IRON MOUNTAIN®

OMPRÖVA ITAD-HANTERINGEN: FALLGROPAR SOM MÅSTE UNDVIKAS

AV: BROOKS HOFFMAN

Kanske har ditt företag köpt in begagnade telefoner eller laptops och sedan upptäckt att de innehåller personlig information från tidigare ägare.

Eller så har du kanske läst om globala storföretag som blivit dömda till böter i miljonklassen för att ha avyttrat sina IT-tillgångar på ett otillåtet sätt.

Eller så har du kanske sett hemska nyhetsreportage om soptippar i utvecklingsländer med enorma högar av kasserad elektronik – vilket förstör områdena där de är belägna och utgör lockbete för cyberbrottslingar som vet att elektroniken kan innehålla värdefull information som är lätt att komma över.

Anskaffning av IT-utrustning är ofta en kritisk aktivitet i de flesta teknikbaserade företags strategier. Vad som händer med IT-enheterna när de når slutet av sin livslängd - och fortfarande innehåller data om företaget och dess kunden - är ofta en tanke som dyker upp alldeles försent.

Med tanke på att produktcyklerna förkortas, tekniken utvecklas i snabbare takt och allt fler företag använder sig av molntjänster, är det viktigt att tänka igenom och ge ITAD ett starkare fokus. Du kommer att tvingas hantera en växande mängd IT-enheter i takt med att de når slutet av sin livslängd. Att göra rätt val kring din ITAD-strategi är ett sätt att begränsa affärsriskerna och skydda miljön.

E-AVFALL: DET SNABBAST VÄXANDE AVFALLSFLÖDET

Globalt genererar vi cirka 53 miljoner ton elektroniskt avfall (e-avfall) varje år, en mängd som beräknas mer än fördubblas fram till år 2050, enligt FN. Det innebär att e-avfall är det snabbast växande avfallsflödet i världen. IT – inte bara energiförbrukningen utan själva hårdvaran – är nu en stor del av vårt miljöavtryck. Och en giftig sådan: tungmetaller (kvicksilver, bly, kadmium och mer) kan läcka ut från dessa enheter och in i ekosystemet, vilket orsakar en lång rad problem. Det är inte förvånande att allt fler länder inte längre tar emot elektroniskt avfall. Thailand är det senaste, per september 2020.

SÄKERHET OCH JURIDISKA UTMANINGAR

E-avfall skapar även omedelbara säkerhets- och juridiska problem. Cirka 25 delstater i USA, plus District of Columbia, har antagit lagar som stipulerar en viss grad av elektronikåtervinning och har infört straff för brott mot processen. Ontario i Kanada har börjat tillämpa nya regler för e-avfall, med målet att uppnå en återvinningsgrad på 70 %. Det finns dessutom många lagar och förordningar - både nationella och internationella - kring dataintegritet och dataskydd som har bred inverkan på hur IT-tillgångar kan avyttras. Till exempel så riskerar företag som berörs av GDPR (EU:s dataskyddsförordning) höga böter för bristande efterlevnad - potentiellt upp till 20 miljoner euro eller 4 % av den årliga globala omsättningen - beroende på överträdelsens allvarlighet och andra omständigheter.

TYPISKA ITAD-MISSTAG

Det är viktigt att ha tydliga rutiner för trygg och säker ITAD-hantering, men det är lätt att göra fel. Här är några vanliga fallgropar som måste undvikas.

ATT TA FÖR LÄTT PÅ SAKEN

Många företag ser det som en struntsak att göra sig av med gammal IT-hårdvara – det är bara att rensa enheterna och få iväg dem. Tyvärr är det inte så enkelt. Krånglet med att rensa, förstöra och avmagnetisera kräver beprövade procedurer och operativ effektivitet. Att bara ta bort, formatera om eller återställa innebär inte med säkerhet att data raderas. Om data inte är ordentligt raderad eller om enheter inte förstörs ordentligt så finns det fortfarande risk för dataintrång.

