IRON MOUNTAIN®
si space

INFORMATIONEN
NEU BETRACHTEN

ARCHIV- UND INFORMATIONSMANAGEMENT:

GEWUSST WIE – VON ANFANG AN

DIE GRUNDLAGEN DER RISIKOVERMEIDUNG

EINFÜHRUNG

DIESE KURZE EINFÜHRUNG SOLL IHNEN HELFEN, EINEN PLAN ZUR REDUZIERUNG IHRES INFORMATIONSRISIKOS ZU ERSTELLEN UND UMZUSETZEN.

Ein erfolgreiches Archiv- und Informationsmanagement muss nicht nur sorgfältig geplant und organisiert werden, es bedarf auch einer Strategie zur Kontrolle physischer und digitaler Akten – von deren Erstellung und aktiven Verwendung bis hin zum sicheren Speichern, dauerhaften Archivieren oder geplanten Vernichten. Mit einem guten Archiv- und Informationsmanagement können Unternehmen Informationsrisiken eingrenzen, Kosten besser verwalten und die Grundlage für Big Data-Analysen legen.

Von grossen, etablierten Unternehmen bis hin zu kleinen Unternehmen und Startups sind alle Organisationen mit dem Problem konfrontiert, ihren Plan zur Reduzierung des Informationsrisikos effektiv umzusetzen.

PROBLEMATISCHES RISIKO

Die Gründe für die Diskrepanz zwischen theoretischem und praktischem Informationsrisikomanagement sind vielfältig. Einerseits produziert und bearbeitet jedes Team und jeder Geschäftsbereich Informationen. In vielen Unternehmen müssen sie mehreren Teams jederzeit und an jedem Ort sofort zur Verfügung stehen. Immer globalere Geschäftsumgebungen erfordern einen schnellen, geräteunabhängigen und sicheren Zugriff auf Informationen.

Angesichts von Volumen, Vielfalt und der Geschwindigkeit, mit der Informationen täglich in den Unternehmen eintreffen, sehen sich Archiv- und Informationsmanager nicht nur einer stetig steigenden Menge an Informationen gegenüber, sondern müssen auch neue Formate berücksichtigen. Von Papierakten über Social Media Posts bis hin zu E-Mails: Die Herausforderungen nehmen zu. Darüber hinaus lässt sich nicht einfach problemlos bestimmen, wer Zugang zu welchen Informationen haben sollte und wer nicht. Dazu kommen ausserdem Überlegungen, wie und von wo aus auf Informationen zugegriffen werden sollte. Der Leiter eines Geschäftsbereichs braucht selbstverständlich Zugang zu potenziell vertraulichen Informationen, doch was geschieht, wenn diese als Ausdruck im Bus liegen gelassen werden? Oder auf einem Laptop gespeichert sind, der in einem Restaurant vergessen wird?

Auch das Speichern von Informationen ist mit Risiken verbunden. Digitale Datenbanken lassen sich ausspionieren, Online-Kommunikationen werden durch Malware, Missbrauch und bösartige Angriffe bedroht. Papierakten gehen leicht verloren oder können schnell vernichtet werden. Zwischen dem Wunsch nach Informationsrisikomanagement und der Umsetzung eines entsprechenden umfassenden Plans liegen Welten.

