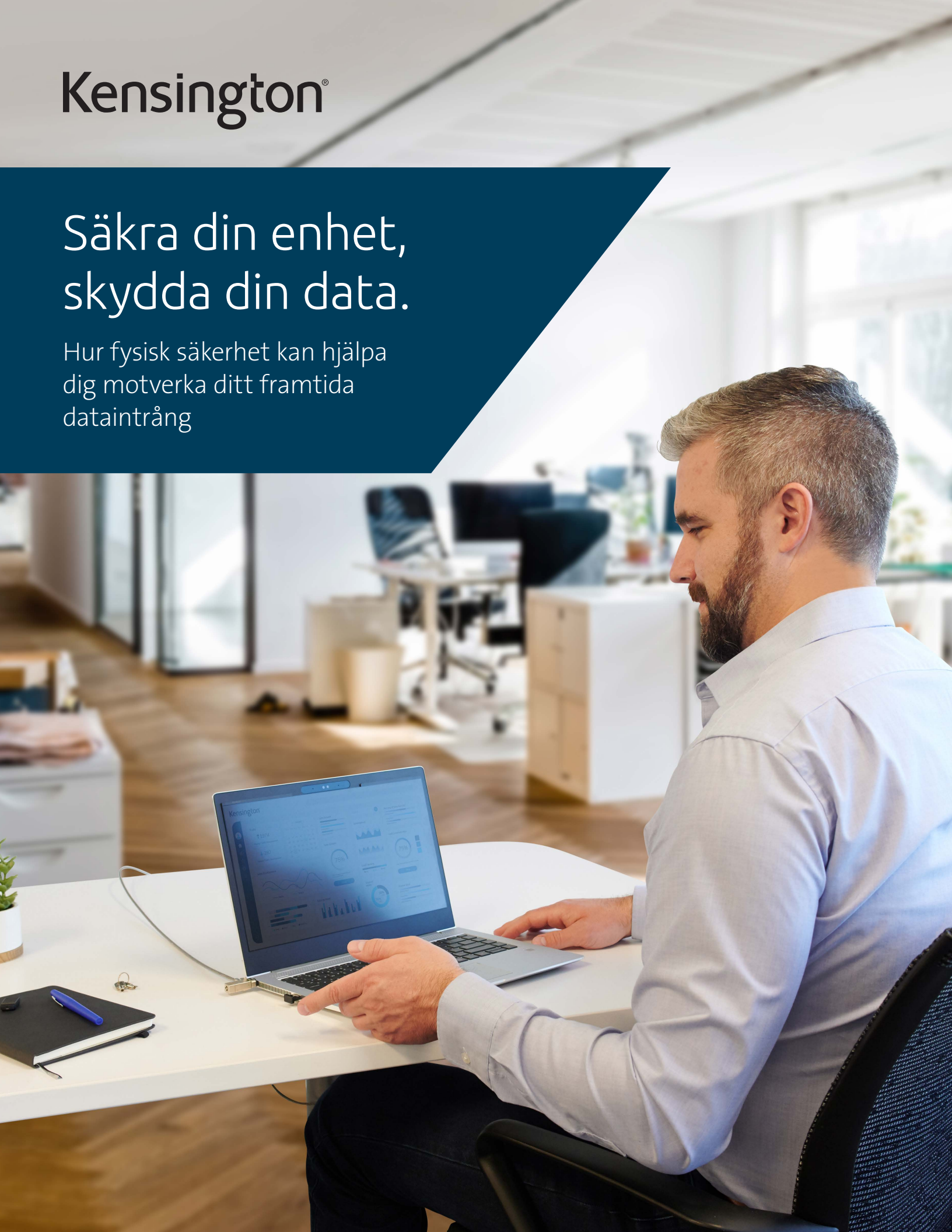
Kensington®

Säkra din enhet, skydda din data.

Hur fysisk säkerhet kan hjälpa dig motverka ditt framtida dataintrång



Introduktion

Säkerhetslandskapet har förändrats dramatiskt under de senaste åren, drivet av stora förändringar i hur och var vi arbetar. Den främsta drivkraften var COVID-19-pandemin, som påskyndade införandet av hybrida och flexibla arbetsmodeller och fundamentalt förändrade prioriteringarna för enhetssäkerhet.

Kensington sponsrade en studie genomförd av den oberoende marknadsundersökningsspecialisten Vanson Bourne, där 1 000 seniora IT-beslutsfattare med ansvar för sina organisationers fysiska hårdvarusäkerhet i USA och EMEA deltog.

Nästan alla som svarade (**92%**) hade skärpt sina säkerhetspolicys som en reaktion på pandemin och insåg de ökade riskerna med decentraliserade arbetsmiljöer. När vi blickar framåt förväntas andelen flexibla arbetsmodeller att öka, vilket understryker att tiden att omvärdera strategier för enhetssäkerhet är nu.

Dataintrång är inte bara ett digitalt problem – varje stulen eller oskyddad enhet utgör en potentiell ingång för obehörig åtkomst till känslig information, vilket innebär betydande risker för organisationer. Med de ekonomiska konsekvenserna av dataintrång som nu uppgår till miljontals dollar varje år har insatserna aldrig varit högre. När organisationer fortsätter att anpassa sina arbetsmodeller har behovet av att adressera enhetssäkerhet ökat avsevärt. Strängare krav på dataskydd och en ökning av dataintrång har ytterligare stärkt vikten av att skydda både fysiska enheter och den känsliga information de innehåller. Denna rapport belyser den avgörande roll som säkerhetslås spelar för att minska dessa risker och understryker varför det är nödvändigt att agera nu för att ligga steget före framtida utmaningar.

