Huidige uitdagingen en oplossingen rondom beveiliging

De flexibele werkplek

Organisaties moeten informatie sneller en op grotere schaal dan ooit tevoren kunnen raadplegen, verplaatsen en delen. Medewerkers verwachten een hoge mate van samenwerking en een flexibele en efficiënte manier van werken. En door de komst van flexibel werken moet informatie net zo mobiel zijn als uw medewerkers.

Dit zijn scenario's waarmee bijna elke organisatie wordt geconfronteerd. Hoewel ze de bedrijfsproductiviteit en innovatie enorm bevorderen, vormen ze mogelijk ook een ernstige bedreiging voor de beveiliging van uw bedrijfsgegevens.

Hoe zorgt u voor een goede balans tussen de verwachtingen van medewerkers en gegevensbeveiliging? In dit handboek beschrijven we welke uitdagingen het bouwen van een flexibele maar veilige digitale werkplek met zich meebrengt. We behandelen de beveiligingsrisico's waarmee rekening moet worden gehouden en er worden enkele tastbare oplossingen omschreven.

RICOH
imagine. change.

De situatie

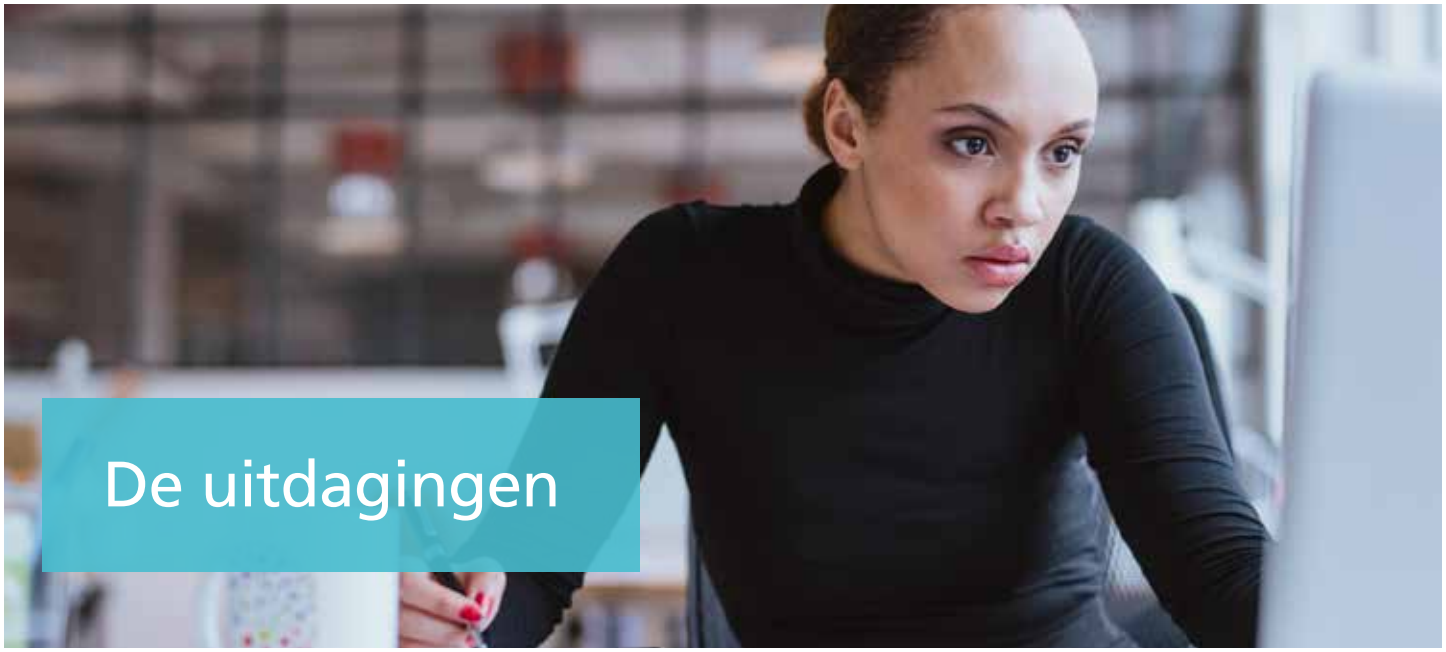
Uw medewerkers verwachten een flexibele werkplek en meer mobiliteit

Medewerkers verwachten dat ze overal kunnen werken door de beschikbare technologieën.

Mobiel en in de cloud werken neemt steeds meer toe. Zelfs als u geen medewerkers heeft die op afstand werken, betekent dit nog steeds dat werken niet meer beperkt is tot een bureau. Het ideaal rondom mobiel werken gaat verder dan alleen zakelijke e-mails op uw telefoon ontvangen. Het gaat om naadloze toegang tot documenten, gegevens, collega's en klanten. Altijd en overal. Deze vrijheid is normaal geworden, dus u moet hier wel in mee als u talent wilt aantrekken en behouden.

Maar is een keerzijde. Een flexibele en mobiele werkplek brengt ook nieuwe potentiële beveiligingsrisico's met zich mee. Wat gebeurt er wanneer een laptop of telefoon verloren raakt of wordt gestolen? Hoe gaat u met gegevensbeveiliging om als medewerkers toegang tot bedrijfsgegevens hebben vanaf persoonlijke apparaten? Hoe verdedigt u zich tegen hackers wanneer medewerkers verbinding maken met een openbaar Wi-Fi?

