IBM Institute for Business Value

Die Rolle der IT-Manager und CIOs im Wandel

Erkenntnisse der globalen IT-Risikostudie 2010 von IBM

IBM Institute for Business Value

IBM Global Business Services gibt über das IBM Institute for Business Value auf Fakten basierende strategische Einblicke für Führungskräfte zu wichtigen Themen im öffentlichen und privaten Sektor. Dieser Bericht beruht auf einer detaillierten Studie durch das Forschungsteam des Instituts. Er ist Teil des laufenden Engagements durch IBM Global Business Services, Unternehmen durch Analysen und Standpunkte zu Geschäftserfolgen zu verhelfen. Für mehr Informationen kontaktieren Sie die Autoren oder senden Sie eine E-Mail an *iibv@us.ibm.com.*

Weitere Studien des IBM Institute for Business Value finden Sie unter *ibm.com/iibv*

Von Linda B. Ban, Richard Cocchiara, Kristin Lovejoy, Rick Telford und Mark Ernest

Steigende Regulierungsanforderungen, das Wachstum des 24x7 Online-Geschäfts und der ständige Schatten einer unsicheren Wirtschaft machen uns bewusst, wie wichtig es heute ist, Risiken in all ihren Formen – ob bezogen auf das Geschäft, auf Daten oder auf Ereignisse – in den Griff zu bekommen. Die globale IT-Risikostudie 2010 von IBM identifiziert die Herausforderungen im Zusammenhang mit dem IT-Risiko und die Maßnahmen, die IT-Manager und CIOs ergreifen, um dieses Problem besser zu verstehen, ihm zu begegnen und eine Lösung zu finden. Von den befragten IT-Managern rechnen die meisten damit, dass ihre Risikoverantwortung zunehmen wird. IT-Risikomanagement hat eindeutig weit reichende Auswirkungen und kann die Wettbewerbsposition eines Unternehmens sowie seinen Ruf bei Kunden, Partnern, Behörden und sonstigen Beteiligten direkt beeinflussen.

Aus einer Geschäftsperspektive nimmt die IT-Infrastruktur an Bedeutung zu. Sie unterstützt und sichert nicht nur die Vermögenswerte eines Unternehmens und gewährleistet eine korrekte Unternehmensführung und Regeleinhaltung, sondern sie ist auch ein wichtiger Faktor, der das Geschäftswachstum ankurbelt. Infolgedessen gilt IT-Risikomanagement nicht länger nur als rein technische Funktion, sondern vielmehr als eine entscheidende Managementaufgabe, die zu direkten Geschäftsvorteilen für das gesamte Unternehmen führen kann.

Um besser zu verstehen, welche Maßnahmen Unternehmen ergreifen, um ihre Geschäftsrisiken – besonders im IT-Bereich – zu verwalten und zu entschärfen, veranlasste IBM die Globale IT-Risikostudie 2010. Sie ist Teil der laufenden Forschungen, die IBM im Bereich IT-Risiko durchführt und die erste einer Serie von Forschungsumfragen zu diesem Thema. Durchgeführt wurde die Umfrage im Mai und Juni 2010 in Zusammenarbeit mit der Economist Intelligence Unit (EIU). Die Umfrage sollte mehr Aufschlüsse über die Fokusbereiche von IT-Managern heute liefern und Bereiche identifizieren, in denen sie kurzfristig Gelegenheiten und Herausforderungen erkennen. Weitere Forschungen werden sich noch eingehender mit diesen Fragen befassen und die Optionen und Entscheidungen untersuchen, mit denen alle Risikomanagementteams konfrontiert werden.

„In dem Zeitraum, in dem IT immer mehr ins Zentrum geschäftlicher Aktivitäten gerückt ist, rückte das IT-Risikomanagement nicht in gleichem Maße auf der Tagesordnung nach oben.“

Befragter, Reise- und Tourismusbranche, Westeuropa

„Obschon manche anmerken, dass die Technologie gereift und im Geschäft weithin verfügbar geworden ist, ist für uns die technologische 'Revolution' erst in ihren Anfängen. Wir legen die Entwicklungen dahingehend aus, dass der strategische Wert der Technologie für das Geschäft noch weiter zunimmt."

Brynjolfsson, Erik und Adam Saunders. "Wired for Innovation: How Information Technology is Reshaping the Economy." Massachusetts Institute of Technology. 2010.

Die Ergebnisse dieser Studie basieren auf einer umfassenden Online-Befragung von 556 IT-Managern und weiteren wichtigen Mitarbeitern in der IT-Funktion (darunter 131 CIOs). In die branchenübergreifende Studie, die unter anderem in Nordamerika, Westeuropa, im Asien-Pazifik-Raum, im Nahen Osten und in Afrika, Osteuropa und Lateinamerika durchgeführt wurde, waren Unternehmen aus den Branchen IT, Finanzdienstleistungen, Gesundheitswesen und Pharma bis hin zu Biotechnologie, Fertigung und Regierung einbezogen. Die Umsätze der befragten Unternehmen variierten von US$500 Millionen bis über US$10 Milliarden.

