INFORMASJONSSIKKERHET I AKSJON!

HVORDAN SKAL BEDRIFTEN DIN HOLDE INFORMASJONEN TRYGG I EN VERDEN DER CYBERANGREP BLIR SMARTERE OG COMPLIANCE VANSKELIGERE?

Canon

INDEKS

Data er alle moderne organisasjoners kronjuveler. Den gir økonomiavdelingen noe ekstra å gå på, lederteamet evnen til å forutse hendelser og de ansatte bedre forretningsintelligens.

Denne dyrebare ressursen må til enhver pris oppbevares trygt.

Etter hvert som verdien av dataene fortsetter å stige, øker også antallet fiender som prøver å stjele den. Fiendtlige angripere venter på å stjele informasjon når du minst venter det. I mellomtiden kan dobbeltagenter prøve å ta verdiene for seg selv.

Men det kreves ikke alltid en fiende for å felle en organisasjon.

En stor makt våker over landet og sørger for at alle følger sikkerhetsreglementet. Men selv om lovene er strenge og straffene er alvorlige, har det likevel aldri vært enklere å gjøre en feil.

Dagens bedrifter er ikke byer omringet av murer, og de er i økende grad fordelt på flere steder. Hybridarbeid betyr at ansatte lagrer, deler og samarbeider om informasjon på flere steder enn noen gang før.

I et slikt komplisert arbeidsmiljø kan det virke som en umulig utfordring å skulle holde informasjonen trygg og prosessene dine i samsvar med kravene.

Du trenger en pålitelig partner som kan sikre skatten din, beskytte deg mot skurker og hjelpe folket ditt med å overholde samsvar med kravene mot alle odds.

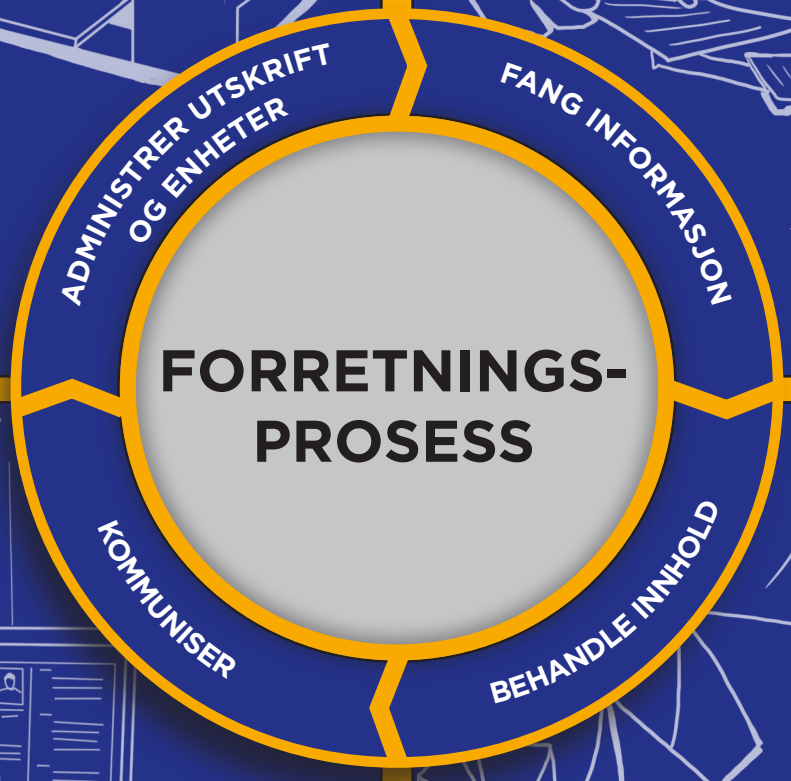
La oss utforske hvordan Canon og de hemmelige våpnene våre kan hjelpe deg med å takle utfordringen.

UTFORDRINGER I DOKUMENTETS LIVSSYKLUS

Dokumenter opprettes, kopieres, lagres og deles i løpet av livssyklusen innad i organisasjonen. Alle disse trinnene skaper utfordringer for å holde dataene trygge og i samsvar med kravene.

Utskrift er utfordrende for sikkerhet og samsvar fordi det er vanskelig å ha full oversikt over bruker- eller dokumentaktivitet, og dette kan føre til datasikkerhetsbrudd.

Skannede dokumenter som inneholder sensitive opplysninger, skal nå ønsket mål på en sikker måte. Brukerfeil under manuell dataregistrering.



Personopplysninger og sensitive opplysninger om kunder og ansatte må lagres, behandles og destrueres på en sikker måte, i samsvar med personvernreglene.

Utgående kommunikasjon, dokumenter og data må administreres på en sikker måte for å unngå problemer med informasjonssamsvar.

UTFORDRING 1

DEN HEMMELIGE STRATEGIEN

Organisasjon X har en stor hemmelighet: Den er klar for å ta fatt på et nytt eventyr. Lederteamet har bestemt seg for å investere i et nytt forretningsområde, i håp om å få ny makt og oppdage utallige rikdommer.

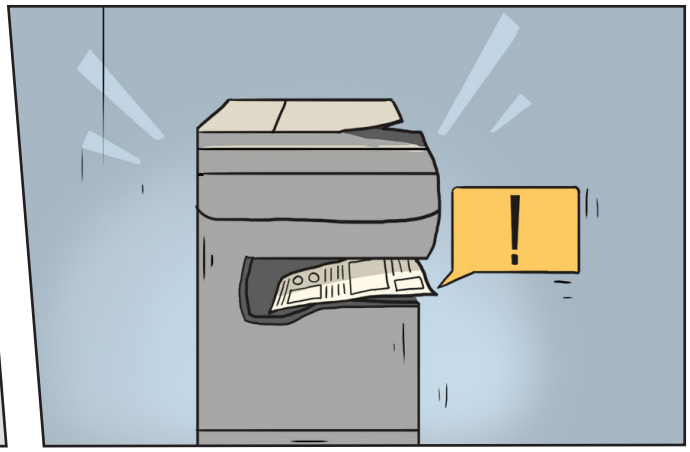
Det er helt avgjørende at disse planene holdes hemmelige frem til de offentliggjøres. Nyheten vil avsløre Organisasjon X' intensjon til konkurrentene, og advare dem om at det er en ny konkurrent i emningen. I mellomtiden er det mye som står på spill for de ansatte i Organisasjon X – kan det dukke opp nye muligheter i avdelingen deres? Nye forretningsområder som kan utforskes? Eller står jobbene deres i fare?

Topplederteamet må gå forsiktig frem hvis de skal sikre at planene deres ikke havner i hendene på sammensvorne ansatte og eksterne fiender. Gjennom hele budsjetterings- og kunngjøringsprosessen må de unngå en rekke feller, fra interne trusler til skadelig programvare og nettverksangrep. Kan de holde hemmeligheten sin trygg?

Kommunikasjonsteamet har utarbeidet en pressemelding som gjenspeiler organisasjonens nye strategiske retning. Informasjonen er fortsatt topphemmelig, og kunngjøringen skrives og godkjennes av en liten gruppe toppledere. Finansdirektøren Selma har bedt om å få se gjennom en fysisk kopi av dokumentet. Assistenten hennes, Polina, er klar til å skrive den ut for henne.

Utskrift representerer en større sikkerhetsrisiko enn organisasjoner er klar over. Typiske sikkerhetsrisikoer og risikoer vedrørende samsvar er at papirdokumenter tas fra skriveren før de hentes av brukeren, eller at de glemmes i sin helhet, slik at sensitive eller konfidensielle opplysninger blir eksponert for uautoriserte personer.

Innovasjon har også åpnet dørene for en rekke nye sikkerhetstrusler. Moderne flerfunksjonsskrivere er like kraftige som en datamaskin, og utstyrt med en harddisk, et minne og en prosessor (CPU), og er ofte koblet til Internett. Som et resultat av dette er det mulig for hackere som forsøker å få tilgang til nettverket og bedriftens data, å finne skriverfastvaren.



HEMMELIGE VÅPEN

imageRUNNER ADVANCE DX C5800

imageRUNNER ADVANCE DX C5800 er utviklet med innebygd sikkerhet som standard. Polina kan bare skrive ut dokumentet ved å logge seg inn på enheten med ID-kortet sitt. Dette betyr at ingen andre kan få tilgang til dokumentet som ligger i kø, og at det ikke blir liggende igjen i skuffen.

Enheten har også Trellix McAfee Embedded Control, som beskytter mot Zero-day-angrep og avanserte vedvarende trusler (APT) ved å blokkere kjøring av uautoriserte programmer via intelligent hvitelisting. McAfee Embedded Control hindrer at en angriper får tak i pressemeldingen gjennom et nettverksangrep, ved å beskytte mot programendringer.

