www.pwc.co.uk

Die wachsende Dringlichkeit des Datenmanagements im europäischen Mittelstandsmarkt

Eine Studie über Standpunkte, Verhaltensweisen und Best Practice in europäischen Unternehmen unter Berücksichtigung eines aktualisierten Informationsrisiko-Index.

Eine Studie herausgegeben von PwC in Zusammenarbeit mit Iron Mountain
Juni 2013

pwc

Inhaltsverzeichnis

Vorwort

Christian Toon, Head of Information Risk, Iron Mountain Europe

Auf Navigationskurs durch die Informationslandschaft

Die europäische Informationslandschaft ist nicht mehr wiederzuerkennen. Europaweit gibt es keine Branche, die sich ohne Schwierigkeiten an diese Veränderungen anpassen kann. Viele sind sich unsicher, wie die rasant steigenden, mehrformatigen Datenmengen untergebracht werden können oder wie mit der Explosion der sozialen Medien umgegangen werden soll. Der Wildwuchs mobiler Geräte, die Änderungen bei Gesetzgebungen und die Zunahme von Schadprogrammen lassen weitere Ungewissheiten aufkommen. Gleichzeitig zeichnet sich eine zunehmende Ambition ab, den Vorteil, der sich aus strukturierten und unstrukturierten Informationen ziehen lässt, gezielt zu nutzen. Der Umgang mit Informationen ist heute somit so komplex wie nie zuvor – und eine höhere Komplexität bedeutet häufig auch ein höheres Risiko.

Iron Mountain und PwC haben aus diesem Grund eine Studie durchgeführt, in der die aktuelle Lage der Informationsrisiken, denen Mittelstandsunternehmen in Europa ausgesetzt sind, untersucht wird. Hierbei handelt es sich um den zweiten Vergleichsindex zum Thema Informationsrisiko. Die Prüfung der vorliegenden Daten stimmt insofern zuversichtlich, als dass sie eine positive Entwicklung in den letzten 15 Monaten zu erkennen gibt. Das Bewusstsein für Informationsrisiken steigt: Alle untersuchten Unternehmen erzielten einen höheren Indexwert. Der Durchschnittswert der europäischen Firmen stieg von 40,6 Punkten im Vorjahr auf 56,8 Punkte. Ingesamt können maximal 100 Punkte erreicht werden. Unsere Studie legt nahe, dass das wachsende Bewusstsein gleichzeitig zu Unsicherheit führt. Unternehmen wissen zwar, dass sie handeln müssen, sind sich aber weiterhin unklar darüber, an wen sie sich wenden können oder was sie als Nächstes tun sollen.

Die Fortschritte bei der Bewusstseinsschaffung müssen nun in strategisches Vorgehen und eine Reihe von Maßnahmen umgesetzt werden, damit das Risikopotenzial reduziert werden kann. Das erfordert jedoch die Überzeugung und Mitwirkung der obersten Geschäftsebene. Die für das Informationsmanagement zuständigen Personen müssen sich mit der Sprache der Chefetage vertraut machen und in einen Dialog mit anderen wichtigen Stakeholdern treten. Einbußen bei der Kundentreue, Rufschädigung und sinkende Verkaufs- und Umsatzzahlen sind die zentralen Probleme, mit denen sich die mit dem Informationsmanagement Beauftragten befassen müssen – und dies muss der Chefetage klar und deutlich vermittelt werden. Es ist jedoch offensichtlich, dass ein wirklicher Fortschritt nur dann erreicht werden kann, wenn Unternehmen über die Reputations- und Kundenloyalitätsrisiken hinaus auch die Chancen und Vorteile erkennen, die durch die richtige Handhabung von Informationen als Wirtschaftsgut erschlossen werden können.

Ziel dieser Publikation ist es, den Umfang und die Komplexität des bestehenden Problems aufzuzeigen und europäischen Unternehmen zugleich eine nützliche Informationsquelle zu bieten. Der Risikoindex und das Online-Tool zur Risikobewertung www.ironmountain.co.uk/risk-assessment sollen Unternehmen die Informationen an die Hand geben, die sie auf ihrem Weg zu einem verantwortungsbewussten Umgang mit Daten benötigen. Dieser Bericht enthält eine Reihe von Maßnahmen, mit denen Unternehmen ihre Vorgehensweise beim Management von Informationsrisiken verbessern und so das Gefahrenpotenzial reduzieren können. Auch sollen sie Unternehmen dabei unterstützen, die Vorteile ihrer Informationen voll auszuschöpfen.

Kurzfassung

„Einfach ausgedrückt, die europäischen Mittelstands-unternehmen messen ihren Informationen nur eine untergeordnete Bedeutung zu oder sehen nicht den wirtschaftlichen Wert dahinter.“

Claire Reid, Partner, PwC Information Security

Unternehmen können mit der Verwaltung ihrer Informationen kaum Schritt halten. Das setzt sie einem ungeahnten Gefahrenpotenzial aus: Betrug, Datenlecks und Social-Media-Desaster – diese Vorfälle ereignen sich schneller, als Unternehmen darauf reagieren können. Europas Mittelstandsunternehmen sind diesen Gefahren in besonderem Maße ausgesetzt, und trotzdem gehen sie weiterhin selbstgefällig mit ihren Praktiken beim Datenmanagement um. Unsere Studie zeigt, dass die Unsicherheit darüber, welche Schritte als Nächstes unternommen werden sollten, den Mittelstand beim Schutz seiner Firmen und der gewinnbringenden Nutzung von Informationen hindert.

Wichtige Erkenntnisse aus der Studie:

Die Bewusstseinsschaffung ist nicht mehr das Problem. Laut unserer Studie sind sich die Mittelstandsunternehmen der Gefahr, die hinter potenziellen Informationsrisiken steckt, zunehmend bewusst, und sie wissen, dass in dieser Hinsicht Handlungsbedarf besteht.

- Der diesjährige durchschnittliche Indexwert liegt bei 56,8 von 100 möglichen Punkten. Im Vergleich zum Vorjahr, in dem der Wert noch bei 40,6 lag und nur wenige Unternehmen ihre Daten in zufriedenstellendem Maße verwalteten, handelt es sich hierbei um einen Schritt nach vorn. Trotz der Fortschritte ist der erzielte Wert niedrig und es ist noch ein langer Weg zurückzulegen, bevor die Praktiken beim Datenmanagement ein vertretbares Niveau erreichen.

- 68% der befragten Unternehmen vertreten die Ansicht, dass ein verantwortungsvoller Umgang mit Informationen von wesentlicher Bedeutung für den Unternehmenserfolg ist. Informationen, d. h. Kunden- und interne Daten in Papier- und digitaler Form, werden als wertvolles Gut betrachtet, und ein guter Umgang damit kann bisher ungenutzte wirtschaftliche Potenziale freilegen (und eventuelle Katastrophen vermeiden).

- Die Studienergebnisse deuten darauf hin, dass Unternehmen entweder nicht genau wissen, welche nächsten Schritte unternommen werden sollen, oder weiterhin nur unzureichend ausgestattet sind, um Bedrohungen einzudämmen. Nur 45% der Unternehmen verfügen über eine Informationsrisiko-Strategie, deren Wirksamkeit kontrolliert wird, während 44% der Befragten davon ausgeht, dass das Risiko von Datenpannen steigen wird.

Das Informationsmanagement als Herausforderung:

Unsere Studie zeigt, dass viele Unternehmen vor einer zunehmenden Datenflut aus nicht-kategorisierten Daten in Papier- und digitaler Form stehen und nicht wissen, was sie damit tun sollen. Das bedeutet, dass vertrauliche und sensible Daten somit einem höheren Risiko eines Datenlecks ausgesetzt sind.

- 36% der Unternehmen bewahren ihre kompletten Informationen für den Fall auf, dass sie diese nochmals benötigen.

- 42% der befragten Unternehmen sind um die Sicherheit ihres Datenbestands besorgt.

In mittelständischen Firmen zeichnet sich ein Bild der Verwirrung, Widersprüchlichkeit und Nachlässigkeit im Umgang mit Informationsrisiken ab. Die Kluft zwischen Einstellung und Handlung wird zunehmend größer.

