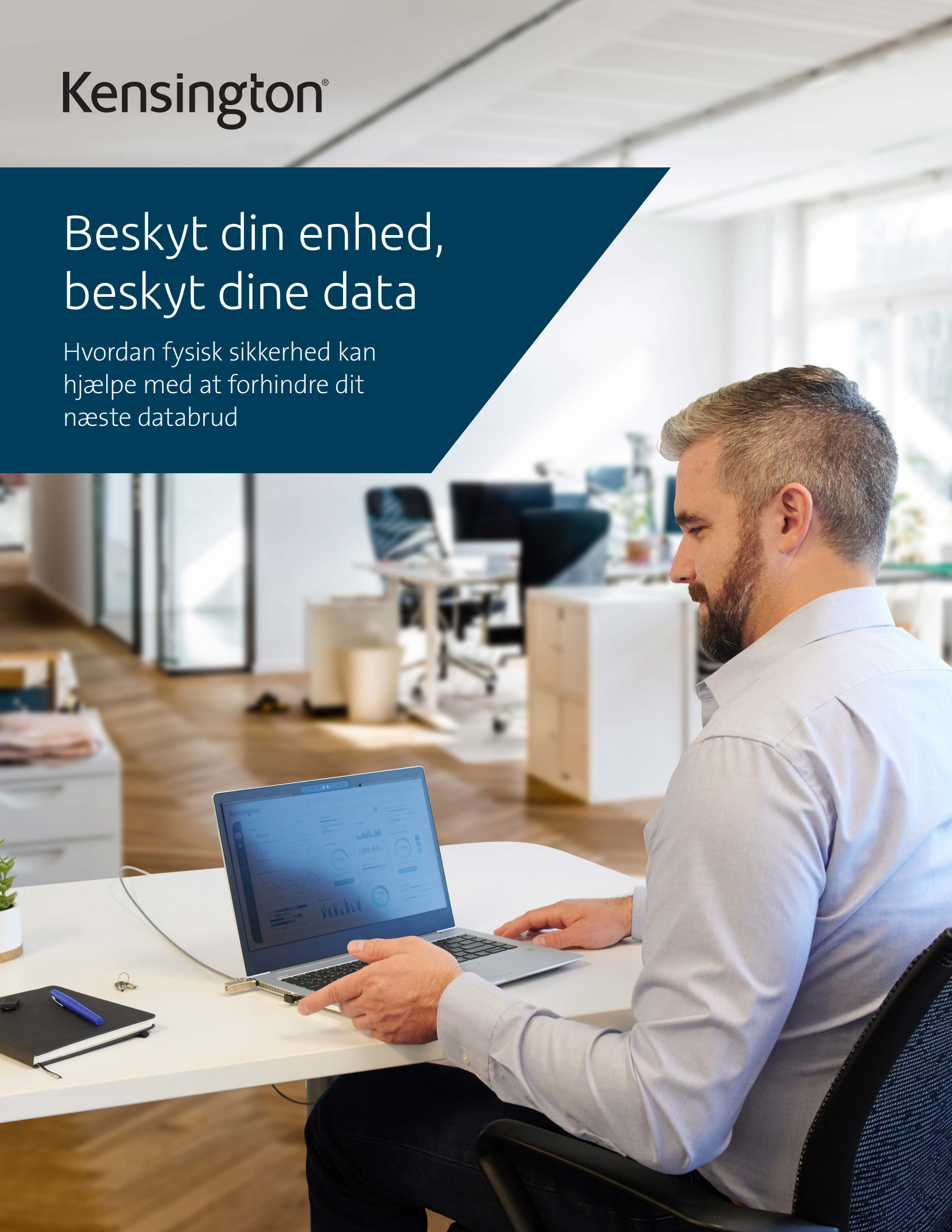
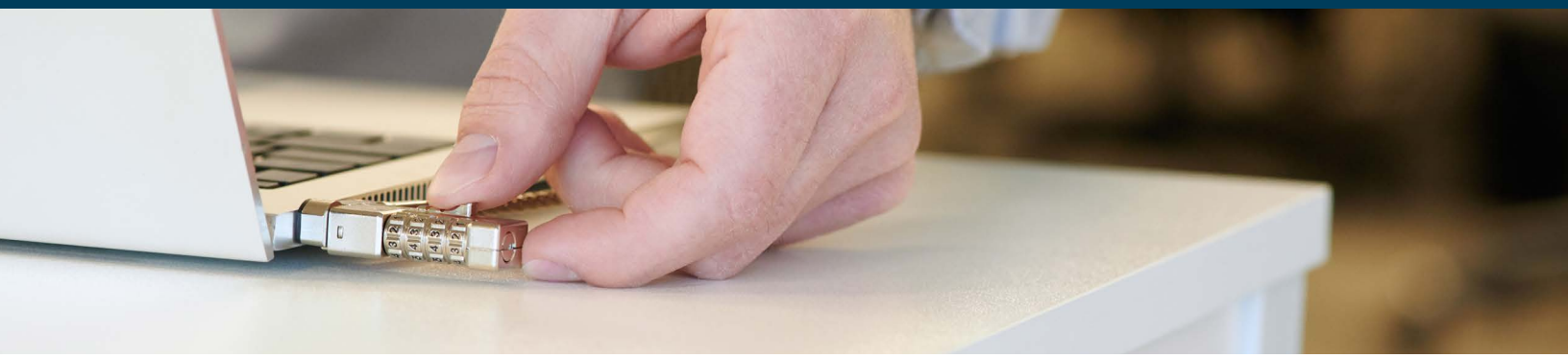
Kensington®

Beskyt din enhed, beskyt dine data

Hvordan fysisk sikkerhed kan hjælpe med at forhindre dit næste databrud





Indledning

Sikkerhedslandskabet har udviklet sig dramatisk i de seneste år, drevet af transformative skift i, hvordan og hvor vi arbejder. Den ultimative drivkraft i dette var COVID-19-pandemien; det fremskyndede vedtagelsen af hybride og fleksible arbejdsmodeller og ændrede grundlæggende enhedssikkerhedsprioriteter.

