



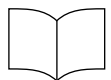
KAPITEL 3

WELCHE

**KOSTEN**

**ENTSTEHEN DURCH IGNORIEREN  
DES INFORMATIONSRISIKOS?**

MINIMIEREN SIE IHRE RISIKEN






E-BOOK ZUM WIRTSCHAFTLICHEN  
UMGANG MIT INFORMATIONEN



IRON MOUNTAIN®

# DAS E-BOOK ZUM WIRTSCHAFTLICHEN UMGANG MIT INFORMATIONEN

Dieses fünfteilige E-Book erläutert umfassend, welche Rolle Informationen in Ihrem Unternehmen spielen. Dabei werden sämtliche Aspekte des wirtschaftlichen Umgangs mit Informationen betrachtet.

1. Was ist Informationsrendite?
2. Wie verbessert man den Zugriff auf Informationen für eine optimale Wertschöpfung?
3. Welche Kosten entstehen durch Ignorieren des Informationsrisikos?
  -  Risiken
  -  Häufige Fehler
  -  Chancen zur Verbesserung
4. Wie entwickelt man ein für Mitarbeiter und Unternehmen gleichermaßen umsetzbares Programm?
5. Wie wirken sich zukünftige Entwicklungen im Informationsmanagement auf mein Unternehmen aus?



**LERNINHALTE**  
Informationsrisiken  
erkennen und  
vermeiden, um  
Datenschutzverstößen  
und mangelnder  
Compliance  
vorzubeugen



# WIRTSCHAFTLICHER UMGANG MIT INFORMATIONEN

## SCHNITTSTELLE ZWISCHEN NUTZEN, RISIKO UND KOSTEN

Beim wirtschaftlichen Umgang mit Informationen geht es darum, Informationen, die in einem Unternehmen generiert und empfangen werden, gewinnorientiert zu verwalten und zu nutzen. Jede Organisation benötigt eine unternehmensweite Strategie mit dem Ziel, Risiken zu verringern, Compliance sicherzustellen, Kosten zu senken und Informationen angesichts der wachsenden Bedeutung von Big Data für die Datenanalyse vorzubereiten. Der wirtschaftliche Umgang mit Informationen basiert auf einer umfassenden Strategie, die von allen Beteiligten unterstützt werden sollte. Sie ermöglicht eine optimale Wertschöpfung der Informationen und minimiert Risiken in den einzelnen Lebenszyklen - von der Entstehung bis hin zur sicheren Vernichtung der Information.

# KAPITEL 3:

## RISIKEN ERKENNEN UND VERMEIDEN

In den vorherigen Kapiteln dieses E-Books wurde erläutert, wie Sie durch maximale Wertschöpfung aus Ihren Akten und Unternehmensinformationen eine Informationsrendite erzielen. Außerdem haben wir Potenziale zur Kostenminimierung untersucht, indem Sie nur die Akten zugriffsbereit halten, zu deren Aufbewahrung Sie gesetzlich verpflichtet sind, und alle anderen Akten entweder dauerhaft archivieren oder sicher vernichten. Doch nicht jeder Aspekt des wirtschaftlichen Umgangs mit Informationen kann im Sinne einer Kosteneinsparung transparent ausgewertet werden.

Obwohl sich das Informationsrisiko wirtschaftlich nur schwer beziffern lässt, muss die Vermeidung einer Informationskatastrophe oberste Priorität haben, weil die Folgen verheerend sein können. Die Notwendigkeit zur Eindämmung der Risiken muss jedoch sorgfältig gegen die wichtigste Aufgabe eines Unternehmens abgewogen werden, seinen Mitarbeitern genügend Freiheit für effizientes Arbeiten zu gewähren.

In diesem Kapitel untersuchen wir die einzelnen Risiken und erklären, wie Sie eine Strategie entwickeln, um eine Katastrophe zu vermeiden und eine Informationsrendite zu erzielen.