Dies waren die Hauptziele der Studie:

- Befragung eines repräsentativen Querschnitts von Unternehmen, um die aktuelle Lage im IT-Risikomanagement genau beurteilen zu können.
- Identifizierung von Faktoren, welche die Risikomanagementstrategien einer Organisation fördern (oder behindern) können.
- Feststellen, inwieweit Unternehmen neue Risikostrategien, -programme und -grundsätze implementieren.
- Verstehen, wie neue Ansätze wie z. B. „Cloud Computing" in die allgemeinen Risikostrategien der Unternehmen passen.
- Untersuchung der sich wandelnden Rolle der IT-Manager, einschließlich CIOs.

Generell waren die Ergebnisse der Umfrage über Regionen, Unternehmen verschiedener Größe, Branche und Funktionen übereinstimmend. (Alle in der Studie vertretenen Regionen bestätigten die Bedeutung von IT-Risikomanagement und arbeiten diesbezüglich an Verbesserungen.) Im Großen und Ganzen drückten die Studienteilnehmer Vertrauen in ihr Risikomanagement und ihre Compliance-Bemühungen aus (siehe Abbildung 1).

Obwohl über 50 % der Befragten berichteten, dass ihre Budgets gleich geblieben oder gestiegen sind, kämpfen 36 % immer noch darum, genügend Mittel zu sichern, um sich mit den Risikoherausforderungen zu befassen. Und trotz der Erkenntnis, dass IT-Risikomanagement spürbare Geschäftsvorteile bringen kann, bleibt die Sicherung der Unterstützung des Führungsstabs ein echtes

Allgemeiner Ansatz zum Entschärfen des IT-Risikos

Der allgemeine Ansatz hat sich in den vergangenen 12 Monaten verbessert

Abbildung 1: **Organisationen und ihr Ansatz zum Entschärfen der größten IT-Risiken.**

Anliegen. Die Rückmeldungen der Befragten deuten anscheinend auf eine Kluft zwischen der Ansicht des Führungsstabs über die Kosten von verbessertem Risikomanagement und dem Wert hin, der sich daraus ableiten lässt.

Raum für Verbesserung schaffen

Angesichts der potenziellen Renditen eines effektiven IT-Risikomanagements planen viele der Befragten, ihre Risikoinitiativen über die nächsten drei bis fünf Jahre zu erweitern. Dennoch gab es einige bemerkenswerte Diskrepanzen. Nur etwa die Hälfte der befragten Unternehmen verfügt über eine offizielle Abteilung für Risikomanagement (46 %) oder eine gut durchdachte Strategie zur Geschäftskontinuität (54 %). Auch der Geschäftszweig und sonstige operative Risikobelange (z. B. finanziell/geschäftsstrategisch) stehen nicht im Brennpunkt.

„IT-Organisationen führen traditionell intensive Tests durch, bevor neue IT-fähige Business-Services eingeführt werden. Das Hauptziel dabei ist, Ausfälle zu vermeiden. Aber der moderne IT-Führungsstab muss die echten Kosten solcher Tests für das Geschäft verstehen. Es sind nicht nur die IT-Kosten, sondern auch die Kosten für verpasste Chancen infolge eines verzögerten Business-Service. Jeder Tag, der auf Tests verwendet wird, ist ein Tag weniger, um Umsätze und Gewinne zu generieren. Wie hoch ist das Risiko, wenn der Service fehlschlägt, gegenüber dem Vorteil, den Service in Gang zu bringen?“

Mark Ernest, IBM Distinguished Engineer

Auf die Frage, wie sie den allgemeinen Ansatz ihrer Organisation zur Entschärfung des IT-Risikos beschreiben würden, beurteilten ihn 66 % der Befragten als gut bis ausgezeichnet. Auch wenn dies die Mehrheit der Unternehmen repräsentiert, bleiben immer noch mehr als 30 %, die ihr Geschäft auf diesem Gebiet als durchschnittlich bis schlecht einstufen. 72 % der Befragten meldeten allerdings, dass sich ihr Unternehmensansatz zum Risikomanagement über die letzten 12 Monate verbessert hat.

Wenig überraschend ist daher die Ansicht von 47 % der Befragten, die IT-Risikoplanung sei größtenteils eine abgesonderte Funktion, die in Geschäftssilos stattfindet. Verschiedene Bereiche der Organisation zur Zusammenarbeit zu bewegen erweist sich daher als schwierig. Eine weitere Erkenntnis: Viele der Befragten gaben zu, dass sie zwar sehr im den Bereichen Risikomanagement und Compliance aktiv sind, aber sich eigentlich noch mehr Beteiligung wünschen. (Während ungefähr die Hälfte der Befragten erklärte, dass ihr Unternehmen eine Risikomanagementabteilung hat, glauben viele, dass das Unternehmen die Mitarbeiter nicht ausreichend über die Risikomanagementpolitik und -besorgnisse informiert).

Positiv ist zu bemerken: Trotz schwieriger Wirtschaftslage blieben IT-Risikomanagement und Compliance weitgehend immun gegenüber Budgetkürzungen oder Kostenabbau. Nach dem Budget ihrer Organisation für Risikomanagement für das Jahr 2010 gefragt, erwarteten 14 % (80 Befragte) eine signifikante Zunahme der Mittel, 39 % rechnen mit einer leichten Zunahme. 36 % erklärten, dass die Finanzierung des Risikomanagements gleich bleiben werde.