Genom dessa insikter, kommer vi att undersöka de mest konkreta konsekvenserna av enhetsstölder, visa hur enkla men effektiva lösningar såsom säkerhetslås kan bidra till att minska risker och vi lyfter även fram hur fysisk säkerhet skapar trygghet i en värld där arbetsmodeller ständigt utvecklas. Från att förstå de förödande konsekvenserna av enhetsstölder till att demonstrera kostnadseffektiviteten och tryggheten med lås, erbjuder denna rapport även insikter och metoder att använda sig av för organisationer som drivs i dagens komplexa säkerhetslandskap.

Viktiga resultat:

76% av de tillfrågade säger att deras organisationer har påverkats av stölder under de senaste två åren, där incidenter är vanligare i organisationer med hybrida arbetsmodeller. Vår forskning visade till exempel att **85%** av organisationer med hybrida arbetsmodeller har upplevt en stöldincident under de senaste två åren, jämfört med **71%** av organisationer vars anställda arbetar helt på kontoret.

Konsekvenserna av enhetsstölder sträcker sig bortom själva förlusten av hårdvara och inkluderar:

- behovet av att förbättra befintliga säkerhetsåtgärder (**33%**)
- juridiska eller regulatoriska konsekvenser på grund av kompromitterad data på stulna enheter (**33%**)
- Minskad produktivitet och arbetstid för anställda till följd av förlorade eller stulna enheter (**32%**)

Organisationer som använder säkerhetslås var **37%** mindre benägna att drabbas av ett dataintrång orsakat av en oskyddad enhet (**38%** jämfört med **60%** bland dem som inte använder säkerhetslås).

Organisationer som för närvarande använder lås var också mer benägna att ha en dubbel säkerhetsstrategi, där tre fjärdedelar (**76%**) använde digitala åtgärder såsom fingeravtryck eller säkerhetsnycklar för tvåfaktorsautentisering, jämfört med **62%** av dem som inte använder lås.

84% instämmer i att säkerhetslås är kostnadseffektiva för att minska risken för potentiella dataintrång och erbjuder ett betydande värde till en relativt låg investering.

- **42%** anser att enhetslås är extremt kostnadseffektiva och ger hög skyddsnivå till låg kostnad, där de mest seniora ledarna (**56%**) är mer benägna än mellanchefer (**36%**) att se deras värde.

Nästan alla de tillfrågade (**97%**) anser att enhetslås kan förhindra stölder och minska risken för obehörig åtkomst till känslig företagsdata.

Stulna enheter ger förödande konsekvenser

Sällan går det en enda dag utan att man hör om någon form av säkerhetsincident som skett – vare sig det handlar om en storskalig attack mot en global koncern eller en mer riktad exploatering av kritisk infrastruktur eller tjänster. Även om dessa exempel antyder att cyberincidenter ofta är de mest omtalade – eller åtminstone förutsätts vara det – är det viktigt att inse att hot mot fysisk säkerhet kan vara minst lika allvarligt.

Det förs alldeles för sällan en bredare diskussion om incidenter som rör fysisk säkerhet, där obehöriga får tillgång till säkrade områden eller komprometterar tillgångar, trots att konsekvenserna kan vara lika allvarliga som vid en genomsnittlig ransomware-attack. Enligt vår forskning uppger över tre fjärdedelar (**76%**) av de tillfrågade att deras organisation har påverkats av enhetsstölder under de senaste två åren.

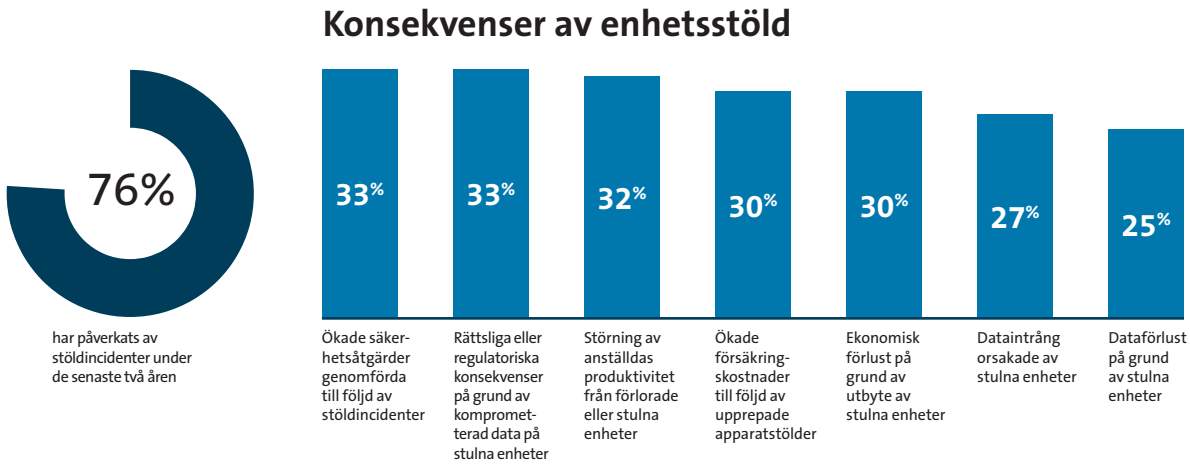


Fig. 1: *Hur har din organisation påverkats av incidenter med enhetsstöld under de senaste två åren? [Frågade till alla svarande: 1000]*

Det är inte bara den tunga men självklara kostnaden för att ersätta en enhet som organisationer står inför (**30%**). De vanligaste konsekvenserna inkluderar en ökning av implementerade säkerhetsåtgärder som en direkt följd (**33%**) eller juridiska och regulatoriska konsekvenser på grund av återkommen data (**33%**). Till exempel kan GDPR[1] -böter uppgå till så mycket som 20 miljoner euro eller 4 % av en organisations globala omsättning, medan även mindre allvarliga överträdelser kan kosta upp till 10 miljoner euro, vilket innebär betydande finansiella risker på grund av bristande säkerhet.