## FAKTEN ZUM INFORMATIONSRISIKO

Eine wichtige Erkenntnis zum Informationsrisiko stammt aus einer gemeinsamen Studie des weltweit angesehenen Wirtschaftsberatungsunternehmens Price Waterhouse Coopers (PwC) und Iron Mountain. Deren Bericht „*Beyond good intentions - the need to move from intention to action to manage information risk*“ von 2014 analysiert Untersuchungen in 600 europäischen und weiteren 600 nordamerikanischen Unternehmen mit 250 bis 2.500 Mitarbeitern.

Im Bericht werden Best Practices zur Minimierung des Informationsrisikos definiert und die Leistung der Unternehmen im Vergleich zu diesem Maßstab mit dem „Information Risk Maturity Index“ bewertet. Der Indexwert 100 besagt, dass ein Unternehmen für die Risiken gut vorbereitet ist. Die europäischen Unternehmen erreichten im Durchschnitt jedoch nur einen Wert von 56,1 %. Dies zeigt, dass die breite Mehrheit der Unternehmen größere Risiken eingeht als notwendig wäre.

DAS  
DURCHSCHNITTLICHE  
EUROPÄISCHE  
UNTERNEHMEN  
ERREICHT

**56,1 %**  
**BEIM PWC-  
REIFEINDEX ZUM  
INFORMATIONSRISIKO  
(INFORMATION RISK  
MATURITY INDEX)**

## RISIKEN

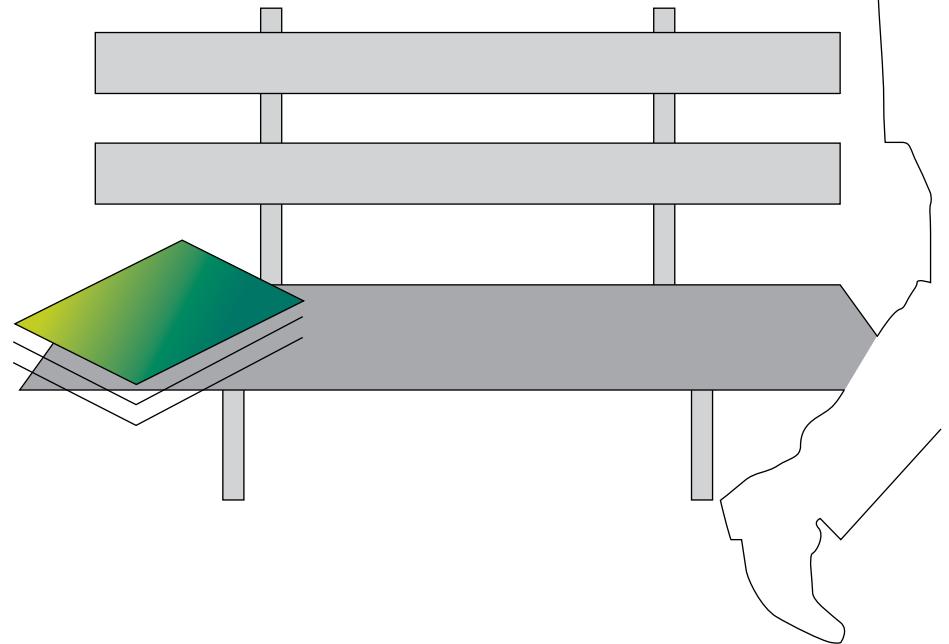


### DATENSCHUTZVERSTÖSSE

Ein katastrophaler Datenschutzverstoß ist der Alptraum aller Unternehmen. Obwohl Hackerangriffe ein ernstzunehmendes Risiko sind, nannten die Führungskräfte, die für die PwC-Studie „Global State of Information Security Survey“ nach möglichen Quellen für Verstöße gegen die Informationssicherheit befragt wurden, aktuelle Mitarbeiter (31 %) fast genau so oft wie Hacker (32 %).

Eine in Großbritannien durchgeführte staatliche Untersuchung ergab, dass 31 % der schlimmsten Sicherheitsverletzungen 2014 durch menschliche Fehler und weitere 20 % durch den absichtlichen Systemmissbrauch durch Mitarbeiter verursacht wurden. Dieselbe Studie zeigte außerdem einen erheblichen Anstieg der Kosten für die einzelnen Vorfälle.