Die Befragten sind sich einig, dass Investitionen in das IT-Risikomanagement signifikante Geschäftsvorteile bringen können, besonders im Bereich der Geschäftskontinuität (74 %) und der Sicherung des Unternehmensimage (32 %, siehe Abbildung 2). Den Befragten zufolge sollte das IT-Risikomanagement als eine eher defensive Taktik betrachtet werden; es kann die Flexibilität eines Unternehmens erhöhen (19 %), Wachstumschancen schaffen (12 %) und gleichzeitig die Kosten abbauen (18 %). Dennoch konzentrieren sich die meisten IT-Manager (57 %) weiterhin auf infrastrukturelle Risiken.

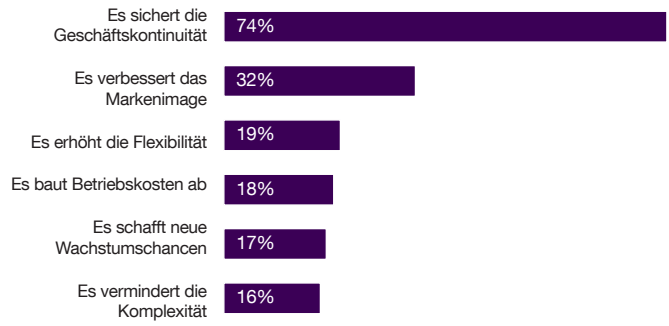

Abbildung 2: **Vorteile eines verbesserten IT-Risikomanagements**

Ganz oben auf der Liste: IT-Sicherheit

Auch wenn das IT-Risiko übergreifend Prozesse, Aktivitäten und Systeme betrifft, so ist die IT-Sicherheit (Schadenpotenzial durch Hacker und unerlaubter Zugriff auf / Nutzung von Unternehmenssystemen) das Hauptanliegen von 78 % der befragten IT-Professionals. Danach folgen Hardware- und Systemstörungen – genannt von 63 % der Befragten. Stromausfall und physische Sicherheit (40 %) lagen nicht weit zurück, gefolgt von Diebstahl, Produktqualität, Compliance, Naturkatastrophen, E-Discovery-Anfragen, Lieferkettenproblemen und Terrorismus, in dieser Reihenfolge.

IT-Manager haben klare Meinungen über die Bedeutung des Risikomanagments und spezifische Schwerpunktbereiche. Was jedoch das Vertrauen in die Fähigkeit ihrer Organisation betrifft, Risiken angemessen zu handhaben und darauf zu reagieren, waren noch erhebliche Lücken erkennbar. Zum Beispiel glauben nur 22 % der Befragten, dass ihre Organisationen im Hinblick auf IT-Sicherheit gut vorbereitet sind.

„Zur Geschäftskontinuität gehört weit mehr als nur ein Plan für Naturkatastrophen, zerstörerische Maßnahmen und Terroraktionen. Vielmehr geht es darum, eine risikobewusste Kultur zu schaffen und sicherzustellen, dass die nötigen Tools, Prozesse und Methoden bereitstehen und jedes Mitglied der Organisation seine Verantwortung für Datensicherheit und -integrität kennt. Bei der Implementierung der Tools und Prozesse ist es schließlich kritisch, ein Gleichgewicht zwischen Vermarktungsgeschwindigkeit und akzeptablem Risiko zu finden.“

Jessica Carroll, Geschäftsführender Direktor für IT-Technologie, US-Golfverband

23 % der Befragten denken dasselbe über die Bereitschaft ihres Unternehmens, für Hardware- und Systemausfälle gewappnet zu sein. Schutz gegen Stromausfälle fand mehr Unterstützung: 32 % der Befragten erklärten, dass ihr Unternehmen in diesem Bereich gut vorbereitet sei. Es besteht jedoch eine deutliche Trennung zwischen dem Bewusstsein, dass das IT-Risiko nie aus dem Auge gelassen werden darf, und dem Vertrauen in die Fähigkeit des Unternehmens, es gut in den Griff zu bekommen und zu entschärfen.

Fallstudie

In der ersten Jahreshälfte 2010 dokumentierte das IBM X-Force Forschungs- und Entwicklungsteam 4.396 neue Schwachstellen – ein Anstieg von 36 % gegenüber dem gleichen Vorjahreszeitraum. Dem Bericht zufolge bleiben die Schwachstellen von Web-Anwendungen die führende Bedrohung – sie machen über die Hälfte aller öffentlich bekannt gewordenen Gefahren aus. Derr Bericht stellte jedoch fest, dass Organisationen sich mehr denn je bemühen, Schwachstellen im Sicherheitsbereich zu identifizieren und offenzulegen. Diese Tatsache wiederum wirkt sich positiv auf die Branche aus, weil es zu einer offeneren Zusammenarbeit anregt, um Schwachstellen zu identifizieren und zu beseitigen, bevor sie durch Cyber-Kriminelle missbraucht werden können.[1]

Die Kommunikationsherausforderung

Es besteht kein Zweifel daran, dass IT-Risikomanagement echte Geschäftsvorteile schaffen kann. Aber ungeachtet der verschiedenen Methoden, mit denen Untenehmen risikobezogene Informationen verbreiten können, erwies sich die Kommunikation als echte Hemmschwelle. Die Sicherung der Unterstützung des Führungsstabs ist für 25 % der Befragten immer noch eine Herausforderung. Für 30 % der Befragten war auch die Kommunikation von Risikostrategien und -verfahren an die Mitarbeiter ein Problem.

