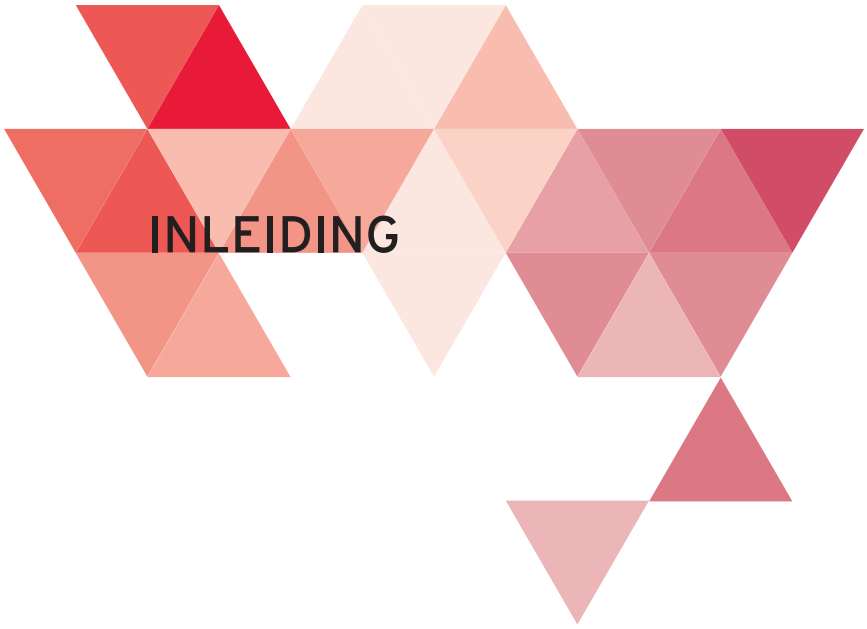
IRON MOUNTAIN®

SEE INFORMATION DIFFERENTLY

ARCHIEF- EN INFORMATIEBEHEER:

EEN GOED BEGIN IS HET HALVE WERK

DE BASISPRINCIPES VAN VOORBEREIDING OP RISICO'S



INLEIDING

EEN BEKNOPTE HANDLEIDING VOOR HET OPZETTEN, UITVOEREN EN PROFITEREN VAN EEN PLAN DAT UW BLOOTSTELLING AAN INFORMATIERISICO'S BEPERKT.

Een geslaagd archief- en informatiebeheer vergt planning, organisatie en een strategie voor het beheer van fysieke en digitale documenten. Vanaf de creatie en actief gebruik tot veilige opslag, permanente opslag of geplande vernietiging. Een goed archief- en informatiebeheer helpt uw organisatie informatierisico's te beperken, kosten te beheren en het fundament te leggen voor analyse van 'big data'.

Alle organisaties, van de grootste en gerenommeerdste tot de kleinste en jongste, hebben moeite om de kloof te overbruggen tussen een plan voor het beperken van informatierisico's en de praktische uitvoering hiervan.

HET PROBLEEM MET RISICO'S

De redenen voor de kloof tussen de theorie en praktijk van informatierisicobeheer lopen uiteen. Aan de ene kant heeft informatie betrekking op elk team en elke divisie. In veel organisaties moet informatie direct beschikbaar zijn, zodat meerdere teams er op elk moment en vanaf elke locatie toegang toe kunnen krijgen. In de steeds internationalere zakelijke omgeving moet toegang tot informatie snel en veilig zijn, ongeacht het apparaat dat wordt gebruikt.

Door een snelle toename van de hoeveelheid, variëteit en snelheid van informatie hebben archief- en informatiebeheerders niet alleen meer informatie te verwerken, maar zijn er ook nieuwe indelingen waarmee rekening moet worden gehouden. Van papieren dossiers tot sociale media en e-mails; de uitdagingen worden er niet gemakkelijker op. Bovendien is het niet altijd eenvoudig te bepalen wie toegang heeft tot welke informatie en wie niet. Daarnaast is er het vraagstuk over hoe mensen toegang moeten krijgen tot informatie en waarvandaan. Het is misschien acceptabel dat het hoofd van een divisie potentieel gevoelige informatie kan bekijken en gebruiken, maar wat gebeurt er als de informatie wordt afgedrukt en wordt achtergelaten in de trein? Of wordt opgeslagen op een laptop die wordt vergeten in een restaurant?