Til slutt støtter imageRUNNER ADVANCE DX C5800 integrasjon av SIEM (administrasjon av sikkerhetsinformasjon og -hendelser), noe som gjør det enklere for organisasjoner å inkludere skrivere i eksisterende systemer for sikkerhetsovervåking (for eksempel Syslog). Disse systemene kan gjenkjenne og flagge sikkerhetshendelser på tvers av en enhetspark i sanntid, og varsler selskapet om eventuelle problemer eller trusler etter hvert som de oppstår.

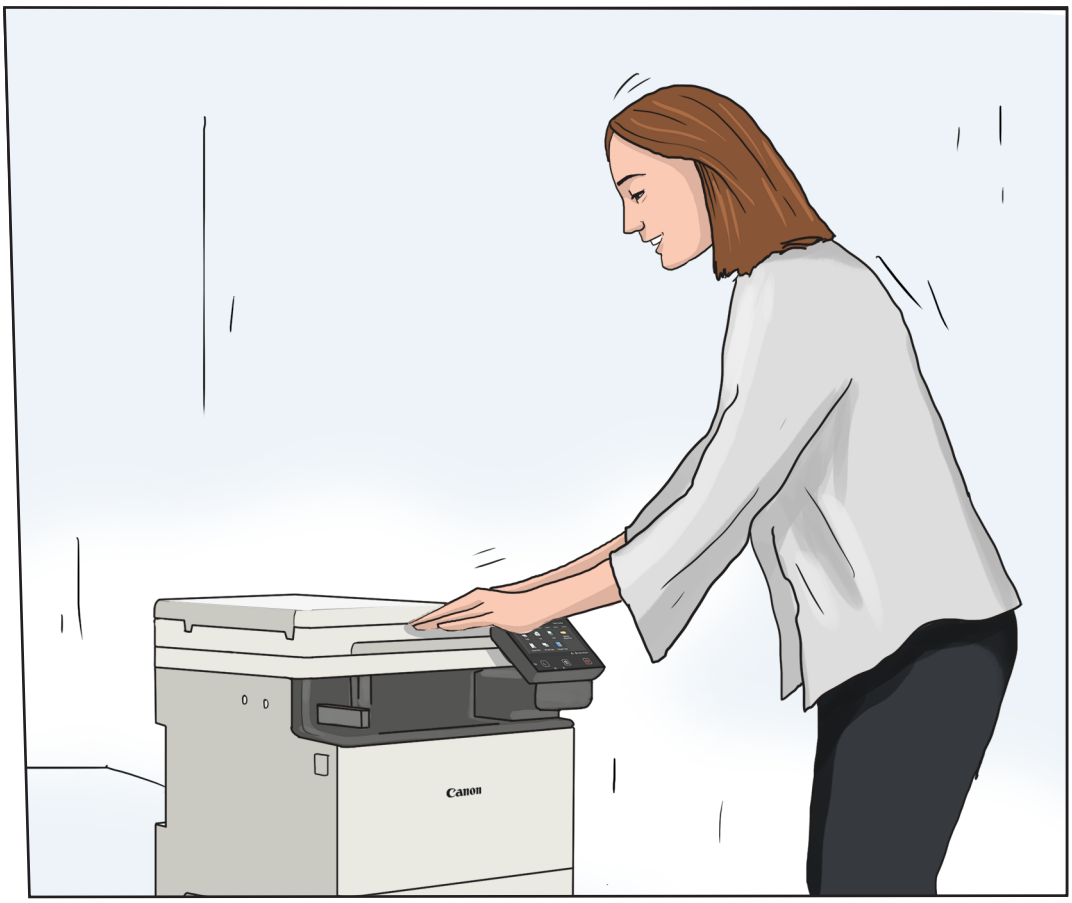
Tjeneste for styrking av enhet

Med Canon ivaretas sikkerheten allerede før du har kjøpt en enhet. Vi konfigurerer imageRUNNER ADVANCE MFD-er slik at sikkerheten styrkes, inkludert forsterking av innebygde sikkerhetskontroller og blokkering av uviktige funksjoner og usikrede porter. Den konfigurerte enheten kontrolleres og etterprøves før den sendes.

imageWARE Secure Audit Manager Express

Denne sikkerhetsløsningen for nettverksenheter gir Selskap X oversikt over dokumentrelaterte aktiviteter. Den kan registrere, arkivere og granske aktivitetene som forekommer på Canon-enheter. Når Polina skriver ut pressemeldingen, sender imageWARE Secure Audit Manager Express et e-postvarsel til IT-avdelingen om at et dokument med høy risiko skrives ut. Dette hjelper Organisasjon X med å holde seg oppdatert angående eventuelle uautoriserte ansatte eller parter som prøver å kopiere eller skrive ut sensitive opplysninger.

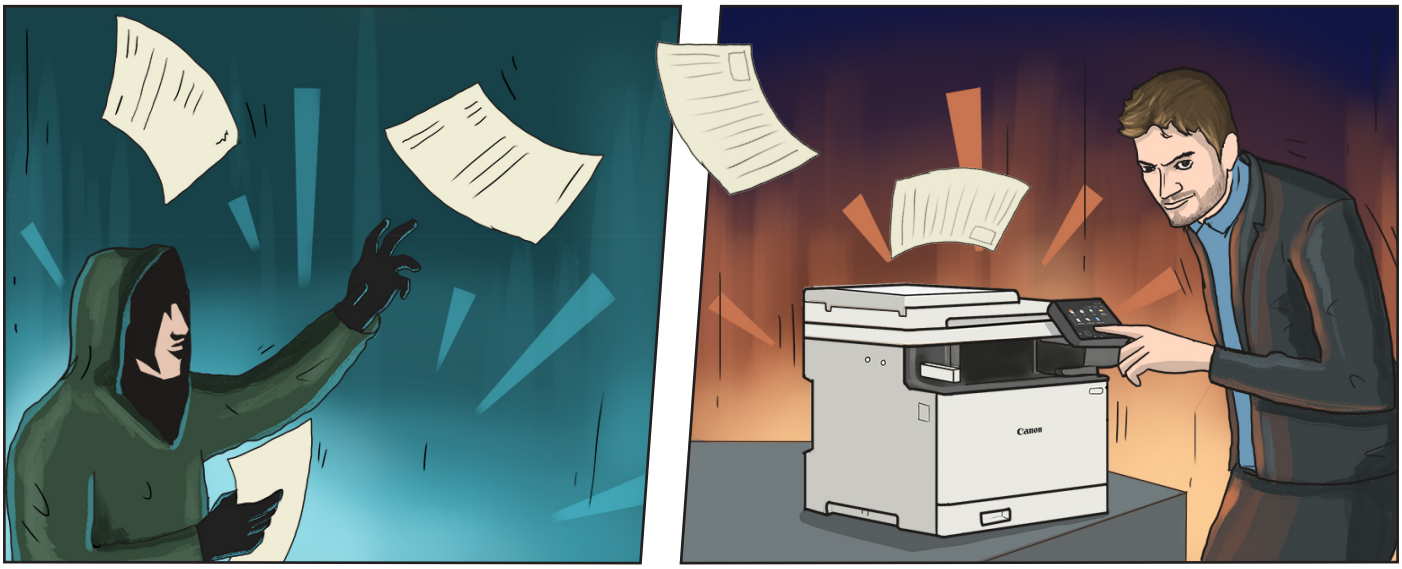
Selma har gjennomgått pressemeldingen og gitt noen skriftlige kommentarer. Polina må dele tilbakemeldingen med Pierre, som er PR-sjef og ansvarlig for kunngjøringen. Siden Pierre jobber hjemmefra, må Polina lage en digital kopi hun kan sende til ham. Når dokumenter skannes og sendes på e-post direkte fra enheten, gis angriperen en mulighet til å fange opp dokumentet.



Dagens skanneenheter er ofte Internett-tilkoblet, slik at brukerne kan sende dokumenter direkte til en mottaker via e-post eller lagre dem i en nettskytjeneste. Som et resultat av dette er det flere muligheter for at digital informasjon kan stå i fare. Derfor er det viktig at skanneenhetene har robuste sikkerhetsfunksjoner. Uten sikre funksjoner er skanneren sårbar for tukling – en intern bruker kan for eksempel endre køene for e-postruting slik at en e-postjobb sendes til en uautorisert bruker.