Viele Organisationen befassen sich eher passiv als proaktiv mit IT-Risikomanagement und seiner Entschärfung. In vielen Fällen sind Informationen nur im Intranet der Organisation zu finden, wo die Mitarbeiter danach suchen müssen. Einige Organisationen integrieren Risikomanagementstrategien in Trainingsmaterial für neue Mitarbeiter, erkennen aber nicht, dass die gesamte Belegschaft über diese Strategien informiert werden sollte. (Nur 22 % der IT-Manager erklärten, dass Risikomanagementstrategien zur offiziellen Schulung aller Mitarbeiter gehören sollten.) Am meisten überrascht vielleicht Folgendes: Weniger als 15 % haben einen integrierten Risikomanagementplan in die physische und technische Infrastruktur ihres Unternehmens integriert.

„Wir tun uns schwer, Geschäftsleitung und Belegschaft davon zu überzeugen, dass sie ihr Verhalten ändern müssen, um sicherer zu arbeiten."

Befragter, Fertigungsindustrie, Westeuropa

„Es wird immer schwieriger, Finanzierung für die Bewältigung von IT-Risiken zu bekommen, auch wenn dem Führungsstab unmissverständlich erklärt wird, wie hoch die Kosten sind, wenn sie sich NICHT damit befassen. Oft ist man einfach nicht zu Investitionen bereit.“

Befragter, Luft-, Raumfahrt- und Verteidigungsindustrie, Nordamerika

Angesichts der Vielfalt der Kommunikations- und Bildungskanäle, die für eine Sensibilisierung der Risikoproblematik verfügbar sind, wären Unternehmen gut beraten, einen strukturierteren und detaillierteren Ansatz zu wählen, um Risikofragen in den Griff zu bekommen, den Mitarbeitern diese Anliegen zu vermitteln und das IT-Risikomanagement in alle Unternehmensbereiche zu integrieren. Auf die Frage, „Wie behält Ihr Unternehmen die Oberhand über das Risiko?“, antwortete die Mehrheit der Befragten, dass Sicherheitsgefahren durch interne wie auch externe Ressourcen (38 %), durch ein funktionsübergreifendes Team von Führungskräften (26 %) oder eine dedizierte Abteilung für Risikomanagement (19 %) behandelt werden.

„Normalerweise betrachten Nutzer, Management und Partner das Risiko aus unterschiedlichen Perspektiven. Ich muss versuchen, all diese Perspektiven sinnvoll unter einen Hut bringen.“

Befragter, Fertigungsindustrie, Westeuropa

Beurteilung neuer Technologien

Die Befragten wurden nach der Bereitschaft ihrer Organisation gefragt, fünf aufkommende Technologien zu erwerben und einzusetzen (siehe Abbildung 3):

- Soziale Netzwerktools (z. B. Intra- und Internet-Foren, Instant Messaging, Bibliotheken, Blogs und Wikis)
- Mobile Plattformen (Windows® Mobile, BlackBerry OS und Google Android OS, um nur drei zu nennen)
- Cloud Computing
- Virtualisierung
- Service-orientierte Architektur (SOA)

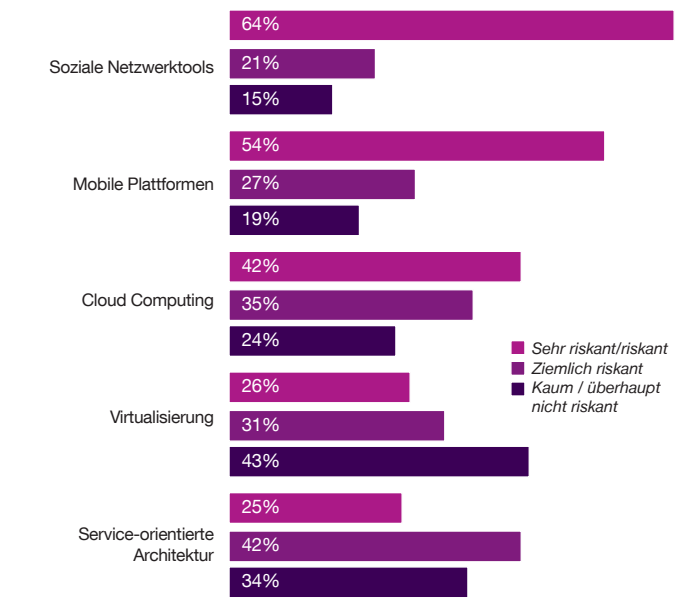

Abbildung 3: **Soziale Netzwerke, mobile Plattformen und Cloud Computing werden als die Technologien mit dem höchsten Risiko betrachtet.**

Von diesen fünf Technologien gaben soziale Netzwerke, mobile Plattformen und Cloud Computing den größten Anlass zur Besorgnis. 64 % der Befragten waren vor allem um die Risiken sozialer Netzwerktools besorgt, knapp dahinter lagen mobile Plattformen und Cloud Computing (54 % bzw. 43 %). Die meisten Risiken betreffen die Zugänglichkeit, Nutzung und Kontrolle von Daten, besonders bei den sozialen Netzwerken, und die Gefahr des unerlaubten Zugriffs auf vertrauliche firmeneigene Informationen. (Viele Organisationen verfügen noch nicht über etablierte Prozesse und Methoden, um soziale Netzwerktools in ihre Infrastruktur und Arbeitsabläufe zu integrieren).