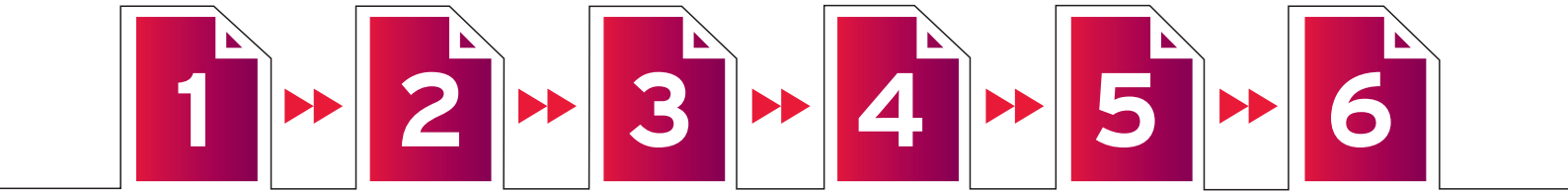
POTENZIELLE INFORMATIONSRISIKEN ERKENNEN

Die von Informationsrisiken ausgehende Bedrohung darf nicht übersehen werden. Negative Zwischenfälle in Bezug auf elektronische Sicherheit nehmen zu. Laut der PwC-Studie „Defending Yesterday – The Global State of Information Security" aus dem Jahr 2014 stieg die Anzahl der erkannten Vorfälle um 25 % an. 24 % der Studienteilnehmer gaben einen Datenverlust an, das sind 16 % mehr als noch im Vorjahr. Die PwC-Studie zu Verstössen gegen die Informationssicherheit aus dem Jahr 2014 (Information Security Breaches Survey 2014) zeigt einen erheblichen Anstieg der Kosten von einzelnen Verstössen. Zudem geht aus der Studie hervor, dass 10 % der britischen Unternehmen, die im vergangenen Jahr von einem Informationssicherheitsverstoss betroffen waren, dadurch so stark in Mitleidenschaft gezogen wurden, dass sie ihr Unternehmen grundlegend umgestalten mussten. Häufigkeit, Ausmass und Kosten der Bedrohungen nehmen zu.

WAS BEDEUTET DAS FÜR IHR UNTERNEHMEN?

Informationssicherheit ist nicht nur ein hilfreiches Extra. Sie ist eine geschäftliche Notwendigkeit, die nicht allein der IT-Abteilung oder Führungskräften überlassen werden kann. Ihre Informationssicherheitsstrategie sollte die Stärken und Schwachstellen Ihres Unternehmens auswerten, um Risiken ermitteln und verwalten zu können. Zudem sollte sie sich an immer neue Bedrohungen anpassen, indem sie die für Ihr Unternehmen wertvollsten Informationen identifiziert. Wenn Sie wissen, wo sich diese Informationen befinden und wer darauf Zugriff hat, können Sie auch Ihre Ressourcen und Investitionen besser priorisieren.

WAS KANN MAN TUN?



1. VERANTWORTUNG TEILEN
2. STÄRKEN UND SCHWACHSTELLEN KENNEN
3. MITARBEITER MIT EINBEZIEHEN
4. PAPIER BERÜCKSICHTIGEN
5. REGELMÄSSIG ÜBERPRÜFEN
6. FÜR DEN NOTFALL PLANEN

VERANTWORTUNG TEILEN

Für das Informationsmanagement sollte jeder Mitarbeiter Ihres Unternehmens verantwortlich sein. Wenn Informationen ausschliesslich in den Verantwortungsbereich der IT-Abteilung fallen, besteht die Gefahr, dass Mitarbeiter, die täglich Informationen produzieren und damit arbeiten, die damit verbundenen Risiken nicht erkennen und verstehen. Ausserdem könnten Ihre Teams neue Arbeitsprozesse unter Umständen nicht nachvollziehen oder umsetzen, wenn sie die Sicherheit von Informationen nicht zu verantworten haben. Richtlinien zur Informationssicherheit sollten von der Unternehmensspitze vorgelebt und auf allen Ebenen verstanden werden. Die Vorstandsebene sollte geeignete Vorgehensweisen zur Gestaltung der Informationssicherheit offen fördern. Die Unternehmensführung steht ebenso in der Verantwortung wie Manager, Benutzer und Entwickler. Letzten Endes kann die IT-Abteilung Informationen nicht schützen, wenn beispielsweise ein Mitarbeiter aus dem Marketing die Richtlinien nicht respektiert oder einhält.

73 % der Unternehmen in Europa und 74 % in Nordamerika sind der Meinung, dass die IT-Abteilung für das Informationsrisiko verantwortlich sein sollte.