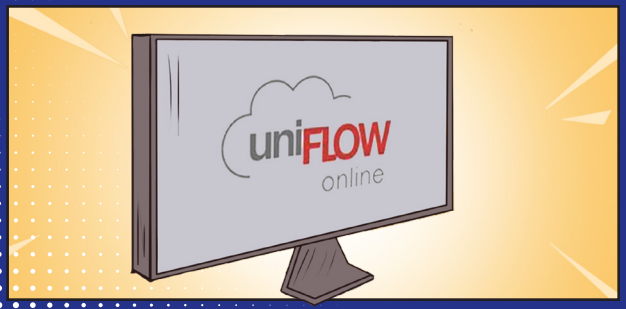
Eller et dokument kan åpnes, redigeres eller skrives ut dersom det ikke er kryptert.

Fra et eksternt perspektiv kan en angriper også få tilgang via nettverket og gjøre endringer i e-postkataloger slik at et dokument kan sendes til mottakere utenfor organisasjonen. Eller de kan fange opp et dokument som overføres over HTTPS, hvis dokumentet og dataene i det ikke er kryptert.



HEMMELIGE VÅPEN

i-SENSYS X C1333iF
Selma er klar til å skanne dokumentet ved hjelp av i-SENSYS X C1333iF. Denne multifunksjonelle enheten (som kombinerer utskrifts- og skannefunksjoner) har sikre skannefunksjoner som bidrar til å holde informasjonen trygg. Når den slås på, kontrollerer funksjonen for verifisering av systemet ved oppstart om det har vært noen forsøk på å sette enhetens integritet på spill, og den kan varsle Selma hvis enheten har blitt tuklet med. Deretter må Selma logge på med et ID-kort og sørge for at det finnes en logg over hvem som kopierer eller deler informasjon. Til slutt leverer IEEE802.1X-støtten på i-SENSYS X C1333iF en godkjenningsmekanisme, slik at den ved tilkobling til selskapets LAN eller WLAN gir en bekreftelse på dens autentisitet.



uniFLOW Online
Når Selma skanner kontrakten, oppretter uniFLOW Online en kryptert PDF og tilbyr valgfri passordbeskyttelse. Dette hindrer uautoriserte brukere i å se, redigere eller skrive ut dokumentet og beskytter informasjonen fra personer som prøver å fange den opp.

Tobias har hørt at selskapet kanskje beveger seg i en ny retning. Som leder for et av teamene som sliter med den nåværende strategien, vet han at dette kan bety alvorlige kutt i budsjettet deres i år, eller til og med en trussel mot jobbene.

Tobias er frustrert over nyhetene, så han planlegger å bekrefte sannheten i ryktene og muligens advare kolleger. Ettersom han tror at han vet hvor toppledelsen ville ha lagret de økonomiske dokumentene sine, begynner han en hemmelig jakt etter alt som kan være knyttet til de nye planene.

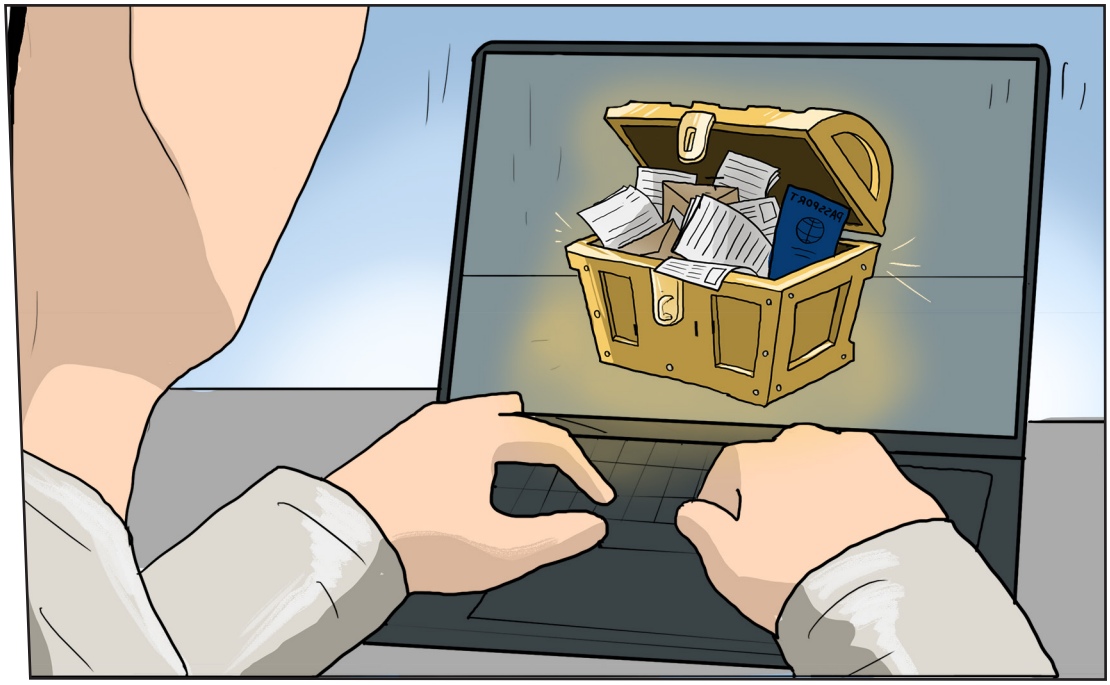
Organisasjoner oppretter og lagrer mer og mer informasjon hvert år. Når mange nå også bruker hybridmodeller, spres denne informasjonen på tvers av et økende antall steder, både fysisk og virtuelt. Som et resultat av dette er det vanlig for organisasjoner å ha problemer med tilfeldige lagringsstrategier, der ansatte bruker alt fra arkivskap til private nettskylagringstjenester som Dropbox, til oppbevaring av bedriftens data.

I tillegg håndterer de ansatte ofte sensitive opplysninger, for eksempel kontrakter, bankopplysninger for ansatte og bedriftsøkonomiske resultater. Det er nesten umulig for IT-teamene å sikre beste praksis for informasjonshåndtering, selv med slike kritiske opplysninger, når dokumenter lagres på en slik måte.

HEMMELIGE VÅPEN

Therefore Online
Therefore Online har robust, innebygd sikkerhet som gir organisasjoner mulighet til å angi automatiske retningslinjer for hvem som får tilgang til dokumenter, og hvordan informasjon lagres, deles og redigeres. Tilgangskontroller forhindrer at uautoriserte ansatte, for eksempel Tobias, åpner private eller sensitive dokumenter som pressemeldingen.

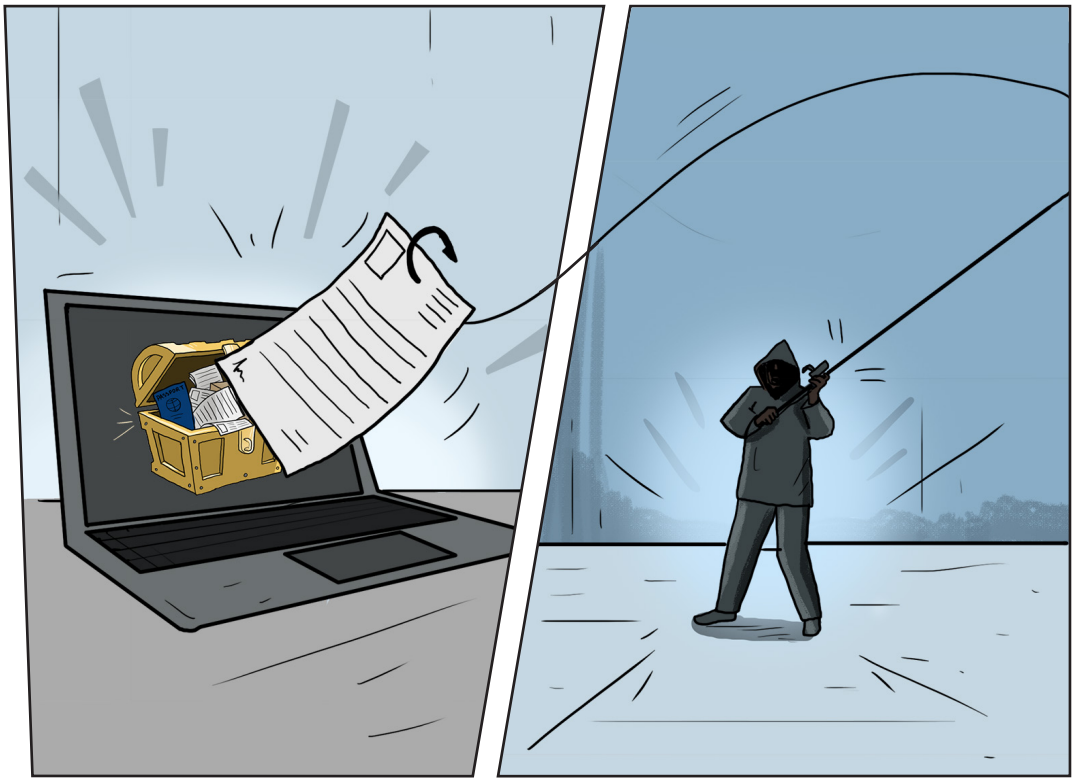
Therefore Online er skybasert, noe som sikrer at plasseringen til en bruker ikke påvirker tilgjengeligheten. Autoriserte brukere som arbeider hjemmefra eller på farten, har fortsatt tilgang til viktige dokumenter. All samhandling med et dokument spores. Dette sikrer at informasjonen administreres nøye, og er synlig fra ende til ende, noe som gir et digitalt spor for revisjon.



