HOOFDSTUK 3

WAT ZIJN DE KOSTEN VAN HET NEGEREN VAN INFORMATIERISICO'S?

HOE U INFORMATIERISICO'S MINIMALISEERT

WAAROM U DIT E-BOOK OVER RISICOVERMINDERING NODIG HEBT

Dit vijfdelige e-book helpt u om meer inzicht te krijgen in de rol die informatie in uw organisatie speelt. Het onderzoekt alle aspecten van de waarde van informatie.

1. Wat is "Return on Information"?
2. Hoe krijg ik toegang tot mijn informatie om de maximale waarde hieruit te halen?
3. Wat kost het als ik informatierisico's negeer?


Dreigingen


Veelgemaakte fouten


Mogelijkheden voor verbetering

4. Hoe kan ik een programma ontwikkelen dat werkt voor onze medewerkers en ons bedrijf?
5. Wat voor een invloed hebben toekomstige trends in informatiebeheer op mijn bedrijf?

U LEERT:

De valkuilen van informatiebeheer herkennen en u hierop voor te bereiden om risico's zoals Datalekken te voorkomen

SEE INFORMATION
DIFFERENTLY

INFORMATIE-ECONOMIE

HET SNIJPUNT VAN WAARDE, RISICO EN KOSTEN

Dit e-book gaat over het beheren en gebruiken van informatie die wordt gecreëerd en ontvangen door een organisatie, en geeft hierbij de belangrijkste punten weer. Elk bedrijf heeft een organisatiebrede informatiestrategie nodig met het doel de risico's te beperken en naleving van wet- en regelgeving te waarborgen tegen de laagst mogelijke kosten. Met de opkomst van big data is hier ook de voorbereiding op analyses bijgekomen. Dit vijfdelige e-book biedt een uitgebreide en samenwerkingsgerichte strategie om organisaties te helpen hun informatiewaarde te maximaliseren en de risico's in elke fase te beperken. Dit geldt voor de gehele levenscyclus van documenten. Van het aanmaken van records en informatie, via het actieve leven tot de veilige vernietiging ervan.

HOOFDSTUK 3:

BEWUST VAN RISICO'S EN VOORBEREID

In de voorgaande hoofdstukken van dit e-book hebben we bekeken hoe we Return on Information (informatierendement) kunnen realiseren door maximale waarde uit uw administratie en informatie te halen. We hebben ook gezien hoe kosten kunnen worden geminimaliseerd door wettelijk vereiste records te bewaren en de overige gegevens permanent op te slaan of op veilige wijze te vernietigen. Maar niet elk aspect van de waarde van informatie kan eenvoudig inzichtelijk worden gemaakt in termen van kosten of besparingen.

Informatierisico's lijken misschien moeilijk te kwantificeren in economische zin, maar het voorkomen van informatierampen moet een topprioriteit zijn aangezien de gevolgen zeer ernstig kunnen zijn. Het vereiste van risicobeperking moet echter worden afgewogen tegen de noodzaak om de mensen binnen een organisatie efficiënt te laten werken, opdat zij optimaal gebruik kunnen maken van de beschikbare informatie.

In dit hoofdstuk komen de verschillende dreigingen aan bod en wordt uitgelegd hoe u een strategie voor rampenbestrijding plant en een positief informatierendement verkrijgt.

INFORMATIERISICO'S: DE FEITEN

Het vooraanstaande, internationale adviesbureau PwC en Iron Mountain hebben een zeer verhelderend onderzoek naar informatierisico's uitgevoerd. Hun rapport uit 2014, *Beyond good intentions – the need to move from intention to action to manage information risk*, analyseert onderzoek onder 600 Europese bedrijven en nog eens 600 Noord-Amerikaanse, allemaal met 250 tot 2500 werknemers.

Het rapport definieert best practices inzake beperking van informatierisico's en zet de prestaties af tegen deze benchmark met behulp van de Information Risk Maturity Index. Een indexcijfer van 100 geeft aan dat een bedrijf is voorbereid op risico's, en het gemiddelde indexcijfer voor Europese bedrijven kwam uit op 56,1, waaruit blijkt dat de overgrote meerderheid van bedrijven aan meer risico's wordt blootgesteld dan nodig is.