Kensington sponsorerede en undersøgelse udført af den uafhængige markedsundersøgelsesspecialist Vanson Bourne af 1.000 senior IT-beslutningstagere med ansvar for deres organisations fysiske hardwaresikkerhed på tværs af USA og EMEA. Næsten alle adspurgte (92%) strammede deres sikkerhedspolitikker som reaktion på pandemien, idet de anerkendte de øgede risici forbundet med decentraliserede arbejdsmiljøer. Når vi ser frem mod 2025, forventes niveauet af mere fleksible arbejdsmodeller at stige, hvilket understreger, at tiden til at genoverveje enhedssikkerhedsstrategier er nu.

Databrud er ikke kun et digitalt problem – enhver stjålet eller usikret enhed repræsenterer en potentiel gateway for uautoriseret adgang til følsomme oplysninger, hvilket udgør betydelige risici for organisationer. Med den økonomiske byrde af et databrud nu i gennemsnit millioner af dollars, har indsatsen aldrig været højere. Efterhånden som organisationer fortsætter med at tilpasse deres arbejdsmodeller, er behovet for at håndtere enhedssikkerhed vokset massivt. Strengere databeskyttelseskrav og en stigning i databrud har yderligere øget vigtigheden af at beskytte både fysiske enheder og de følsomme oplysninger, de har. Denne rapport fremhæver den kritiske rolle, sikkerhedslåse spiller for at mindske disse risici, og understreger, hvorfor det er vigtigt at handle nu for at være på forkant med nye udfordringer.

Gennem disse resultater vil vi undersøge de håndgribelige konsekvenser af enhedstyveri, vise, hvordan enkle, men effektive løsninger som sikkerhedslåse kan hjælpe med at mindske risici, og fremhæve, hvordan fysisk sikkerhed giver ro i sindet i en verden, hvor arbejdsmodeller konstant udvikler sig. Fra at forstå de svimlende konsekvenser af enhedstyveri til at demonstrere omkostningseffektiviteten og sikkerheden ved låse, giver denne rapport brugbar indsigt til organisationer, der navigerer i nutidens komplekse sikkerhedslandskab.

Nøglefund:

76% af de adspurgte siger, at deres organisation er blevet påvirket af tyverihændelser i de sidste 2 år, med hændelser mere almindelige i organisationer med mere fleksible arbejdsmodeller. For eksempel afslørede vores forskning, at (**85%**) af organisationer med fleksible arbejdsmodeller oplevede en hændelse med tyveri inden for de sidste 2 år, sammenlignet med **71%** af organisationer, hvis medarbejdere er fuldt på stedet.

Virkningerne af enhedstyveri rækker ud over hardwaretab, herunder:

- behovet for at forbedre eksisterende sikkerhedsforanstaltninger (**33%**)
- juridiske eller lovgivningsmæssige konsekvenser på grund af kompromitterede data på stjålne enheder (**33%**)
- forstyrrelse af medarbejdernes produktivitet fra mistede eller stjålne enheder (**32%**)

Organisationer, der bruger sikkerhedslåse, var **37%** mindre tilbøjelige til at opleve et databrud forårsaget af en usikret enhed (**38%** vs. **60%** blandt dem, der ikke bruger sikkerhedslåse).

Organisationer, der i øjeblikket bruger låse, var også mere tilbøjelige til at bruge en dobbelt tilgang til sikkerhed, hvor tre fjerdedele (**76%**) brugte digitale foranstaltninger som fingeraftryk eller sikkerhedsnøgler til tofaktorautentificering, sammenlignet med **62%** af dem, der slet ikke brugte låse.

84% er enige om, at sikkerhedslåse er omkostningseffektive til at afbøde potentielle databrud, hvilket giver betydelig værdi for relativt lave investeringer.

- **42%** mener, at enhedslåse er ekstremt omkostningseffektive og giver høj beskyttelse til lave omkostninger, hvor de mest ledende ledere er mere tilbøjelige til at anerkende deres værdi (**56%**) sammenlignet med ledelse på mellemniveau (**36%**).

Næsten alle adspurgte (**97%**) mener, at enhedslåse kan forhindre tyveri, hvilket reducerer sandsynligheden for uautoriseret adgang til følsomme virksomhedsdata.

Stjålne enheder, svimlende konsekvenser

Der går sjældent en dag, hvor du ikke hører om en form for sikkerhedshændelse – uanset om det er et storstilet angreb på et globalt konglomerat eller mere målrettet udnyttelse af kritisk infrastruktur eller service. Og selvom disse eksempler tyder på, at cyberhændelser ofte er de mest omtalte – eller i det mindste antages at være – er det vigtigt at erkende, at fysiske sikkerhedstrusler kan være lige så kritiske.

Der er lidt udbredt samtale om fysiske sikkerhedshændelser, hvor uautoriserede personer får adgang til sikrede områder eller kompromitterer aktiver, som har lige så alvorlige konsekvenser som det gennemsnitlige ransomware-angreb. Ifølge vores undersøgelse siger over tre fjerdedele (**76%**) af de adspurgte, at deres organisation er blevet påvirket af hændelser med enhedstyveri i de sidste to år.