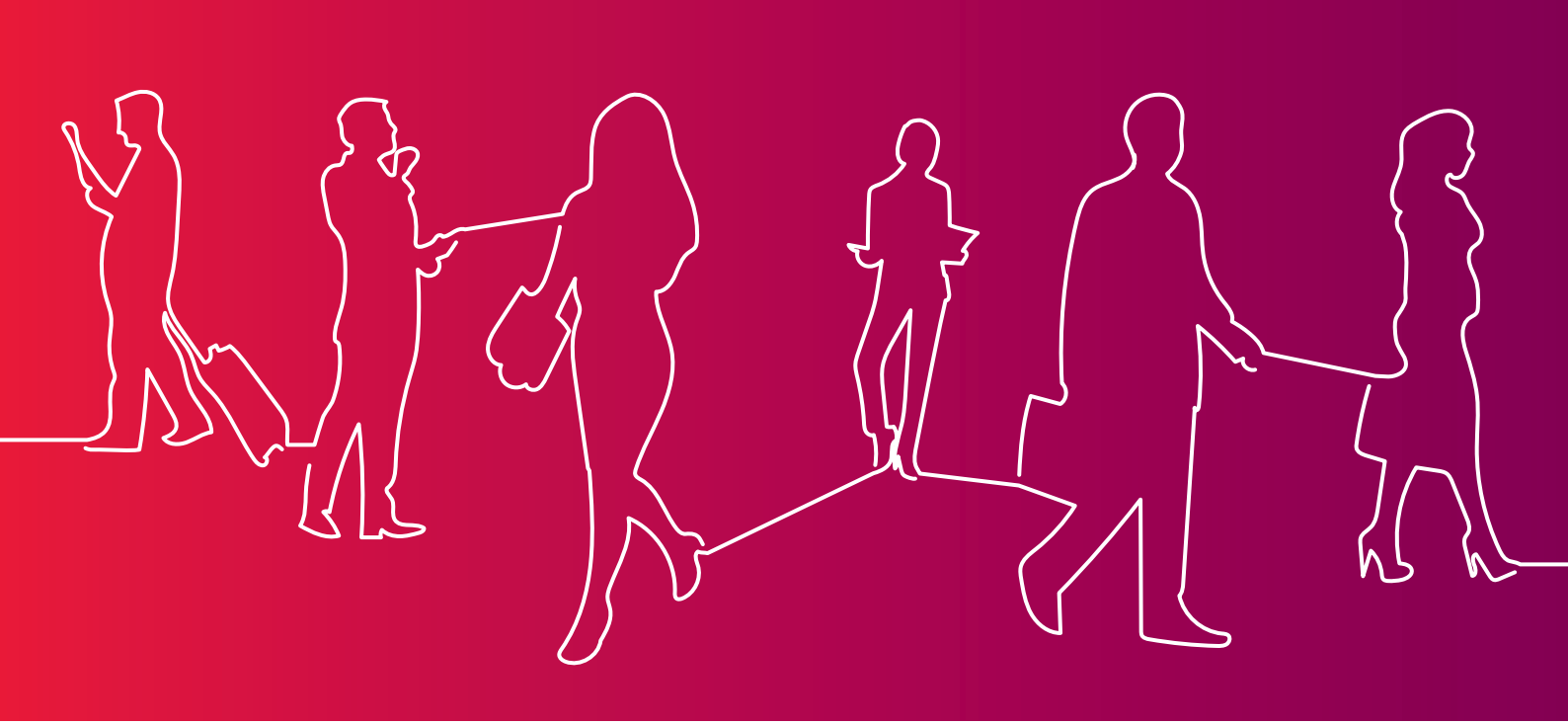
Beyond good intentions, The need to move from intention to action to manage information risk in the mid-market, PwC und Iron Mountain 2014

STÄRKEN UND SCHWACHSTELLEN KENNEN

Finden Sie heraus, wo sich die Informationen befinden, die für Ihr Unternehmen am wertvollsten sind bzw. die am gefährdetsten sind. Stellen Sie fest, wer darauf Zugriff hat. Ihre Risikobewertung sollte sich auf das gesamte Unternehmen einschliesslich aller Aspekte und Standorte erstrecken. Berücksichtigen Sie dabei sowohl die Fragen Ihrer Mitarbeiter, die für das Risikomanagement zuständig sind, als auch die Bereiche IT-Sicherheit, Compliance und Rechtsangelegenheiten sowie Unternehmenseinheiten und das Archivmanagement. Beziehen Sie physische und digitale Bestände, Clouds und mobile Geräte mit ein. Und vergessen Sie Ihre Drittanbieter nicht. Nutzen Sie die gewonnenen Ergebnisse als Rahmen, um Investitionen zu planen und zu beschliessen. Überprüfen Sie Ihre Ergebnisse regelmässig, da sich das Risikoprofil verschiedener Geschäftsbereiche verändern kann.

87 % der europäischen und 80 % der nordamerikanischen Unternehmen glauben nicht, dass ehemalige Mitarbeiter Informationen aus dem Besitz der bisherigen Firma zu ihrem neuen Arbeitgeber mitgenommen haben.

Beyond good intentions, The need to move from intention to action to manage information risk in the mid-market, PwC und Iron Mountain 2014



3 MITARBEITER MIT EINBEZIEHEN

Das Risikomanagement steht und fällt mit Ihren Mitarbeitern:

▶▶ Mit zunehmender Menge, Vielfalt und Geschwindigkeit von Informationen wächst auch der Bedarf an Partnern, die Unternehmen bei Sicherheitsmassnahmen unterstützen, die über die Informationsrichtlinien hinaus gehen. Datenanalysten helfen Ihrem Unternehmen, das Gleichgewicht zwischen Werten und Risiken zu finden. Sie können zudem auch Datenwissenschaft und -analyse in die Geschäftsfunktionen integrieren.