EUROPESE BEDRIJVEN SCOREN GEMIDDELD

56,1 %

OP RISICOVOORBEREIDING

DREIGINGEN

DATELEKKEN

Een rampzalige datalek is de ergste nachtmerrie van elk bedrijf. Hoewel hacken wordt beschouwd als een ernstige bedreiging, wees in de enquête van PwC uit 2014 (Global State of Information Security) 31% van de leidinggevenden de huidige werknemers aan als waarschijnlijke bron van informatiebeveiligingsincidenten: bijna net zo veel als de 32% die hackers noemde.

Uit recent onderzoek van de Britse overheid blijkt dat 31% van de ergste datalekken in 2014 werd veroorzaakt door menselijke fouten, terwijl nog eens 20% werd veroorzaakt door opzettelijk misbruik van systemen door medewerkers[1]. Deze enquête toont ook een aanzienlijke stijging van de kosten van individuele incidenten aan.

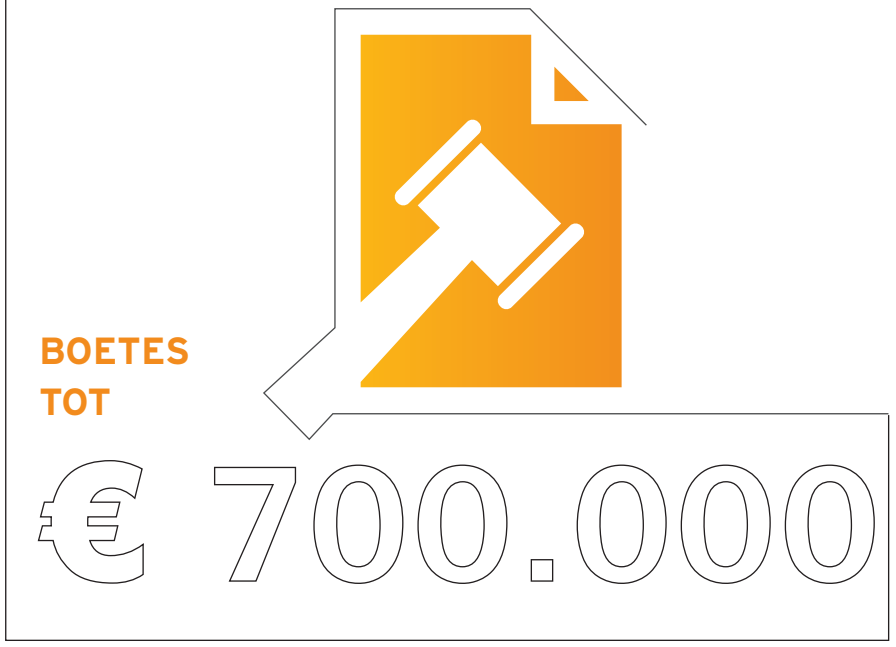
31% VAN DE ERGSTE DATALEKKEN IN 2014 WERD VEROORZAAKT DOOR MENSELIJKE FOUTEN

[1] Information Security Breaches Survey 2014 - UK Department for Business Innovation and Skills

NIET NALEVING VAN REGELGEVING

In hoofdstuk 1 van dit e-book werd gekeken naar informatierendement en het belang van het reduceren van uw administratieve belasting om kantoorruimte vrij te maken en de toegang tot informatie te verbeteren. Een afdwingbare planning voor het bewaren van documentatie kan u helpen beide te realiseren en de regelgeving na te leven. Bij de regelgeving omtrent gegevensbescherming vormen de straffen misschien wel de belangrijkste factor, met boetes tot wel € 700.000 voor ernstige overtredingen[2].

Bij gegevensverlies is de boete wellicht nog uw kleinste zorg, vooral als het gevoelige klantinformatie betreft. Reputatieschade kan u op de lange termijn veel meer kosten. 90% van de bedrijven die een aanzienlijke hoeveelheid gegevens verliest, gaat binnen twee jaar failliet[3].



