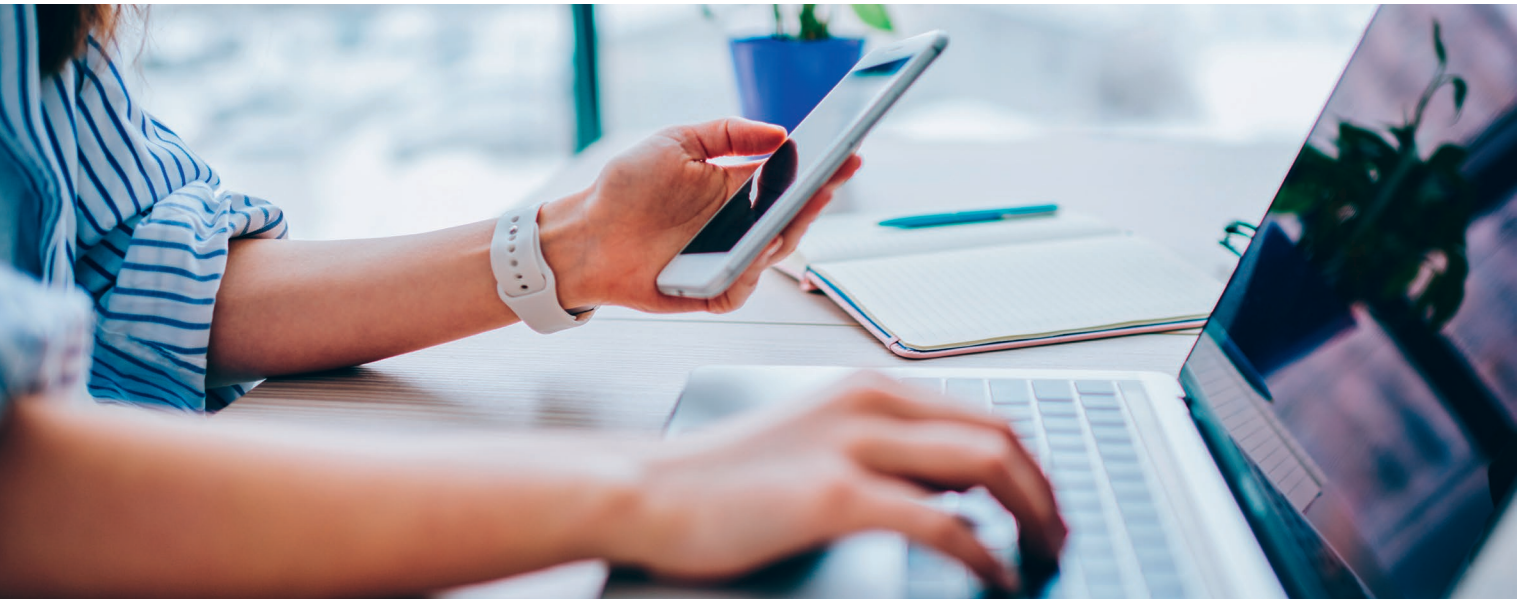
Die begeisterte Annahme der Informationstechnologie durch die Unternehmen hat ihre Arbeitsweise verändert. Im Vergleich zu den alten Zeiten zentralisierter Einrichtungen mit Heerscharen von Mitarbeiter*innen, die von strengen Manager*innen in strikten Hierarchien beaufsichtigt wurden, sind die Unternehmen heute lockerer, flexibler und weitaus produktiver geworden – vor allem dank der Digitalisierung. Computer, Automatisierung und das Internet haben die Arbeitsmodelle tiefgreifend verändert, und künftige Entwicklungen wie das Quantencomputing, ein allumfassendes Internet der Dinge und das Metaverse versprechen ebenso grundlegende Veränderungen.

Im Großen und Ganzen hat die digitale Revolution dreierlei Auswirkungen auf das Risikomanagement in Unternehmen: Risiken treten plötzlicher auf und breiten sich viel schneller aus; Daten, ihre Speicherung, Übermittlung und Auswertung sind zu einem entscheidenden Bestandteil der Geschäftstätigkeit geworden; und während die Digitalisierung neue Risikobereiche geschaffen hat, hat sie auch neue Instrumente hervorgebracht, mit denen sie angegangen werden können.

