IRON MOUNTAIN®

BEST PRACTICES GUIDE VOOR HEALTHCARE

JE BENT NET ZO STERK ALS JE ZWAKSTE SCHAKEL

Hoe houd je rekening met menselijk gedrag bij intern risicomanagement?

INLEIDING

De turbulentie van de afgelopen jaren heeft organisaties gedwongen hun risicostrategieën te heroverwegen, met de nadruk op het verzekeren van weerstand op lange termijn.

Nergens is dit duidelijker dan in de gezondheidszorg, waar steeds geavanceerdere cyberaanvallen de vertrouwelijke gegevens van patiënten in gevaar brengen. Ondertussen nemen de kwetsbaarheden toe naarmate medische dossiers verhuizen naar digitale platforms, telegezondheidszorg een enorme groei doormaakt en medische internet of things (IoT)-apparaten steeds meer worden gebruikt. Het is nog nooit zo belangrijk geweest om patiënten op afstand en effectief van dienst te kunnen zijn en tegelijkertijd hun informatiebeveiliging en naleving van de regelgeving hoog in het vaandel te houden.

WIST U DAT?

In mei 2021 legde een **ransomware-aanval de IT-systemen** van de Ierse gezondheidsdienst plat, waardoor de meeste ziekenhuizen van het land meer dan een week zonder computers zaten[1].

In 2020 had een ransomware-aanval op een ziekenhuis in Europa **ernstige gevolgen voor patiënten**[2].

Maar hoe beschermt u uw gezondheidsorganisatie tegen dergelijke toenemende aanvallen?

Een belangrijk aspect dat vaak over het hoofd wordt gezien, is de dreiging van binnen de organisatie. Menselijk gedrag en fouten zijn meestal onbedoeld, maar brengen zorgverleners in gevaar doordat ze levens op het spel zetten en financiële verliezen veroorzaken. Om nog maar te zwijgen van de aanzienlijke reputatieschade bij verlies van gevoelige medische informatie. In een tijd van snelle digitalisering hebben organisaties in de gezondheidszorg meer te verliezen dan de meeste andere.

In een recent IBM onderzoek worden de gemiddelde kosten van een datalek in de gezondheidszorg geschat op **9,23 miljoen dollar** per incident - meer dan in welke andere sector dan ook[3].

Daarom heeft Iron Mountain een pan-EMEA onderzoek[4] laten uitvoeren naar de potentiële beheerrisico's die organisaties zouden moeten overwegen in verband met menselijke zwakheden - met verrassende resultaten.

Lees verder voor inzichten en praktische tips over hoe je risico's in hybride teams kunt beheren en een betrouwbare bedrijfsstrategie kunt bouwen.

1. 10 dagen na ransomware-aanval heeft Iers gezondheidssysteem het moeilijk.
2. Nieuw-Zeelands ziekenhuis wordt geconfronteerd met tweede week van verstoring na grote cyberaanval.
3. IBM Cost of a Data Breach Report, 2021.
4. Onderzoek onder 11.000 werknemers in 10 landen, uitgevoerd in september 2021 door One Poll.

HOOFDSTUKKEN:

1 SNELLE OPLOSSINGEN

2 CREËER EEN RISICOBEWUSTE CULTUUR

3 INTEGREER UW STRATEGIE MET 'RESILIENCE BY DESIGN'

SNELLE OPLOSSINGEN

1

Laten we beginnen met het laaghangende fruit.

Hier zijn een paar verrassende feiten over hoe we werken - thuis en op kantoor.

Aan hoeveel van de onderstaande punten maakt **u zich** schuldig?

'KLIK' OP DE ICOONTJES EN ONTDEK MEER

Gelukkig zijn deze relatief eenvoudige problemen op te lossen. Overweeg:

- het delen van deze statistieken om het probleem onder de aandacht te brengen zonder 'vingers te wijzen'
- het benadrukken van het belang van een gedragsverandering
- het benadrukken welke hulpmiddelen, trainingen en ondersteuning beschikbaar zijn om te helpen
- nogmaals wijzen op het verschil tussen een weloverwogen en een onnodig risico
- het beleid bijwerken om een maximaal begrip van en verantwoordelijkheid voor risico management te garanderen

CREËER EEN RISICOBEWUSTE CULTUUR

2

We kunnen de menselijke aard niet veranderen, maar we kunnen wel veranderen hoe we met risico's omgaan – terwijl we klinische perfectie stimuleren - door een risicobewuste cultuur op te bouwen.