Er zijn ook risico's verbonden aan de opslag van informatie. Digitale databases kunnen worden geschonden en online communicatie staat bloot aan malware, fraude en cyberaanvallen. Papieren dossiers kunnen gemakkelijk verloren gaan of worden vernietigd. Het is één ding om informatierisico's te willen beperken, maar het realiseren van een allesomvattend plan is een totaal andere zaak.

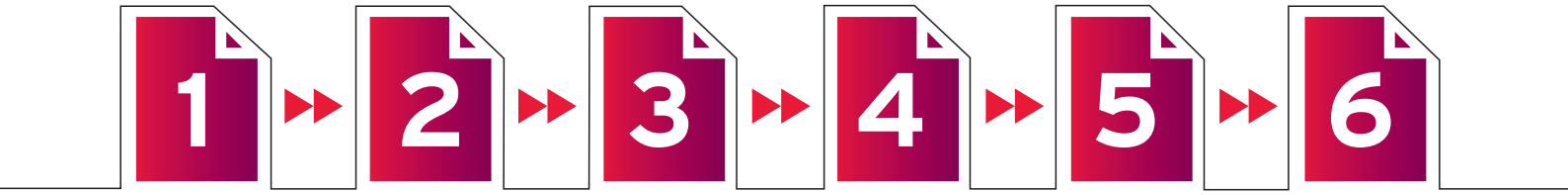
WAAROM MOET U ZICH ZORGEN MAKEN OVER INFORMATIERISICO'S?

De dreiging van informatierisico's mag niet worden genegeerd. Het aantal incidenten dat een bedreiging kan vormen voor de elektronische beveiliging neemt toe. Volgens Defending Yesterday - key findings from The Global State of Information Security (PwC 2014) is er een toename van 25% in waargenomen incidenten. In feite rapporteerde 24% van de respondenten een verlies van gegevens; een stijging van 16% ten opzichte van het voorgaande jaar. Volgens de enquête Information Security Breaches van PwC uit 2014 blijkt dat er een aanzienlijke stijging is geweest van de kosten van de afzonderlijke inbreuken. Verder wordt gemeld dat 10% van de Britse bedrijven die in het afgelopen jaar slachtoffer waren van een inbreuk, zodanig waren getroffen dat de bedrijfsvoering volledig moest worden aangepast. Dreigingen nemen toe in frequentie, ernst en kosten.

WAT BETEKENT DIT VOOR UW ORGANISATIE?

Informatiebeveiliging is niet alleen prettig om te hebben. Het is een noodzaak. Beveiliging kan niet simpelweg worden overgelaten aan IT of zelfs senior managers. Uw strategie voor informatiebeveiliging moet uw sterke en zwakke punten in kaart brengen om risico's te kunnen identificeren en beheren. Uw strategie moet zich ook aanpassen aan de veranderende bedreigingsomgeving door uw waardevolste informatie te identificeren. Als u weet waar deze informatie zich bevindt en wie er toegang toe heeft, kunt u gemakkelijker prioriteiten stellen met betrekking tot uw middelen en investeringen.

STAPPENPLAN



1 DEEL DE VERANTWOORDELIJKHEID

Informatiebeheer moet de verantwoordelijkheid zijn van iedereen in uw organisatie. Als de verantwoordelijkheid voor informatie uitsluitend bij IT ligt, bestaat het gevaar dat de mensen die elke dag met informatie werken niet begrijpen welke risico's hieraan zijn verbonden. En als informatie niet ieders verantwoordelijkheid is, begrijpen of accepteren uw teams nieuwe manieren van werken mogelijk niet. Het beleid voor informatiebeveiliging moet zichtbaar zijn tot in de top van de organisatie en worden begrepen op elk niveau. Het hoger management dient goede praktijken van informatiebeveiliging openlijk te steunen. Leidinggevenden zijn net zo verantwoordelijk als de beheerders, gebruikers en ontwikkelaars. IT is immers niet in staat informatie te beschermen als de iemand van marketing de richtlijnen niet naleeft.

73% in Europa en 74% in Noord-Amerika vindt dat IT uiteindelijk verantwoordelijk moet zijn voor informatierisico's.