Pierre forbereder seg på å sende ut den hemmeligstemplede kunngjøringen til mottakere, inkludert hovedaksjonærer og utvalgte journalister. Det er viktig at dokumentet bare sendes til disse kontaktene. Han kan ikke risikere at det havner i feil hender.

I mellomtiden må han være forsiktig med den ekstra informasjonen som Organisasjon X holder hemmelig. Bedriftens database inneholder utallige skatter: sensitive opplysninger om mottakerne, inkludert deres e-postadresser og telefonnumre, samt journalistenes passinformasjon fra tidligere pressereiser.

Disse dataene er en potensiell skattkiste for tyver som kan bruke disse legitimasjonsopplysningene til å lekke kunngjøringen tidlig, eller, hvis de er så tilbøyelige, bruke opplysninger om personer i databasen til å utføre identitetstyveri eller organisere phishing-angrep.

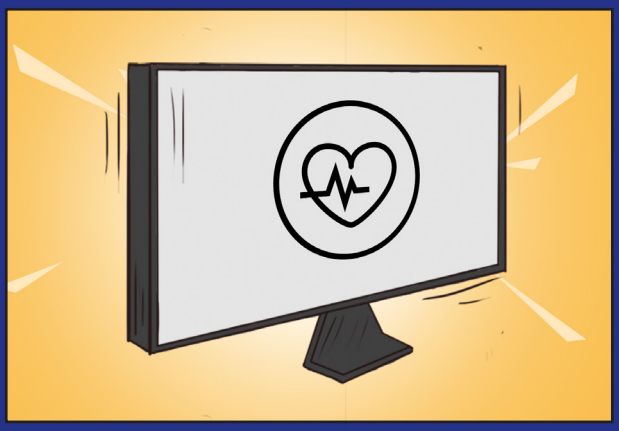


Bedrifter har ofte svært personlige og konfidensielle opplysninger om kunder, partnere og andre parter de arbeider tett med. Denne informasjonen finnes ikke bare på selskapets servere, men er inkludert i utgående kommunikasjon, som for eksempel kontoutskrifter, fakturaer og korrespondanse med disse partene.

Denne informasjonen er en risiko for bedriften fordi dersom den mistes eller blir stjålet av angripere, vil den utsette bedriften for betydelige bøter og skade på omdømmet. Hvis en organisasjon kommuniserer med disse kontaktene, er det imidlertid avgjørende at personlige opplysninger i kommunikasjonen bare når frem til mottakeren.

HEMMELIGE VÅPEN

Office Health Check
Tilstandskontroll på kontoret hjelper organisasjoner med å gå gjennom IT-miljøet for å sikre at det er trygt fra starten av. Den globale nettsikkerhetseksperten NCC Group vil utføre en ekstern analyse av organisasjonens interne og eksterne IT-infrastruktur, inkludert kommunikasjonskanaler og porter, for å avdekke eventuelle sikkerhetsproblemer. Ved å identifisere eventuelle problemer kan organisasjonen unngå at de utnyttes av en potensiell angriper, noe som forhindrer at Pierres kommunikasjon fanges opp, eller at opplysninger om journalistene eller interessentene blir stjålet fra databasene til Organisasjon X.



uniFLOW sysHub
uniFLOW sysHUB gir brukerne god kontroll og oversikt over kundekommunikasjonen, noe som gjør det enklere for Pierre å sikre at kommunikasjonen når riktig destinasjon. Denne løsningen befester interne kommunikasjonsprosesser og programmer i én arbeidsflyt og administreres fra ett enkelt operasjonspunkt. uniFLOW sysHUB automatiserer deretter denne arbeidsflyten for å gjøre den mer effektiv og redusere risikoen for feil. Hvert trinn i arbeidsflyten logges og lagres i et sysHUB-bibliotek for senere revisjon og for å støtte revisjonsspor, noe som gjør det vanskelig for en ansatt å bevisst lekke et dokument uten at det blir registrert. I mellomtiden kan Pierre kontrollere leveringsbeviset for å sikre at kommunikasjonen har kommet til rett person.

UTFORDRING 2

DEN KONFIDENSIELLE ANSATTE

Organisasjon Y må tiltrekke seg nye medarbeidere for å styrke det voksende kongeriket. Arbeidsstyrken pleide å være basert på ett sted, men takket være hybridarbeid er de modige ansatte spredt over hele landet. Det travle HR-teamet har måttet tilpasse seg raskt. Nye ansatte registreres nå gjennom virtuelle ansettelses- og tiltredelsesprosesser. HR-teamet må ha øyne overalt og kommunisere på tvers av store avstander for å dele konfidensielle dokumenter knyttet til nye ansatte.

HR-teamets store makt kommer hånd i hånd med stort ansvar. De er i besittelse av et fjell av verdifulle og sensitive opplysninger, fra lønnsopplysninger til helsestatus og resultatregistre. De vet at det er deres ansvar å holde denne informasjonen trygg og i tråd med samsvarslovgivingen. Revisorene er alltid i horisonten, og HR-teamet vet at de forventes å vise hvordan informasjon lagres og deles. Dette er ikke enkelt. Selv om HR-teamet jobber hardt, har de ikke superkrefter. Det er enkelt for teamet å havne i trøbbel på grunn av feil.

Uten de riktige teknologiløsningene på plass for å redde dagen kan dette føre til problemer for Organisasjon Y.

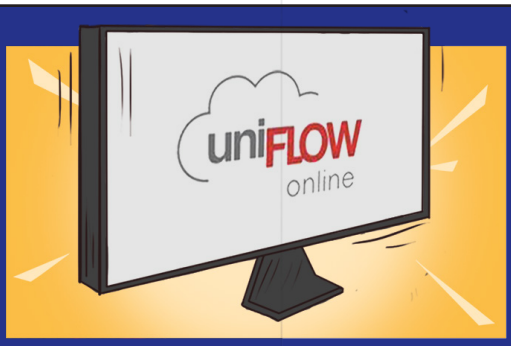
Etter en vellykket intervjuprosess har Organisasjon Y blitt enige om å ansette en ny medarbeider. Kandidaten har besøkt hovedkontoret for å levere passet sitt og undertegne kontrakten med Fatima, som er rekrutteringsansvarlig. Fatima ønsker å lage kopier av dokumentene til sine egne registre og for å dele dem med HR-sjefen som jobber hjemmefra. Det er enkelt for Fatima å skrive inn feil mottaker ved et uhell eller å lagre dokumentet på et sted der det er tilgjengelig for alle. Hvis feil person mottar det, kan de ganske enkelt åpne de registrerte dokumentene for å få tilgang til informasjonen.

Organisasjoner har et ansvar for å sikre at alle dokumenter som skannes, bare ses av de som har tillatelse til å se dem. En enkel feil kan føre til potensielle datatap eller -brudd, noe som kan ha en alvorlig innvirkning når det gjelder samsvar.

Hvis organisasjonen ikke innser at de har opplevd et alvorlig datasikkerhetsbrudd, og ikke rapporterer det, kan regulatoren for databeskyttelse utstede en bot på opptil 4 % av organisasjonens globale omsetning.

