

A modern vállalkozásokat érintő biztonsági kihívások és megoldásuk

A rugalmas munkahely problémája



A modern vállalatoknak korábban soha nem tapasztalt sebességgel és mértékben kell az információkhoz hozzáférniük, azokat mozgatniuk és megosztaniuk. Az alkalmazottak rugalmasabb, hatékonyabb és együttműködőbb munkamódszereket várnak el. Ahogy a munkahely kilép a hagyományos irodák falai közül, Önnek olyan információkra van szüksége, amelyek éppannyira mobilak, mint az alkalmazottjai.

Ezek olyan körülmények, melyekkel napjainkban szinte minden vállalatnak szembe kell néznie – és miközben nagyszerű lehetőségeket hordoznak magukban az üzleti teljesítmény és az innováció szempontjából, potenciálisan komoly fenyegetéseket is jelentenek az üzleti adatok biztonságára.

Hogyan egyeztetni össze a munkavállalók elvárásait és az információk biztonságát? Ebben a tanulmányban megvizsgáljuk, hogy milyen kihívásokat jelent egy rugalmas, de egyúttal biztonságos digitális munkahely kiépítése. Áttekintjük, hogy milyen biztonsági kockázatokat kell mérlegelnie, és néhány kézzel fogható megoldást is kínálunk.

RICOH
imagine. change.



A helyzet

Az alkalmazottai rugalmas munkahelyet és nagyobb mobilitást várnak el.

A modern technológiáival rendelkező munkavállalók azt várják el, hogy bárholnan dolgozhassanak.

Ha nincsenek is távolról dolgozó alkalmazottai, a mobil és felhő alapú technológia terjedésével a munka már nem csupán az íróasztalokra korlátozódik. A szakemberek számára ideális mobilitás sokkal többet jelent, mint a mobiltelefonon való e-mailezés – ez a dokumentumok, adatok, munkatársak és ügyfelek zökkenőmentes elérését jelenti, bárhol, bármikor. Ez a szabadság olyan aduásszá vált, amit nem vonhat meg az alkalmazottjaitól, ha be akarja vonzani és meg akarja tartani a tehetségeket.

A valóban rugalmas és mobil munkahely megteremtése azonban a vállalkozásokat számos új, biztonsági fenyegetéssel állítja szembe. Mi történik, ha elveszik egy laptop vagy egy telefon? Hogyan gondoskodik az információi biztonságáról, amikor az alkalmazottak azokat a személyes eszközeikről is elérhetik? Hogyan védekezik a kíváncsi digitális tekintetektől, amikor az alkalmazottjai nyilvános WiFi-hez csatlakoznak?



A kihívások

Ha nem megfelelő rendszeren tárolja és osztja meg az információkat az alkalmazottjaival az irodán belül és kívül, az drasztikus hatással lehet a teljesítményre és a biztonságra.

Ha az alkalmazottjai úgy érzik, hogy nem állnak a rendelkezésükre a szükséges eszközök, akkor az általuk ismert technológiát fogják használni. A fájlokat a személyes e-mail-fiókjaikba küldik el, és az otthoni számítógépeikről nyitják meg. A dokumentumokat felhő alapú megoldásokban tárolják és osztják meg. A különféle felhő szolgáltatások jóvá nem hagyott használatával egy jól tervezett információs rendszer is hamar a darabjaira hullhat szét.

Ezek a kerülőutas megoldások a vészjósló nevű „adatszivárgáshoz” vezetnek, amely az információk felletti kontroll azonnali elvesztését jelenti.

A jóindulatú kerülő megoldások veszélyeztetik az értékes információit

Az alkalmazottak 84%-a használja a személyes e-mail-címét érzékeny fájlok küldéséhez¹

Egyre nagyobb teret hódít a „hozd a saját eszközödet” megközelítés

Az észak-amerikai és európai vállalatok több mint fele dolgoz ki „hozd a saját eszközödet” programokat a munkaerő által megfogalmazott igényekre reagálva²

Számos adatvédelmi incidens véletlen történik

2017-ben több mint 28 millió adatot ért biztonsági incidens az Egyesült Királyságban. Ennek 38%-a véletlen elvesztés miatt következett be.³