▶▶ Entwickeln Sie Informationsschulungen und führen Sie sie durch, damit Ihre Mitarbeiter Risiken erkennen und verstehen und sich entsprechend verhalten. Tauschen Sie sich regelmässig mit Ihren Mitarbeitern aus, um sicherzustellen, dass das Wissen aus den Schulungen in die täglichen Arbeitsabläufe einfliesst. Informationen sind ein Vermögenswert und eine entsprechende Informationskultur wird diesen Wert schützen und fördern. Dies beginnt auf der Führungsetage und schliesst sämtliche Mitarbeiter sowie Drittanbieter und Lieferanten mit ein.

▶▶ Mitarbeiter kündigen. Und wenn sie das Unternehmen verlassen, nehmen sie oftmals wertvolle oder vertrauliche Informationen mit. Richten Sie ein Verfahren ein, das Informationen davor schützt. Schaffen Sie Bewusstsein und fördern Sie ein entsprechend korrektes Unternehmensverhalten.

Nur 26 % der europäischen und 20 % der nordamerikanischen Unternehmen prüfen durch regelmässige Wiederholungen die Wirksamkeit ihrer Schulungen zum Thema Informationsrisiko.

Beyond good intentions, The need to move from intention to action to manage information risk in the mid-market, PwC und Iron Mountain 2014

4 PAPIER BERÜCKSICHTIGEN

Papier stellt eine erhebliche Bedrohung der Informationssicherheit dar. Erwägen Sie die Investition in eine kombinierte Lösung aus Scannen und sicherer Dokumentenaufbewahrung. Eine Hybridlösung kann Ihnen bei der Kontrolle Ihrer Papierakten helfen. Das Fachwissen und die Ressourcen von Iron Mountain haben sich seit Jahren bewährt und sind für Unternehmen möglicherweise genau richtig.

Ungefähr zwei Drittel der Befragten gaben Papierakten als grösstes Risiko an. Halb so viel Befragte sehen externe Bedrohungen auf dem zweiten Platz der Informationsrisiken.

Beyond good intentions, The need to move from intention to action to manage information risk in the mid-market, PwC und Iron Mountain 2014

5 REGELMÄSSIG ÜBERPRÜFEN

Um wirksam sein zu können, müssen Veränderungen überprüft werden. Definieren Sie Ihre Leistungskennzahlen und erstellen Sie Berichtsmetriken und Zeitpläne. Stellen Sie sicher, dass die Mitarbeiter die umgesetzten Überprüfungsmassnahmen kennen. Teilen Sie der Unternehmensleitung Ihre Ziele mit und bieten Sie Schulungen für die Kernteams an. Ernennen Sie einen Verantwortlichen für die Auswertung und Berichterstellung der von Ihnen gewonnenen Ergebnisse.

Lediglich 37 % der europäischen und 47 % der amerikanischen Unternehmen verfügen über eine vollständig überwachte Informationsrisikostrategie.

Beyond good intentions, The need to move from intention to action to manage information risk in the mid-market, PwC und Iron Mountain 2014

6 FÜR DEN NOTFALL PLANEN

Welche Pläne – zusätzlich zu Ihren Sicherheitsmassnahmen – haben Sie für den Notfall? Ihre Pläne zur Geschäftskontinuität und zum Krisenmanagement sollten eine Strategie für den Umgang mit den Folgen eines Verstosses gegen die Informationssicherheit beinhalten. Die Art und Weise, wie Sie mit Mitarbeitern, Kunden und der Öffentlichkeit kommunizieren, wird sich auf das Ergebnis auswirken.

SCHLUSSÜBERLEGUNGEN

Immer neue Informationen und Informationsformen sind auch mit neuen Risiken verbunden. Damit Unternehmen Informationen als Gewinn und Vermögenswert erkennen und verwenden können, müssen sie deren konsistente und effektive Verwaltung sicherstellen. Um in Zukunft erfolgreich zu sein, werden Unternehmen ihre Informationen in dem Masse schützen müssen, in dem sie sie zur Generierung von Innovation und Wachstum freigeben. Das Ziel besteht darin, Informationen nicht zu sperren, sondern sie uneingeschränkt zu nutzen.

Sie können auch den vollständigen PwC-Bericht über Informationsrisiken lesen.

IRON MOUNTAIN®
si space
+41 58 810 22 88 | ironmountain.ch