Wenn sich Informationen mit Lichtgeschwindigkeit durch ein globales digitales Netz bewegen, ändern sich die Dinge schneller, als ein Mensch reagieren kann. Da anstelle von Menschen zunehmend Computer Entscheidungen treffen, können Prozesse zahlreiche Wiederholungen durchlaufen, bevor ein Fehler oder ein unbeabsichtigtes Ergebnis entdeckt wird. Und da alle Kund*innen, Partner*innen und Verbraucher*innen Zugriff auf die globalen Kommunikationsmedien haben, kann der Ruf einer Marke in den Fokus der öffentlichen Meinung geraten, bevor die Führungskräfte des Unternehmens die Geschehnisse vollständig erfasst haben.

Mit der generativen KI entsteht ein neues potenzielles Cyberrisiko. Das Tempo, mit dem sich diese Technologie durchsetzt, hat die Gesellschaft in ihren Bann gezogen, und die politischen Entscheidungsträger*innen und Regulierungsbehörden – und ebenso die Pionier*innen, die diese Technologie entwickelt haben – haben Mühe, mit ihr Schritt zu halten. Risikomanager*innen wissen nicht, an wen sie sich wenden sollen, wenn sie in diesem frühen Stadium einer Entwicklung, die sich für Geschäftsmodelle als ebenso destabilisierend erweisen könnte wie das Internet selbst, den besten Rat suchen. „Wer verfügt heute über risikorelevante Kenntnisse darüber, wohin sich die generative KI entwickelt?“, fragt Fishman. „Welche ausgefeilten Methoden können wir einsetzen, um die Cloud-Konzentration besser zu überwachen? Wie können wir in Anbetracht der sich verändernden Cyber-Landschaft die Widerstandsfähigkeit in unsere Infrastruktur und Prozesse integrieren?“

Risiko-Reset: Verlagerung des Schwerpunkts von Reaktion auf Antizipation



Dieser Bereich bringt für Risikomanager*innen und Unternehmen dringende Fragen und komplexe Herausforderungen. In solchen Fällen ist die Vermittlung der Grundlagen ein guter Anfang. Es ist nach wie vor von entscheidender Bedeutung, dass sich Unternehmen bei der Verwaltung ihrer digitalen Ressourcen auf drei Hauptrisikobereiche konzentrieren:

- Data Governance: Gewährleistung der Genauigkeit, Konsistenz und Zugänglichkeit von Daten.
- Datensicherheit: Schutz der Daten vor unbefugtem Zugriff, Verwendung, Offenlegung, Unterbrechung, Änderung oder Zerstörung.
- Datenschutz: Schutz der Privatsphäre des Einzelnen durch Kontrolle der Erhebung, Verwendung und Weitergabe seiner personenbezogenen Daten.

Die gleichen Grundsätze der Proaktivität und des Blicks über den Tellerrand hinaus gelten weiterhin, aber mit größerer Dringlichkeit als früher. Auch die Compliance ist in einem sich so schnell verändernden und unsicheren rechtlichen Umfeld eine größere Herausforderung, jedoch nicht weniger wichtig.

Die Ergebnisse unserer Befragung zeigen, dass sich die Unternehmen engagiert und konsequent darum bemühen, Daten- und Cybersicherheitsrisiken durch verschiedene Maßnahmen zu mindern. In den letzten drei Jahren investierten 49 % der Unternehmen in Notfallwiederherstellungs-/Business-Continuity-Pläne für digitale Systeme und 48 % in Cloud-Dienste/-Speicher sowie in die laufende Überwachung und Prävention von Cyberrisiken und -bedrohungen. Im gleichen Zeitraum gaben 46 % der befragten Führungskräfte an, dass sie in IT- und Cybersicherheitstalente investieren und Schulungen zu Daten- und Technikkenntnissen durchführen.

In der Zwischenzeit sollten Risikomanager*innen ein großes Interesse an der Entwicklung der KI haben, nicht nur als Risikoquelle, sondern auch als Mittel zur Risikominderung. 43 % der Befragten gaben an, kognitive Technologien und KI in Risikomanagementprozessen einzusetzen. Richtig trainiert und gelenkt, kann KI auffällige Muster erkennen, Trends identifizieren, Szenarien entwerfen und Risikobereiche ausmachen, die menschlichen Analyst*innen möglicherweise entgangen wären.