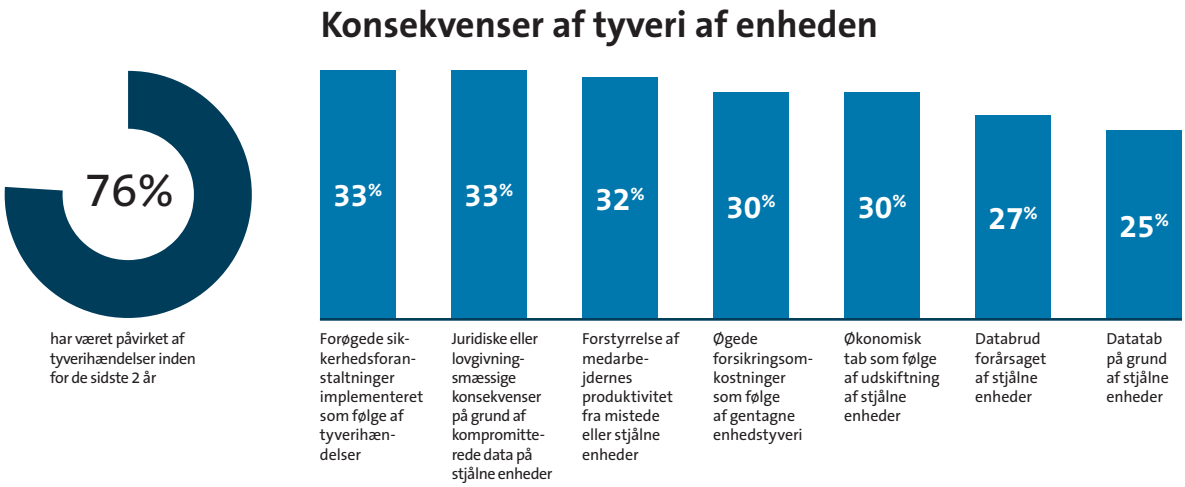


Fig. 1: *Hvordan er din organisation blevet påvirket af hændelser med enhedstyveri i de seneste to år? [Spørget til alle respondenter: 1000]*

Det er ikke kun de åbenlyse omkostninger ved at udskifte en enhed, som organisationer står over for (**30%**). De mest almindelige konsekvenser omfatter en stigning i sikkerhedsforanstaltninger, der er implementeret som følge heraf (**33%**) eller juridiske eller regulatoriske konsekvenser på grund af kompromitterede data (**33%**), hvor sidstnævnte ofte er tydeligt beskrevet. For eksempel GDPR[1] bøder kan nå op til 20 millioner euro eller **4%** af en organisations globale omsætning, med endnu mindre alvorlige overtrædelser, der koster op til 10 millioner euro, hvilket udgør betydelige økonomiske risici for manglende overholdelse. Ud over de økonomiske konsekvenser er omkostningerne ved afbrydelse af medarbejdernes produktivitet fra mistede eller stjålne enheder (**32%**) også. På baggrund af enhver af disse påvirkninger er der en klar økonomisk eller tidsmæssig betydning for organisationens bundlinje. Så det er ikke kun digitale sikkerhedshændelser, der kræver opmærksomhed – fysiske trusler udgør også betydelige risici. Ved at uddybe deres forståelse af disse sårbarheder kan organisationer tage enkle, omkostningseffektive trin for at beskytte deres enheder. Da fysiske sikkerhedsforanstaltninger er både overkommelige og nemme at implementere (som vi vil udforske senere), repræsenterer de et praktisk første skridt i at styrke den overordnede sikkerhed.

"Ud over cybersikkerhedsforanstaltninger **er fysisk sikkerhed lige så vigtig.** Sikre kabler er en del af en stærkere cybersikkerhedsstrategi."

øverste ledelse; Fremstilling og produktion; 1.000 eller flere ansatte; Fuldt onsite arbejdsmodel; Frankrig

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

I nutiden er det ikke et tilfælde af, om der opstår et databrud, men hvornår. Faktisk er hvert enkelt enhedstyveri et databrud, der venter på at ske, og de økonomiske konsekvenser er svimlende for organisationer. Ifølge IBMs seneste rapport om databrudsomkostninger[2] ligger den globale gennemsnitlige pris for et databrud i 2024 på 4,88 millioner USD; en stigning på **10%** på et år fra gennemsnittet af $4,45 millioner USD i 2023. Dette tal varierer på tværs af branche og organisationsstørrelse, så nogle organisationer kan stå over for endnu højere.

Fokus på data:

- **Sektor:** Det er mest sandsynligt, at organisationer inden for forbrugerservice (**95%**), energi, olie/gas og forsyningsvirksomheder (**90%**) og bygge- og ejendomsindustrien (**89%**) er blevet ramt af enhedstyveri. Den højere mobilitet af medarbejdere og enheder på tværs af disse virksomheder udsætter dem for større risiko for tyveri
- **Størrelse:** Sandsynligheden for enhedstyveri i mindre organisationer (100-249 ansatte) er steget mere (**82%**) end i større organisationer med mere end 1.000 ansatte (**69%**), hvilket fremhæver den relative indvirkning på mindre organisationer, hvor ressourcerne er mere begrænsede, virkningerne kan være mere udtalte
- **Anciennitet:** De i højere stillinger er meget mere tilbøjelige til at rapportere, at de er blevet påvirket af tyverihændelser (**87%**) end ledere på mellemniveau (**67%**). Det er sandsynligt, at de, der har ansvaret for at drive en virksomheds daglige drift, er dårligt informeret om de potentielle trusler, som usikre enheder står over for. At øge deres bevidsthed om truslerne og de dermed forbundne konsekvenser vil hjælpe med at tilskynde virksomheder til at integrere sikkerhedsløse i deres kulturelle behov og tilpasse perspektiver på tværs af alle niveauer for at understøtte en omfattende sikkerhedsstrategi

Hvordan spiller arbejdsmodeller en rolle her?

Vi bemærkede, da vi introducerede denne forskning, den store ændring i måder at arbejde på i de seneste år, hvor vedtagelsen af mere fleksible arbejdsmodeller væk fra en fast arbejdsplads er blevet fremskyndet af COVID-19-pandemien.

Hvor vi ser over tre fjerdedele (**76%**) af alle de adspurgte rapportere, at deres organisation er blevet påvirket af enhedstyveri i de sidste 2 år, bliver dette mere tydeligt, hvor arbejdsmodellerne er mere fleksible – stigende til over 9 ud af 10 (**94%**), hvor medarbejderne er helt fjerntliggende.