„93% der Unternehmen, die über 250 Mitarbeiter beschäftigen, haben im vergangenen Jahr eine Datenpanne erlebt. Die durchschnittlichen Kosten betrugen in schweren Fällen zwischen 450.000 und 850.000 £ pro Panne.“

Quelle: PwC Information Security Breaches Survey 2013

- 78% glauben, dass alles daran gesetzt werden müsse, um Datenpannen zu vermeiden. Beunruhigende 47% geben an, dass der Datenschutz vom Vorstand nicht als wichtige Angelegenheit erachtet wird.
- Mittelstandsunternehmen erwarten von ihren Zulieferern die höchsten Sicherheitsstandards. Nur 14% der Befragten würden mit einem Unternehmen zusammenarbeiten, das zuvor eine Datenpanne erlebt hat. Bei sich selbst legen sie jedoch nicht die gleichen Maßstäbe an.
- Der mittleren und unteren Führungsebene sowie dem Support-Personal wird ein hohes Maß an Vertrauen beigemessen – wirksame, überwachte Richtlinien und Kontrollen für den Schutz von Daten sind dagegen Mangelware. Bei 58% der Unternehmen gibt es beispielsweise keine Überwachung der Kontrollsysteme für den Zugang zu Informationen.

In diesem Bericht befassen wir uns in erster Linie mit den Denk- und Verhaltensweisen, die sich aus der Studie ableiten lassen. Wir heben einige wesentliche Faktoren hervor, die mittelständische Unternehmen daran hindern, ihr volles Potenzial auszuschöpfen.

Bewährte Praktiken zur Reduzierung von Informationsrisiken:

Aufbauend auf der letztjährigen Studie haben wir eine Reihe von Schritten und Maßnahmen ausgearbeitet, die Mittelstandsunternehmen dabei unterstützen sollen, wirkliche Fortschritte zu erzielen und die wirtschaftlichen Vorteile zu nutzen, die sich aus dem Schutz und der Wertschätzung der bedeutendsten Wirtschaftsgüter im Unternehmen – Informationen in Papier- und digitaler Form - ergeben. Diese Maßnahmen umfassen:

- **Oberste Führungsebene einbeziehen** – Suchen Sie die Unterstützung der Vorstandsetage und gehen Sie das Informationsmanagement dabei strategisch an.
- **Informationen im Griff haben** – Seien Sie im Bilde darüber, welche Informationen Sie haben, wo sie sind und ob Sie sie noch benötigen.
- **Mitarbeiter überzeugen**– Schaffen Sie ein Klima des Vertrauens, das durch eine Reihe von Überwachungsinstrumenten, -richtlinien und -verfahren untermauert wird.

Der heutige Stand der Informationsrisiken

Die Botschaft ist eindeutig: Jedes Unternehmen, das Informationen verwaltet – unabhängig von Größe und Branche – ist potenziell gefährdet. In einer Zeit, in der Datenpannen, Cyber-Angriffe und Social-Media-Desaster einen historischen Höchststand verbuchen, sehen sich Unternehmen einem beispiellosen Gefährdungspotenzial ausgesetzt. Dennoch lassen Mittelstandsunternehmen ihre Türen weiterhin für die möglichen irreparablen Schäden eines Datenlecks sperrangelweit offen stehen.

Nachlässigkeit, widersprüchliche Verhaltensweisen, schlechte Praktiken beim Datenmanagement und die fehlende Wertschätzung von Informationen setzen Unternehmen nicht nur einem Risiko aus, sondern hindern sie zudem dabei, ihr wirtschaftliches Potenzial voll auszuschöpfen. Es ist belegt, dass Unternehmen, die eine Datenpanne erlitten haben, Vertrauenseinbußen hinnehmen mussten. Hingegen haben Firmen, die Ihre Daten nachweislich sicher im Griff haben, einen klaren Wettbewerbsvorteil.

Unsere jüngste Forschungsstudie, die von Iron Mountain in Auftrag gegeben wurde, belegt, dass Mittelstandsunternehmen beim sicheren Umgang mit Daten noch immer Defizite haben. Zwar haben die europäischen Mittelstandsunternehmen hinsichtlich ihrer Praktiken im Datenmanagement nachweislich Fortschritte gemacht; der schlechte Umgang mit Daten ist jedoch noch immer weit verbreitet. Im Rahmen seiner jährlichen Studien hat PwC eine zweite Umfrage bei 600 mittelständischen Unternehmen (d. h. Firmen mit 250 - 2.500 Mitarbeitern) in sechs europäischen Ländern durchgeführt: Großbritannien, Frankreich, Deutschland, Niederlande, Spanien und Ungarn. Diese Studie baut auf den Ergebnissen des Vorjahresberichts „Bedrohungen im Netz als Herausforderung“ auf. Dieser Bericht aus dem Jahr 2012 stellt den ersten Informationsrisiko-Index Europas vor und weist darauf hin, dass Mittelstandsunternehmen zukünftig viel besser für den Umgang mit Informationsrisiken gerüstet sein müssen.

Der Index für das Jahr 2013 zeigt, dass sich die Praktiken mittelständischer Unternehmen im Bereich Informationssicherheit verbessert haben. Gleichzeitig weist der erreichte Indexwert von 56,8 Punkten jedoch darauf hin, dass Unternehmen das Ziel noch lange nicht erreicht haben.

Informationsrisiko-Index „Farbcodes“

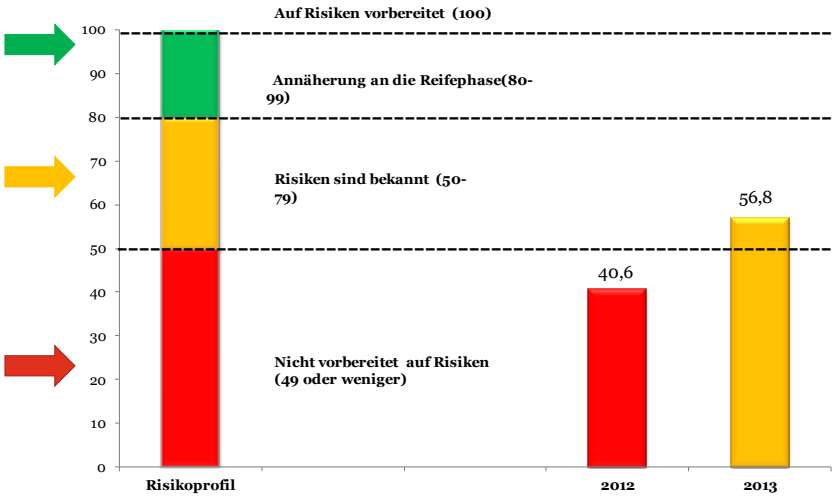
Auf Risiken vorbereitet
Unternehmen verfügen über ein verantwortungsvolles Konzept, das folgende Punkte umfasst: Strategie, Mitarbeiter, Kommunikation und Sicherheit von oben nach unten. Das Konzept für den Umgang mit potenziellen Risiken wird effektiv überwacht, bewertet und verbessert.

Annäherung an die Reifephase
Die Unternehmen haben einige Maßnahmen eingeführt, und die oberste Führungsetage hat ein besseres Verständnis der Risiken. Sie haben das Risikopotenzial reduziert, konnten dafür aber bisher noch keine solide Strategie durchsetzen.

Risiken sind bekannt
Den Unternehmen ist inzwischen bewusst geworden, dass ein Risikomanagement erforderlich ist. Sie wissen jedoch nicht genau, was zu tun ist, oder sind nach wie vor nur unzureichend ausgestattet, um die Gefahr einzudämmen.

Nicht vorbereitet auf Risiken
Unternehmen sind Informationsrisiken in schwerwiegendem Maße ausgesetzt. Eine Informationsrisiko-Strategie ist aller Wahrscheinlichkeit nicht vorhanden und die oberste Management-Ebene ist sich der potenziellen Folgen für das Unternehmen nicht bewusst.

Informationsrisiko-Index 2012-2013



Grundlage:600

Nachlässigkeit im Mittelstandsmarkt besteht weiter…

Nur 45% verfügen über eine Informationsrisiko-Strategie und überwachen deren Wirksamkeit.

Nur 38% haben einen formellen Business Recovery Plan.

Nur 32% überwachen die Wirksamkeit ihres Risikoregisters.

Nur 28% führen Mitarbeiterkommunikationsprogramme durch und werten diese aus, um ihre Informationsrisikoverfahren zu optimieren.

Nur 45% überwachen die Effektivität des für den Bereich Informationsrisiko zuständigen Teams.

Nur 39% überwachen die Effektivität ihrer Datenklassifikation.

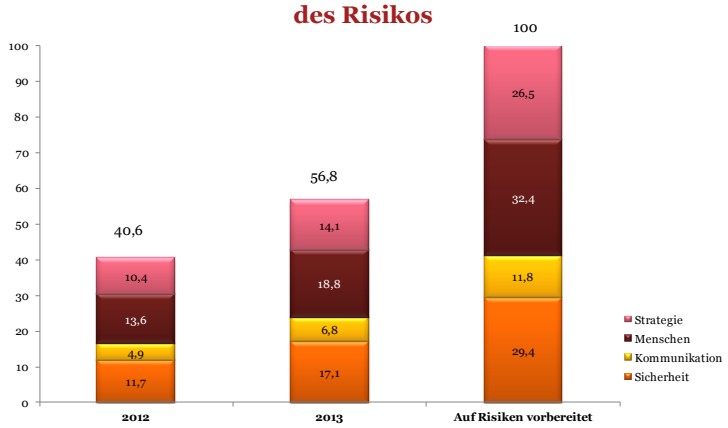
Nur 26% ermitteln die Rendite ihrer Ausgaben für Informationssicherheit.