Risiko-Reset: Verlagerung des Schwerpunkts von Reaktion auf Antizipation

Kaum ein Unternehmen ist frei von Cyberrisiken, einige Branchen sind jedoch anfälliger als andere. Im Gesundheitswesen und im Finanzsektor werden beispielsweise große Mengen an sensiblen Kundendaten erfasst. Die optimale Nutzung dieses Datenschatzes, nicht zuletzt zur Berechnung des Risikos für Kund*innen oder Unternehmen, bei gleichzeitiger Gewährleistung der Sicherheit, ist eine Mammutaufgabe. Die Kosten eines Scheiterns dieses Unterfangens können verheerend sein. Es überrascht nicht, dass von allen Branchen das Gesundheitswesen mit 83 % den höchsten Prozentsatz an Befragten aufwies, was auf die wachsende Bedeutung von Technologieindikatoren in den letzten drei Jahren hinweist. Dazu gehörten die Netzwerkverfügbarkeit, Vorfälle im Bereich der Cybersicherheit und Softwarefehler.

Der Energiesektor ist ebenfalls auf Daten angewiesen, um seine Abläufe zu rationalisieren, während der moderne Staat in hohem Maße auf Bürgerdaten zurückgreift, um öffentliche Dienstleistungen mit maximaler Effizienz zu erbringen. Im Falle von Regierungen können die Kosten des Versagens für den Ruf besonders schädlich sein und Politiker*innen und ihre Parteien in einen direkten Konflikt mit ihren Wähler*innen bringen.

Nachhaltigkeit

Die Industrialisierung hat der Menschheit Fortschritte gebracht, die für unsere vorindustriellen Vorfahren unvorstellbar waren. Durch die Verbrennung fossiler Brennstoffe haben wir jedoch die Nachhaltigkeit unseres Lebensstils – und unser Leben – in Gefahr gebracht. Die Treibhausgase (THG), die vor allem aufgrund unserer Wirtschaftstätigkeit in die Atmosphäre gelangen, erhöhen die globale Durchschnittstemperatur. Die Auswirkungen werden in den nächsten Jahrzehnten potenziell katastrophal sein, aber so lange müssen wir nicht warten. Extreme Wetterereignisse nehmen zu, der Meeresspiegel steigt, und die Artenvielfalt ist gefährdet.

Dies wirkt sich in zweierlei Hinsicht auf Unternehmen aus. Erstens sind Betriebe und Lieferketten anfällig für Störungen durch extreme Wetterereignisse und andere schwer vorhersehbare Umwelteinflüsse. Die Ereignisse der letzten drei Jahre haben 47 % der befragten Unternehmen dazu veranlasst, sich auf den Aufbau vielfältiger und flexibler Lieferkettennetze zu konzentrieren. Zweitens erwarten die Stakeholder*innen der Unternehmen – von Kunde*innen über Investor*innen bis hin zu Mitarbeiter*innen – zu Recht, dass die Unternehmen ihren Beitrag zur Bekämpfung von Ressourcenerschöpfung, Umweltzerstörung und Treibhausgasemissionen leisten.

Im Moment ist die zweite Ausprägung für Risikomanager*innen dringlicher (obwohl auch die erste eine wachsende Bedrohung darstellt). Aktivistengruppen kritisieren die ihrer Meinung nach ungeheuerlichen Verstöße gegen nachhaltige Praktiken immer schneller und verfügen über ein wachsendes Arsenal an kreativen Mitteln, um die Öffentlichkeit auf sich aufmerksam zu machen. Erdöl- und Energieunternehmen sowie die Investor*innen und Banken, die sie finanzieren, stehen immer wieder in der Kritik. Solche Kampagnen können den Geschäftsbetrieb direkt stören, sie haben jedoch noch schädlichere Auswirkungen, indem sie den Ruf und die „soziale Akzeptanz“ eines Unternehmens untergraben.

Die Bedeutung von Kennzahlen für das Reputationsrisiko hat in den letzten Jahren bei Führungskräften zugenommen, da die Betriebsumgebungen immer komplexer werden und die Unternehmen transparenter, rechenschaftspflichtiger und sozial verantwortlicher sein müssen. Beachtliche 80 % der Befragten gaben an, dass die Kennzahlen für das Reputationsrisiko die größte Bedeutung für ihre Risikoüberwachung haben.