**31 % DER SCHLIMMSTEN  
SICHERHEITSVERSTÖSSE  
WURDEN 2014 DURCH  
MENSCHLICHE FEHLER  
VERURSACHT**



<sup>1</sup> Information Security Breaches Survey 2014 - Britisches Ministerium für Wirtschaft, Innovation und Ausbildung (Department for Business, Innovation and Skills (BIS))

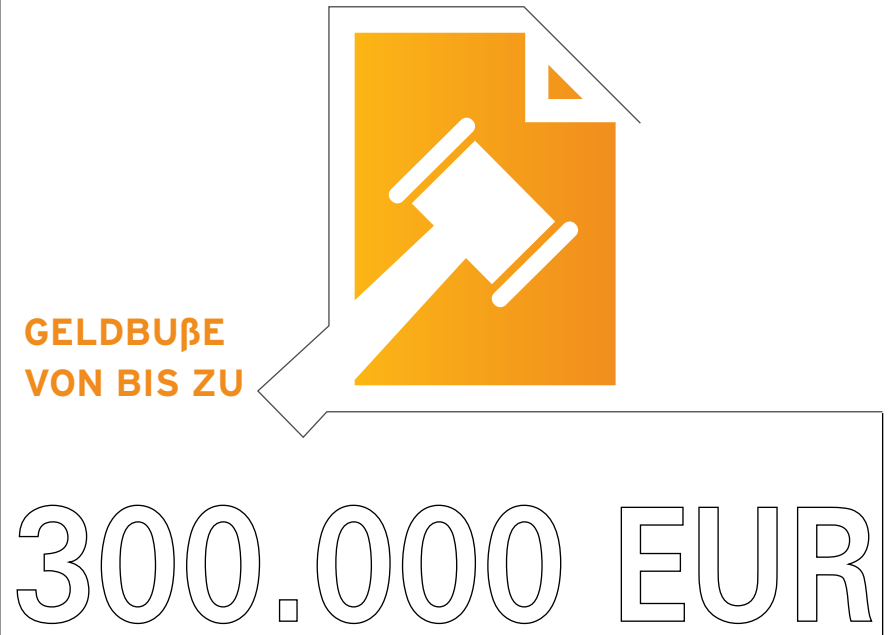
## MANGELNDE COMPLIANCE

In Kapitel 1 dieses E-Books ging es um die Informationsrendite und die Notwendigkeit, sich von der Last der Akten zu befreien, um Büroflächen für andere Zwecke nutzbar zu machen und den Zugriff auf Informationen zu verbessern. Mit einem durchsetzbaren Aufbewahrungsplan für zu archivierendes Material können Sie beide Ziele erreichen - und darüber hinaus die Compliance verbessern. Dabei sind die Datenschutzvorschriften wohl die wichtigsten Vorgaben, weil schwere Verstöße mit sehr hohen Geldbußen bis 300.000 EUR<sup>2</sup> geahndet werden.

Bei einem Verlust von Daten, insbesondere sensiblen Kundendaten, sind die Geldbußen jedoch Ihre geringste Sorge. Denn die damit einhergehende Rufschädigung verursacht langfristig weitaus höhere Kosten. 90 % der Unternehmen, die einen schwer wiegenden Datenverlust zu verkraften haben, geben innerhalb von zwei Jahren auf<sup>3</sup>.

<sup>2</sup> Bundesdatenschutzgesetz (BDSG)

<sup>3</sup> Britische Handelskammer



**BEI SCHWEREN  
VERSTÖSSEN**

## HÄUFIGE FEHLER



### IT-ZENTRIERTE DENKWEISE

Die PwC-Studie ergab, dass 73 % der europäischen Unternehmen glauben, die Gesamtverantwortung für die Informationssicherheit sollte der IT-Sicherheitsleiter tragen. In derselben Studie gaben jedoch 62 % an, dass Papierakten die größte Gefahr für die Informationssicherheit darstellten. Dies macht die verzerrte Wahrnehmung des Informationsrisikos sehr deutlich.

Stellen Sie sich selbst die Frage: Welche Informationen sind durch spezifische Sicherheitsmaßnahmen besser geschützt: die auf Ihrer Festplatte oder die in Ihren Papierakten?