Utöver de ekonomiska konsekvenserna tillkommer även kostnaden för produktivitetsförluster när anställda förlorar eller får sina enheter stulna och inte kan arbeta (**32%**). Dessa effekter har både ekonomiska och tidsmässiga konsekvenser för organisationens resultat. Det är alltså inte bara digitala säkerhetsincidenter som kräver uppmärksamhet – fysiska hot utgör också betydande risker.

Genom att fördjupa sin förståelse för dessa sårbarheter kan organisationer vidta enkla och kostnadseffektiva åtgärder för att skydda sina enheter. Eftersom fysiska säkerhetsåtgärder både är prisvärda och enkla att implementera (vilket vi kommer att utforska senare), utgör de ett praktiskt första steg för att stärka den övergripande säkerheten.

"Utöver cybersäkerhetsåtgärder **är fysisk säkerhet minst lika viktigt.** Säkerhetskablar är en del av en starkare cybersäkerhetsstrategi."

Högsta ledningen; Tillverkning och produktion; 1 000 eller fler anställda; Helt på plats arbetsmodell; Frankrike

1 GDPR Fines/Penalties, Intersoft Consulting, https://gdpr-info.eu/issues/fines-penalties/

I dagens samhälle handlar det inte om ifall ett dataintrång sker, utan det det handlar snarare om när det kommer ske. Varje enhetsstöld är ett potentiellt dataintrång, och de ekonomiska konsekvenserna för organisationer är enorma om man saknar skydd.

Enligt IBMs senaste rapport [2] om kostnaden för dataintrång uppgick den globala genomsnittliga kostnaden för ett dataintrång år 2024 till 4,88 miljoner USD, en ökning med **10%** från genomsnittet på 4,45 miljoner USD år 2023. Denna siffra varierar mellan olika branscher och beroende på organisationens storlek – vissa organisationer kan drabbas av ännu högre kostnader.

Fokus på data:

- **Bransch:** Organisationer inom konsumenttjänster (**95%**), energi, olja/gas och försörjning (**90%**) samt bygg- och fastighetsbranschen (**89%**) är de mest sannolika att ha påverkats av enhetsstölder. Den högre rörligheten och möjligheten att jobba på distans för anställda och enheter inom dessa branscher utsätter dem för större risk för stöld.
- **Storlek:** Sannolikheten för enhetsstöld i mindre organisationer (100–249 anställda) har ökat mer (**82%**) än i större organisationer med mer än 1 000 anställda (**69%**), vilket belyser den betydliga påverkan på mindre organisationer där resurserna är mer begränsade och konsekvenserna kan vara mer påtagliga.
- **Senioritet:** De som har mer seniora positioner är mycket mer benägna att rapportera att de har påverkats av stöldincidenter (**87%**) än mellanchefer (**67%**). Detta tyder på att de som är ansvariga för den dagliga verksamheten är mindre informerade om de potentiella hoten mot oskyddade enheter. Genom att öka deras medvetenhet om dessa hot och de sammanhängande konsekvenserna, kan man hjälpa företag att integrera säkerhetslås i sina dagliga behov och skapa en gemensam kännedom om fysisk säkerhet på alla nivåer för att stödja en omfattande säkerhetsstrategi.

Hur spelar arbetsmodeller en roll här?

Vi har noterat den stora förändringen i arbetsmetoder under de senaste åren, där anpassningen av hydbridarbete bortom en fast arbetsplats har påskyndats av COVID-19-pandemin.

Över tre fjärdedelar (**76%**) av de tillfrågade, rapporterade att deras organisation hade påverkats av enhetsstöld under de senaste två åren. Detta blev mer tydligt med hybrida arbetsmodeller – som steg till **94%** när anställda arbetade helt på distans.

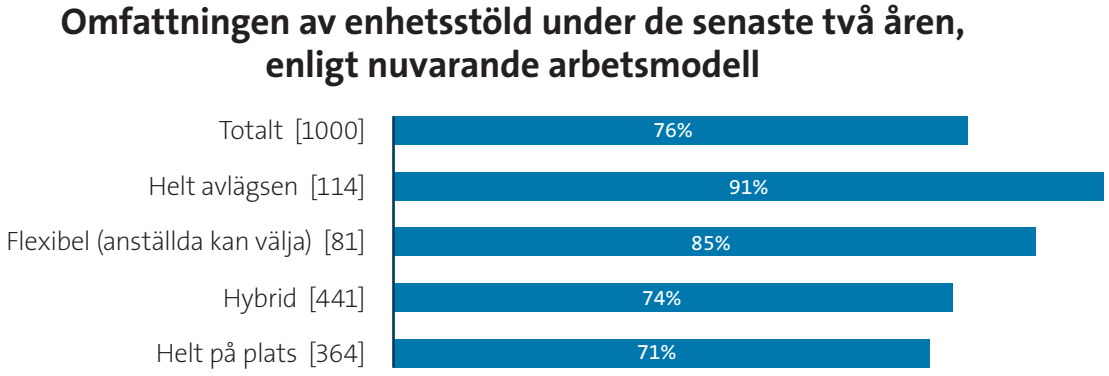


Fig. 2: *Andel respondenter vars organisation har påverkats av incidenter med enhetsstöld under de senaste två åren [Frågade till alla respondenter, visar data uppdelat efter aktuell arbetsmodell, basnummer i diagrammet]*

2 Cost of Data Breach Report 2024, IBM, juli 2024, https://www.ibm.com/reports/data-breach

Även om det är viktigt för alla organisationer att vara uppmärksam på fysisk enhetssäkerhet och försiktig med effekterna av enhetsstöld, förstärker flexibla och distansarbetande modeller avsevärt risken för enhetsstöld, vilket gör robusta säkerhetsåtgärder mer kritiska än någonsin.