Wie die Cybersicherheit weisen auch das Thema Nachhaltigkeit und die verbundenen Bereiche Soziales und Governance (Environmental, Social and Governance – ESG) eine sich schnell verändernde Risikolandschaft auf. Umweltbelange haben in der Öffentlichkeit an Bedeutung gewonnen und Unternehmen reagieren darauf mit Erklärungen, in denen sie ihre „grüne“ Geschäftstätigkeit betonen. Solche Erklärungen werden jedoch häufig als „Greenwashing“ abgetan und reichen nicht aus, um die Unternehmen vor dem Zorn der Öffentlichkeit zu schützen. An die Stelle grüner Leitbilder sind zunehmend Zusagen getreten, „Netto-Null“-Treibhausgasemissionen zu erreichen, begleitet von Roadmaps, die zeigen, wie dies erreicht werden soll.

Für größere Unternehmen ist dies jedoch nicht mehr ausreichend. Die Bürger*innen

drängen auf eine „naturfreundliche" Haltung der Unternehmen und des öffentlichen Sektors und die Unternehmen werden aufgefordert, Pläne für die Wiederherstellung des vorindustriellen Zustands der Umwelt vorzulegen oder zumindest die Klimakennzahlen wieder auf ein Niveau zu bringen, das mit einer nachhaltigen Wirtschaft vereinbar ist. Frau Heading verweist auf „eine Verlagerung des Risikomanagements von einer strikt regulatorischen und Compliance-bezogenen Aufgabe hin zu einer weitaus strategischeren Funktion, die auch gesellschaftlichen Werten wie ESG gerecht wird."

Unsere Befragung zeigt, dass ESG nun in den Risikoregistern der Unternehmen auftaucht. Fast die Hälfte der befragten Unternehmen hat mehr Ressourcen für ESG-Initiativen bereitgestellt, während eine ähnliche Anzahl sich auf die Berichterstattung zur ESG-Leistung konzentriert, die in einigen Ländern von den Aufsichtsbehörden vorgeschrieben ist.

Operative Effizienz

Für die Unternehmen und ihre Risikomanager*innen sind die internen Abläufe am greifbarsten. Die meisten Unternehmen können wenig tun, um die Umstände jenseits ihrer physischen oder virtuellen Mauern zu beeinflussen, aber das, was intern geschieht, unterliegt meist ihrer direkten Kontrolle. Ob Menschen, Prozesse oder regulatorische Anforderungen – die Effizienz der inneren Abläufe eines Unternehmens entscheidet über Erfolg und Misserfolg. Und sie ist mit Risiken behaftet: Mitarbeiter*innen können nicht die erwartete Leistung erbringen, wenn sie von den Geräten, auf die sie angewiesen sind, im Stich gelassen werden oder wenn Schwachstellen in den Prozessen bestehen, die ihre kollektive Produktivität gewährleisten sollen.

Die Absicherung gegen solche Risiken ist seit den Anfängen des Risikomanagements ein zentrales Merkmal dieser Disziplin. Risikomanager*innen können daher leicht in das alte Bild verfallen, sie seien nicht viel mehr als interne Polizist*innen, die anderen Abteilungen Steine in den Weg legen. Die Risikofunktion wird daher als Kostenstelle und als Belastung für die unternehmerische Initiative der „wertschöpfenden" vertikalen Bereiche angesehen. Diese Wahrnehmung war (und ist manchmal immer noch) ein Klotz am Bein der Risikomanager*innen, aber die Dinge ändern sich. Risikomanager*innen sind heute besser darin, die Kosten von Betriebsausfällen zu messen und sie gegen die Kosten der Aufrechterhaltung einer zweckmäßigen Risikofunktion abzuwägen. Verglichen mit der Unterbrechung des Betriebs zur Wiederherstellung eines fehlgeschlagenen Prozesses, einer saftigen behördlichen Strafe für den unsachgemäßen Umgang mit Kundendaten oder dem Verlust von Geschäften aufgrund eines öffentlichkeitswirksamen ethischen Fehlverhaltens, sind die Kosten für ein flexibles Risikomanagement weniger belastend.