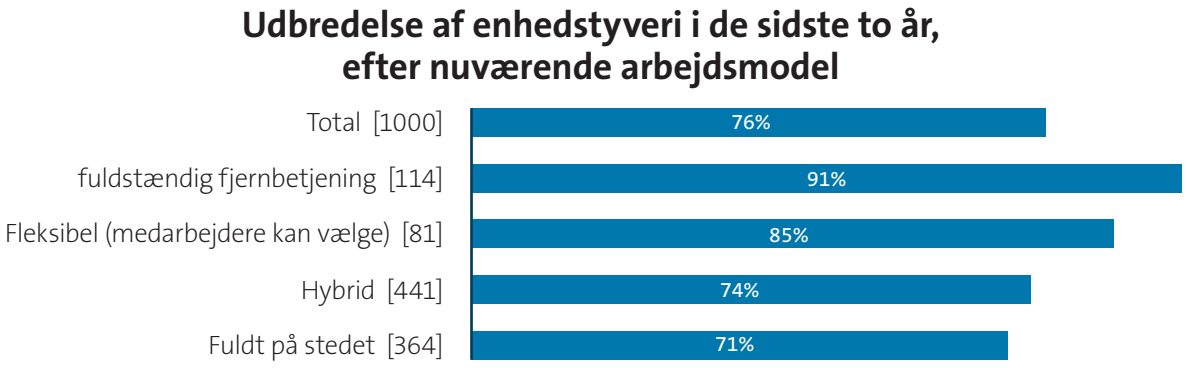


Fig. 2: *Andel af respondenter, hvis organisation er blevet påvirket af hændelser med enhedstyveri i de seneste to år [Spørget til alle respondenter, viser data opdelt efter nuværende arbejdsmodel, basistal i diagrammet]*

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

Selvom det er vigtigt for enhver organisation at være opmærksom på fysisk enhedssikkerhed og på vagt over for virkningerne af enhedstyveri, forstærker fleksible og fjernarbejdsmodeller risikoen for enhedstyveri markant, hvilket gør robuste sikkerhedsforanstaltninger mere kritiske end nogensinde.

Det er vigtigt at bemærke, at niveauet af enhedstyveri generelt er højt, selv når medarbejderne er helt på stedet – organisationer har ikke plads til at være selvtilfredse, uanset hvor deres medarbejdere arbejder. Truslen mod enhedstyveri er ikke ny og har heller ikke kun dukket op som en del af denne post-pandemiske verden. Vores forskning i 2016[3] undersøgte de sikkerhedsrisici, der er skabt af it-tyveri i virksomheden. Undersøgte it-professionelle rangerede risikoen for enhedstyveri på kontoret (**23%**) næsten lige så høj som tyveri i biler og transport (**25%**) og mere end tyveri i lufthavne og hoteller (**15%**) eller restauranter (**12%**). Dette viser, hvordan enhedstyveri forbliver en vedvarende trussel, selv i helt onsite-miljøer, hvilket understreger behovet for årvågenhed og proaktive fysiske sikkerhedsforanstaltninger uanset arbejdspladsens omgivelser.

Denne udfordring er blevet yderligere forstærket i post-COVID-19-verdenen, hvor **93%** af organisationerne rapporterer en stigning i sikkerhedsrisici på grund af skiftet til fleksible og hybride arbejdsmodeller. Disse risici strækker sig ud over fysisk enhedstyveri og omfatter øgede sårbarheder i databeskyttelse, uautoriseret adgang og brud forårsaget af usikrede hjemmenetværk og decentraliserede arbejdsmiljøer.

"**Det er den nemmeste måde** at sikre, at vores enheder er under bogstavelig talt lås og nøgle! Det gør det, så **vi ved, at alt er trygt og sikkert**"

Bestyrelsesmedlem/C-niveau; IT, teknologi og telekommunikation; 100-249 ansatte; Fleksibel arbejdsmodel; USA

Sikkerhedsrisikoen øges som følge af hybride eller fjerntliggende arbejdsmiljøer

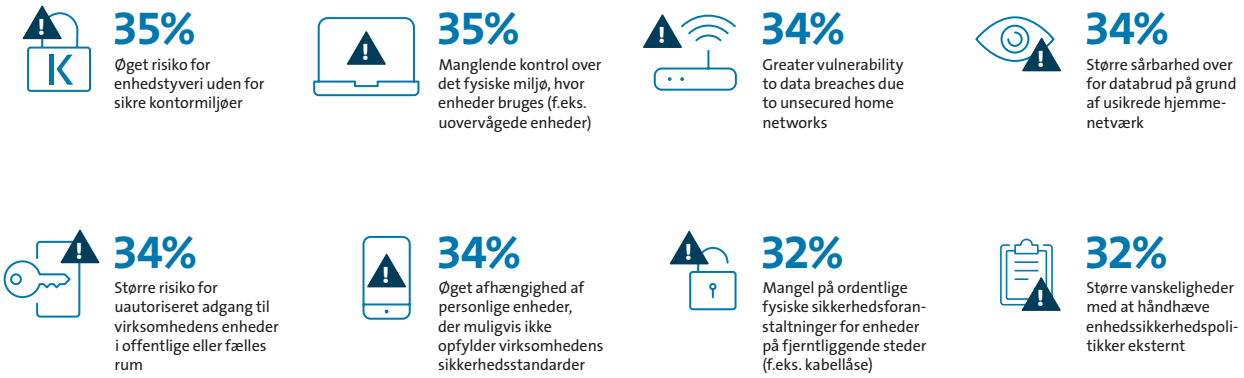


Fig. 3: *Hvilke sikkerhedsrisici er efter din mening steget som følge af hybride eller fjerntliggende arbejdsmiljøer efter COVID-19-pandemien? [Adspurgt til respondenter, hvis organisation så et skift i retning af hybrid-/fjernarbejde efter COVID-19-pandemien: 494]*

Med dette i tankerne ligger den bedste tilgang til sikkerhed i at kombinere robuste fysiske foranstaltninger med avancerede digitale sikkerhedsforanstaltninger, der sikrer omfattende beskyttelse af både enheder og data i en stadig mere decentraliseret verden.