Det är viktigt att notera att nivån av enhetsstölder generellt är hög, även när anställda är helt på plats – organisationer har ingen plats för självbelåtenhet, oavsett var deras anställda arbetar. Hotet om enhetsstöld är inte nytt och har inte just uppstått i den post-pandemiska världen. Vår forskning från 2016[3] undersökte de säkerhetsrisker som IT-stölder skapar i företagsvärlden. Enkätsvarande IT-professionella rankade risken för enhetsstöld på kontoret (**23%**) nästan lika hög som stöld i bilar och kollektivtrafik (**25%**) och högre än stöld på flygplatser och hotell (**15%**) eller restauranger (**12%**). Detta visar hur enhetsstöld förblir ett ihållande hot, även i miljöer där alla är på plats, vilket understryker behovet av vaksamhet och proaktiva säkerhetsåtgärder oavsett arbetsplatsmiljö.

Denna utmaning har blivit ännu mer uttalad i den post-COVID-19-världen, där **93%** av organisationerna rapporterade en ökning av säkerhetsrisker på grund av övergången till flexibla och hybrida arbetsmodeller. Dessa risker sträcker sig bortom fysisk enhetsstöld och inkluderar ökad sårbarhet för dataskydd, obehörig åtkomst och intrång orsakat av oskyddade hemmanätverk och decentraliserade arbetsmiljöer.

"**Detta är det enklaste sättet** att se till att våra enheter är bokstavligen under lås och nyckel! Det gör att vi vet att **allt är säkert och skyddat.**"

Styrelseledamot/C-nivå; IT, teknik och telekom; 100-249 anställda; Flexibel arbetsmodell; USA

Säkerhetsrisken ökar till följd av hybrid- eller distansarbetsmiljöer

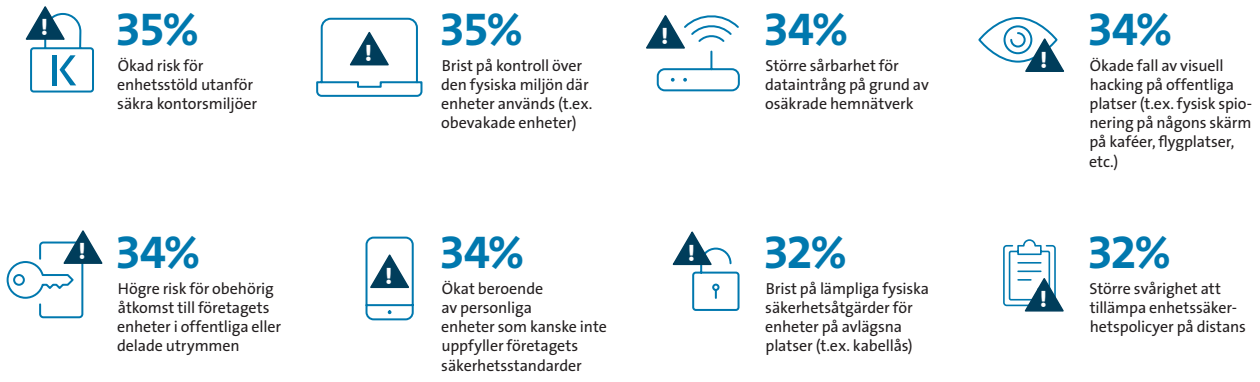


Fig. 3: *Vilka säkerhetsrisker enligt din åsikt har ökat till följd av hybrid- eller distansarbetsmiljöer efter covid-19-pandemin? [Frågad till respondenter vars organisation såg en förändring mot hybrid-/distansarbete efter covid-19-pandemin: 494]*

Med detta i åtanke ligger den bästa strategin för säkerhet i att kombinera robusta fysiska åtgärder med avancerade digitala skyddsåtgärder, vilket säkerställer ett omfattande skydd för både enheter och data i en allt mer decentraliserad värld.

3 IT-säkerhet och stöldundersökning av bärbara datorer, Kensington, augusti 2016, https://www.kensington.com/news/news-press-center/2016-news--press-center/kensington-survey-data-reveals-that-it-theft-in-the-office-ranks-nearly-as-high-as-theft-in-cars-and-more-than-in-airports-or-restaurants/?srsltid=AfmBOooRTMdZ4gjmcNB3viXIJcIL4GY47XxO5I08AldL-hLEB5LjnH0Ts

Lås som förhindrar förlusten – och sparar in på kostnader

"Bristen på ett säkerhetslås på enheterna ledde till dataintrång, **vilket resulterade i förödande förluster för företaget.**"

Ledning på mellannivå; IT, teknik och telekom; 1 000 eller fler anställda; Flexibel arbetsmodell; USA

Hittills har vi undersökt konsekvenserna av enhetsstölder och hur utbrett detta kan vara oavsett arbetsmiljö. Men detta är inte den enda oro som våra tillfrågade seniora IT-beslutsfattare har. Det finns ett brett spektrum av aspekter de oroar sig för när det gäller säkerhet, både inom fysiska och digitala områden.

Några av dessa bekymmer rör nyare faktorer kring fysisk säkerhet. Till exempel, nästan en fjärdedel (**23%**) är oroade över visuell hackning, där känslig data är i händerna på vem som helst om någon har sin skärm synlig på en offentlig plats – på ett café eller när man åker i kollektivtrafiken. Faktum är att de som arbetar flexibelt (**48%**) är mer benägna att rapportera visuell hackning som en oro än de som arbetar helt på distans (**36%**) eller med hybridmodeller (**33%**). Detta belyser att visuell hackning inte bara är kopplat till arbete hemifrån, utan snarare till att arbetsgivare ger friheten och tilliten till sina anställda och dom blir svårare att kontrollera. Organisationer måste överväga att skydda sin data när anställda är ute och rör sig i offentliga miljöer, genom ytterligare skydd som till exempel sekretessfilter.