A nyilvános WiFi egy aknamező

A becslések szerint a nyilvános WiFi-s internetelési helyek pusztán 5%-a titkosított, de az emberek 95%-a használja ezeket munkához legalább hetente egyszer⁴

Még a veszély mértékével sem lehet tisztában

Az informatikai vezetők több mint fele nem lát rá a szervezetükben folyó fájl- és adatátvitelre⁵

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” (Az alkalmazottak veszélyeztetik a vállalata adatait? Felmérési eredmények a személyek közötti kockázatos fájlmegosztási gyakorlatokról. Elektronikus könyv formátumú jelentés.) www.ipswitchft.com. 2. [www.forrester.com/Bring-Your-Own-Device-\(BYOD\)](http://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 jelentés elektronikus könyv formátumban www.ipswitchft.com



A megoldások

A biztonságos mobilitás kezdetén meg kell érteni, hogy az információ hogyan áramlik a vállalkozásban, hol kerülnek tárolásra, és hogyan használják fel őket. Mivel az adatok számos eszközön futnak keresztül, így hatékony biztonsági intézkedésekkel kell megvédeni őket.

Juttassa be a rendszerbe az információit

A legjobb fájlzinkronizáló és megosztó rendszer sem hatékony, ha a szükséges információ még mindig egy irattartó mélyén lapul. A Scan-to-cloud megoldással a dokumentumait intelligensen, közvetlenül a választott szolgáltatáshoz küldheti el, és lehetővé teszi azok biztonságos tárolását.

Szkeneljen felhőbe egyszerűen és biztonságosan a Ricoh Streamline NX szoftveres megoldásával.

Férjen hozzá, amikor szüksége van rá

A digitális fájlok praktikussága és rugalmassága ellenére adódhat olyan helyzet, amikor fizikai példányokra van szükség. Gondoskodjon arról, hogy a megfelelő információ mindig a megfelelő helyre jusson olyan **biztonságos nyomtatási megoldásokkal, mint a Ricoh Streamline NX Print2Me funkció.**

Mobil és vendégnyomtatás

Ha egy látogatónak vagy vendégnek sürgősen nyomtatnia kell, azt gyakran úgy oldják meg, hogy az anyagot elküldik valakinek mellékletben az irodában. Ez növeli annak a kockázatát, hogy akaratlanul vírusokat és rosszindulatú kódokat is továbbítanak. A végpontok közti kommunikáció az eszköz és a mobiltelefon között, valamint a felhő alapú lekéréses nyomtatás csökkenti a kockázatot. **Tudjon meg többet a Ricoh's MyPrint mobil nyomtatásról.**

Kezelje az információit

Egy dokumentumkezelő megoldás biztosíthatja, hogy minden alkalmazott megfelelő szinten férjen hozzá az információkhoz. A megoldás arról is információkkal szolgálhat, hogy ki, mikor és hogyan tekint meg vagy szerkeszt egy dokumentumot. **Fedezze fel, hogy a Ricoh és a DocuWare hogyan működik együtt a biztonságos és hatékony dokumentumkezelés lehetővé tételében.**

Forduljon
szakértőhöz

Látogasson meg minket a www.ricoh.hu webhelyen, vagy forduljon a helyi Ricoh márkaképviselőhöz, és ismerje meg, hogyan segíthetjük egy olyan munkahely felé vezető úton, amely épp annyira biztonságos, mint amennyire rugalmas.



Ricoh Hungary Kft.
2040 Budaörs
Puskás Tivadar út 14.



+36 23 806 800



www.ricoh.hu

RICOH
imagine. change.

Az ebben a brosrában közölt információk és ábrák meghatározott üzleti körülményekre vonatkoznak. Az egyedi körülmények eltérő eredményeket vonhatnak maguk után. Az összes vállalati, márká-, termék- és szolgáltatásnév a meghatározott tulajdonosok tulajdona és bejegyzett védjegye. Copyright © 2017 Ricoh Europe PLC. Minden jog fenntartva. Ez a brosrú, a tartalma és/vagy az elrendezése nem módosítható és/vagy nem kiigazítható, részben vagy egészben nem másolható, és/vagy más munkákba nem építhető be a Ricoh Europe PLC előzetes írásos engedélye nélkül.