Bei der Frage, die zwei höchsten Risiken zu nennen, die sie mit Cloud Computing verbinden, nannte die Mehrheit der Befragten den Datenschutz und die Privatsphäre (siehe Abbildung 4). Für mehr als die Hälfte der Befragten war es ganz klar die Geschäftskontinuität, während 44 % glauben, dass private Clouds riskanter sind als traditionelle IT-Dienste, und 77 % äußerten Besorgnis bezüglich der Privatsphäre.

„Cloud ist nur dann eine Möglichkeit zur Problemlösung, wenn man die besten Vorteile der Cloud nutzen kann. Deshalb muss dieser Faktor berücksichtigt werden."

Befragter, IT-Industrie, Nordamerika

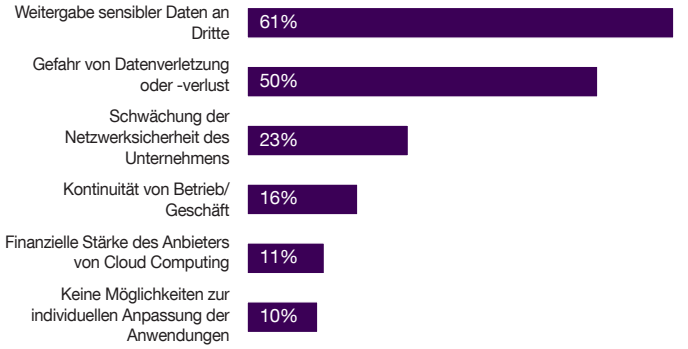

Abbildung 4: **Risken in Zusammenhang mit Cloud Computing.**

Daten an Dritte weiterzugeben hielten 61 % für riskant, während nur 23 % sich Sorgen um unerlaubte Zugriffe auf Netzwerke machten.

Lediglich 26 % der Befragten sehen Virtualisierung als ein erhebliches Risiko für ihre Organisation. Auch die Service-orientierte Architektur erregte nur bei 25 % Besorgnis.

Vertrauen auf die Cloud

IT-Manager spüren den Druck, unternehmensweit die Kosten für Infrastrukturen zu senken, die Effizienz zu steigern und das Serviceniveau zu verbessern. Viele denken, dass die Verlagerung von Datenspeichern ins Internet ihnen beim Erreichen dieser Ziele helfen kann. Ähnlich wie seine Vorgänger – Client/Server- und Mainframe-Computing – stellt Cloud Computing einen bedeutenden Fortschritt in Computing-Modellen dar. Die Verarbeitung erfolgt über ein verteiltes, global zugängliches Netzwerk von IT-Ressourcen, die den Service auf Anfrage bereitstellen. Cloud Computing bietet eine stark automatisierte, dynamische Alternative für den Erwerb und die Bereitstellung von IT-Diensten. Der Nutzer kann Rechenressourcen und -dienste aus öffentlichen, privaten und hybriden Clouds beziehen, ohne sich direkt mit der zugrunde liegenden Technologie befassen zu müssen. Unternehmen nutzen heute die enorme Skalierbarkeit und die Möglichkeiten der Zusammenarbeit, um Probleme in einer Weise zu lösen, wie es bislang nicht möglich war. Und sie entfalten neue Dienste schneller und ohne zusätzliche Kapitalinvestition. Dennoch müssen Organisationen bei der Wahl des Anbieters vorsichtig und informiert vorgehen, besonders angesichts der damit verbundenen Risiken.

Konsequenzen für IT-Manager

Von den befragten IT-Managern erwarten die meisten eine Zunahme ihrer Verantwortungen über die nächsten drei Jahre – von der Ausführung von Grundsätzen und Verfahren und Mithilfe bei der Strategieformulierung für die Entschärfung der Risiken bis hin zur Hilfe bei der Einrichtung und/oder Überwachung der IT-Risikostrategien für die Organisation (siehe Abbildung 5). Über 65 % der Befragten waren sich einig, dass Risikoentschärfung mehr in ihre Arbeit integriert wird, während 83 % glauben, dass IT-Manager sich mehr an der Risikoentschärfung beteiligen sollten.

Angesichts der zunehmenden Verflechtung von Geschäftsabläufen und Rechnungswesen überraschen diese Antworten nicht. Tatsächlich glaubten die befragten IT-Manager und CIOs, dass zu ihren Aufgaben die Unterstützung der allgemeinen Geschäftsstrategie sowie des Markennamens gehören wird (z. B. bei Marketing und Kundendienst). Da immer mehr Unternehmen ihre Strategien, Prozesse und Verfahren in Bezug auf das Risikomanagement stabilisieren oder „festigen“, wird die Verantwortung für die Infrastruktur eventuell zu einem Lieferanten oder Partner verlagert. Dann können IT-Manager sich wieder mehr auf die Sicherheit, die Resilienz und die Kontinuität des Geschäfts konzentrieren.

Ein Vergleich der Daten von den 131 befragten CIOs lieferte die interessante Beobachtung, dass es keine signifikanten Abweichungen zu den befragten IT-Managern gab.

Die Signifikanz von IT-Risikomanagement und Regelüberwachung wird industrieweit von den Organisationen anerkannt, und viele arbeiten an einer Verbesserung dieser Aspekte ihres Geschäfts. Trotzdem sind nur wenige auf alle eventuell entstehenden Situationen im Zusammenhang mit Risiko und Compliance völlig vorbereitet.