De mest oroande områdena för enhetssäkerhet

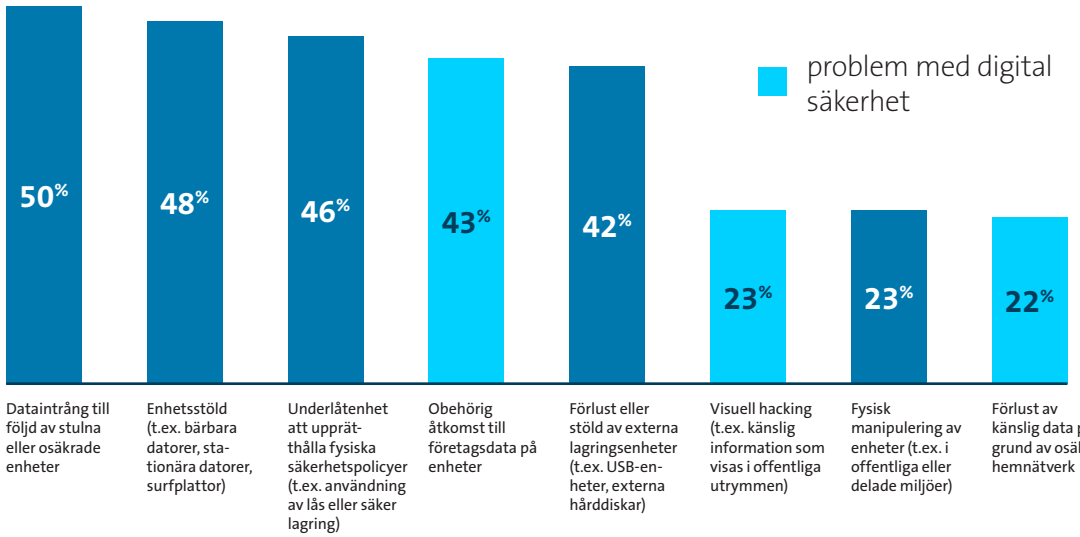


Fig. 4: *Vilka områden av enhetssäkerhet i din organisation berör dig mest? [Frågade till alla svarande: 1 000, visar kombinationen av svar på första, andra och tredje plats]*

Dataintrång är dock det största problemet, vilket är välgrundat eftersom en anmärkningsvärd andel (**46%**) har upplevt ett dataintrång som en direkt följd av en osäkrad enhet.

Det är här som ett säkerhetslås kan hjälpa till. Organisationer som använder säkerhetslås är **37%** mindre benägna att ha upplevt ett dataintrång på grund av en oskyddad enhet jämfört med de som inte använder dem.

Organisationer som har upplevt ett dataintrång eller förlust av känslig data på grund av en osäkrad enhet

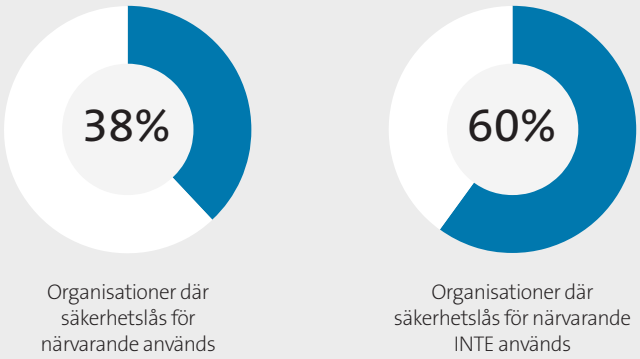


Fig. 5: *Har din organisation upplevt ett dataintrång eller förlust av känslig data som en direkt följd av att en enhet lämnats osäkrad? [Frågade till alla svarande, uppdelat på de som för närvarande använder säkerhetslås: 629; och de som för närvarande inte använder säkerhetslås: 371]*

Resultatet är tydligt: Det visar på en betydlig minskning av dataintrång eller dataförlust och bekräftar värdet av säkerhetslås som ett kritisk och omfattande skydd för enheter. Denna övertygande bevisning belyser hur säkerhetslås omedelbart minskar risker och lyfter dem som en nödvändig investering för organisationer som är engagerade och vill skydda sina data och minimera attacker.

Fokus på data:

- **Bransch:** Baserat på enkätresultaten är organisationer inom konsumenttjänster (**65%**) och offentlig/privat sjukvård (**57%**) mer benägna att ha upplevt ett dataintrång som en konsekvens av att antingen inte ha skydd eller fel typ av skydd. Konsumenttjänster var bland de mest benägna att ha påverkats av enhetsstöld generellt. När det gäller sjukvården belyser detta kanske större oro för den decentraliserade naturen hos vårdinstitutioner och att allmänheten kommer i närmare kontakt med enheter. Att ha en så stor mängd känslig data gör denna sektor mer utsatt.
- **Storlek:** Ytterligare ett exempel på de begränsade resurserna hos mindre organisationer är att de är mer benägna (**59%**) än sina större motsvarigheter (**40%**) att ha upplevt ett dataintrång på grund av en oskyddad enhet. De kämpar inte bara med de initiala avskräckande åtgärderna utan också med den snöbollseffekt som följer.
- **Senioritet:** De mer juniora bland de tillfrågade är mindre benägna att rapportera ett dataintrång eller förlust av känslig data på grund av en oskyddad enhet (**30%**) jämfört med sina kollegor på styrelse- eller högsta ledningsnivå (**59%**). Det finns en tydlig obalans inom företagen när det gäller en verklig förståelse av fysisk säkerhet för sina enheter och konsekvenserna av att denna inte är på plats – ett behov av större kännedom och förståelse.

"En liten investering i säkerhetsåtgärder (lås) kan **avsevärt minska risken för kostsamma produktkostnader** eller ett förlängt driftstopp inom organisationen."