Da keine zwei Unternehmen gleich sind, gibt es kein Patentrezept für die Erreichung operativer Effizienz. Tatsächlich kann das, was unter „operativ" verstanden wird, innerhalb eines Unternehmens und zwischen mehreren Unternehmen sehr unterschiedlich sein. Der Energiesektor konzentriert sich auf Anlagen und Verfahren, da Ölbohrungen oder die Gewinnung von Mineralien sehr kapitalintensiv sind und ein Ausfall zu Katastrophen für Mensch und Umwelt führen kann. Der Finanzsektor ist sowohl datenintensiv als auch anfällig für Fehler bei seinen Mitarbeiter*innen durch Verstöße gegen Richtlinien und Aufgaben, schlechte Ausführung, mangelnde Schulung und unethisches Verhalten. Diese können zu direkten Verlusten sowie zu regulatorischen, rechtlichen und Umstrukturierungskosten führen. Die Einhaltung von Gesetzen und Vorschriften ist besonders wichtig und wird durch die Tatsache erschwert, dass viele Banken und Finanzinstitute in verschiedenen Rechtsordnungen tätig sind. Andere Branchen unterscheiden sich in der Ausrichtung ihres operativen Risikomanagements – einer der vielen Faktoren, die die Arbeit von Risikomanager*innen erschweren.

Unsere Befragung spiegelt die Bedeutung des operativen Risikos für Unternehmen wider, wobei deutlich wird, dass Investitionen in diesem Bereich die Leistung und die finanziellen Ergebnisse verbessern. Besonders bemerkenswert ist, dass 42 % der Befragten von

einer Leistungsverbesserung berichten, die sich aus der Anwendung guter Managementpraktiken bei der Planung von Einrichtungen und physischen Arbeitsplätzen ergibt. Ein ähnlicher Prozentsatz berichtet von einer deutlichen Verbesserung der betrieblichen Effizienz ihres Unternehmens. Zwei Drittel der Befragten erkennen jedoch an, dass es sich hierbei um ein langfristiges Vorhaben handelt und dass die Investitionen in das Risikomanagement den Betrieb kurzfristig stören.

Laut Dr. Henisz ist es von entscheidender Bedeutung, den Zusammenhang zwischen Investition und Ertrag zu erkennen. „Wir können die Auswirkungen des Risikos monetarisieren, indem wir die Ausfalltage und Produktionsausfälle berechnen. Die Übersetzung der Daten in die Sprache der Finanz- oder Betriebsabteilung ist entscheidend. Andernfalls wird die Risikomanagementfunktion nur als Kostenfaktor betrachtet, während alle anderen Umsatz generieren."

Herausforderungen für das Risikomanagement

Das Risikomanagement ist im Laufe der Zeit immer einflussreicher und ausgefeilter geworden und ist in die Kultur und Struktur der meisten großen Unternehmen eingebettet. Ihre Rolle und ihre Methoden stehen jedoch unter dem ständigen Druck, mit einem sich ständig verändernden Risikoumfeld Schritt zu halten. Es besteht die Tendenz, eine Risikostrategie, die mit jeder in der Vergangenheit aufgetretenen Bedrohung fertig wird, als ausreichend zu betrachten, doch ist die Vergangenheit oft ein schlechter Indikator dafür, wie sich Risiken in der Zukunft manifestieren werden. Daher muss das Risikomanagement ständig weiterentwickelt werden, wenn neue Bedrohungen und Störfaktoren ins Blickfeld geraten. Insbesondere muss der Berufsstand den Weg von der Reaktion zur Antizipation fortsetzen, indem er seine Widerstandsfähigkeit gegen künftige Bedrohungen ausbaut, anstatt nur auf bekannte Bedrohungen zu reagieren.

In dieser Hinsicht zeigt unsere Befragung einige Fortschritte, aber auch, dass noch mehr getan werden muss. Eine überwältigende Mehrheit der befragten Führungskräfte ist davon überzeugt, dass die von ihren Unternehmen durchgeführten Risikomanagementinitiativen ausreichen, um Schäden durch Risiken zu mindern oder zu verhindern. Dies deutet auf ein gewisses Maß an Selbstvertrauen der Unternehmen hin, das sie stärker gefährdet, als sie glauben. Um dieses potenzielle Defizit zu beheben, müssen drei Schwerpunkte gesetzt werden: Messung, Bereitstellung von Ressourcen und Koordinierung.