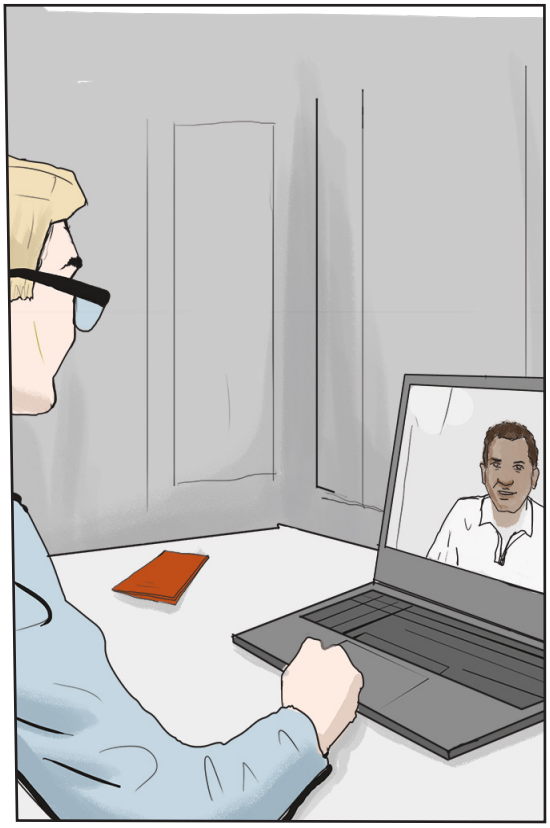
HEMMELIGE VÅPEN

uniFLOW Online
uniFLOW Online har innebygde arbeidsflyter for sikker skanning som gjør det mulig for Organisasjon Y å forhåndskonfigurere bestemte skannearbeidsflyter for hver bruker. Dokumentarbeidsflyter som HR-innrullering er allerede forhåndsdefinert, noe som hindrer at Fatima lagrer skanningen av en ny ansatt på feil sted.



imageFORMULA DR-S150
Fatima er klar til å skanne dokumentet ved hjelp av imageFORMULA DR-S150. Denne skanneren har sikre funksjoner som bidrar til å holde informasjonen trygg. Brukeren må logge seg på med et ID-kort for å sikre at det bare er brukeren som har tilgang til dokumentet som er registrert. Den bruker også automatisk kryptering på den digitaliserte versjonen, noe som betyr at det bare er en mottaker med et passord som kan lese, redigere og skrive den ut. imageFORMULA DR-S150-enheter har også alternativer for å sende dokumenter via sikre protokoller, som skanning til FTPS, SFTP og SMTPS.

IRISPowerscan
Selskapet har også IRISPowerscan, noe som betyr at dokumentene automatisk identifiseres som pass og kontrakt når de digitaliseres. Programvaren korrigerer alle skannefeil, for eksempel skjevheter, og bruker optisk tegngjenkjenning til å gjenkjenne viktige detaljer som den ansattes navn og passnummer. Disse opplysningene legges til i indekseringen, noe som gjør det enklere for organisasjonen å finne dem i fremtiden. I tillegg ruter IRISPowerscan skanninger av kontrakter og pass automatisk til riktig sikkert lagringssted i bedriftens system.



Under rekrutteringsprosessen var flere ansatte, inkludert Fatima og Nick, en kollega, involvert i intervjuer med kandidatene og gjennomgang av CV-er. Begge ansatte arbeider virtuelt, på forskjellige steder i Europa. Både Fatima og Nick har kopier av kandidatenes CV-er og notater om intervjuene lagret på deres private bærbare PC-er og på delte Dropbox-steder. Når den nye kandidaten har fått tilbud om jobben, er det lett for Fatima og Nick å glemme å slette disse dokumentene.

Nylig innstrammet lovgivning betyr at samsvar er viktigere enn noen gang. Lover som personvernforordningen har innført bestemte regler som regulerer hvordan informasjon må lagres. Organisasjoner skal for eksempel ikke bevare personlig identifiserbar informasjon lenger enn det som er strengt nødvendig. Likevel sliter mange organisasjoner fortsatt med tilfeldige lagringsstrategier, uten offisielle plasseringer for å lagre dokumenter, eller muligheten til å finne dokumenter lagret på egne servere.

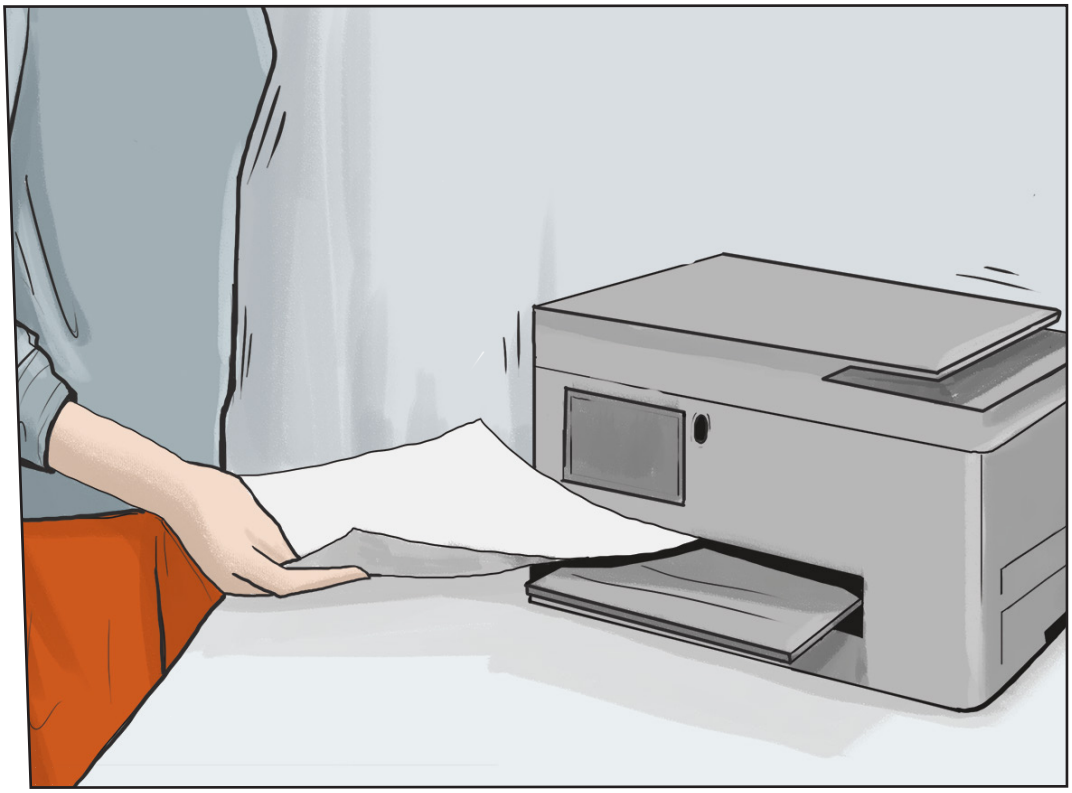
Dersom en tidligere ansatt, eller en tidligere kandidat, ber organisasjonen om tilgang til et emne, vil det være svært vanskelig for selskapet å oppgi hvilken informasjon de har. I tillegg vil organisasjonen ha problemer med å vise at de har kontroll over hvor personlig identifiserbar informasjon lagres, når det kommer til revisjonsformål.

HEMMELIGE VÅPEN

Therefore Online
Therefore Online har robust, innebygd sikkerhet som gir organisasjoner mulighet til å angi automatiske retningslinjer for hvem som får tilgang til dokumenter, og hvordan informasjon lagres, deles og redigeres. Den sporer all samhandling med et dokument som finner sted, holder informasjonen nøye administrert og synlig fra ende til ende, noe som gjør revisjonsprosessen mye enklere.

Organisasjon Y kan også angi automatiske retningslinjer for oppbevaring, for å sikre at gamle dokumenter som inneholder sensitive opplysninger, slettes etter en passende lagringsperiode, noe som gjør at de overholder reglene. Ettersom Therefore Online er skybasert, kan teamene laste opp dokumenter og være sikre på at de er trygge og sikre, selv når de befinner seg på en ekstern plassering.

Ingrid, den ansattes nye linjeleder, jobber hjemmefra og forbereder seg på å gjennomføre et innledningsintervju på kontoret neste dag. Hun ønsker å skrive ut en kopi av brevet som bekrefter den nyansattes lønn, sammen med andre skjemaer, for å dele med dem i løpet av den prosessen. Ingrid har nettopp begynt å jobbe hjemmefra og har ikke blitt utstyrt med en jobbskriver, så hun bruker sin private enhet.

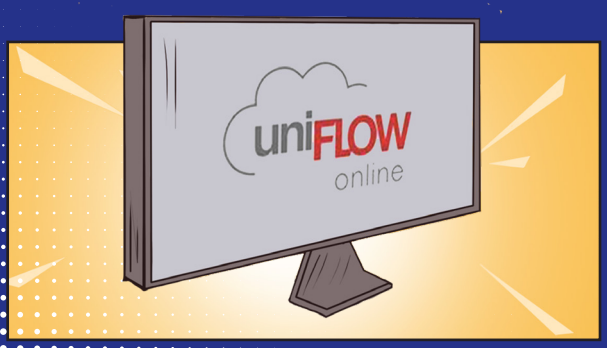


Det er lett for organisasjoner å glemme at skrivere spiller en stor rolle når det kommer til sikkerhet og overholdelse av arbeidsflyter, med enhetene som inneholder verdifulle data og dokumenter. Som en del av juridiske forpliktelser når det gjelder samsvar, forventes det at organisasjoner deler revisjonsspor som rapporterer hvordan sensitive opplysninger brukes.