„Unternehmen müssen umdenken. Eine neue Denkweise ist gefordert, bei der Informationssicherheit als Mittel zum Datenschutz und als Möglichkeit zur Wertschöpfung für das Unternehmen gesehen wird.“

PwC Global State of Information Security Survey 2013

Die Mittelstandsunternehmen haben den Gefahrenbereich verlassen. Dennoch sollten sie die möglichen Risiken nicht auf die leichte Schulter nehmen. In einer Welt, in der die tägliche Wahrscheinlichkeit eines Datenlecks exponentiell steigt, benötigen Unternehmen bessere Pläne, um sich schützen zu können. Es gibt keinen Grund, warum sich nicht alle Mittelstandsunternehmen die Erreichung der maximalen Punktzahl von 100 zum Ziel setzen sollten. Denn das würde bedeuten, dass sie für den Eintritt von Risiken gerüstet sind.

Informationsrisiko-Index 2012 und 2013 – analysiert nach Art des Risikos



Grundlage:600

Um 100 Punkte zu erreichen, müssen Unternehmen die in unserem Index dargelegten 34 Maßnahmen (siehe Anhang) umgesetzt haben und deren Wirksamkeit prüfen. Keine dieser Maßnahmen ist unseres Erachtens schwierig durchzuführen oder zu überwachen, und dennoch zeigt unsere Studie, dass mittelständische Unternehmen noch einen langen Weg vor sich haben. Auch scheinen sie unsicher zu sein, wie sie dabei weiter vorgehen sollen.

Ein positiver Trend ist, dass mittelständische Unternehmen inzwischen viel genauer auf die Überwachung der Wirksamkeit ihrer Informationsmanagementpraktiken achten, insbesondere was den Bereich der Datensicherheit betrifft. Ferner rückt der Themenschwerpunkt Mitarbeiter immer weiter in den Mittelpunkt. Insgesamt gesehen besteht jedoch bei etwa der Hälfte der in unserer Studie untersuchten Unternehmen ein erheblicher Verbesserungsbedarf, hinsichtlich derPraktiken im Umgang mit Informationen betrifft.

Wesentliche Studienergebnisse

55% der französischen Firmen haben eine überwachte Informationsrisiko-Strategie. In Großbritannien verfügen dagegen 34% und im Gesamtdurchschnitt 45% der Unternehmen über eine solche Strategie.

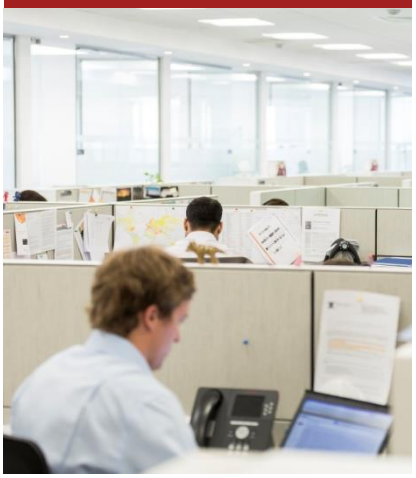
40% der niederländischen und 38% der ungarischen Firmen verfügen über ein überwachtes Risikoregister, im Vergleich zu 21% in Deutschland und 32% im Gesamtdurchschnitt.

52% der niederländischen Firmen haben eine Strategie zur sicheren Entsorgung von Hardware und vertraulichen Unterlagen. Lediglich 26% der spanischen und 41% der Unternehmen insgesamt haben eine solche Strategie implementiert.

61% der ungarischen und 59% der niederländischen Firmen haben klare Mitarbeiterleitlinien zur sicheren Entsorgung von Dokumenten in Papierform. In Spanien verfügen dagegen 36% und im Länderdurchschnitt 50% der Unternehmen über solche Leitlinien.

35% der Rechtsanwaltskanzleien haben eine überwachte Strategie für Informationsrisiken. In der Versicherungsbranche haben dagegen 55% und im Gesamtdurchschnitt 45% eine derartige Strategie.

54% der in Produktion und Technik tätigen Unternehmen und 34% der Rechtsanwaltskanzleien verfügen über ein spezielles Team für Informationsrisiken. Insgesamt haben 45% der Unternehmen ein solches Team.



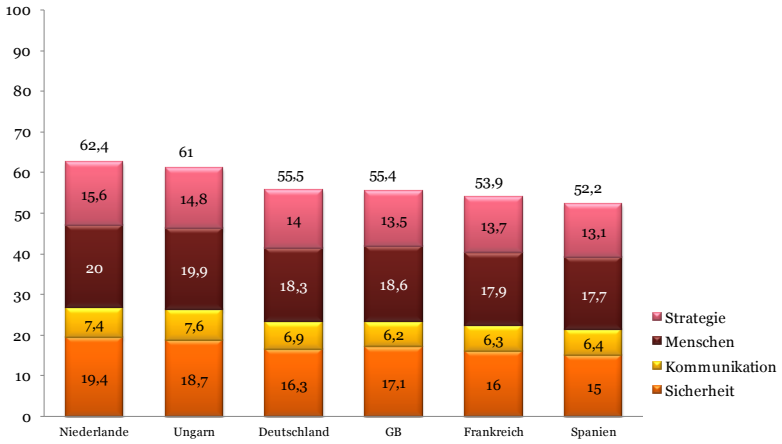
Verbesserungsbedarf besteht hauptsächlich im Bereich der strategischen Ausrichtung auf das Informationsmanagement. Mehr als die Hälfte der Mittelstandsunternehmen überprüft die Wirksamkeit ihrer Informationsrisiko-Strategie nicht – sofern eine solche überhaupt vorhanden ist.

Es ist von entscheidender Bedeutung, dass der Mittelstandsmarkt kurzfristig erkennt, dass Informationen ein entscheidendes strategisches Gut für Unternehmen sind, die daher entsprechend behandelt und berücksichtigt werden müssen. Gerade in Zeiten der wirtschaftlichen Rezession ist dies besonders wichtig. Mehr Leistungen mit weniger Mitteln zu erbringen, heißt vor allem auch, klüger vorzugehen – und nicht nur härter zu arbeiten. Die erfolgreichsten Unternehmen erreichen dies nicht nur, indem sie Informationen als Wirtschaftsgut erschließen und verwerten, sondern auch, indem sie diesem Wirtschaftsgut einen Wert beimessen. Sie haben begriffen, dass man nur auf die Dinge wirklich achtgibt, die man zu schätzen weiß.

Länderspezifische Unterschiede

Die Niederlande und Ungarn haben mit jeweils 62,4 und 61,0 Punkten den höchsten Indexwert erreicht. Die Niederlande machten dabei im Vergleich zum Vorjahr deutliche Fortschritte.

Informationsrisiko-Index 2013 – analysiert nach Land



Grundlage:600

Unter den sechs Ländern, die an der Studie teilnahmen, hoben sich die Niederlande beim strategischen Umgang mit Informationsrisiken klar von den anderen ab. So verfügen niederländische Unternehmen im Vergleich zu denen der anderen Länder eher über einen Notfallplan für kleinere Datenpannen, ein Risikoregister, eine Sicherheitsstrategie für Mobiltelefone, personalisierte Geräte und Laptops sowie eine Strategie zur sicheren Entsorgung von Hardware und vertraulichen Unterlagen. Ferner tendieren die Niederländer und die Franzosen eher dazu, das Thema Informationsrisiko als Vorstandsangelegenheit zu behandeln.

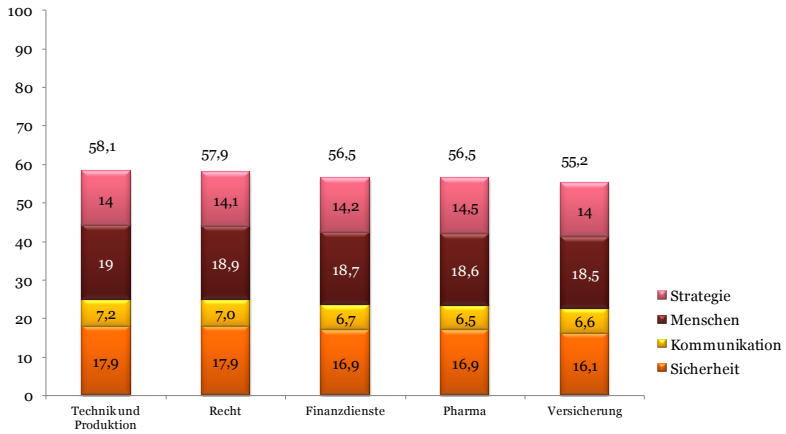
In Ungarn ließen sich wesentliche Fortschritte in den Bereichen Mitarbeiterschulung und Kommunikation beobachten. Dabei stellen Vorgaben zur Aufbewahrung und Entsorgung von elektronischen und in Papierform vorliegenden Dokumenten einen besonders wichtigen Schwerpunkt dar.