Högsta ledningen; Utbildning – tillhandahålls av staten/staten; 1 000 eller fler anställda; Hybrid arbetsmodell; USA

Så, hur bör en organisation se ut för att få bukt på detta?

Organisationer står inför många digitala och fysiska säkerhetsproblem – konsekvenserna av enhetsstöld är förödande för organisationer och deras resultat. De bör leta efter den mest kostnadseffektiva lösningen. En lösning kan det vara ett enkelt säkerhetslås.

Majoriteten (**84%**) av de tillfrågade seniora IT-beslutsfattarna säger att säkerhetslås är kostnadseffektiva för att minska potentiella dataintrång – och att de erbjuder ett stort värde för att förhindra stöld och intrång. Vidare tror **42%** att de är extremt kostnadseffektiva.

Detta är en universell åsikt som delas av de som redan använder säkerhetslås och även de som inte gör det – vilket väcker frågan: "Varför inte?" Organisationer kan se lås som en logistisk utmaning för enhetshantering eller så kanske ett starkare fokus på digital säkerhet över fysisk leder till en undervärdering av låsens värde, vilket hindrar adoption. Men när man jämför med de förödande ekonomiska konsekvenserna av enhetsstöld, representerar kostnaden för ett säkerhetslås – vanligtvis mellan 24 och 40 pund per enhet – en minimal investering för att minska risker. När vi dyker djupare i detta ser vi tydliga skillnader i åsikter mellan olika nivåer av hierarki.

Fig. 6: *När det gäller kostnadseffektivitet, hur ser du på de fysiska säkerhetslåsens roll för att mildra potentiella dataintrång eller stöld? [Frågade till alla respondenter, visar data uppdelat efter tjänsteår, bastal i diagrammet]*

Dessa resultat betonar det kritiska behovet av att ta itu med de grundläggande orsakerna till enhetsstöld och dess större påverkan inom organisationer. Medan seniora ledare är mer benägna att se säkerhetslås som extremt kostnadseffektiva (**56%**), minskar denna uppfattning ju längre ner man kommer inom hierarkin. Troligtvis kommer seniora ledare alltid att vara mer fokuserade på de större konsekvenserna (t.ex. regleringsböter, rykte), medan chefer på lägre nivå tenderar att fokusera på de dagliga problemlösningarna (t.ex. produktivitetsförlust).

Denna diskrepans belyser vikten av att samtliga inom bolaget bör få en större förståelse kring värdet av säkerhetslås – inte bara som ett kostnadseffektivt verktyg, utan som en proaktiv lösning för att förhindra betydande förluster innan de inträffar. Att övervinna dessa klyftor inom allas olika åsikter, kommer att säkerställa ett sammandraget och effektivt sätt för att minska riskerna för enhetsstöld och skydda känslig data.

"När skadan väl är skedd orsakar det betydande förluster. Vi måste **lösa problemet från grunden.**"

på mellannivå ; Sjukvård - privatägt; 1 000 eller fler anställda; Hybrid arbetsmodell; USA

Lås fungerar till att säkra upp och förstärka skyddet

Vi har fortsatt att undersöka hur säkerhetslås inte bara är effektiva för att minska stöld, utan även erbjuder en kostnadseffektiv lösning för att mildra andra säkerhetsrisker. Deras olika tillämpningar belyser deras mångsidighet när det gäller att hantera säkerhetsutmaningar i olika miljöer – en fördel som många organisationer börjar inse men också redan inser.

Många använder redan säkerhetslås för att säkra sina enheter i sin organisation. De vanligaste enheterna som säkras är bland annat bärbara datorer (**44%**), stationära datorer (**43%**) och servrar (**42%**), vilket återigen påvisar vilket produktområde som bör se till att skyddas, de hårdvarorna som ofta innehåller känslig data. Denna omfattande anpassning belyser erkännandet från många människor om att de ser lås som ett viktigt verktyg för att skydda mot stöld och obehörig åtkomst.

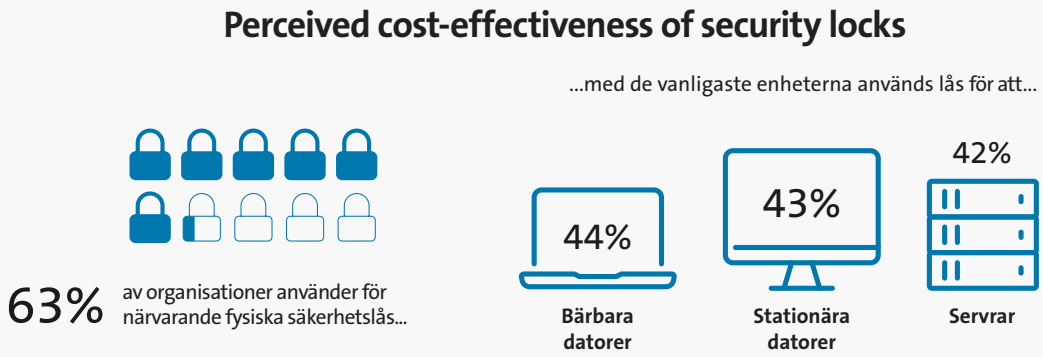


Fig. 7: *För vilka av följande elektroniska enheter används fysiska säkerhetslås i din organisation? [Frågade till alla svarande: 1000]*

Nästan **40%** av de tillfrågade säger att deras organisationer känner till vilken betydande roll som lås har för att öka skyddet och slippa den oro som kan komma med att man inte är skyddad. Särskilt när det gäller enheter som ofta används i mobila eller hybrida arbetsmiljöer.