3 IT-sikkerhed og tyveriundersøgelse af bærbare computere, Kensington, august 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=AfmBOooRTMdZ4gjmcNB3viXlJcIL4GY47XxO5I08AldLhLEB5LjnH0Ts

Låse, der stopper tab - og sparer omkostninger

"Manglen på en sikkerhedslås på udstyret førte til et databrud, **hvilket resulterede i betydelige tab for virksomheden.**"

Mid-level ledelse; IT, teknologi og telekommunikation; 1.000 eller flere ansatte; Fleksibel arbejdsmodel; USA

Indtil videre har vi afdækket konsekvenserne af enhedstyveri, og hvor omfattende dette kan være uanset arbejdsmiljø. Dette er dog ikke den eneste bekymring for vores adspurgte senior IT-beslutningstagere. Der er en lang række aspekter, de er bekymrede over, når det kommer til sikkerhed, på tværs af både fysiske og digitale områder.

Nogle af disse bekymringer præsenterer nye er faktorer omkring fysisk sikkerhed. For eksempel er næsten en fjerdedel (**23%**) bekymret over visuel hacking, hvor følsomme data er prisgivet enhver, hvis en persons skærm vises på et offentligt sted – på en kaffebar eller i offentlig transport. Faktisk er det mere sandsynligt, at de, der arbejder fleksibelt (**48%**) end dem i fuldt fjerntliggende (**36%**) eller hybride (**33%**) opsætninger, rapporterer visuel hacking som en bekymring. Dette fremhæver, at visuel hacking ikke kun er forbundet med at arbejde hjemmefra, men snarere med at give overdrevne friheder, der er sværere at kontrollere. Organisationer bliver nødt til at tage hensyn til at beskytte deres data, når medarbejderne er på farten, gennem yderligere afskrækkende midler som privatlivsskærme.

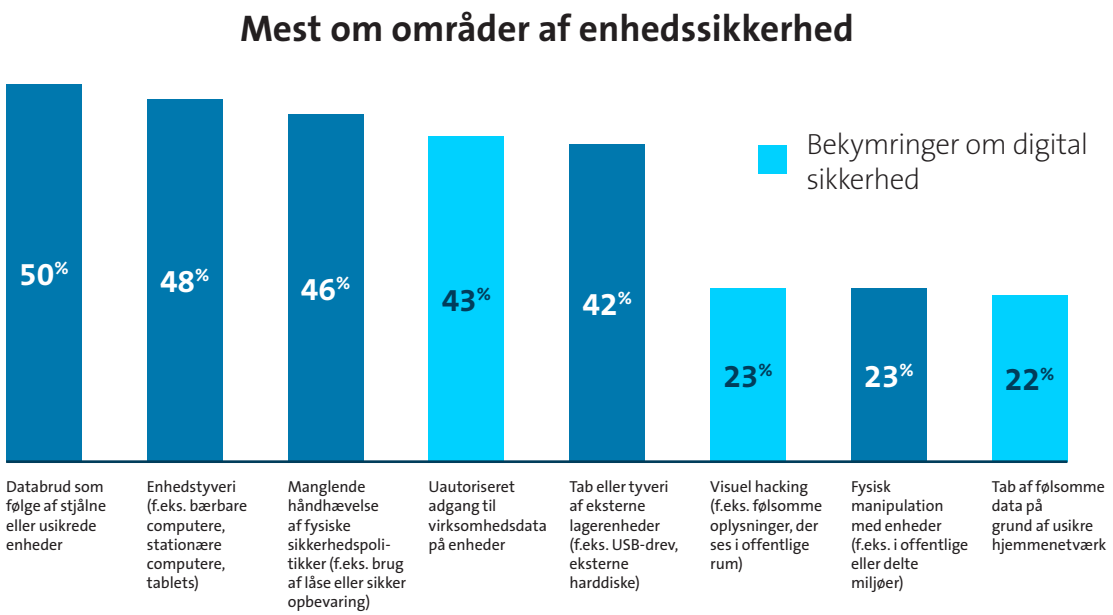


Fig. 4: *Hvilke områder af enhedssikkerhed i din organisation bekymrer dig mest? [Spørget til alle respondenter: 1000, viser kombinationen af svar placeret på første, anden og tredjeplads]*

Databrud er dog den største bekymring, hvilket er velbegrundet, da en bemærkelsesværdig andel (**46%**) har oplevet et databrud som en direkte konsekvens af en usikret enhed.

Det er her en sikkerhedslås kan hjælpe. Organisationer, der bruger sikkerhedslåse, er **37%** mindre tilbøjelige til at have oplevet et databrud på grund af en usikret enhed sammenlignet med dem, der slet ikke bruger sikkerhedslåse.

Organisationer, der har oplevet et databrud eller tab af følsomme data på grund af en usikret enhed

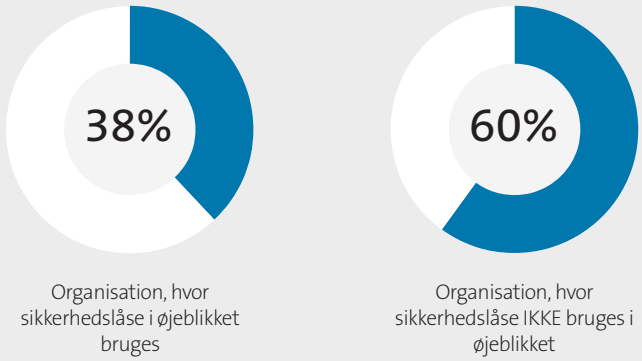


Fig. 5: *Har din organisation oplevet et databrud eller tab af følsomme data som en direkte konsekvens af, at en enhed ikke er sikret? [Spørget til alle respondenter, opdelt efter dem, der i øjeblikket bruger sikkerhedslåse: 629; og dem, der ikke i øjeblikket bruger sikkerhedslåse: 371]*

Resultatet er klart: at demonstrere en målbar reduktion i databrud eller datatab forstærker værdien af sikkerhedslåse som en kritisk komponent i omfattende enhedsbeskyttelse. Dette overbevisende bevis fremhæver, hvordan sikkerhedslåse direkte mindsker risikoen og placerer dem som en vigtig investering for organisationer, der er forpligtet til at beskytte deres data og minimere sikkerhedssårbarheder.