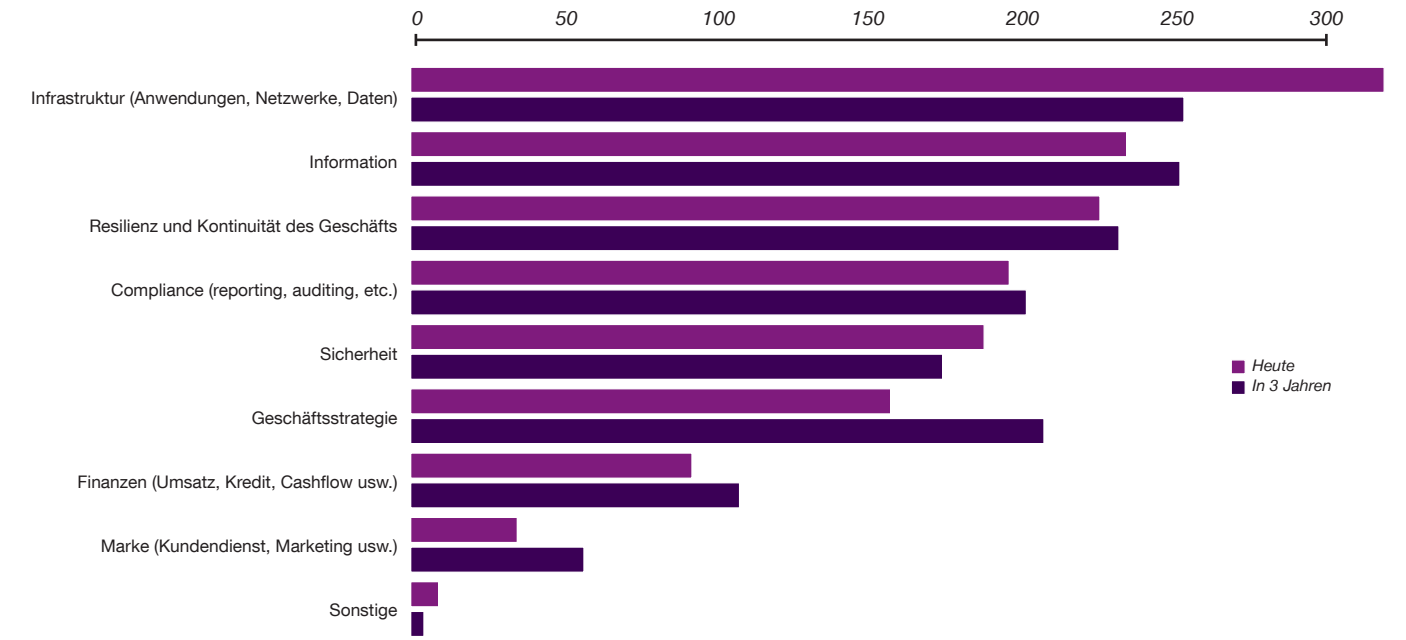

Abbildung 5: **IT-Manager erwarten, dass sich ihre Verantwortungsbereiche in den nächsten drei Jahren verlagern werden.**

Die Ergebnisse der Globalen IT-Risikostudie 2010 von IBM zeigten Schwerpunkte auf, die IT-Managern helfen können, ihre Risikoreife zu beurteilen, Lücken zu erkennen, Prioritäten festzulegen und Strategien in mehreren Bereichen zu entwickeln:

- Innerhalb eines Unternehmens ist jeder für die Risikosensibilisierung verantwortlich. Aber wenn in der Unternehmenskultur keine Risikostrategien und -verfahren verwurzelt sind, könne viele Initiativen für die Handhabung und Entschärfung von IT-Risiken unzulänglich sein oder völlig scheitern. Die Ergebnisse der Studie bestätigen, dass Unternehmen die Initiativen für Risikomanagement und Compliance unternehmensweit besser vermitteln, kommunizieren und unterstützen müssen.
- Daten sind ein gemeinsames Anliegen in allen Aspekten des IT-Risikomanagements, von Sicherheit, Geschäftsresilienz und -kontinuität bis hin zu Verfügbarkeit, Notfallwiederherstellung, Hackern, Compliance, Infrastruktur und Datenmanagement. Deshalb sollten Unternehmen sich dem IT-Management mit einem einheitlichen, holistischen Ansatz nähern. Dabei müssen alle Elemente berücksichtigt werden, um die allgemeinen Ziele von Umsatz- und Effizienzsteigerungen zu erreichen.

- Bei der Annahme neuer Technologien, Architekturen und Strategien, der Entwicklung neuer Anwendungen oder der Integration existierender Systeme muss Risikoentschärfung ein obligatorisches Gesprächsthema sein. Die Berücksichtigung des positiven Risikos (das ein Unternehmen auslöst, weil sich eine Gelegenheit bietet, die mit dem Risiko verbunden ist) und des negativen Risikos (potenzielle Vorfälle, die dem Geschäft schaden können) können mehr Geschäftswert schaffen und eventuell sogar den Umsatz steigern, aber nur, wenn eine entsprechende Finanzierung des IT-Risikomanagements einbezogen wird.

  Nicht alle neuen Technologien sind gleich. Aber einige, wie z. B. Virtualisierung und Cloud Computing, können in Bezug auf Unterstützung und Optionen für Risikoentschärfung viele Vorteile bieten. Zwar muss beim Cloud Computing auf die Datensicherheit geachtet werden, aber bei korrekter Entfaltung kann es dazu beitragen, Kosten abzubauen und die Risiken im Zusammenhang mit der Geschäftsresilienz abzuschwächen. Es ist jedoch unabdingbar, über Prozesse zu verfügen, um die Risiken zu handhaben, die mit jeder neuen Technologie verbunden sind.