Hier zijn onze vijf stappen voor het bouwen van weerbaarheid door ontwerp:

1 VERANDER DE MINDSET VAN UW ORGANISATIE

HET FEIT:

Een op de drie werknemers (32%) **zegt een "kritieke" fout te hebben gemaakt** op het werk en 14% heeft een **risico genomen** dat hun organisatie geld heeft gekost.

DE OPLOSSING:

Begin met elke werknemer in staat te stellen om een risico-ambassadeur te worden en **veranker risicobewustzijn in uw cultuur**. Boor er een mentaliteit in dat dit een fundamentele verantwoordelijkheid van de werknemer is. Het is voor velen, niet voor weinigen.

VINK DE CHECKBOXES AF TIJDENS HET MAKEN VAN JE **STRATEGISCHE PLAN**

2 HERVORM UW INFORMATIE-MANAGEMENTBELEID

HET FEIT:

De helft (49%) van alle werknemers vindt het de moeite **waard om risico's te nemen op het werk**, ook al is 25% het **slachtoffer geworden van scams of phishing**.

DE OPLOSSING:

Healthcare organisaties stelden noodreacties in op de wereldwijde Covid-pandemie, maar die zijn nu verschoven naar langetermijnstrategieën die zijn opgebouwd rond hybride werken. Denk aan goed **geformuleerde beleidsregels voor informatiebeheer** die van toepassing zijn op kantoor-, hybride en/of externe medewerkers, maar ook op verkopers en aannemers.

Nu zorgverleners zich haasten om patiëntendossiers te digitaliseren, is het van cruciaal belang te zorgen voor een volledige bewakingsketen tijdens alle processen van inzameling, vervoer, digitalisering en verwijdering.

3 MAAK U STERK VOOR EEN ONDERSTEUNENDE CULTUUR

HET FEIT:

51% van de mensen is **gestrest achtergebleven door een fout** die ze op het werk hebben gemaakt.

DE OPLOSSING:

Het is bewezen dat hybride werkomgevingen de productiviteit voeden, maar deze kan worden verstikt door stress, wat natuurlijk een belangrijk punt van aandacht is in de gezondheidszorg. Zorg ervoor dat uw **workflows zijn ontworpen om risico's te beheersen** en dat ze aangepast zijn aan de groeiende complexiteit en volume van datapunten. Overweeg nieuwe technologieën die worden ondersteund door kunstmatige intelligentie en machine learning om uw **processen te stroomlijnen en te verbeteren.** Zodat uw personeel zich kan concentreren op het leveren van betere patiëntenzorg en op het afwerken van door een pandemie veroorzaakte wachtlijsten.

Wat is 'resilience by design'?

Weerbaarheid - of het vermogen van uw organisatie om een aanval of andere uitzonderlijke gebeurtenissen af te slaan - mag nooit een bijzaak zijn. Het moet worden ingebouwd in elke stap van uw bedrijfsbeleid en -processen.

Integratie van technologie na de pandemie

Meer dan de helft (59%) van de datamanagers die we hebben gesproken, heeft tijdens de pandemie **nieuwe software aangeschaft** en twee derde (62%) heeft **tools voor het delen van gegevens**, zoals Microsoft Teams, geïmplementeerd. Deze moeten worden geïntegreerd in programma's voor het beheer van de levenscyclus van informatie, **waaronder de vaststelling van bewaringstermijnen voor ongestructureerde gegevens**, zoals patiëntenchats en opnames van vergaderingen, en een gecentraliseerd systeem voor compliance en beleidsbeheer dat is aangepast aan de complexere technologische omgeving van vandaag.

4 EVOLUEER UW PROCESSEN

HET FEIT:

36% is zich op kantoor meer **bewust van de veiligheid** van werkgerelateerde gegevens dan thuis.

DE OPLOSSING:

Nu virtuele spreekuren en digitale ziekenhuisdossiers snel de norm worden, ontstaan er steeds grotere hoeveelheden gegevens. Dit vereist dat u **opnieuw nadenkt over informatiegovernance**: van het beheer van toegangsrechten tot het digitaal delen van informatie, tot dataretentie en veilige datavernietiging, in overeenstemming met de geldende wettelijke voorschriften. Als eerste stap **kunt u overwegen een datakaart** te maken om te begrijpen hoe gegevens in en uit uw organisatie stromen.

5 MAAK UW TRAINING ONVERGETELIJK

HET FEIT:

Terwijl 60% van de datamanagers zegt dat **risicomanagementtrainingen** goed worden bezocht, zegt 36% van de werknemers dat ze er nog nooit een hebben bijgewoond.