Fokus på data:

- **Sektor:** baseret på undersøgelsesresultater er der større sandsynlighed for, at organisationer inden for forbrugerservice (**65%**) og offentlig/privat sundhedspleje (**57%**) har oplevet et databrud som følge af en usikret enhed. Førstnævnte var blandt de mest tilbøjelige til at være blevet påvirket af enhedstyveri generelt. Med sidstnævnte fremhæver dette måske større bekymringer for den decentraliserede karakter af sundhedsinstitutioner og medlemmer af offentligheden, der er i tættere kontakt med enheder. At have sådan et væld af følsomme data sætter denne sektor i større risiko
- **Størrelse:** For yderligere at fremhæve de begrænsede ressourcer i mindre organisationer, er de mere tilbøjelige (**59%**) end deres større kolleger (**40%**) til at have oplevet et databrud på grund af en usikret enhed. Ikke kun kæmper de med de indledende afskrækkende midler, men også den sneboldeffekt, der følger
- **Anciennitet:** Jo yngre af de adspurgte er mindre tilbøjelige til at rapportere et databrud eller tab af følsomme data på grund af en usikret enhed (**30%**) end deres bestyrelse/C-niveau kolleger (**59%**). Der er en klar fejljustering inden for virksomheder, når det kommer til en sand forståelse af fysisk enhedssikkerhed og konsekvenserne af, at dette ikke er på plads – en opfordring til bredere uddannelse og videndeling

"En lille indledende investering i sikkerhedsforanstaltninger (låse) kan **reducere muligheden for dyre enhedsudskiftninger** eller længere nedetid betydeligt."

øverste ledelse; Uddannelse – staten/staten leveret; 1.000 eller flere ansatte; Hybrid arbejdsmodel; USA

Så hvordan skal organisationer se ud for at overvinde dette?

Organisationer står over for så mange digitale og fysiske sikkerhedsproblemer, og virkningerne af enhedstyveri er svimlende for organisationer og deres bundlinjer. De bør lede efter den mest omkostningseffektive løsning. Og med deres dokumenterede succes, kunne det sidde med den enkle sikkerhedslås.

Størstedelen (**84%**) af vores adspurgte senior IT-beslutningstagere siger, at sikkerhedslåse er omkostningseffektive til at afbøde potentielle databrud – at de giver betydelig værdi til at forhindre tyveri og brud. Derudover mener **42%**, at de er ekstremt omkostningseffektive.

Dette er en universel mening, som deles af dem, der allerede bruger sikkerhedslåse og endda dem, der ikke gør det – hvilket rejser spørgsmålet, hvorfor ikke? Organisationer kan se låse som en tilføjelse af logistiske udfordringer til enhedshåndtering, eller måske fører et stærkere fokus på digital over fysisk sikkerhed til en undervurdering af værdien af låse, hvilket hindrer adoption. Men sammenlignet med de svimlende økonomiske konsekvenser af enhedstyveri, repræsenterer prisen på en sikkerhedslås - typisk i gennemsnit så lidt som $30 til $50 pr. enhed - en minimal investering for at reducere risici. Dykker vi yderligere ned i dette, ser vi en klar forskel i mening på tværs af det organisatoriske hierarki.

Oplevet omkostningseffektivitet af sikkerhedslåse

Fig. 6: *Med hensyn til omkostningseffektivitet, hvordan ser du på den rolle, fysiske sikkerhedslåse spiller for at afbøde potentielle databrud eller tyveri? [Spørget til alle respondenter, viser data opdelt efter anciennitet, basistal i diagrammet]*

Disse resultater understreger det kritiske behov for at løse de grundlæggende årsager til enhedstyveri og dets bredere konsekvenser på tværs af en organisation. Mens seniorledere er mere tilbøjelige til at se sikkerhedslåse som ekstremt omkostningseffektive (**56%**), mindskes denne tro på lavere niveauer i hierarkiet. I sidste ende vil seniorledere altid være mere fokuserede på bredere implikationer (f.eks. reguleringsbøder, omdømme), mens ledere på lavere niveauer på de daglige konsekvenser (f.eks. produktivitetstab).

Denne afbrydelse fremhæver vigtigheden af organisatorisk tilpasning og uddannelse omkring værdien af sikkerhedslåse – ikke kun som et omkostningseffektivt værktøj, men som en proaktiv løsning til at forhindre betydelige tab, før de opstår. At bygge bro over disse huller i opfattelsen vil sikre en samlet og effektiv tilgang til at mindske risikoen for enhedstyveri og beskytte følsomme data.

"Når det først er tabt, vil det forårsage betydelige tab. Vi er nødt til at **dløse dette problem ved roden.**"

Mid-level ledelse; Sundhedspleje - privatejet; 1.000 eller flere ansatte; Hybrid arbejdsmodel; USA

Låse arbejder for at sikre og berolige

Vi er fortsat med at udforske, hvordan sikkerhedslåse ikke kun er effektive til at reducere tyveri, men også tilbyder en omkostningseffektiv løsning til at afbøde bredere sikkerhedsrisici. Deres forskellige applikationer fremhæver deres alsidighed til at håndtere sikkerhedsudfordringer på tværs af forskellige miljøer - en fordel, som mange organisationer allerede er klar over.

Mange bruger allerede sikkerhedslåse til at sikre elektroniske enheder i deres organisation. De mest almindeligt sikrede enheder omfatter bærbare computere (**44%**), stationære computere (**43%**) og servere (**42%**), hvilket afspejler den prioritet, der er lagt på at beskytte kritisk hardware, der ofte indeholder følsomme data. Denne udbredte anvendelse fremhæver anerkendelsen af låse som et vigtigt værktøj til at beskytte mod tyveri og uautoriseret adgang.

Fig. 7: *Til hvilke af følgende elektroniske enheder bruges fysiske sikkerhedslåse i din organisation? [Spørget til alle respondenter: 1000]*

Men det faktum, at næsten 4 ud af 10 af de adspurgte siger, at deres organisationer ikke bruger låse, vækker bekymring over sårbarheder i enhedssikkerhedsstrategier, især for enheder, der ofte bruges i mobile eller hybride arbejdsmiljøer.