ATT LÅTA IT TA HAND OM ITAD

Att lägga ITAD-ansvaret på din IT-personal kan verka logiskt, men om det inte är en självklarhet för dem så är det heller inte nödvändigtvis logiskt. Processen att på ett tryggt och säkert sätt avveckla IT-utrustning har tekniska, juridiska, logistiska och administrativa aspekter för vilka din IT-avdelning kanske är, eller inte är, rustad - som bland annat:

- Samordning med de personer och avdelningar som är beroende av att data och enheterna som har nått sitt livsslut.
- Implementering av de specifika procedurer som krävs för att helt radera alla befintliga data.
  - Bedöma om chain-of-custody (spårbarhetskedjan - spåra vem som hade tillgång till enheterna och när) uppfattas korrekt
  - Utvärdera miljö- och datasäkerhetsreferenserna för tredjepartsleverantörer

Självklart har IT-avdelningen en viktig roll men det har även andra administratörer, avdelningar och företagsledningen.

ATT UNDERSKATTA DITT JURIDISKA ANSVAR

I takt med att mängden e-avfall ökar, så ökar även antalet lagar och förordningar som styr detta, och även sanktionerna för bristande lagefterlevnad. En finansiell tjänsteleverantör dömdes nyligen till en bot på 60 miljoner USD för att ha misskött avvecklingen av två datacenter. De är långt ifrån det enda företaget som har fått betala ett högt pris.

Det är inte bara de lagar och förordningar som specifikt reglerar e-avfall som du måste känna till. Som nämnts ovan faller e-avfall också under GDPR, industristandarder, nationella integritetslagar och mera vida omfattande regler såsom Sarbanes- Oxley (SOX) med flera.

ATT FÖRLITA SIG PÅ GRATISTJÄNSTER

Det finns företag som erbjuder ITAD-tjänster gratis eller till ett mycket lågt pris. Dessa hävdar vanligtvis att de täcker sina kostnader genom vidareförsäljning av dina enheter. Som alltid så får du vad du betalar för. Att förlita sig på en gratis ITAD-leverantör eller en som erbjuder ett mycket lågt pris är inget undantag och innebär sannolikt att leverantören gör en eller flera av följande:

- Behåller betydande intäkter från återvinning av din utrustning, dvs att tjänsten inte alls är gratis.
- Snålar med saker såsom säker chain-of-custody eller att de inte helt kan säkerställa att data förstörs på alla enheter. Gör sig av med din utrustning på ett sätt som är miljömässigt oansvarigt (t.ex. skicka utomlands eller dumpa på soptippar här hemma).

Kort sagt, du kanske sparar pengar på mycket kort sikt, men du utsätter din verksamhet för risker och bidrar till den mycket negativa miljöpåverkan som återvinning är tänkt att undvika.

ATT BORTSE FRÅN CHAIN-OF-CUSTODY

Du kanske inte omedelbart associerar ett juridiskt koncept såsom chain-of-custody med ITAD-hantering, men det är faktiskt nyckeln till att göra det korrekt. Oavsett om du hanterar ITAD på egen hand eller förlitar dig på en extern part, behöver du en fullständig registrering över var och till vem dina IT-tillgångar transporterats. Bara då kan du avgöra om din ITAD-process faktiskt är ansvarsfull och lever upp till både miljömässiga och datasäkra perspektiv. Det finns också ytterligare en fördel med en säkra chain-of-custody - den är stöldavskräckande. Stöld av enheter under ITAD-hanteringen kan skapa allvarliga problem. Ju mindre och mer värdefullt ett föremål är, desto mer sannolikt är det att det försvinner och tjuvar är mindre benägna att försöka stjäla en tillgång om de vet att den spåras.

Detta är alla exempel på fallgropar som även företag med goda intentioner kan hamna i. Men den största fallgropen av alla är att inte - förrän det är försent - tänka igenom vad som kommer att hända med IT-utrustningen efter dess livstid.

Tänk istället på det här som en kritisk del av din fortlöpande livscykel för informationshantering. En viktig del som skyddar både känsliga information och miljön.

Brooks Hoffman arbetar med Product Management inom Iron Mountains tjänst för Secure IT Asset Disposition ("SITAD"). Innan han kom till Iron Mountain var han en av grundarna till och finanschef för LifeSpan, ett IT Asset Disposition-företag med huvudkontor i Denver, Colorado.