Dette krever at de har bedre oversikt og sporing av hvordan dokumenter samhandler med enheter. Når Ingrid bruker sin private skriver, er den imidlertid ikke koblet til bedriftsnettverket. Det er dermed ingen sporbarhet, ingen registre med dataene som er lagret på enheten, og ingen garanti for at de er sikre.

HEMMELIGE VÅPEN

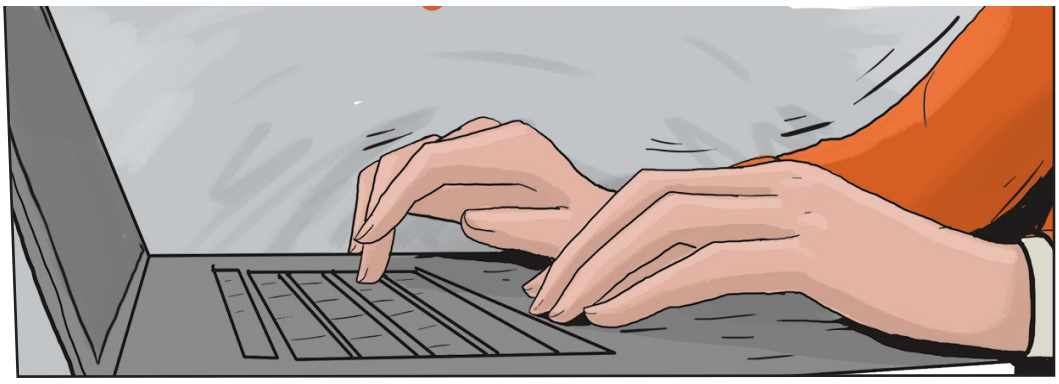
MAXIFY GX6050
Denne effektive skrivebordsskriveren produserer utskrifter av høy kvalitet for hjemmekontorer, og den bidrar også til å holde dokumenter sikre og i samsvar med kravene, takket være den innebygde integrasjonen med uniFLOW Online. Skann til meg selv-funksjonen hindrer Ingrid fra å sende dokumenter til andre enn sin egen e-postadresse eller private mappe, for å unngå at hun sender forretningsdokumenter til personlige kontakter ved et uhell. Funksjonen for sikker frigivelse av utskriftsjobber betyr at Ingrid bare skriver ut dokumenter når hun er klar, noe som betyr at sensitive forretningsdokumenter ikke blir liggende på enheten.



uniFLOW Online
Denne innebygde programvaren integrerer MAXIFY GX6050 med organisasjonens miljø, slik at IT-teamet til Organisasjon Y kan spore Ingrids utskriftsaktivitet og rapportere hvordan sensitive opplysninger brukes, selv når hun jobber hjemmefra.

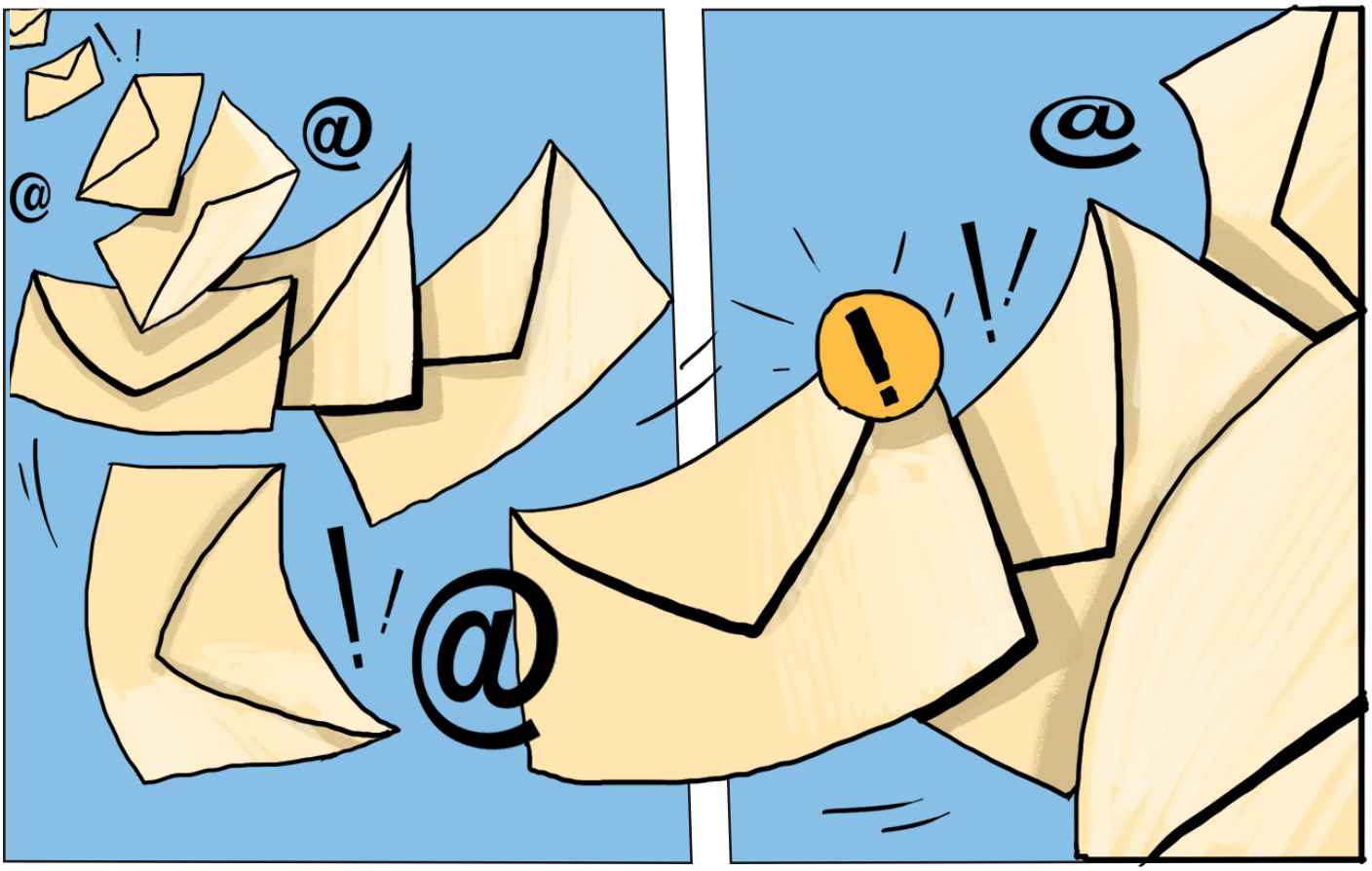
Det er slutten på den nyansattes første måned, og Fatima fra personalavdelingen er i ferd med å sende ut lønnsslipper. Dessverre har den nyansatte samme fornavn som en annen ansatt. Fatima sender ved et uhell begges lønnsslipper til feil mottaker, noe som betyr at begge kan se hvor mye den andre tjener.

Organisasjonen har brutt medarbeidernes konfidensialitet. Teknisk sett har de grunn til å ta selskapet til en arbeidsdomstol. Etter å ha sett kollegaens lønnsslipp, tar den nyansatte nå opp sin egen lønn med personalavdelingen og føler kanskje ikke lenger at han/hun er komfortabel med å bli værende i rollen sin.



Kommunikasjon er et høyrisikostadium i alle dokumentarbeidsflyter fordi det innebærer å dele informasjon, enten det er internt med ansatte eller eksternt med kunder, leverandører og andre interessenter.

Ved en standardrevisjon forventes det at organisasjoner viser hvordan sensitive opplysninger deles med andre parter. Gitt det store volumet av kommunikasjon som en organisasjon gjennomfører i løpet av en gitt uke, er det helt avgjørende å ha løsninger på plass som gjør det mindre vanskelig å spore disse prosessene.



HEMMELIGE VÅPEN

uniFLOW sysHub
uniFLOW sysHU gir brukerne tett kontroll og oversikt over den interne kommunikasjonen, noe som gjør det enklere for Fatima å holde personalkommunikasjonen konfidensiell. Løsningen samler interne kommunikasjonsprosesser og programmer i én arbeidsflyt, samtidig som det administreres fra ett enkelt operasjonspunkt. uniFLOW sysHUB automatiserer denne arbeidsflyten for å gjøre den mer effektiv og redusere risikoen for feil. I dette eksemplet vil ikke Fatima kunne sende konfidensiell informasjon til en annen ansatt ved et uhell.