For organisationer understreger disse data behovet for at evaluere deres nuværende sikkerhedsforanstaltninger grundigt. Mens låse er en pålidelig og udbredt løsning, kan en udvidelse af deres brug på tværs af en bredere vifte af enheder og parre dem med komplementære digitale beskyttelser hjælpe med at lukke eksisterende sikkerhedshuller og mindske risici mere effektivt.

Næsten alle adspurgte (**97%**) erkender den kritiske rolle, sikkerhedslåse spiller for at hjælpe med at forhindre tyveri og den uautoriserede adgang, der ofte følger. Denne udbredte anerkendelse afspejler den tillid, organisationer har til fysisk sikkerhed som en grundlæggende foranstaltning til at beskytte enheder og følsomme data. Låse fungerer som et frontlinjeforsvar, der reducerer mulighederne for tyveri og mindsker risici forbundet med kompromitteret hardware.

"At have låse i åbne kontorer, coworking-rum eller andre områder, hvor flere personer kan være til stede, **reducerer risikoen for tyveri.**"

Bestyrelsesmedlem/C-niveau; Uddannelse – privatejet; 100-249 ansatte; USA

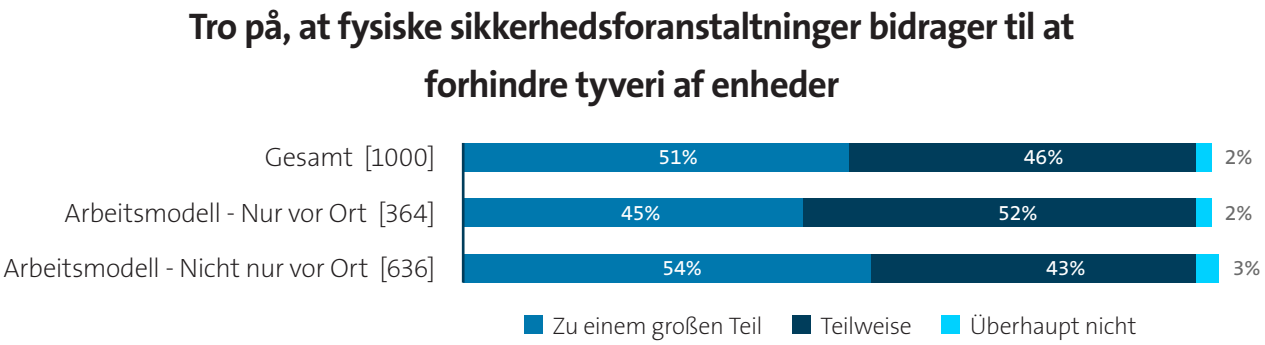


Fig. 8: *I hvilket omfang mener du, at fysiske sikkerhedsforanstaltninger såsom sikkerhedslåse bidrager til at forhindre enhedstyveri, som kan føre til uautoriseret adgang til virksomhedens data? [Spørget til alle respondenter, viser data opdelt efter type arbejdsmodel, basistal i diagrammet]*

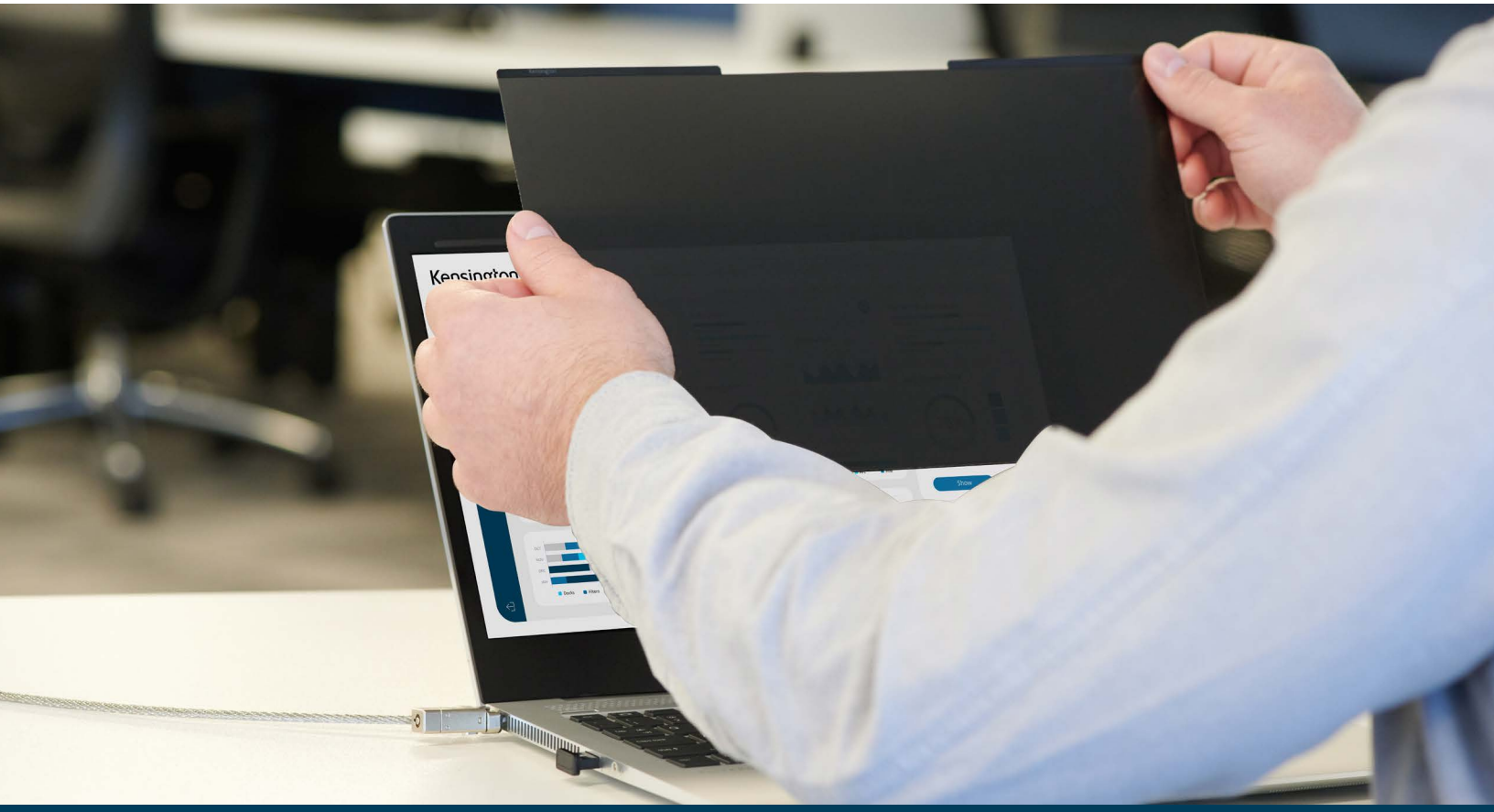
Denne anerkendelse bliver mere fremtrædende, hvor organisationer har vedtaget fleksible og hybride arbejdsmodeller. I disse decentraliserede miljøer bruges enheder i stigende grad på usikrede steder, såsom hjemmekontorer eller offentlige rum, hvilket forstærker risikoen for tyveri eller utilsigtet eksponering. Databrud forårsaget af usikrede enheder er betydeligt mere almindelige i de mere fleksible arbejdsopsætninger (**50%** kombineret mod **39%** for en fuldt onsite arbejdsmodel).