Messung

Die Leistungsverfolgung im Risikomanagement gestaltet sich von Natur aus schwierig. Wenn das Risikomanagement versagt, können die entstandenen Kosten dem Risikomanagementprogramm angelastet werden. Dies scheint auf der Hand zu liegen. Die Bestimmung des Prozentsatzes der Kosten, der der Funktion zugewiesen werden sollte, ist jedoch alles andere als einfach. Im Kreditrisikomanagement ist dies sogar noch schwieriger, wenn es nicht zu Vorfällen kommt. Es besteht die Tendenz, dies als „business as usual" zu betrachten und den Beitrag von Risikomanagern gänzlich zu leugnen. Selbst wenn man sich bemüht, die Funktion zu würdigen, ist es schwierig, zu quantifizieren, was als positiver Wert notiert werden sollte.

Sollte von der Risikofunktion erwartet werden, dass sie über Investitionen Rechenschaft ablegt, die in Erwartung von Risiken getätigt wurden, die nie eingetreten sind? Sollte sie für Black-Swan-Ereignisse (schwer vorhersehbar, die jedoch im Nachhinein als unvermeidlich erscheinen) verantwortlich sein, die die Aufmerksamkeitsschwelle nicht überschritten haben? Nach der globalen Finanzkrise 2008–2009, die weithin als Black-Swan-Ereignis angesehen wurde, wurde die Risikodisziplin – einschließlich der Ratingagenturen – in ihren Grundfesten erschüttert. Zweifelsohne war die Kreditkrise ein Hinweis auf das Versagen beim Verständnis und Management von Risiken, aber auch politische Fehler und öffentlicher Leichtsinn waren an diesem Ereignis beteiligt. Unter diesen Umständen ist es schwierig, die Leistung des Risikomanagements auch nur annähernd genau zu überprüfen.

Auch das Risikomanagement hat mit den Schwierigkeiten zu kämpfen, die in vielen operativen Bereichen auftreten, wenn es darum geht, kurzfristige Investitionen mit langfristigem Nutzen zu rechtfertigen. „Wenn Sie heute eine Investition tätigen, sehen Sie den Nutzen vielleicht erst in fünf oder zehn Jahren, vielleicht aber auch in drei Monaten", so Frau Heading. „Je nachdem, was man zu kontrollieren versucht, kann es sehr schwierig sein, das Kosten-Nutzen-Verhältnis so darzustellen, dass es von den Führungskräften verstanden wird."

Die Führungskräfte sind sich der Herausforderungen bei der Messung der Risikomanagementleistung bewusst. Rund drei Viertel der Befragten sind der Meinung, dass das Fehlen standardisierter Bewertungsmaßstäbe zur Risikomessung den Nachweis von Fortschritten erschwert.

„Die Entwicklung von Kennzahlen, die die Risiken mit den Unternehmenszielen verknüpfen, und die Sicherstellung, dass diese für die unterste Unternehmensebene genauso klar sind wie für den Vorstand und die Geschäftsführung, sind von entscheidender Bedeutung", so Fishman. „Tools können dabei helfen, aber die Struktur der Messung von Risiken, die direkt mit Aktivitäten und deren Auswirkungen verbunden sind, ist von grundlegender Bedeutung. Man darf nicht nur die Auswirkungen betrachten, sondern muss auch die kausalen Faktoren verstehen. Zum Beispiel ist die Messung von Cyber-Ereignissen zwar wichtig, aber genauso wichtig ist es, zu messen, wie effizient Prozesse und Systeme Schwachstellen beheben und die Geschäftskontinuität sicherstellen."

Beschaffung

Nur wenige Abteilungen halten sich selbst für angemessen finanziert, aber die Risikomanager*innen sind hier besonders stark vertreten. Dies liegt zum Teil daran, dass Unternehmen dazu neigen, diese Funktion so zu finanzieren, dass sie die Risikolandschaft der Vergangenheit widerspiegelt, anstatt für die Zukunft gerüstet zu sein. Umfang und Komplexität der Risiken, mit denen sich Unternehmen konfrontiert sehen, nehmen stetig zu, da sich die Lieferketten verlängern und verschlanken und die Technologie das Tempo der Veränderungen beschleunigt. In ähnlicher Weise können Unternehmen eine wachsende Zahl von Instrumenten für die Risikoüberwachung und den Aufbau von Widerstandsfähigkeit nutzen, aber sie erfordern hohe Vorabinvestitionen, und wie bereits erwähnt, sind Zeitpunkt und Umfang der Investitionsrendite schwer zu quantifizieren.