För organisationer understryker dessa data behovet av att utvärdera sina nuvarande säkerhetsåtgärder på ett omfattande sätt. Medan lås är ett pålitligt och allmänt använd lösning, kan en utökning av deras användning över ett bredare utbud av enheter och att kombinera dem med kompletterande skydd hjälpa till att stänga befintliga säkerhetsluckor och mildra risker mer effektivt.

Nästan alla de tillfrågade (**97%**) erkänner den avgörande roll som säkerhetslås spelar för att förhindra stöld och obehörig åtkomst som ofta följer. Detta omfattande erkännande speglar det förtroende som organisationer har för fysisk säkerhet som en grundläggande åtgärd för att skydda enheter och känslig data. Lås fungerar som ett frontlinjeförsvar, vilket minskar möjligheterna för stöld och mildrar risker som är kopplade till kompromitterad hårdvara.

"Att ha lås i offentliga kontorer, co-working spaces eller andra områden där flera personer kan vistas **minskar risken för stöld..**"

Styrelseledamot/C-nivå; Utbildning – privatägt; 100-249 anställda; USA

Tron om att implementering av fysisk säkerhet bidrar till att motverka enhetsstölder

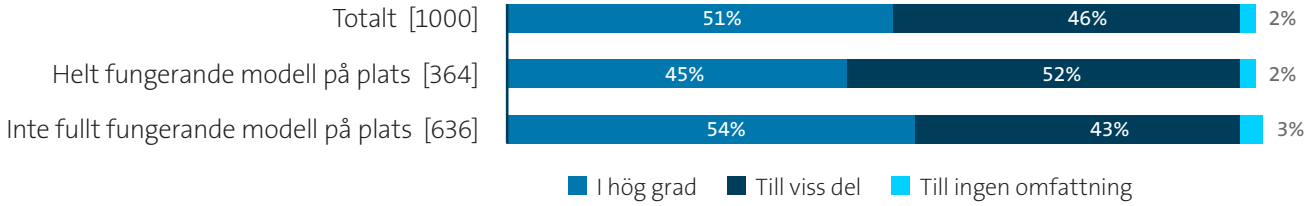


Fig. 8: *I vilken utsträckning tror du att fysiska säkerhetsåtgärder som säkerhetslås bidrar till att förhindra enhetsstöld som kan leda till obehörig åtkomst till företagsdata? [Frågade till alla respondenter, visar data uppdelat efter typ av arbetsmodell, bastal i diagrammet]*

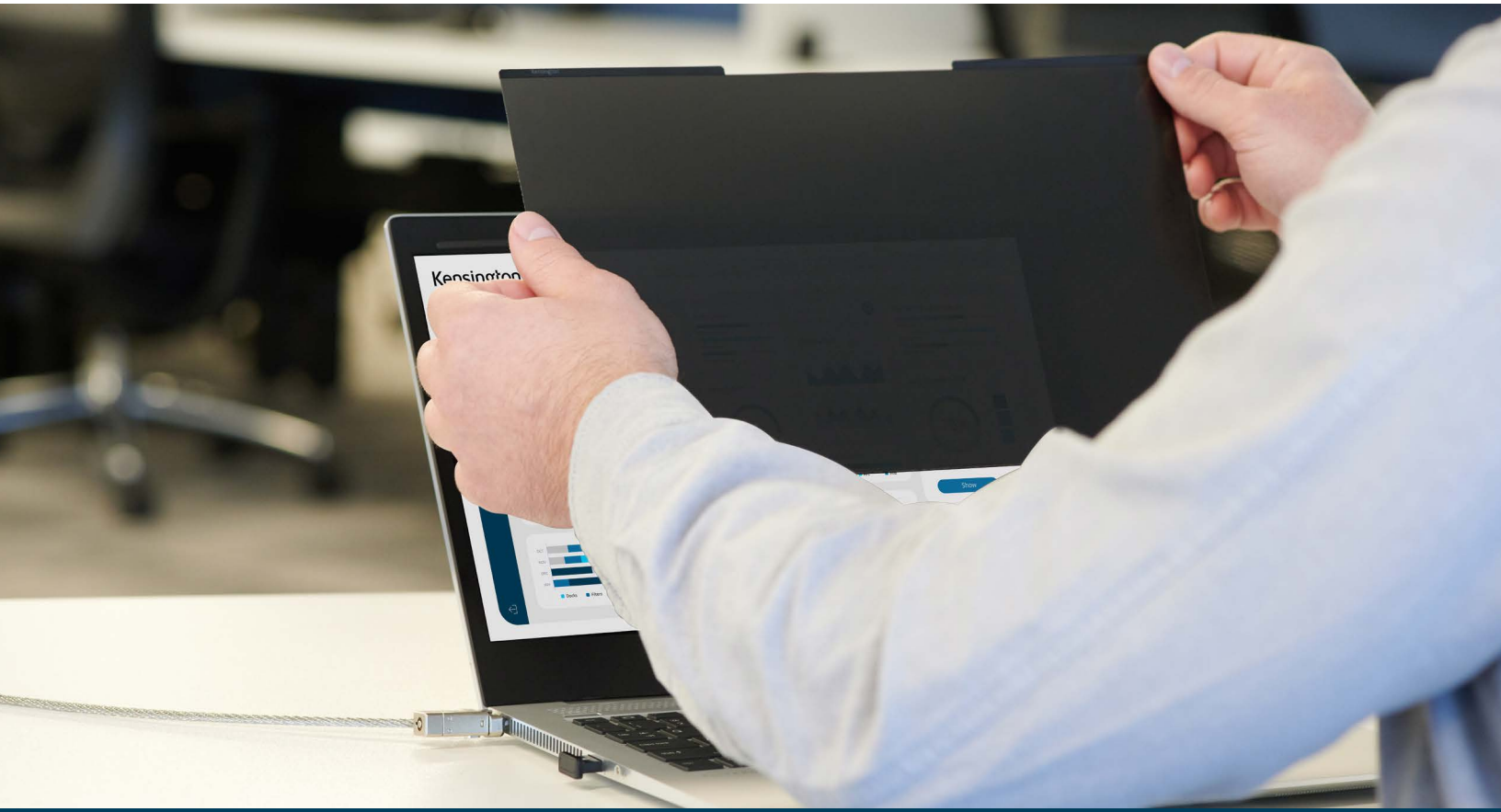
Detta erkännande blir mer och mer framträdande när organisationer har anpassat sig efter hybrida arbetsmodeller. I dessa decentraliserade miljöer används enheter allt mer i osäkra miljöer, såsom hemmakontor och offentliga platser, vilket ökar risken för stöld eller oavsiktlig exponering. Dataintrång orsakade av oskyddade enheter är betydligt vanligare i de mer flexibla arbetsuppsättningarna (**50%** sammanlagt jämfört med **39%** för dom som jobbar på fasta platser på kontor).