DE OPLOSSING:

Hoewel u ongetwijfeld beschikt over opleidingsmodules over risico's, blijkt uit onze bevindingen dat ze snel worden vergeten. Om de impact te vergroten, **moet u de training boeiender, relevanter en relateerbaarder maken**, zodat mensen de dagelijkse mogelijkheden zien om het geleerde toe te passen en ze begrijpen hoe het hen en hun patiënten beïnvloedt.

"We zijn allemaal mensen en maken allemaal fouten, dus risico is - per definitie - een altijd aanwezige factor op het werk. Maar het is niet constant. Nieuwe bedrijfsmodellen, hybride werken en de toenemende dreiging van cyberaanvallen maken het belangrijker dan ooit om interne risico's effectief te beheersen en zo te bouwen aan weerbaarheid op de lange termijn."

Sue Trombley, Managing Director of Thought Leadership, Iron Mountain

INTEGREER UW STRATEGIE MET 'RESILIENCE BY DESIGN'

3

"Het nemen van risico's kan een organisatie in staat stellen te innoveren, maar een gebrek aan bewustzijn van alledaagse gevaren kan de weerbaarheid ondermijnen. Wij adviseren om iedere werknemer een risico-ambassadeur te maken door risicobewustzijn in uw cultuur te integreren. Dit creëert een veilige ruimte waarin individuen kunnen innoveren en organisaties kunnen floreren."

Sue Trombley, Managing Director of Thought Leadership, Iron Mountain

Volgens ons onderzoek is **70%** van de Europese datamanagers van mening dat alle werknemers verantwoordelijk zijn voor risico management.

Voor een blijvende impact moet weerbaarheid 'by design' worden gedreven. Het moet worden ingebouwd in elke stap van uw bedrijfsprocessen, en worden versterkt door de dagelijkse acties van alle werknemers. - zowel medisch als administratief.

Terwijl zorgverleners werken aan een snelle digitalisering van hun activiteiten, is het belangrijk om te beseffen dat de verhoogde dreiging van cyberaanvallen waarschijnlijk zal blijven terwijl we herstellen van de terugslag van COVID-19.

Daarom zijn **hybride werkoplossingen met 'resilience by design'** essentieel voor het succes op lange termijn van elke in de gezondheidszorg. Oplossingen die bijvoorbeeld veilige informatietoegang vanaf elke locatie mogelijk maken, workflows voor het archiveren en digitaliseren van bestanden stroomlijnen en de volledige levenscyclus van uw gegevens en die van uw patiënten effectief helpen beheren, ongeacht het formaat of type. Oplossingen die u in staat stellen uw informatie te beschermen en de toegankelijkheid ervan te verbeteren, terwijl uw medische besluitvorming wordt verbeterd en de patiëntenzorg toeneemt.

Voor ondersteuning bij het aanpakken van de veranderende uitdagingen op het gebied van informatiebeheer in uw bedrijf en voor het bespreken van oplossingen om u te helpen de weerbaarheid in een hybride werkomgeving te vergroten, kunt u contact opnemen met het team of een bezoek brengen aan www.ironmountain.com/nl/industries/healthcare-services.

OVER IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), opgericht in 1951, is wereldwijd marktleider op het gebied van opslag- en informatiebeheerdiensten. Vertrouwd door meer dan 220.000 organisaties over de hele wereld en met een netwerk van meer dan 85 miljoen vierkante meter in meer dan 1.400 vestigingen in meer dan 50 landen, bewaart en beschermt Iron Mountain miljarden informatiedragers en documenten, waaronder bedrijfskritische informatie, zeer gevoelige gegevens en culturele en historische artefacten. Iron Mountain biedt oplossingen voor onder meer veilige opslag, informatiebeheer, digitale transformatie, veilige vernietiging en datacenters, kunstopslag en logistiek, en cloud-diensten. Iron Mountain helpt organisaties om kosten en risico's te verlagen, te voldoen aan wet- en regelgeving, te herstellen van calamiteiten en een meer digitale manier van werken mogelijk te maken. Bezoek www.ironmountain.com voor meer informatie.

© 2021 Iron Mountain Incorporated. Alle rechten voorbehouden. Iron Mountain en het ontwerp van de berg zijn gedeponeerde handelsmerken van Iron Mountain Incorporated in de VS en andere landen. Alle andere handelsmerken en gedeponeerde handelsmerken zijn eigendom van hun respectieve eigenaren.

0800 272 4433 | IRONMOUNTAIN.NL
+32 2 712 2020 | IRONMOUNTAIN.BE

IRON MOUNTAIN®