RICOH
imagine. change.



De uitdagingen

Als uw systeem voor het opslaan en delen van informatie met werknemers binnen en buiten kantoor ontoereikend is, kan dit vergaande gevolgen hebben voor zowel de productiviteit als de beveiliging.

Als uw medewerkers het gevoel hebben dat ze niet over de benodigde hulpmiddelen beschikken, gebruiken ze datgene wat voorhanden is. Bestanden worden naar persoonlijke e-mailaccounts verzonden en zijn daardoor toegankelijk vanaf thuiscomputers. Documenten worden opgeslagen en met behulp van cloudoplossingen voor consumenten gedeeld. Ongecontroleerd gebruik van verschillende cloudservices maakt van een goed ontworpen informatiesysteem al snel één grote puinhoop.

Dergelijke workarounds leiden mogelijk tot gegevenslekken, waardoor u steeds meer de controle over uw informatie verliest.

Waardevolle informatie komt op straat te liggen door workarounds

84% van de medewerkers gebruikt persoonlijke e-mailaccounts om gevoelige bestanden te verzenden.[1]

BYOD wint aan populariteit

Meer dan de helft van de Noord-Amerikaanse en Europese bedrijven ontwikkelt BYOD-programma's (Bring Your Own Device) op aandringen van medewerkers.[2]

Veel gegevenslekken ontstaan per ongeluk

De veiligheid van meer dan 28 miljoen gegevensrecords in het Verenigd Koninkrijk is in gedrang gekomen in 2017. Hiervan werd 38%toegeschreven aan verlies dat per ongeluk heeft plaats gevonden.[3]

Openbare Wi-Fi-netwerken zijn een mijnenveld

95% van de mensen gebruikt minstens een keer per week een Wi-Fi-hotspot voor hun werk, maar slechts 5% van de openbare Wi-Fi-hotspots wordt gecodeerd.[4]

Misschien onderschat u het risico

Meer dan de helft van de IT-managers heeft geen zicht op de bestands- en gegevensoverdracht binnen hun organisatie.[5]

1. Ipswitch File Transfer, 'Are Employees Putting Your Company's Data at Risk? Survey Results Exposing Risky Person-to-Person File Sharing Practices: An eBook report' www.ipswitchft.com.
2. www.forrester.com/Bring-Your-Own-Device-(BYOD).
3. www.theregister.co.uk/2017/09/20/gemalto_breach_index/
4. gfi.com/blog/survey-95-6-of-commuters-in-the-us-put-company-data-at-risk-over-free-public-wi-fi/
5. Ipswitch File Transfer eBook report www.ipswitchft.com

RICOH
imagine. change.

De oplossingen

Flexibel werken begint bij het begrijpen hoe de informatie door de organisatie stroomt, waar deze wordt opgeslagen en hoe deze wordt gebruikt. Aangezien gegevens zich op ontelbare apparaten binnen het bedrijf bevinden, moeten deze met geavanceerde beveiligingsmaatregelen worden beschermd.

Stop informatie in een systeem

U heeft niet veel aan een synchronisatie- en deelsysteem van bestanden als de informatie die u nodig heeft, zich in een archiefkast bevindt. Met een oplossing voor scannen naar de cloud worden documenten op intelligente wijze rechtstreeks naar de door u gewenste service verzonden. Dit maakt tevens beveiligde opslag mogelijk. **Scan eenvoudig en veilig naar de cloud met de Streamline NX-software van Ricoh.**

Altijd toegang tot informatie

Ondanks het gemak en de flexibiliteit van digitale bestanden, hebben we documenten toch ook nog in papieren vorm nodig. Zorg ervoor dat de juiste informatie altijd bij de juiste persoon terechtkomt met **oplossingen voor beveiligd afdrukken, zoals de Print2Me-functionaliteit in Streamline NX van Ricoh.**

Mobiel printen voor medewerkers en gasten

Het probleem dat medewerkers en gasten die op bezoek zijn niet kunnen afdrukken, wordt vaak opgelost door documenten als bijlage in een e-mail naar een contactpersoon op kantoor te sturen. Zodat zij de documenten kunnen afdrukken. Dit levert echter een beveiligingsrisico op, omdat virussen en kwaadaardige software zo eenvoudig kunnen worden doorgegeven. Peer-to-peer-communicatie tussen de printer/MFP en mobiele telefoons en pull-printing via de cloud beperken dit risico. **Ontdek meer over mobiel printen van Ricoh met MyPrint.**

Beheer uw informatie

Een oplossing voor documentbeheer zorgt ervoor dat elke medewerker over een passend toegangsniveau tot informatie beschikt. Een dergelijke oplossing biedt u ook inzage in hoe, wanneer en door wie documenten zijn bekeken of bewerkt. **Ontdek de oplossing voor veilig en efficiënt documentbeheer van Ricoh en DocuWare.**

Vraag een expert

Ga naar **www.ricoh.nl** of neem contact met ons op. Ontdek hoe Ricoh u kan helpen aan een digitale werkplek die zowel veilig als productief is.

Ricoh Nederland
Magistratenlaan 2
5223 MD ‘s-Hertogenbosch

073 645 11 11

www.ricoh.nl

RICOH
imagine. change.