Im Gegensatz dazu weist Spanien mit 52,2 Punkten den niedrigsten Indexwert auf. Interessanterweise tendieren die spanischen Unternehmen am wenigsten dazu, in ihren Mitarbeitern eine Gefahr für die Informationssicherheit zu sehen. Gleichzeitig hinken sie ihren europäischen Nachbarn bei der Bereitstellung von Mitarbeiterleitlinien in Bezug auf interne Richtlinien und Verfahren hinterher. Zudem verfügen sie seltener über grundlegende Sicherheitsmaßnahmen wie etwa Due-Diligence-Programme zum Umgang mit Kunden-, Mitarbeiter- oder persönlichen Daten oder Angriffserkennungssysteme und anerkannte Datenklassifizierungssysteme.

Branchenspezifische Unterschiede

Betrachtet man die fünf Branchen, die in unserer Studie näher untersucht wurden, so lässt sich feststellen, dass alle einen Schritt nach vorne gemacht haben und jetzt einen ähnlichen Reifegrad aufweisen. Dennoch befinden sie sich noch immer im unteren Teil des „gelben“ Bereichs.

Informationsrisiko-Index 2013 – analysiert nach Branche



Grundlage:600

Die Branchen Recht, Produktion und Technik haben seit 2012 die deutlichsten Fortschritte gemacht. Es gibt Hinweise darauf, dass Unternehmen aus der Produktions- und Technikbranche zunehmend nach einem strategischeren Konzept verfahren: Mehr Unternehmen haben nun eine Informationsrisiko-Strategie und einen formellen Business Recovery Plan umgesetzt. Zudem tendiert diese Branche im Gegensatz zu den anderen eher dazu, ihre Mitarbeiter als Gefahr für die Informationssicherheit zu betrachten. Im Vergleich zum Vorjahr hat die Produktions- und Technikbranche überdies ihren Schwerpunkt stärker auf Personal- und Kommunikationsmaßnahmen gelegt.

Die Juristik-Branche verzeichnete in fast allen der 34 Maßnahmen Fortschritte. Gleichwohl neigt sie im Gegensatz zu den anderen am ehesten dazu, keine Strategie für Informationsrisiken oder ein spezielles Team bzw. eine Einzelperson mit Zuständigkeit für den Bereich Informationsrisiko zu haben.

Informationsrisiko-Index Länder-Ranking:2012 – 2013

Land	2012	2013
Niederlande	**Platz 5**	**Platz 1**
Ungarn	**Platz 1**	**Platz 2**
Deutschland	**Platz 4**	**Platz 3**
GB	**Platz 6**	**Platz 4**
Frankreich	**Platz 3**	**Platz 5**
Spanien	**Platz 2**	**Platz 6**

Die Notwendigkeit einer effektiven Verwaltung der zunehmenden Datenflut

„In der heutigen hybriden Informationswelt aus Print- und Digitalmedien drohen Unternehmen im Sumpf der Komplexität und Verwirrung zu versinken, sofern Sie nicht Herr der Lage der Verwaltung Ihrer Daten werden. *Ein verantwortungsvoller und rechenschaftspflichtiger Umgang mit Daten ist entscheidend, wenn Unternehmen die Vorteile aus diesem wichtigen Wirtschaftsgut schöpfen wollen.Diese Verfahrensweise ist für Unternehmen von zentraler Bedeutung, wenn sie ihre hart erarbeitete Reputation und Kundentreue verdienen und beibehalten möchten.“*

Christian Toon
Head of Information Risk
Iron Mountain

„Stündlich wird eine Datenmenge im Internet übertragen, mit der man 7 Millionen DVDs beschreiben könnte.Übereinander-gestapelt würden sie 95 Mal so hoch sein wie der Mount Everest.“

Aus einer IMS-Studie für IBM, 2013

Viele mittelständische Unternehmen verlieren in einer Flut aus unstrukturierten Daten nach und nach den Überblick. Sie wissen nicht, was sie damit tun sollen. Die Datenflut ist das Ergebnis fehlender Richtlinien, Prozesse oder Technologien, mit denen sich Informationen kategorisieren lassen und ermittelt werden kann, welche Daten aufzubewahren oder zu vernichten sind und nach welcher Aufbewahrungsmethode vorgegangen werden soll. Viele Unternehmen bewahren daher all ihre digitalen und in Papierform vorliegenden Informationen auf. Dies führt dazu, dass Mitarbeiter oder Auftragnehmer Zugriff auf große vertrauliche und sensible Datenbestände haben, was wiederum die Wahrscheinlichkeit eines Datenlecks erhöht.

Mehr als ein Drittel der in unserer Studie untersuchten Unternehmen bewahren all ihre Informationen für den Fall auf, dass sie diese später noch einmal benötigen. Ein weiteres Drittel lässt sich erst rechtlich beraten, bevor eine Entscheidung bezüglich der Daten getroffen wird. Es ist allgemein bekannt, dass die Menge an Daten in digitaler und in Papierform Jahr für Jahr exponentiell in die Höhe schnellt. Wenn Unternehmen also weiterhin alles aufbewahren, müssen sie bei der Pflege ihres wachsenden Datenbestands neben hohen Kosten auch mit möglichen Risiken für das Unternehmen rechnen. Verdeutlichen wir dieses Argument an einem Beispiel: Bestimmte Unterlagen müssen nach einer gesetzlich vorgesehenen Aufbewahrungsfrist sicher vernichtet werden. Für Unternehmen, die sich nicht daran halten, kann das Geldstrafen und Rufschäden nach sich ziehen. Darüber hinaus sorgen sich viele Unternehmen um die Sicherheit ihrer hinterlegten Daten. Datenlecks lassen sich selbstverständlich nur dann vermeiden, wenn der Zugriff auf hinterlegte Daten entsprechend verwaltet und kontrolliert wird.

Die Zunahme digitaler Daten in den verschiedensten per Fernzugriff abrufbaren Formaten, einschließlich der steigenden Zahl von Shared-Data-Anbietern, schafft außerdem ein Umfeld, in dem Mittelstandsunternehmen nur schwer die Datenkette kontrollieren können. Entscheidende Geschäftsinformationen stehen nun größeren Personengruppen in diversen Formaten zur Verfügung – auf Papier oder elektronisch – was die Wahrscheinlichkeit der Gefahr eines Datenlecks nochmals erhöht.

Je mehr Informationen ein Unternehmen aufbewahrt, desto größer die Wahrscheinlichkeit, dass sie in die Hände unkritischer, neugieriger, ungeschulter, verärgerter oder böswilliger Mitarbeiter geraten. Wie bereits in unserer Publikation *„Bedrohungen im Netz als Herausforderung“* erwähnt, geht die größte Bedrohung für die Unversehrtheit von Informationen am Arbeitsplatz vom Verhalten und der Einstellung der Mitarbeiter aus. Unternehmen, die vor einem wachsenden Berg aus unkategorisierten Daten stehen, verschärfen diese Gefahr bis ins Unermessliche.

„90% der Daten auf der Welt, wurden in den letzten zwei Jahren erstellt.“

IBM Understanding Big Data - IBM Big Data Platform

„75% der Arbeitgeber in Großbritannien gaben an, sie hätten kein durchsetzbares System, um Mitarbeiter vom unbefugten Zugriff auf Unternehmensdaten abzuhalten.“

Insider Threat Survey, LogRhythm, Großbritannien April 2013

Selbst die Spitzenreiter – Unternehmen, die bei Informationssicherheit führend sind – haben Schwierigkeiten mit der Aufbewahrung von Daten. Unsere Studie zeigt, dass sie genauso wie die anderen Firmen dazu neigen, für den Fall der Fälle alle Informationen aufzubewahren.

Im Ländervergleich hat Frankreich den größten Datenberg: 50% der Unternehmen in unserer Studie heben all ihre Daten auf. Spanische Firmen haben dagegen den niedrigsten Bestand an aufgehobenen Daten und greifen bei der Datenaufbewahrung eher auf ein Drittunternehmen zurück.