Hvert trinn i arbeidsflyten logges og lagres i et sysHUB-bibliotek for senere revisjon og for å støtte revisjonsspor, noe som betyr at Fatima kan kontrollere leveringsbeviset for å sikre at kommunikasjonen har nådd riktig person.

HVORDAN KAN VI HJELPE TIL?

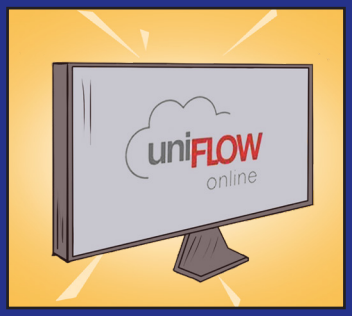
Alle bedrifter ønsker å holde informasjonen sin sikker og i samsvar med kravene. Men som Organisasjon X og Y har vist, er det et fiendtlig landskap der ute. Organisasjoner kjemper ikke bare mot flere skurker enn tidligere, men strengere lovgivning betyr at innsatsen er høy når det gjøres feil. Det kan virke som en tapt kamp, men det trenger ikke å være det. Hemmeligheten er å ha riktig teknologi og partner på din side.

Canon er ledende innen IDC MarketScape for løsninger og tjenester for utskrifts- og dokumentsikkerhet, samt innen Quocirca Print Security Landscape. Maskinvarene, programvarene og tjenestene våre er utformet for å bidra til at organisasjonen din drives så effektivt som mulig i en komplisert verden. Teknologien vår støtter alle arbeidsmiljøer, uansett hvor medarbeiderne dine er basert, eller hvor du befinner deg på den digitale transformasjonsreisen din.

Med vår «sikker utforming»-tilnærming tar vi det harde arbeidet med å holde informasjon trygg. Løsningene våre er bygget for å hindre angrep, beskytte data og opprettholde og sikre samsvar, slik at du kan dra nytte av nye funksjoner uten å skape mer arbeid for teamet ditt.

ENHETER FOR UTSKRIFT OG SKANNING
Vår utskrifts- og skanneportefølje er utstyrt med de nyeste sikkerhetsfunksjonene for å sikre viktige data i alle trinn i dokumentarbeidsflyten. Alle Canon-produkter sikkerhetskontrolleres i design- og utviklingsfasene samt før de utgis.

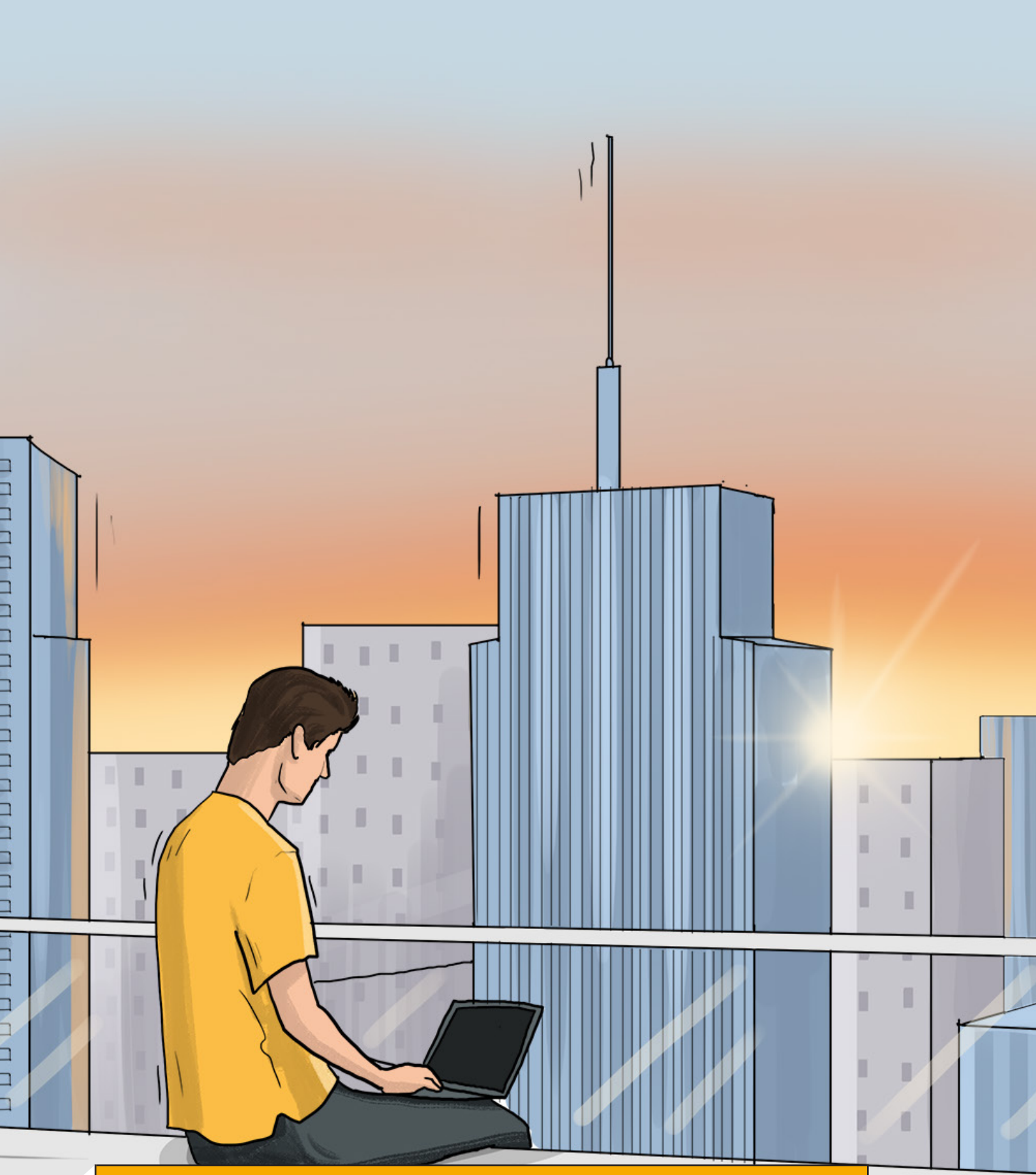
Vi fortsetter å bygge sterke partnerskap med industriledere, for eksempel Trellix og Microsoft, for å sikre størst mulig dekning og kompatibilitet ved sikring av enhetsparken. Og vi har et dedikert team for respons på produktsikkerhetshendelser.



PROGRAMVARE
Vi forstår at informasjon ikke er bundet av stedet, og derfor tilbyr vi programvare som beskytter data uansett hvor de befinner seg. Vi samarbeider også med eksterne organisasjoner som IOActive for å utføre penetrasjonstester på utgivelsesstadiet og for store programvareoppdateringer.

TJENESTER
Vi tilbyr sikkerhetstjenester som er utviklet for å hjelpe deg med å opprettholde databeskyttelsessamsvar og beskytte sensitive data gjennom hele levetiden til utskrifts- og skanneinfrastrukturen.


PASSPORT



Er du klar til å bekjempe sikkerhets- og samsvarsbrudd? Kom og se hvordan teknologien vår fungerer i utstillingsrommet vårt, eller bestill en demonstrasjon med vårt dyktige salgsteam for å se hvilke løsninger som er best egnet for bedriften din.

Vil du vite mer om de hemmelige våpnene våre? Besøk nettstedet vårt for digitale transformasjonstjenester for å finne ut mer.

OM CANON

Canon er bilder. Vi prøver å gjøre en forskjell og skape mulighet for endring.
For kundene våre når de gjør digitale endringer og arbeider på nye måter.
For større samfunnsmessige endringer med vårt kontinuerlige fokus på bærekraft som en del av vår bedriftskultur.

Til slutt er vi i endring ved at vi investerer i nye markeder, produkter og teknologier.
Dermed har vi et langsiktig perspektiv som er til fordel for alle: kundene våre, medarbeiderne våre og samfunnet generelt.

CANON ER BYGD PÅ FIRE HOVEDPILARER:

Innovasjon

En lang historie med innovasjon drevet av bildebehandling, som har levert nyskapende teknologi i mer enn 80 år. Banebrytende ideer for bransjen og et sterkt engasjement for teknologiske nyvinninger.

Støtte

Et variert utvalg av tjenester som sikrer toppkvalitet og fornøyde kunder. Intern ekspertise arbeider for å øke effektiviteten og er fokusert på å frigi potensiale for kundene våre.