Sikkerhedslåse er designet til at tilpasse sig forskellige miljøer og giver en pålidelig beskyttelse af enheder, uanset om de bruges på kontorer, fjernarbejdsområder eller offentlige omgivelser, hvilket giver organisationer ro i sindet på tværs af alle arbejdsmodeller.

De økonomiske konsekvenser af enhedstyveri kan være svimlende, og omkostningerne ved at erstatte stjålet hardware er ofte overskyggede af den bredere indvirkning på produktivitet, overholdelse af lovgivning og databrud. For organisationer øger enhver stjålet eller usikret enhed risikoen – ikke kun for driften, men for bundlinjen. Sikkerhedslåse tilbyder en gennemprøvet og omkostningseffektiv løsning, som mange allerede har tillid til at reducere sandsynligheden for tyveri og det deraf følgende økonomiske og omdømmemæssige nedfald. Ved at håndtere disse risici ved deres rod, kan organisationer tage en proaktiv holdning til at beskytte deres aktiver og følsomme data.

Selvom fysiske sikkerhedsforanstaltninger som låse er effektive, skal de være en del af en bredere strategi for at tackle de udviklende sikkerhedsrisici forbundet med hybridarbejde. Kombination af låse med komplementære digitale beskyttelser, såsom kryptering og to-faktor autentificering, sikrer omfattende dækning mod både fysiske og digitale trusler. Uddannelsesprogrammer til at uddanne medarbejderne om vigtigheden af denne integrerede tilgang kan yderligere styrke den organisatoriske sikkerhed. For organisationer, der navigerer i kompleksiteten af moderne arbejdsmodeller, er integration af fysiske og digitale sikkerhedsforanstaltninger afgørende for at minimere risici, beskytte deres arbejdsstyrke og opretholde operationel modstandskraft.

At forhindre enhedstyveri og de deraf følgende databrud er langt mere omkostningseffektivt end at håndtere eftervirkningerne. Ved at tage forebyggende foranstaltninger som at bruge bærbare låse i dag kan du beskytte din organisation mod betydelige økonomiske og operationelle konsekvenser i fremtiden. For at sikre, at disse foranstaltninger er effektive, er tilpasning på tværs af ledende ledelse, ledelse og teams afgørende. En fælles forpligtelse til sikkerhedsprioriteter sikrer, at alle forstår deres rolle i at beskytte værdifulde aktiver og reducere risikoen.



Metode

Kensington bestilte den uafhængige markedsundersøgelsesspecialist Vanson Bourne til at udføre den forskning, som denne rapport er baseret på. I alt 1.000 senior IT-ledere , der er involveret eller har indflydelse på fysisk it-hardwaresikkerhed i deres organisation, blev interviewet i efteråret 2024 med repræsentation i USA, Storbritannien, Frankrig og Tyskland.

Respondenterne skulle være fra organisationer med 100 eller flere ansatte og fra en række private og offentlige sektorer.

Interviewene blev gennemført online og blev foretaget ved hjælp af en streng screening på flere niveauer for at sikre, at kun egnede kandidater fik mulighed for at deltage. Medmindre andet er angivet, er de diskuterede resultater baseret på den samlede prøve.

Om Kensington

Kensington er en førende leverandør af tilbehør til desktop og mobilenhed, som IT, undervisere, erhvervsfolk og hjemmekontorer har haft tillid til i mere end 40 år. Kensington stræber efter at forudse behovene og udfordringerne på den stadigt udviklende arbejdsplads og udvikle prisvindende løsninger på professionelt niveau til organisationer, der er forpligtet til at give topprofessionelle de værktøjer, de har brug for for at trives. Virksomheden er stolt af de professionelles valg og på sine kerneværdier omkring design, kvalitet og support.

I kontor- og mobile miljøer giver Kensingtons omfattende portefølje af prisvindende produkter pålidelig sikkerhed, innovationer i desktopproduktivitet, professionelle videokonferencer og ergonomisk velvære.

Med hovedkvarter i Burlingame, Californien, er Kensington opfinderen og en verdensomspændende førende inden for sikkerhedslåse til bærbare computere. Kensington er en afdeling af ACCO Brands, Home of Great Brands Built by Great People, som designer, fremstiller og markedsfører forbruger- og slutbrugerprodukter, der hjælper folk med at arbejde, lære og lege. Ud over Kensington® omfatter ACCO Brands' bredt anerkendte mærker AT-A-GLANCE® , Five Star® , Leitz® , Mead® , PowerA® , Swingline® , Tilibra og mange andre. Flere oplysninger om ACCO Brands Corporation (NYSE:ACCO) kan findes på www.accobrands.com.

FOR MORE INFORMATION CONTACT: sales@kensington.com

Kensington
The Professionals' Choice™