Hierbei handelt es sich nicht um unbekümmerte Unwissenheit, sondern vielmehr um die Ratlosigkeit darüber, was zu tun ist. Auf die Frage, worin die Unternehmen ihre größte Herausforderung für die Zukunft sehen, gaben 41% an, dass ihnen die Verwaltung ihres alten Datenbestands Sorgen bereite. Dieser Meinung sind insbesondere Unternehmen in Deutschland und Ungarn sowie die Juristik-Branche quer durch Europa: Nahezu 50% der von uns befragten Firmen sehen die Verwaltung ihrer Papierdokumente als eine anspruchsvolle Aufgabe. Eine weitere Schwierigkeit, mit der sich der Mittelstandsmarkt konfrontiert sieht, ist die Sicherheit hinterlegter Daten. 42% der Unternehmen sehen darin ein Problem. In Frankreich sind es sogar 48% und im Versicherungssektor 52%.

Neben der Förderung der richtigen Verhaltensweisen von Mitarbeitern müssen sich mittelständische Unternehmen auch ihrer Datenflut stellen, bevor es zu spät ist. Das Vertrautmachen mit Gesetzen und Leitlinien zur Datenaufbewahrung ist dabei von zentraler Bedeutung. Die Klassifizierung und sichere Hinterlegung von Daten, die aufbewahrt werden müssen, sowie die sichere Vernichtung unnötiger Informationen ist ein Muss. Unternehmen müssen jetzt handeln, bevor die Datenflut aus dem Ruder läuft und irgendwann ein Leck bekommt.

Wesentliche Studienergebnisse

36% bewahren all ihre Informationen für den Fall auf, dass sie gebraucht werden.

31% nehmen rechtliche Beratung zur Datenaufbewahrung in Anspruch, bevor Maßnahmen ergriffen werden.

41% betrachten die „Verwaltung ihrer Papier-Altlasten“ als eine große Herausforderung für die Zukunft.

42% machen sich Sorgen über die Sicherheit ihres Datenbestands.

61% überwachen die Effektivität ihrer ggf. bestehenden Datenklassifizierungssysteme nicht.

Die Pflicht zur Aufklärung von Mitarbeitern: Kann man sich auf das Vertraute verlassen?

Wesentliche Studienergebnisse

Nur 14% würden Geschäfte mit einem Unternehmen tätigen, bei dem es schon einmal eine Datenpanne gab.

Nur 25% betrachten Mitarbeiter als ernste Gefahr für die Informationssicherheit.

82% vertrauen darauf, dass ihre Mitarbeiter die Richtlinien für Informationsrisiken befolgen.

45% überwachen nicht die Social-Media-Nutzung der Mitarbeiter.

Fallstudie

Ein Pilotprojekt der Polizei im britischen Kent, bei dem erstmalig eine Jugendpolizeisprecherin ernannt werden sollte, schlug auf eindrucksvolle Weise fehl, als Einzelheiten über das Social-Media-Account des Teenagers bekannt wurden. Die 17-jährige Paris Brown wurde aus über 160 Bewerbern ausgewählt, um als „Stimme der Jugend“ die Polizei zu beraten. Später stellte sich jedoch heraus, dass sie einige Monate zuvor auf ihrem Twitter-Konto rassistische, homophobische und obszöne Kommentare veröffentlicht hatte. Ein Sprecher der Polizei gestand, dass die Social-Media-Konten der Jugendlichen vor ihrem Amtsantritt nicht überprüft worden waren.

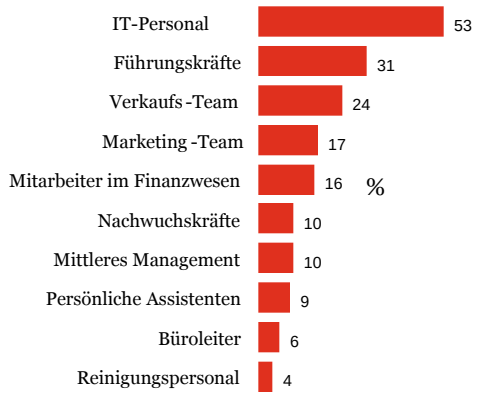
In mittelständischen Unternehmen zeichnen sich Verwirrung und Widersprüchlichkeiten beim Umgang mit Informationsrisiken ab. Aus unserer Studie geht hervor, dass der Großteil (58%) der Befragten keine Geschäfte mit einem Unternehmen tätigen würde, bei dem es schon einmal zu einem Datenleck kam. Viele Firmen schaffen es aber selber nicht, ihr eigenes Datenrisiko einzudämmen. Da nur 45% eine überwachte Strategie für Informationsrisiken in ihrem Unternehmen verankert haben, weist dies im Grunde auf eine Doppelmoral hin: wachsam nach außen, nachlässig im Inneren.

Mittelstandsunternehmen müssen damit beginnen, die Maßstäbe, die sie von ihren Lieferanten und Auftragnehmern verlangen, auch bei sich selbst anzulegen. Sie erkennen nicht, dass ihre eigenen Kunden dieselbe Auffassung haben könnten und Aufträge zurückhalten, falls es zu einer Datenpanne kommt.

Im Vorjahresbericht *Bedrohungen im Netz als Herausforderung* wurde darauf hingewiesen, dass in der Unternehmenskultur und im Mitarbeiterverhalten ein Richtungswechsel erforderlich ist, um die vorhandenen Datenbestände der europäischen Mittelstandsunternehmen schützen zu können. Die diesjährige Studie macht deutlich, dass sich die Unternehmen der Folgen einer Datenpanne auf ihr Geschäft zwar durchaus bewusst sind, sich aber weiterhin im Wissen um das Risiko aus den eigenen Reihen unbekümmert zeigen. 25% der von uns befragten Unternehmen sind der Meinung, dass Mitarbeiter eine ernste Gefahr für die Informationssicherheit sind. Gleichwohl vertrauen 82% darauf, dass sich ihre Mitarbeiter an die Richtlinien für Informationsrisiken (sofern diese überhaupt vorhanden sind) halten.

Die Unternehmen geben weiter an, dass die Verantwortung für ihre Informationen – und somit auch für das Informationsrisiko – hauptsächlich in den Händen des IT-Sicherheitsmanagers liegt. Auf die Frage, von wem ihrer Ansicht nach die größte Gefahr eines Datenlecks ausgehe, gaben paradoxerweise über die Hälfte die IT-Abteilung an. Es ist nachvollziehbar, dass Personen, die für höchst sensible und vertrauliche Daten die größte Verantwortung tragen und auf diese einen umfassenden Zugriff haben, als größte Gefahr angesehen werden.

Von wem geht Ihrer Meinung nach die größte Gefahr eines Datenlecks aus?



Grundlage: 600
Mehrfachantworten

„80% der Arbeitgeber in Großbritannien gaben an, dass ihre Mitarbeiter ihrer Ansicht nach keine vertraulichen Informationen entwenden würden. Eine Umfrage unter Arbeitnehmern zeigte jedoch, dass 23% schon einmal auf vertrauliche Daten zugegriffen bzw. von ihrem Arbeitsplatz mitgenommen haben."

Insider Threat Survey, LogRhythm, Großbritannien, April 2013

Laut unserer Studie werden das mittlere Management, Nachwuchskräfte, persönliche Assistenten und das Reinigungspersonal als die Mitarbeitergruppen mit dem geringsten Gefahrenpotenzial hinsichtlich der Verursachung einer Datenpanne wahrgenommen, was vermutlich auf ihren relativ eingeschränkten Datenzugriff zurückzuführen ist. Allerdings haben selbst die vertrauenswürdigsten Mitarbeiter das Potenzial, Fehler zu machen. Dennoch verfügen viele Unternehmen über keine Kontrollen, die sie vor einfachem menschlichen Versagen schützen. So überwachen beispielsweise 61% der von uns befragten Unternehmen nicht die Wirksamkeit ihrer Datenklassifikationssysteme und 58% haben entweder keine Kontrollsysteme für den Zugang zu Unternehmensarchiven und anderen sensiblen Informationen oder werten diese Systeme nicht aus.

Ferner gibt es in vielen Mittelstandsunternehmen keine Verfahren zur Überprüfung von Mitarbeitern: Weniger als 50% prüfen Arbeitszeugnisse und lediglich 40% holen polizeiliche Auskünfte oder Führungszeugnisse ein. Überdies prüfen nur wenige Firmen die öffentlichen und leicht zugänglichen Informationen auf Social-Media-Websites wie Twitter. Es scheint, als würden mittelständische Unternehmen Personen, die sie kaum kennen, sehr viel Vertrauen schenken. Viele Unternehmen zeigen zudem nur wenig Einsatz, ihre Mitarbeiter hinsichtlich datenrelevanter Richtlinien und Verfahren (sofern es diese gibt) zu informieren und zu schulen. Stattdessen setzen sie ein hohes Maß an Vertrauen in ihre Mitarbeiter.