„Mitunter sehen wir einen Projektplan zu vereinfacht. Wir glauben zu wissen, wo die Risiken liegen und teilen die Ressourcen auf dieser Grundlage zu.“

Befragter, IT- und Technologieindustrie, Naher Osten und Afrika

Nach dort von hier

Effizientes IT-Risikomanagement ist ein vielschichtiges Unterfangen. Bei ihrem Ansatz müssen IT-Manager Folgendes berücksichtigen:

Die IT-Risikofähigkeit der Organisation untersuchen und beurteilen

- Eine unternehmensweite Planung für alle Risikokategorien (Daten, Sicherheit, Resilienz, Notfallwiederherstellung und neue Technologien) einführen..
- Den Umfang der Risikoherausforderungen berücksichtigen und bestätigen, dass ein Plan zur Bewältigung der Risiken vorliegt (z. B. die „Nachteile“ des Risikos priorisieren und entschärfen, beispielsweise Systemausfälle und Sicherheitsverstöße), und überprüfen, wie man die „Vorteile“ des Risikos (z. B. kürzere Vermarktungszeit und neue Kundenkontakte) nutzen kann.

Champions im Führungsstab suchen

- Ein zuverlässiger Berater und eine wertvolle Ressource für den CIO werden; auf die Vorteile hinweisen, die sie und andere Führungskräfte für die Handhabung des IT-Risikos bringen.
- Die Vorteile der Risikoentschärfung „verkaufen“, z. B. mehr Geschäftswachstum, mehr Flexibilität und bessere Markenbekanntheit.

Entscheiden, wie man das Risikobewusstsein auf allen Ebenen und innerhalb der Organisationskultur erhöht

- Das Risikobewusstsein in das Alltagsgeschäft und die IT-Prozesse einbauen. Sicherstellen, dass verschiedene Methoden verfügbar sind, um das ganze Unternehmen diesbezüglich aufzuklären.
- Eine Strategie erstellen, um regelmäßig die Breite des Risikomanagements sowie Fragen zum Thema Compliance zu kommunizieren. Dabei muss betont werden, dass es sich um mehr als nur eine „einmalige“ Aktivität handelt.

Innovative Wege suchen, um Verfahren zur Risikoentschärfung zu implementieren

- Risikoverfahren in die IT-Infrastruktur integrieren, statt sie stückweise zu Anwendungen hinzuzufügen.
- Geschäftsprozesse auf potenzielle Risiken untersuchen und einen spezifischen IT-Risikosteuerungsplan einrichten, der organisationsweit ausgeführt werden kann.

Sicherstellen, dass Schutzmaßnahmen vorhanden sind, um unbefugten Zugriff auf Unternehmensdaten und -systeme zu verhindern

- Geschäftskontinuitätspläne überprüfen. Bei der Geschäftskontinuität geht es um mehr als die Planung für eine Naturkatastrophe; sie umfasst ein breites Spektrum an Szenarien für Geschäftsunterbrechung, von Serverausfällen bis hin zu Pandemien.
- Jedem seine Verantwortung für Datensicherheit und -schutz bewusst machen und ihm erklären, wie er seine Verantwortung wahrnehmen muss.
- Tools, Prozesse und Methodologien für die Datensicherheit identifizieren. Berücksichtigen, dass viele vielleicht schon existieren (Identitätszugriff und -kontrolle; Masterdatenmanagement; Management des Lebenszyklus von Informationen; Dateneigentümerschaftsprozesse).

Die Frage lautet nicht länger, ob neue Technologien in eine Organisation eingeführt werden, sondern wann. Wie zuvor schon erwähnt, sind nicht alle neuen Technologien gleich, aber einige können signifikante Vorteile für das IT-Risikomanagement mit sich bringen. Neuere Technologien wie Virtualisierung und Cloud Computing bieten eindrucksvolle Optionen für die Risikoentschärfung und den Kostenabbau.

Sind Sie bereit?

- **Wie beurteilt Ihr Unternehmen seine Risikoreife, und wie handhabt es seine Risiken, im geschäftlichen Bereich wie auch in Bezug auf IT-Infrastruktur und Vermögenswerte?**
- **Welche Strategien hat Ihre Organisation eingerichtet, um den Erfolgsmethoden aus Industrie und IT zur Entschärfung von Risiken zu folgen, angefangen von der Sicherheit bis hin zur Resilienz und Geschäftskontinuität?**
- **Wie verbessern die Risikoinitiativen Ihres Unternehmens die Transparenz und Kontrolle und gewährleisten die Einhaltung von Vertragsbedingungen, Industriestandards, Vorschriften und internen Kontrollen?**
- **Wie unterstützt Ihre IT-Infrastruktur die aktuellen Leistungsziele des Unternehmens hinsichtlich Flexibilität, Sicherheit, Verfügbarkeit, Betriebsführung, Skalierbarkeit und Resilienz?**
- **Welchen Plan hat Ihre Organisation um sicherzustellen, dass Humanressourcen, Prozesse und Systeme in der Lage sind, auf einen Störfall zu reagieren und sich davon zu erholen?**

Eine energische, zyklische IT-Risikosteuerung – von Technologie- und Geschäftsperspektiven – untersucht permanent die Anfälligkeit des Unternehmens für IT-Risiken, priorisiert diese Risiken und handelt entsprechend. Folglich ist es wichtig, Risikomanagementprotokolle in neue Technologien zu integrieren, sobald diese implementiert werden.