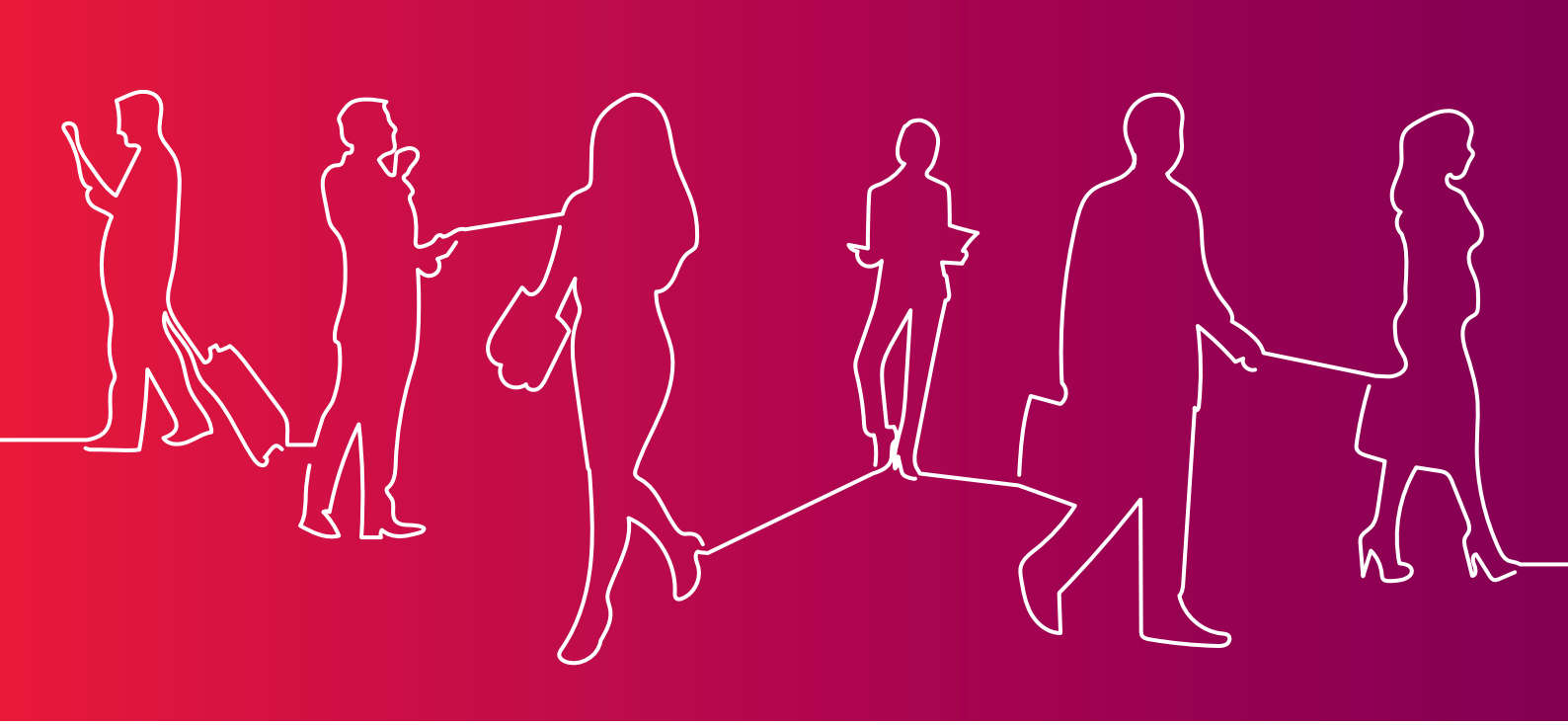
Beyond good intentions, The need to move from intention to action to manage information risk in the mid-market, PwC en Iron Mountain 2014

2 KEN UW STERKE EN ZWAKKE PUNTEN

Ontdek waar de meest waardevolle en meest kwetsbare bedrijfsinformatie zich bevindt. Bepaal wie hier toegang toe heeft. Uw risicobeoordeling moet de volledige organisatie omvatten; elk aspect en elke locatie. Uw risicobeoordeling moet ook ingaan op vragen van mensen die verantwoordelijk zijn voor het beheren van risico's. Overweeg het opnemen van IT-beveiliging, compliance en juridische aspecten, business units en archiefbeheer. Kijk naar fysieke en digitale archieven en ook naar de cloud en mobiele apparaten. Vergeet uw externe leveranciers niet. Gebruik uw resultaten als een kader voor planning en besluitvoering inzake investeringen. Herzie regelmatig uw conclusies, aangezien het risicoprofiel van verschillende bedrijfsonderdelen kan veranderen.