Vertrauen in die Belegschaft zu haben, kann eine gute Sache sein. Das Problem besteht jedoch darin, dass viele der Datenlecks, die sich bis heute ereignet haben, durch menschliches Versagen verursacht wurden. Damit also Informationen vor vorsätzlichen Verstößen und Irrtümern geschützt werden können, ist es wichtig, nach einer Politik des kontrollierten Vertrauens zu verfahren und angemessene Richtlinien, Schulungen, Kommunikationsmaßnahmen und Sicherheitskontrollen im Einsatz zu haben.

In einer Welt mit starker Social-Media-Präsenz, in der zudem 88% der Verbraucher dasselbe mobile Gerät für berufliche als auch private Zwecke nutzen (Quelle: PwC), ist das Gefahrenpotenzial enorm, und es gibt viele prominente Beispiele, die dies belegen.

Der durchschnittliche Datendieb ist:

- *Ein aktueller Mitarbeiter*
- *Männlich*
- *37 Jahre*

In etwa der Hälfte der untersuchten Fälle haben Mitarbeiter Geschäftsgeheimnisse entwendet, gefolgt von Geschäftsinformationen (Rechnungsdaten oder Preislisten), und in 75% der Fälle hatten sie befugten Zugriff auf die Daten, die sie gestohlen haben.

Insider Data Theft: When Good Employees Go Bad
Symantec, Dezember 2011

Der Wert der Informationen

Die Geschäftswelt hat sich verändert. Unternehmen aller Länder und Branchen tauschen nun routinemäßig Informationen über Unternehmensgrenzen hinweg aus, ganz gleich, ob dies zwischen Geschäftspartnern oder den personalisierten Geräten der Mitarbeiter geschieht.Diese Herausforderung betrifft nicht mehr nur die IT-Abteilung. Unternehmensleiter müssen sicherstellen, dass sie das schützen, was für das Wachstum und den Ruf ihres Geschäfts am wichtigsten ist.

Andrew Miller, PwC Information Security Director

Wesentliche Studienergebnisse

59% sind der Ansicht, die Kosten eines wirksamen Datenschutzes übertreffen die Risiken bzw. stünden nicht im Verhältnis zum Aufwand.

54% vertreten die Auffassung, die Geschwindigkeit des Wandels sei so schnell, dass sie niemals damit mithalten können.

Informationen sind ein strategisches Wirtschaftsgut. Behandelt man sie als solches, kann dies die Aussichten auf eine Vielzahl kommerzieller Vorteile verbessern und nicht zuletzt einen starken Wettbewerbsvorteil schaffen. Zwar geht der Großteil der mittelständischen Unternehmen davon aus, dass der Umgang mit Informationen als Wirtschaftsgut „der nächste große Trend“ sein wird, die Daten zeigen jedoch, dass nur sehr wenige sich dieses Ziel auf die Fahnen geschrieben haben.

Mittelstandsunternehmen sind sich der Konsequenzen eines Datenlecks nur allzu bewusst. 75% sind der Ansicht, dass sich eine Datenpanne nachteilig auf Kundenvertrauen und Kundentreue auswirken würde. Die Tatsache, dass die meisten Unternehmen in unserer Studie einer Firma, die ein Datenleck erlitten hat, nicht trauen würden, verdeutlicht diesen Standpunkt. Rund die Hälfte der Unternehmen glauben, dass ein Datenleck ihrer Reputation schaden und zu Umsatzeinbußen führen könnte.

Welche Folgen würde ein Datenleck Ihrer Meinung nach für Ihr Unternehmen haben?

Hauptmotivation für den besseren Umgang mit Informationen ist für Unternehmen eindeutig die Kundenbindung und nicht die Einhaltung von Regeln.

„Wir haben mehr als 15 Jahre und über 100 Mio. £ in die Entwicklung bürstenloser Hochgeschwindigkeitsmotoren für unsere Staubsauger und Airblade-Händetrockner gesteckt.Wir fordern die sofortige Rückgabe unseres geistigen Eigentums.“Gerichtsakten von Dyson zu einer Rechtssache im Zusammenhang mit Betriebsspionage. Oktober 2012

.

Mitglieder des britischen Civil Service Sport Clubs, mit landesweit 130.000 Niederlassungen, wurden darüber informiert, dass ihr Name, ihre Anschrift, ihr Geburtsdatum und ihre Sozialversicherungsnummern aus einer zentralen Computerdatenbank gestohlen wurden. Die Daten wurden anschließend missbräuchlich verwendet.

Daily Telegraph 27.11.2012

Wir wissen, dass Nachlässigkeit ein großes Problem darstellt, aber gibt es noch etwas anderes, was Unternehmen zurückhält? Unsere Studie legt nahe, dass europäische Mittelstandsunternehmen vor allem mit den strategischen Aspekten des Informationsmanagements zu kämpfen haben. Sie sorgen sich zudem um Kosten und fühlen sich mit der Geschwindigkeit der Veränderungen überfordert.

Nur eine Minderheit der Unternehmen nähert sich ansatzweise dem Ziel, Informationen als Wirtschaftsgut zu behandeln. Noch weniger schreiben ihnen überhaupt einen Wert zu. Der Großteil (74%) ermittelt nicht die Rendite der Ausgaben für Informationssicherheit bzw. weiß nicht, wie diese zu ermitteln ist. Viele der befragten Unternehmen haben nicht das Können und die Fähigkeiten, um ihr Informationsgut angemessen verwalten zu können, und 35% sehen darin eine Herausforderung. Mitarbeiter, die nicht wissen, wie etwas zu erledigen ist, erledigen es selten gut.

Die Erkenntnisse aus dieser Studie werden durch wissenschaftliche Untersuchungen gestützt, die zeigen, dass der Wert von Informationen im Vergleich zu Sachgütern, sowohl absolut als auch relativ gesehen, von Unternehmen durchweg unterschätzt wird. Aus diesem Grund müssen Unternehmen (a) Zeit und Geld in die Entwicklung von wirksam integrierten und überwachten Informationsmanagementprogrammen investieren und (b) ihre Prioritäten neu gewichten, indem sie Informationen nicht nur als Kosten- oder Risikofaktor, sondern vielmehr als Geschäftswert betrachten.

Einführung bewährter Praktiken

„Übertragene und ruhende Daten können nur durch eine zentrale Strategie zur Informationssicherheit geschützt werden, bei der Gefahrenpotenziale für das Unternehmen erkannt werden und ein vielschichtiges Überwachungssystem für die Sicherheit von Daten über den gesamten Lebenszyklus hinweg implementiert wird.“

Claire Reid
PwC Information Security Partner

Die in diesem Bericht dargelegten Ergebnisse sind Herausforderungen, die in der gesamten Geschäftswelt verbreitet sind. Erfreulicherweise finden Sicherheitsexperten immer wieder Lösungen und Maßnahmen, mit denen das Risiko eines Informationsverlustes reduziert werden kann. Die hier aufgezeigten Maßnahmen zählen unseres Erachtens zu den effektivsten, um gute Resultate zu erlangen.

Schritt 1: Oberste Führungsebene einbeziehen

Suchen Sie die Unterstützung der Vorstandsetage und gehen Sie das Informationsmanagement dabei strategisch an.

- Entwickeln Sie eine effektive Informationsrisiko-Strategie und überwachen Sie deren Wirksamkeit. Gehen Sie bei der Entwicklung einer Strategie strukturiert vor:
    - Ermitteln Sie, wie Daten in internen und externen Netzwerken gespeichert, übertragen und entsorgt werden.
    - Bestimmen Sie die Technologien, Prozesse und Mitarbeiterkontrollen, die für das Informationsmanagement je nach Lebenszyklusphase erforderlich sind.
    - Entwickeln und implementieren Sie Kontrollen anhand der Grundprinzipien für die Sicherheit, Widerstandsfähigkeit und Verlässlichkeit von Informationen.
    - Verankern Sie im gesamten Unternehmen eine Kultur des verantwortungsbewussten Umgangs mit Informationen. Kooperieren Sie mit der Personalabteilung, deren Mitarbeiter bei der Eindämmung von Informationsrisiken eine führende Rolle einnehmen.
    - Vergessen Sie nicht Ihre Papierunterlagen: Einfache Schritte, wie die Klassifikation von Dokumenten, eine sichere Aufbewahrung der Unterlagen und zugängliche Aktenvernichter, helfen dabei, die Unternehmenskultur zu prägen, um diesen Richtungswechsel zu erreichen.
- Setzen Sie die Informationssicherheit auf die Tagesordnung des Vorstands. Beeinflussen Sie die Tagesordnung, indem Sie sich in die Lage der Vorstandsmitglieder versetzen und herausfinden, was ihnen wichtig ist. Es besteht eine Verbindung zwischen kontinuierlicher Kundentreue und der Wahrnehmung, wie Unternehmen Kundendaten verwalten und schützen. Wenn die Geschäftsleitung Mitarbeitern hinsichtlich Verhaltens- und Vorgehensweisen Orientierungshilfen bietet, kann dies wirtschaftliche Vorteile schaffen, sofern die Umsetzung und Überwachung effektiv abläuft.
- Betrachten Sie Ihre Daten als wirtschaftliches Gut und vermitteln Sie dies Ihren Mitarbeitern: Nehmen Sie es in die Bilanz auf oder lassen Sie sich beraten, wie die Rendite gemessen an den Ausgaben für Informationssicherheit ermittelt werden kann. Finden Sie heraus, wie viel es kosten würde, wenn Sie Ihre Daten ersetzen müssten.
- Schaffen Sie eine Unternehmenskultur, bei der Ihre Mitarbeiter eine gemeinsame Verantwortung für das Informationsmanagement tragen. Stellen Sie dabei sicher, dass Ihre Mitarbeiter wissen, dass auch sie eine persönliche Verantwortung tragen.