73%

### RICHTLINIEN UND SCHULUNGEN

Die Ergebnisse der PwC-Studie decken die zentralen Fehler bei der Vermeidung von Informationsrisiken in europäischen Unternehmen auf. Nur 27 % der Unternehmen wenden Richtlinien für die sichere Aufbewahrung, Speicherung und Vernichtung vertraulicher Informationen an. Und nur 26 % überprüfen die Effektivität<sup>5</sup> ihrer Schulungen zu Informationsrisiken.

Informationssicherheit kann nur erreicht werden, wenn jeder im Unternehmen jeden Tag das Richtige tut. Dazu sind regelmäßige Schulungen über Richtlinien und Abläufe für alle Mitarbeiter erforderlich - ebenso wie es auch für jeden anderen unternehmensweiten, geschäftskritischen Aspekt des Betriebsablaufs üblich ist.

**DER EUROPÄISCHEN UNTERNEHMEN  
GLAUBEN, DIE IT-ABTEILUNG SEI  
FÜR DIE ÜBERWACHUNG DES  
INFORMATIONSMANAGEMENTS  
VERANTWORTLICH**

<sup>45</sup> Beyond good intentions - PwC-Bericht, 2014



## CHANCEN ZUR VERBESSERUNG



### GOVERNANCE

Nur 37 % der europäischen Unternehmen haben eine überwachte Informationsrisikostrategie<sup>6</sup> festgelegt. Eine Überprüfung der unternehmensweiten Richtlinien ist ein guter Ausgangspunkt zur Verbesserung. Sie umzusetzen, ist natürlich weitaus schwieriger.

Die auf höchster Ebene beginnende Erfassung von Kennzahlen auf allen Ebenen und in allen Abteilungen durch externe Berater, ist ein Schritt in die richtige Richtung. Richten Sie einen Ausschuss für Informationsmanagement ein, der die Initiative leitet, und machen Sie das Thema so wichtig, dass niemand es mehr ignorieren kann. Legen Sie einen Zeitplan für regelmäßige Treffen fest und halten Sie ihn auch ein.



### SICHERE AUFBEWAHRUNG

Natürlich muss die Informationssicherheit gegen den effektiven Zugriff auf Informationen abgewogen werden. Akten einfach wegzuschließen, mag sie wohl vor Diebstahl und Missbrauch schützen, erschwert jedoch auch den Zugriff darauf, sodass sie an Wert für Ihr Unternehmen verlieren. Auch der Schutz vor Zerstörung durch Feuer, Überschwemmung oder gar Tieren kann eine Rolle spielen. Und auch die Kosten für die Vor-Ort-Aufbewahrung und die Büroflächenbelegung können fast immer durch eine kosteneffektivere Nutzung aufgewogen werden.

Die externe Aufbewahrung in speziellen Hochsicherheitsarchiven mit modernsten Sicherheitsmaßnahmen und bedarfsgesteuertem Zugriff auf die Informationen bietet normalerweise die beste Informationsrendite für Papierakten.

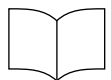
<sup>6</sup> Beyond good intentions - PwC-Bericht, 2014



MINIMIEREN SIE IHRE  
**RISIKEN**

LESEN SIE DAS NÄCHSTE KAPITEL  
KAPITEL 4: WIE ENTWICKELT  
MAN EIN FÜR MITARBEITER  
UND UNTERNEHMEN  
GLEICHERMASSEN  
UMSETZBARES PROGRAMM?

Laden Sie unseren Leitfaden „GEWUSST WIE - VON ANFANG: GRUNDLAGEN DER RISIKOVERMEIDUNG“  
herunter, um mehr über die Vermeidung von Informationsrisiken zu erfahren.



E-BOOK ZUM WIRTSCHAFTLICHEN UMGANG  
MIT INFORMATIONEN

© 2015 Iron Mountain Incorporated. Alle Rechte vorbehalten. Iron Mountain und das Design des Bergsymbols sind eingetragene Marken von Iron Mountain Incorporated in den USA und anderen Ländern. Alle anderen Marken und eingetragenen Marken sind Eigentum ihrer jeweiligen Inhaber.