Säkerhetslås är designade för att anpassas till olika miljöer, vilket erbjuder ett pålitligt skydd för enheter oavsett om de används på kontor, på resande fot eller offentliga miljöer och ger organisationer tryggheten att de har ett skydd som passar till alla de olika arbetsmodellerna.

De ekonomiska konsekvenserna av dessa typer av stölder kan vara förödande, där kostnaden för att ersätta stulen hårdvara ofta överröstar den större påverkan som detta har på produktivitet, alla de nya anpassningarna som ska göras efter incidenten för att förhindra att detta uppstår igen. För organisationer innebär varje stulen eller oskyddad enhet en ökad risk – inte bara för verksamheten men också för resultatet en tid framåt.

Säkerhetslås erbjuder en beprövad, pålistlig och kostnadseffektiv lösning, som många redan har förtroende för när det gäller att minska risken för stöld och de följande ekonomiska och ryktemässiga konsekvenserna. Genom att ta itu med dessa risker från grunden kan organisationer ta en proaktiv ställning för att skydda sina tillgångar och känslig data. Medan fysiska säkerhetsåtgärder som lås är effektiva, måste de vara en del av en bredare strategi för att hantera de säkerhetsrisker som är kopplade till hybridarbete. Att kombinera lås med ett komplett sekretesskydd och tvåfaktorsautentisering, innebär att man säkerstället ett heltäckade skydd mot både fysiska och digitala hot. Säkerhetsutbildningar för att informera anställda om vikten av denna integrerade strategi kan ytterligare stärka organisationens säkerhet. För organisationer som drivs i de komplexa moderna arbetsmodellerna är det avgörande att implementera fysiska och digitala säkerhetsåtgärder för att minimera risker, skydda sin arbetsstyrka och bibehålla operativ motståndskraft gentemot sina konkurrenter och eventuella hot från omvärlden.

Genom att förhindra enhetsstöld och dess förödande konsekvenser med dataintrång efter att enheten är stulen, har man ett kostnadseffektivt sätt att motverka det, än att hantera konsekvenserna i efterhand. Genom att vidta förebyggande åtgärder som att använda laptop-lås, kan organisationer skydda sig mot större ekonomiska och operativa konsekvenser i framtiden. För att säkerställa att dessa åtgärder är effektiva är det avgörande med samspel mellan seniora ledare, chefer och team. Ett gemensamt åtagande för säkerhetsprioriteringar säkerställer att alla förstår sin roll i att skydda värdefulla tillgångar och minska risker.



Metodik

Kensington beställde oberoende marknadsundersökningsspecialisten Vanson Bourne att genomföra den forskning som denna rapport baseras på. Totalt intervjuades 1 000 seniora IT-ledare som är involverade i eller har inflytande över fysisk IT-hårdvarusäkerhet inom sina organisationer under hösten 2024, med representation från USA, Storbritannien, Frankrike och Tyskland.

Respondenterna kom från organisationer med 100 eller fler anställda och från både privata och offentliga sektorer.

Intervjuerna genomfördes online och utfördes med en rigorös urvalsprocess för att säkerställa att endast lämpliga kandidater fick möjlighet att delta. Om inte annat anges, baseras de resultat som diskuterats, på hela urvalet.

Om Kensington

Kensington är en ledande leverantör av tillbehör för stationära och mobila enheter, betrodd av IT-specialister, utbildare, företag och hemarbetsproffs världen över i mer än 40 år. Kensington strävar efter att förutse behoven och utmaningarna i den ständigt utvecklande arbetsplatsen och skapa professionella, prisbelönta lösningar för organisationer som är engagerade i att ge topprofessionella de verktyg de behöver för att blomstra. Företaget är stolt över att vara det professionella valet och om sina grundvärderingar som rör design, kvalitet och support.

I kontors- och mobila miljöer erbjuder Kensingtons omfattande portfölj av prisbelönta produkter pålitlig säkerhet, innovationer för produktivitet på skrivbordet, professionell videokonferens och ergonomiskt välmående.

Med huvudkontor i Burlingame, Kalifornien, är Kensington uppfinnaren och en världsledare inom laptop-säkerhetslås. KKensington är en division av ACCO Brands, Home of Great Brands Built by Great People, som designar, tillverkar och marknadsför konsument- och slutanvändarprodukter som hjälper människor att arbeta, lära sig och leka. Förutom Kensington® inkluderar ACCO Brands välkända varumärken AT-A-GLANCE®, Five Star®, Leitz®, Mead®, PowerA®, Swingline®, Tilibra och många fler. Mer information om ACCO Brands Corporation (NYSE:ACCO) finns på www.accobrands.com.

Kensington® är ett registrerat varumärke för ACCO Brands. Alla andra registrerade och oregistrerade varumärken tillhör sina respektive ägare.

FOR MORE INFORMATION CONTACT: sales@kensington.com

Kensington
The Professionals' Choice™