Schritt 2: Informationen im Griff haben

Seien Sie im Bilde darüber, welche Informationen Sie haben, wo sie sind und ob Sie sie noch benötigen.

- Schnell könnte man meinen, die gespeicherten Daten seien lediglich elektronische Informationen. Dabei sollte jedoch nicht vergessen werden, wie man mit Unterlagen in Papierform und anderen verwendeten Formaten verfährt.
- Ermitteln Sie Befürworter in der Geschäftsleitung (Business Sponsors), die sich für den verantwortungsbewussten Umgang mit Informationen in den genannten Formaten unternehmensweit stark machen.
- Bestimmen Sie, was Sie haben: elektronische Speicherkapazitäten je nach Dateityp oder Datenbank, Anzahl der Unterlagen in Papierform bzw. Multimediadaten. Gliedern Sie dies idealerweise nach Geschäftsfunktion oder -art auf.
- Finden Sie heraus, wo sich die Daten befinden. Werden sie im Unternehmen, bei einem Dritten, in Ihrem Land oder außerhalb der EU aufbewahrt?
- Sie sollten ermitteln, was Sie haben und wo es sich befindet. Das zeigt Ihnen die Prioritäten beim Risiko- und Kostenmanagement auf.
- Entwickeln und vermitteln Sie ein Verfahren für Information-Governance, das folgende Punkte umfasst: Datenklassifizierung, Speicherprotokoll, Verhältnisse der Datenverarbeitung, Regeln zur Datenaufbewahrung oder -überprüfung und Back-up.
- Die Aufbewahrungsfristen von Informationen sind für das Kosten- und Compliance-Management entscheidend. Behalten Sie nichts länger, als es sein muss.
- Sobald Sie eine Richtlinie zur Klassifizierung haben, sollten Sie ein Zugriffskontrollsystem für sensible Informationen und Übertragungsbeschränkungen für große Datenmengen einführen.
- Berufen Sie eine Übergangsphase ein, damit interne Mitarbeiter sich umgewöhnen können und das Information-Governance-Modell befolgen. Das bedeutet, dass Mitarbeiter Daten entweder auf entsprechend dafür vorgesehenen Servern speichern oder dezentrale Daten, die nicht weiter gebraucht werden, löschen.
- Belohnen Sie positives Verhalten und sprechen Sie Defizite beim Informationsmanagement offen an.
- Lassen Sie Ihr Information-Governance-Modell von Ihren Business Sponsoren überwachen und prüfen.

Schritt 3: Mitarbeiter überzeugen

Schaffen Sie ein Klima des kontrollierten Vertrauens.

- Es ist wichtig – und auch von Vorteil – wenn Geschäftsführer ihren Mitarbeitern vertrauen. Angesichts der stetig wachsenden Bedrohungen (sowohl vorsätzliche als auch unbeabsichtigte) muss dieses Vertrauen jedoch in einem kontrollierten Rahmen definiert werden.
- Das lässt sich mithilfe eines festgelegten Überwachungsinstrumentariums sowie mit Richtlinien und Verfahren erreichen, die das übergeordnete Vertrauen untermauern und komplettieren.
- Entwickeln Sie klare Mitarbeiterrichtlinien für die Nutzung von Social Media und führen Sie ein Schulungsprogramm dazu durch.
- Fördern Sie Social-Media-Nutzung durch angemessene Kanäle, einschließlich klarer Anweisungen dazu, was gesagt werden kann und was nicht.
- Legen Sie konkret fest, was Mitarbeiter posten können und was nicht. Vorgaben wie „unangemessene Kommentare sind nicht gestattet“ sind zu vage. Weisen Sie Ihre Mitarbeiter darauf hin, dass Firmennamen, spezifische Projekte und Personen nicht erwähnt werden dürfen.
- Ermutigen und befähigen Sie Mitarbeiter, „Botschafter“ des Unternehmens zu werden, indem sie positive Kommentare über Ihre Firma als Arbeitsplatz auf ihren persönlichen Social-Media-Seiten schreiben.
- Führen Sie kontrollierte interne Monitoring-Übungen durch, um zu ermitteln, wie sich die Mitarbeiter bei einer potenziellen Sicherheitsbedrohung verhalten.
- Vermitteln Sie den Zweck und die Art der Monitoring-Übungen und nutzen Sie diese als Gelegenheit, Ihre Mitarbeiter hinsichtlich angemessener Verhaltensweisen bei einer Datenpanne zu schulen.
- Gehen Sie beim Entwurf, Erstellen und Speichern von vertraulichen Daten disziplinierter vor. Kennzeichnen Sie beispielsweise vertrauliche Dokumente als solche und verfassen Hauptdokumente sowie Dokumentvorlagen in einem Format, das erkennbar macht, wenn sie aus dem Unternehmen entfernt werden (mit entsprechenden Abwehrtools für Datenverlust).
- Kontrollieren Sie den E-Mail-Verkehr, der an private E-Mail-Adressen geht, indem Sie Kontrollen am E-Mail-Gateway einführen.

Anhang: Studienmethodik

Einführung

Im Rahmen dieser Studie entwickelten PwC und Iron Mountain eine robuste Forschungsmethodik, um die gezogenen Schlussfolgerungen zu untermauern. Diese Methodik hat auf die Erkenntnisse und Erfahrungen aus der in Jahr 2012 durchgeführten Studie aufgebaut. Zunächst arbeiteten wir eng mit Iron Mountain zusammen, um die Themenstellungen, die sich aus der Vorjahresstudie ergeben hatten, zu bewerten. Anhand der gewonnen Erkenntnisse arbeiteten wir anschließend einen umfassenden Fragebogen aus. Dieser Fragebogen befasste sich größtenteils mit den wichtigsten Themen dieser Studie: Umfang und Wirksamkeit der Unternehmenskonzepte beim Umgang mit Informationsrisiken unter Berücksichtigung von Mitarbeitern, Kommunikationsmaßnahmen und Sicherheit.

Hinzu kam eine Reihe „verhaltensbezogener Aussagen“, mit denen ein tieferer Einblick in das Warum gewonnen werden sollte: Warum verfahren Unternehmen bzw. einzelne Branchen und Länder nach bestimmten Praktiken. Um einen Vergleich zu ermöglichen, haben die zentralen Aussagen, die den Risikoindex untermauern, das gleiche Format wie im Jahr 2012. Der Fragebogen wurde von einem internen PwC-Team aus Marktforschungsspezialisten entworfen und durch fachkundige Erkenntnisse und Beiträge des von Claire Reid geleiteten PwC - Risk Assurance Teams unterstützt.

Wir arbeiteten zudem sehr eng mit unserem Forschungspartner Coleman Parkes zusammen. So stellen wir sicher, dass die Gestaltung des Fragebogens in einem kompatiblen Format erfolgte, damit er auf die computerunterstützte Telefoninterview-Programmfolge (CATI) hochgeladen und in den Muttersprachen der Befragten zur Verfügung gestellt werden konnte.

Wen haben wir befragt?

Die am Telefon befragten Personen waren in der Regel Vorstandsvorsitzende (CEOs), Finanzleiter (CFOs), IT-Leiter (CIOs) und Direktoren. Ziel war es, den Standpunkt der Chefetagen in Erfahrung zu bringen und einen Einblick in Art und Ausmaß der drängendsten Informationsrisiken und die Art des Umgangs zu erhalten und wie mit diesen auf besagter Ebene umgegangen wird. Die Telefoninterviews wurden anteilmäßig mit Befragten aus den Kernmärkten und -branchen durchgeführt, um die Durchführung einer vergleichende Analyse auf ausführlichem Niveau zu ermöglichen.