Abschließend sind die Bedürfnisse des Unternehmens beim Implementieren von Tools und Prozessen zu berücksichtigen. Vermarktungsgeschwindigkeit und akzeptables Risiko müssen ausgewogen sein. Durch einen proaktiven Ansatz zum IT-Risikomanagement können Unternehmen den Schwachstellen immer einen Schritt voraus sein, und sie sind gegen geplante oder ungeplante Vorfälle besser abgesichert und resilienter.

Für mehr Informationen

Um mehr über diese Studie des IBM Institute for Business Value zu erfahren, kontaktieren Sie uns bitte *über iibv@us.ibm.com.* Einen kompletten Katalog unserer Forschungsarbeiten finden Sie unter:

ibm.com/iibv

Zugriff auf weitere IT-Risikomanagementressourcen erhalten Sie unter:

ibm.com/smarterplanet/security

Autoren

Linda Ban ist die CxO Studienprogrammdirektorin und AIS Lead für das IBM Institute for Business Value. In dieser Position leitet sie das globale Team, das für die Entwicklung, Entfaltung und Unterstützung der Denkansätze von IBM im Rahmen des CIO-Programms verantwortlich ist, sowie die AIS (Application Innovation Services)-Organisation von IBM. Durch ihre vielseitige Berufslaufbahn verfügt Linda über umfassende Erfahrung mit neuen und kollaborativen Technologien, Geschäfts- und Betriebsstrategie, Systementwicklung und Betriebsmanagement. Zusätzlich zu ihrer Arbeit mit Kunden gibt es von ihr viele Publikationen zu den verschiedensten Geschäftsthemen, -herausforderungen und -lösungen. Sie erreichen Linda unter *lban@us.ibm.com*.

Richard Cocchiara ist ein IBM Distinguished Engineer und der Chief Technology Officer für Business Continuity und Resiliency Services bei IBM Global Services. Er verfügt über 28 Jahre I/S-Erfahrung und wurde von vielen Fortune-500-Unternehmen als Berater engagiert, insbesondere im Finanz- und Wertpapierbereich. Zur Zeit ist Rich verantwortlich für die Forschung und Entwicklung von Lösungen und Diensten für Geschäftskontinuität und -resilienz innerhalb der IBM Global Technology Services. Sie erreichen ihn unter *rmcocch@us.ibm.com*.

Kristin Lovejoy ist als Vizepräsidentin für die Sicherheitsstrategie von IBM verantwortlich. Sie wurde 2005 von InfoWorld zu den Top 25 CTOs nominiert, und 2006 zählte Security Magazine sie zu den 25 einflussreichsten Sicherheits-Executives. Sie ist Inhaberin von US- und EU-Patenten für Object Oriented Risk Management Model and Methodology (Modell und Methodologie für objektorientiertes Risikomanagement). Kristin erreichen Sie unter *klovejoy@us.ibm.com*.

Ric Telford ist Vizepräsident von IBM Cloud Services und verantwortlich für die Definition neuer Geschäftschancen und Services im Rahmen des breit gefächerten IBM-Portfolios an Cloud-Computing-Angeboten. Während seiner Beschäftigung bei IBM war Ric Telford maßgeblich an verschiedenen Software- und Serviceinitiativen für das Unternehmen beteiligt, darunter Dokumentmanagement, Netzwerke, Systemmanagement und IT-Infrastrukturdienste. Zuvor war Ric VP von Autonomic Computing, wo er die Entwicklung von autonomeren Systemen leitete. Ric erreichen Sie unter *rtelford@us.ibm.com*.

Mark Ernest ist ein IBM Distinguished Engineer und Mitglied der IBM Academy of Technology. Er unterstützt Kunden beim Entwurf und der Implementierung von IT-Managementsystemen, um den Wert ihrer IT-Investitionen zu maximieren und für eine bessere Effizienz ihrer Nutzung von Informationstechnologie zu sorgen. Mark erreichen Sie unter *lernest@us.ibm.com*.

Der richtige Partner für eine Welt im Wandel

Bei IBM arbeiten wir gemeinsam mit unseren Kunden daran, Geschäftseinblicke, moderne Forschung und Technologie zusammenzubringen, um unseren Kunden einen eindeutigen Vorteil angesichts der schnellen Veränderungen in der Geschäftsumgebung zu verschaffen. Durch unseren integrierten Ansatz zu Geschäftsdesign und -ausführung helfen wir, Strategien umzusetzen. Und mit Know-how in 17 Branchen und globalen Fähigkeiten in 170 Ländern können wir unseren Kunden helfen, Wandel und Gewinne durch neue Chancen zu antizipieren.

Literaturnachweis

1 The IBM X-Force 2010 Mid-Year Trend and Risk Report. IBM Corporation, 2010.

IBM United Kingdom Limited
Postfach 41
Portsmouth
PO6 3AU
Großbritannien

IBM Ireland Limited
Oldbrook House
24-32 Pembroke Road
Dublin 4
Irland

IBM Ireland Limited ist in Irland unter der Unternehmensnummer 16226 eingetragen.

Die IBM-Homepage finden Sie auf ibm.com.

Bitte recyceln Sie.

GBE03365-DEDE-00