87% van de Europese en 80% van de Noord-Amerikaanse bedrijven gelooft niet dat ex-werknemers bedrijfseigen informatie hebben meegenomen naar een nieuwe werkgever.

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



3 BETREK UW MENSEN

Risicobeheer is afhankelijk van uw werknemers:

▶▶ Als de hoeveelheid, snelheid en variatie van informatie toeneemt, groeit ook de behoefte aan mensen die organisaties kunnen helpen het informatiebeleid verder te ontwikkelen. Het inzetten van gegevensanalisten helpt uw bedrijf de balans tussen meerwaarde en risico te bepalen. U kunt gegevensanalyse ook onderdeel maken van bedrijfsfuncties.

▶▶ Ontwikkel en implementeer informatietraining, zodat uw mensen zich bewust zijn van risico's en de mogelijkheid krijgen om hun gedrag te veranderen. Communiceer regelmatig met uw medewerkers om er zeker van te zijn dat de training zijn weerslag vindt in de dagelijkse werkzaamheden. Informatie is een bedrijfsmiddel en het creëren van een cultuur van respect voor informatie zal de waarde van informatie beschermen en laten toenemen. Dit moet beginnen bij de hoogste managers en moet alle werknemers inclusief externe leveranciers en onderaannemers omvatten.

▶▶ Mensen veranderen van baan. Daarbij nemen ze vaak waardevolle of gevoelige informatie met zich mee. Ontwikkel een proces om informatie te beschermen tegen werknemers. Vergroot het bewustzijn en bevorder gewenst gedrag.

Slechts 26% van de Europese en 20% van de Noord-Amerikaanse bedrijven geeft opvolging aan hun eigen risicotraining om te zien of deze effectief is geweest.

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

4 DENK AAN PAPIER

Papier is een grote bedreiging voor informatiebeveiliging. Overweeg om te investeren in een combinatie van scannen en beveiligd opslaan van documenten. Een hybride oplossing kan u helpen om de controle over uw papieren dossiers te optimaliseren. De expertise en middelen van Iron Mountain hebben de tand des tijds doorstaan en vormen wellicht de juiste keuze voor uw organisatie.

Ongeveer tweederde van de respondenten noemde papieren dossiers één van de grootste risico's. Dat is twee keer zo veel als het aantal dat externe dreigingen noemde, dat op de tweede plaats kwam.

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

5 BLIJF EVALUEREN

Verandering is alleen zinvol als deze wordt bijgehouden. Definieer uw belangrijkste prestatie-indicatoren en stel rapportagecriteria en tijdschema's op. Zorg ervoor dat mensen zich bewust worden van uw maatregelen door uw doelstellingen aan het senior management te communiceren en belangrijke teams training te bieden. Wijs aan iemand de verantwoordelijkheid toe voor het beoordelen en rapporteren van uw resultaten.

Slechts 37% van de Europese en 47% van de Amerikaanse respondenten beschikte over een volledig gecontroleerde informatierisicostrategie.

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

6 WEES VOORBEREID OP HET ERGSTE

Wat doet u als ondanks uw voorzorgsmaatregelen het noodlot toeslaat? Uw plannen voor bedrijfscontinuïteit en crisisbeheer moeten een strategie omvatten voor de nasleep van een inbreuk op de informatiebeveiliging. De manier waarop u communiceert met medewerkers, klanten en het publiek is van invloed op het resultaat.

TOT SLOT

Informatie en de manier waarop informatie wordt gepresenteerd is onderhevig aan verandering, en dat geldt ook voor de risico's die hieraan zijn verbonden. Als bedrijven informatie willen gebruiken als bedrijfsmiddel, moeten zij ervoor zorgen dat risico's consistent en effectief worden beheerd. De succesvolste bedrijven vinden een balans tussen het beschermen van informatie en het vrijgeven van informatie ten behoeve van innovatie en groei. Het doel is niet om informatie achter slot en grendel te verstoppen, maar om deze optimaal te benutten.

Lees het volledige rapport van PwC over informatierisico's.

IRON MOUNTAIN®

NL 0800 272 4433 | ironmountain.nl