Um möglichst viele Erkenntnisse aus dieser Studie zu erlangen, begaben wir uns auf den Weg zu einer umfassenden „Datengewinnung“. Dabei unterlegten wir die wichtigsten Erkenntnisse mit konkreten Sachverhalten, insbesondere in Bezug auf markt- und branchenspezifische Trends. Bei dieser Analyse wurden auch die zentralen Veränderungen bei den Erkenntnissen aus den Jahren 2012 und 2013 bewertet und durch die verhaltensbezogenen Aussagen gestützt und verdeutlicht. Darüber hinaus haben wir die Meinung von Fachexperten unseres PwC-Netzwerks herangezogen. Diese Experten kamen aus den europäischen Ländern, die in dieser Studie vertreten sind.

Ähnlich wie in der im Jahr 2012 durchgeführten Studie haben wir auch in diesem Jahr einen Informationsrisiko-Index entwickelt. Dieser Index wurde mit Daten befüllt, und zwar durch Anwendung eines gewichteten Durchschnitts aus den einzelnen Unternehmensantworten auf 34 Aussagen, die in unserer Studie enthalten waren. Die 34 Aussagen wurden in die vier definierten Bereiche „Strategie“, „Mitarbeiter“, „Kommunikation“ und „Sicherheit“ gegliedert und wie umseitig dargestellt, kategorisiert.

Welche der folgenden Maßnahmen hat Ihr Unternehmen ergriffen?

Strategie

1. Eine Strategie bzw. ein Konzept zum Informationsrisiko.
2. Ein formeller Business Recovery Plan bzw. eine entsprechende Strategie.
3. Ein Notfallplan, um auf kleinformatige Informationspannen oder Datenverluste zu reagieren.
4. Regelmäßige Überprüfung der Datenschutzregelungen.
5. Ein Unternehmensrisikoregister.
6. Eine Informationssicherheitsstrategie, die die Sicherheit von Mobiltelefonen, personalisierten Geräten und Laptops gewährleistet.
7. Eine Strategie für den Umgang mit strukturierten und unstrukturierten Informationen in Papier- und digitaler Form an sämtlichen Standorten.
8. Eine Strategie für die sichere Entsorgung von IT-Hardware und vertraulichen Unterlagen.
9. Eine Strategie, die beim Zugriff auf unternehmenswichtige Dokumente und Hochrisikounterlagen, die am häufigsten in Compliance-Anfragen vorkommen, Prioritäten setzt.

Mitarbeiter

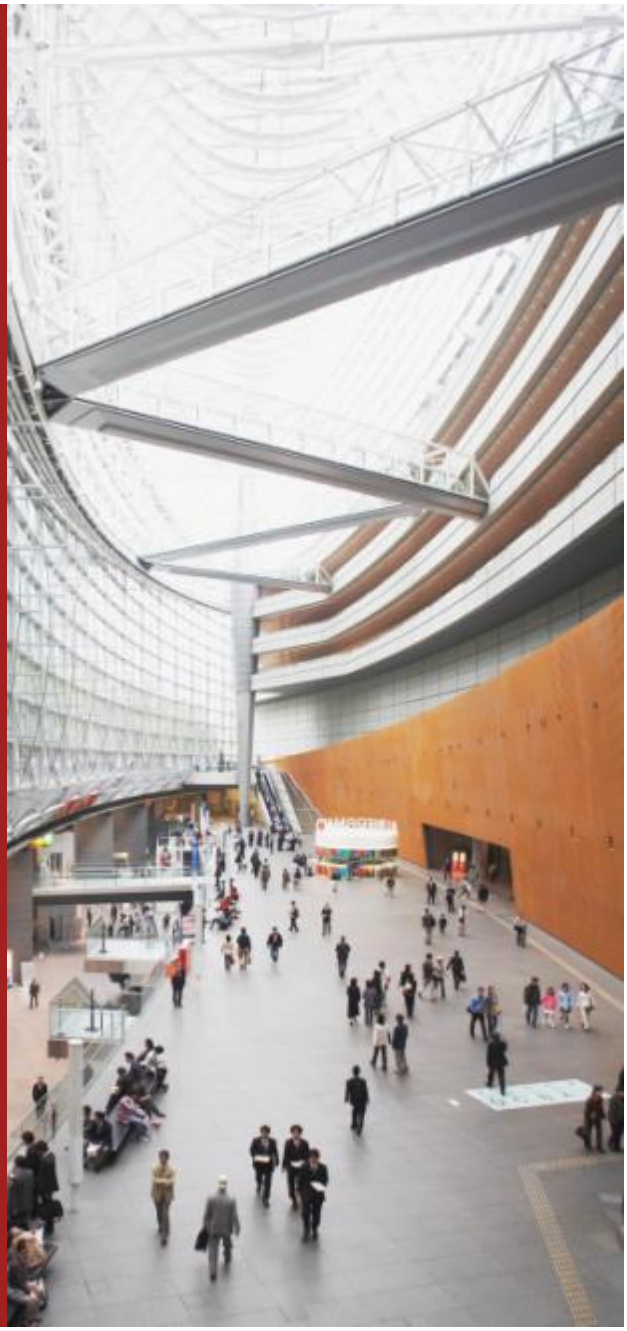
10. Eine bestimmte Einzelperson oder ein Team mit Verantwortung für das Informationsrisiko innerhalb Ihres Unternehmens.
11. Ein Verfahren für Mitarbeiter, die Ihr Unternehmen verlassen, um Diebstahl oder das Kopieren von Informationen zu verhindern.
12. Schulungsprogramme zur Unterweisung von Mitarbeiter hinsichtlich des Informationsrisikos.
13. Informationsrisikobewusstsein als Teil der Einarbeitung.
14. Laufende Auffrischungskurse.
15. Effektive computergestützte Schulungsprogramme zu Informationsrisiken.
16. Mitarbeiterüberprüfungen.
17. Verhaltenskodex in Bezug auf die richtigen Verhaltensweisen sämtlicher Mitarbeiter.
18. Instrument zur Messung des Vertrauens von Mitarbeitern hinsichtlich der Wirksamkeit Ihrer Informationsrisikoverfahren.
19. Internet-Nutzungsrichtlinien für alle Mitarbeiter.
20. Nutzungsrichtlinien für Social Media für alle Mitarbeiter (z. B. Facebook, Twitter und LinkedIn).

Kommunikation

21. Vorhandensein leicht zugänglicher Risikoinformationen für alle Mitarbeiter.
22. Mitarbeiterkommunikationsprogramme, um Informationsrisikoverfahren zu stützen.
23. Klare Mitarbeiterleitlinien bei internen Verfahren für die sichere Entsorgung und Aufbewahrung physischer Unterlagen.
24. Klare Mitarbeiterleitlinien bei internen Verfahren für die sichere Entsorgung und Lagerung elektronischer Unterlagen.

Sicherheit

25. Unternehmensrichtlinien für den sicheren Schutz sowie die sichere Aufbewahrung und Entsorgung von vertraulichen Informationen.
26. Due-Diligence-Programme für den Umgang mit Kunden-, Mitarbeiter- oder persönlichen Daten.
27. Bestandsaufnahme der Orte, wo Ihre Daten gespeichert werden.
28. Zentralisierte Sicherheitsdatenbank zur Informationsverwaltung.
29. Technologie, um Angriffserkennungs- und Angriffsabwendungssysteme einzusehen.
30. Überprüfung durch eine Drittpartei, z. B. Penetrationstests.
31. Klare, aktualisierte und anerkannte Dateneinstufungen.
32. Kontrollverfahren für den Zugang zu Gebäuden, Sicherheitsbereichen, Unternehmensarchiven und anderen sensiblen Informationen.
33. Anwendung unterschiedlicher Regeln und Abläufe hinsichtlich der Datenspeicherung unter Berücksichtigung verschiedener Aufbewahrungsfristen für Unterlagen und Datenschutzanforderungen.
34. Störfall-Meldeverfahren, z. B. wie erkannt werden kann, dass sich etwas am falschen Ort befindet.



Berichtsautoren

Claire Reid

Partner, PwC Risk Assurance

T: +44 (0)207 212 5513

M:+44 (0)7734 607594

claire.reid@uk.pwc.com

David Armstrong

Partner, PwC International Survey Unit

T: +44 (0)28 90 245454

M: +44 (0)7713 680266

david.m.armstrong@uk.pwc.com

Julie McClean

Senior Manager, PwC International Survey Unit

T: +44 (0)28 90 245454

M: +44 (0)7738 313241

julie.mcclean@uk.pwc.com

Biju Mukund

Senior Manager, PwC Risk Assurance

T: +44 (0)207 213 1701

M: +44 (0)7850 907913

biju.mukund@uk.pwc.com

Kieran Jones

Senior Associate, PwC International Survey Unit

T: +44 (0)28 90 245454

M: +44 (0)7845 635383

kieran.p.jones@uk.pwc.com

www.pwc.com