Die Befragten sind der Meinung, dass die Risikoabteilungen nicht ausreichend mit Ressourcen ausgestattet sind. Die Führungskräfte sind der Meinung, dass die finanziellen, technologischen und personellen Ressourcen ihres Unternehmens für das Risikomanagement unzureichend sind, wobei fast zwei Drittel sagen, dass ihr Unternehmen in diesem Bereich Verbesserungen vornehmen muss.

Ein Teil der Herausforderung besteht darin, dass Risikomanager*innen angesichts der zunehmenden Digitalisierung von Unternehmen über ein breiteres Spektrum an Fachwissen verfügen müssen. Das bedeutet, dass Unternehmen mehr Geld ausgeben müssen, um die erforderlichen Qualifikationen für das Risikomanagement zu gewinnen, selbst wenn sie nur ein einheitliches Schutzniveau aufrechterhalten wollen. „Risikomanager*innen sind begehrt", so Herr Fishman. „Selbst bei den massiven Entlassungen im Finanz- und Technologiesektor sind gute Risikomanager*innen schwer zu finden."

Angesichts von Entwicklungen wie KI, Automatisierung und Robotik, die alle Aufmerksamkeit erfordern, wird sich dieser Engpass wahrscheinlich noch verschärfen. In Verbindung mit dem breiten Einsatz von Technologien wie dem Quantencomputing und der Distributed-Ledger-Technologie wird es in der Risikomanagement-Branche in absehbarer Zukunft keinen Platz für Selbstzufriedenheit geben.

Koordinierung

Wie bereits erörtert, wird eine zentrale Anforderung an das Risikomanagement in den kommenden Jahren die Fähigkeit sein, das Risikoverständnis in alle Bereiche des Unternehmens zu tragen. Die Informationsflüsse müssen von unten nach oben im gesamten Unternehmen koordiniert werden, wobei die Risikomanager*innen die Regeln und Instrumente festlegen, die alle Abteilungen und Mitarbeiter*innen verwenden sollten. Die oberste Führungsebene muss den Ton angeben, damit die zentrale Rolle des Aufbaus von Resilienz gegen bekannte und unbekannte Bedrohungen die Unternehmenskultur durchdringt. Partner*innen, Lieferant*innen und Kund*innen müssen in dieses Netzwerk einbezogen werden, sodass das Risikoradar des Unternehmens weit über die eigenen Mauern hinausgeht.

Der gesamte Risikomanagementapparat muss sich auf die täglichen Abläufe innerhalb des Unternehmens konzentrieren, aber auch, und das ist entscheidend, im Blick haben, was angesichts neuer Trends in Zukunft geschehen könnte. Die erfolgreichsten Unternehmen werden diejenigen sein, in denen diese Bemühungen von erstklassigen Risikomanager*innen konzipiert und koordiniert werden, die über die Fähigkeiten und Ressourcen verfügen, die in einem sich schnell verändernden Umfeld erforderlich sind, und die von den höchsten Führungskräften unterstützt werden.

Die Reise des Risikomanagements ist noch nicht abgeschlossen, aber die Richtung, in die es geht, ist vielversprechend.

Schlussfolgerung

Das Risikomanagement hat eine beeindruckende Entwicklung genommen, seit es erstmals als eigenständige Unternehmensfunktion in Erscheinung trat. Es hat sich von einer Disziplin, die in erster Linie auf das Bankwesen beschränkt war, wo die Lösung darin bestand, großzügigere Finanzpolster aufzubauen, um die Liquidität bei ungünstigen Marktentwicklungen zu gewährleisten, zu einem Kernstück des modernen Managements entwickelt. Risikomanager*innen sind in Unternehmen aller Branchen, sowohl im privaten als auch im öffentlichen Sektor, von großer Bedeutung. Sie erfassen und quantifizieren Bedrohungen in einem breiten Spektrum von Faktoren, die sowohl innerhalb als auch außerhalb des Unternehmens, wo Sichtbarkeit und Kontrolle weniger ausgeprägt sind, auftreten können. Das Risikomanagement wurde auf immer mehr Führungsebenen des Unternehmens eingeführt und viele Risikomanager*innen sind heute in der C-Suite tätig und haben Kontakt zum CEO oder Vorstand. In diese Richtung geht die Entwicklung schon seit einigen Jahrzehnten und die Funktion wird immer tiefer in den Unternehmen verankert.