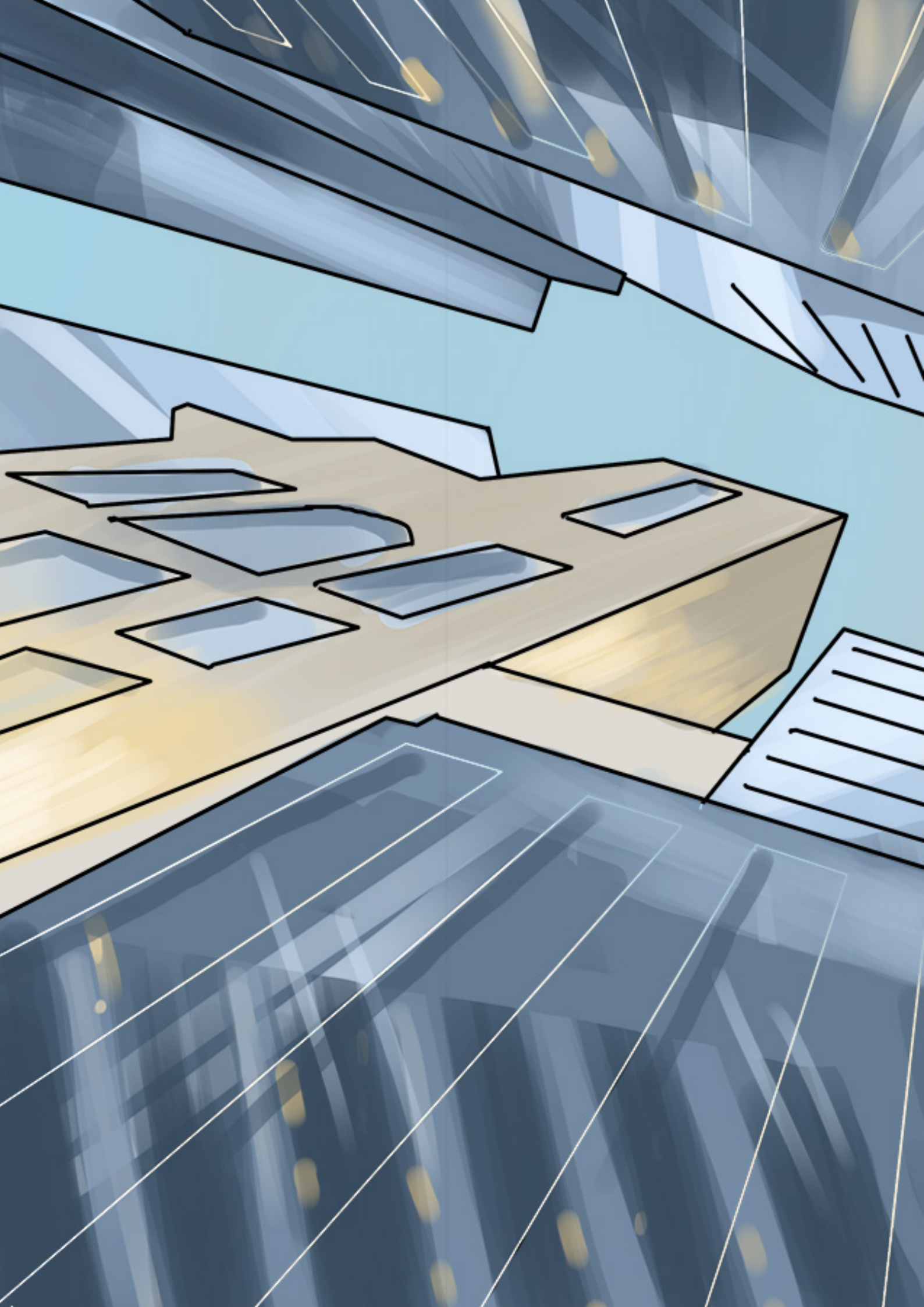
Sikkerhet

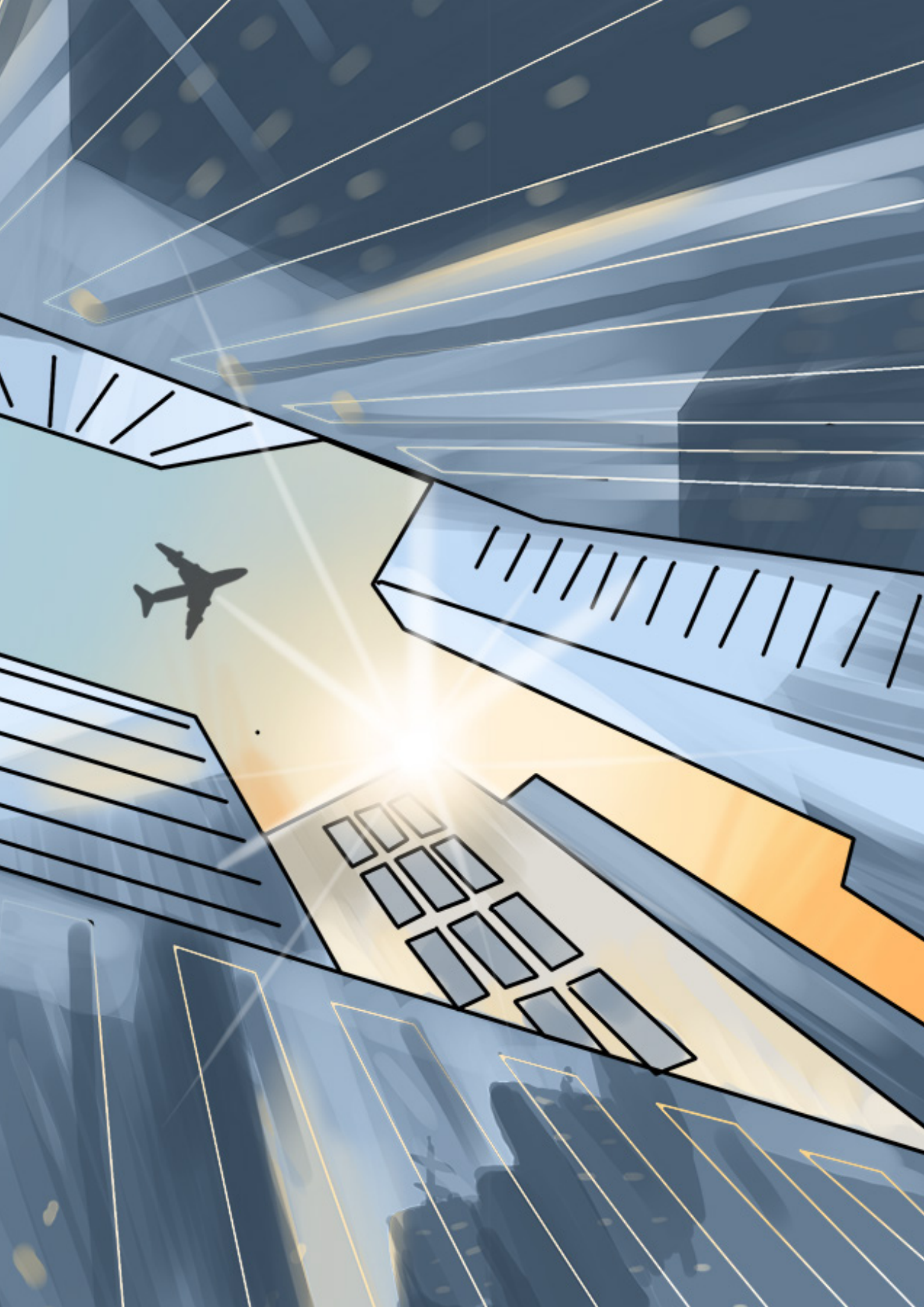
Canons løsninger og tjenester bidrar til å sikre alle dokumenter og sensitive data, enten de er på papir eller i digitalt format, gjennom hele dokumentlivssyklusen. Sikker utforming: Enhetene, løsningene og tjenestene er utviklet med sikkerhet i tankene.

Bærekraft

Canon har innrettet sin praksis for bærekraft etter FNs bærekraftsmål, som forpliktelser til å redusere CO2-utslipp i hele produktets livssyklus ved å redusere emballasjemengden og konsolidere distribusjonssentre.

ALT DETTE GJØR CANON TIL DEN RETTE PARTNEREN FOR DEG.





Canon Inc.
Canon.com

Canon Europe
canon-europe.com
Norwegian edition

Canon Norge AS
Hallagerbakken 110
Postboks 33
Holmlia
1201 OSLO
Tlf. +47 2262 9200
canon.no