VOOR ERNSTIGE OVERTREDINGEN

[2] UK Information Commissioner's Office
[3] Kamer van Koophandel in Londen

VEELVOORKOMENDE FOUTEN

IT-GERICHT DENKEN

In het PwC-rapport wordt geconstateerd dat 73% van de Europese bedrijven vindt dat de algehele verantwoordelijkheid voor informatiebeveiliging bij de IT-beveiligingsmanager moet liggen. Maar dezelfde enquête onthult dat 62% papieren dossiers als de grootste bedreiging voor informatiebeveiliging ziet[4]. Er is dus duidelijk sprake van een denkfout in de manier waarop tegen informatierisico's wordt aangekeken.

Bedenk het volgende: wat wordt beter beschermd door specifieke veiligheidsmaatregelen, de gegevens op uw harde schijf of uw papieren dossiers?

73%

VAN DE EUROPESE BEDRIJVEN VINDT DAT DE IT-AFDELING TOEZICHT MOET HOUDEN OP INFORMATIEBEHEER

BELEID EN TRAINING

De bevindingen van PwC tonen het algemene gebrek aan voorbereiding op informatierisico's binnen Europese bedrijven aan. Slechts 27% heeft een beleid ontwikkeld voor de beveiliging, opslag en vernietiging van vertrouwelijke informatie. En slechts 26% geeft een vervolg aan de informatierisicotrainingen om de doeltreffendheid ervan te bepalen[5].

Bij informatiebeveiliging draait het erom dat iedereen in het bedrijf elke dag het juiste doet. Dit vraagt om universele, permanente training in beleidslijnen en procedures, net zoals bij alle andere ondernemingsbrede en bedrijfskritieke activiteiten.

[4,5] Beyond good intentions – A PwC report, 2014

MOGELIJKHEDEN TOT VERBETERING

BESTUUR

Slechts 37% van de Europese bedrijven beschikt over een volledig gecontroleerde informatierisicostrategie[6]. Een evaluatie van ondernemingsbrede beleidslijnen vormt een goed beginpunt. De implementatie ervan is natuurlijk een andere zaak.

Steun van sleutelfiguren op alle niveaus en op alle afdelingen, te beginnen bij de top, is de juiste start. Stel een commissie voor informatiebeheer samen die leiding kan geven aan uw initiatief. Vergroot daarnaast de zichtbaarheid van het probleem, zodat dit niet kan worden genegeerd. Plan vergaderingen en evaluaties en houd u aan deze planning.

[6] Beyond good intentions – A PwC report, 2014

VEILIGE OPSLAG

Natuurlijk moet informatiebeveiliging in evenwicht zijn met informatietoegang. Door gegevens simpelweg achter slot en grendel te bewaren kunt u deze beveiligen tegen diefstal en misbruik. Als de toegankelijkheid wordt beperkt, kan de meerwaarde voor uw organisatie echter wel in het geding komen. Andere overwegingen zijn het risico van schade door brand, overstroming en zelfs ongedierte. Ook zijn er kosten verbonden aan lokale opslag en kantoorruimte kan vrijwel altijd kosteneffectiever worden ingezet.

Externe opslag in veilige, speciaal gebouwde voorzieningen met de allernieuwste beveiligingen en toegang tot de administratie op pay-as-you-go-basis biedt meestal het beste informatierendement inzake papieren dossiers.

MINIMALISEER RISICO

KIJK UIT NAAR ONS VOLGENDE HOOFDSTUK

HOOFDSTUK 4: HOE KAN IK EEN PASSEND PROGRAMMA VOOR ONZE MEDEWERKERS EN ONS BEDRIJF ONTWIKKELEN?

Als u uw informatierisico wilt beperken, downloadt u EEN GOED BEGIN IS HET HALVE WERK, de basisbeginselen van voorbereiding op risico's

IRON MOUNTAIN®

BE +32 2 712 2020| ironmountain.be