Es entstehen jedoch auch neue Herausforderungen und die alten verändern sich, da Technologie, Geopolitik und sozialer Wandel das Arbeitsumfeld beeinflussen. Das Risikomanagement war schon immer eine dynamische Disziplin, aber der Bedarf an Veränderungen wird immer dringender. Dieses junge Jahrhundert hat bereits eine Reihe globaler Zerrüttungen gesehen. Von der globalen Finanzkrise 2008–2009 und der anschließenden Vertrauenskrise in die liberale Demokratie über die COVID-19-Pandemie bis hin zum Krieg Russlands gegen die Ukraine – die tektonischen Bewegungen im Weltgeschehen haben die Unsicherheit vervielfacht. Dies alles geschah vor dem Hintergrund eines seit langem bestehenden, aber sich beschleunigenden Wandels hin zu einer digitalen Landschaft sowie vor dem Hintergrund von Umweltthemen, die sich auf Wirtschaft, Gesellschaft, Politik und die globale Wirtschaft auswirken.

Die Beschleunigung des digitalen Wandels, der durch das Aufkommen von generativen, vorab trainierten großen Sprachmodellen veranschaulicht wird, birgt sowohl Chancen als auch Risiken. Dies könnte zwar eine neue Generation von Tools hervorbringen, die Unternehmen bei der Überwachung von und der Reaktion auf Risiken helfen, es birgt jedoch auch die Gefahr, dass böswillige Akteur*innen mit ähnlich innovativen Tools ausgestattet werden, um wertvolle Daten zu stehlen oder zu beeinträchtigen. Neue Arbeitsmuster, insbesondere die Zunahme der Fernarbeit, erweitern und verwischen die digitale Grenze des Unternehmens und eröffnen neue Wege für Cyberbedrohungen.

Die Risikomanager*innen setzen den vor Jahrzehnten begonnenen Weg fort, indem sie im gesamten Unternehmen einen „risikobewussten“ Ansatz für die Geschäftstätigkeit einführen. Sie müssen sich mit dem zunehmend ungewissen Charakter des Risikos auseinandersetzen, bei dem ein Ereignis in einem entlegenen Teil der Lieferkette unvorhergesehene Auswirkungen an anderer Stelle haben kann.

Entscheidend ist auch der Übergang von einer reaktiven zu einer proaktiven Haltung. Der reaktive Ansatz konzentriert sich auf

den Aufbau von Widerstandsfähigkeit gegen erwartete Bedrohungen und die Reaktion auf diese, wenn sie eintreten. Beim proaktiven Ansatz wenden die Risikomanager*innen Ressourcen und Anstrengungen auf, um über ihren Tellerrand hinaus nach Bedrohungen zu suchen, die nicht im Risikoregister enthalten sind, und sich auf Szenarien vorzubereiten, die unwahrscheinlich erscheinen und ein hohes Schadenspotenzial haben.

In der sich wandelnden Risikolandschaft von heute, die breiter, schneller und komplexer ist als je zuvor, ist ein proaktiver Ansatz vielleicht die wirksamste Maßnahme, die das Risikomanagement ergreifen kann, um sich auf die Zukunft vorzubereiten.

ECONOMIST IMPACT

LONDON

The Adelphi
1-11 John Adam Street
London WC2N 6HT
United Kingdom
Tel: (44) 20 7830 7000
Email: london@economist.com

GENEVA

Rue de l'Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
Email: geneva@economist.com

SÃO PAULO

Rua Joaquim Floriano,
1052, Conjunto 81
Itaim Bibi, São Paulo,
SP, 04534-004
Brasil
Tel: +5511 3073-1186
Email: americas@economist.com

NEW YORK

900 Third Avenue
New York, NY 10022
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
Email: americas@economist.com

DUBAI

Office 1301a
Aurora Tower
Dubai Media City
Dubai
Tel: (971) 4 433 4202
Fax: (971) 4 438 0224
Email: dubai@economist.com

HONG KONG

1301
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
Email: asia@economist.com

SINGAPORE

8 Cross Street
#23-01 Manulife Tower
Singapore
048424
Tel: (65) 6534 5177
Fax: (65) 6534 5077
Email: asia@economist.com