Kensington®

Beveilig uw apparaat, bescherm uw gegevens.

Hoe fysieke beveiliging u kan helpen uw volgende datalek te voorkomen

Inleiding

Het beveiligingslandschap is de afgelopen jaren drastisch geëvolueerd, gedreven door verschuivingen in hoe en waar we werken. De ultieme drijfveer hiervoor was de COVID-19-pandemie; het versnelde de adoptie van hybride en flexibele werkmodellen en veranderde fundamenteel de prioriteiten voor apparaatbeveiliging.

Kensington heeft een onderzoek gesponsord dat werd uitgevoerd door onafhankelijk marktonderzoeksdeskundige Vanson Bourne, onder 1.000 senior IT-besluitvormers die verantwoordelijk zijn voor de fysieke hardwarebeveiliging van hun organisatie in de VS en EMEA. Bijna alle ondervraagden (**92%**) hebben hun beveiligingsbeleid aangescherpt als reactie op de pandemie, waarbij ze de verhoogde risico's erkennen die gepaard gaan met gedecentraliseerde werkomgevingen. Nu we vooruitkijken naar 2025, zal het niveau van flexibelere werkmodellen naar verwachting toenemen, wat benadrukt dat het nu tijd is om de strategieën voor apparaatbeveiliging te heroverwegen.

Datalekken zijn niet alleen een digitaal probleem: elk gestolen of onbeveiligd apparaat is een potentiële toegangspoort voor ongeautoriseerde toegang tot gevoelige informatie, wat aanzienlijke risico's voor organisaties met zich meebrengt. Nu de financiële last van een datalek gemiddeld miljoenen dollars bedraagt, is de inzet nog nooit zo hoog geweest. Naarmate organisaties hun werkmodellen blijven aanpassen, is de urgentie om de beveiliging van apparaten aan te pakken enorm toegenomen. Strengere eisen voor gegevensbescherming en een toename van datalekken hebben het belang van het beschermen van zowel fysieke apparaten als de gevoelige informatie die ze bevatten, verder vergroot. Dit rapport benadrukt de cruciale rol die beveiligingssloten spelen bij het beperken van deze risico's en onderstreept waarom het essentieel is om nu actie te ondernemen om opkomende uitdagingen voor te blijven.

Met deze bevindingen onderzoeken we de tastbare gevolgen van diefstal van apparaten, laten we zien hoe eenvoudige maar effectieve oplossingen zoals beveiligingssloten kunnen helpen om risico's te beperken en benadrukken we hoe fysieke beveiliging gemoedsrust biedt in een wereld waarin werkmodellen voortdurend evolueren. Van het begrijpen van de verbijsterende gevolgen van diefstal van apparaten tot het aantonen van de kosteneffectiviteit en geruststelling van sloten, dit rapport biedt bruikbare inzichten voor organisaties die door het complexe beveiligingslandschap van vandaag navigeren.

Belangrijkste bevindingen:

76% van de respondenten zegt dat hun organisatie de afgelopen 2 jaar te maken heeft gehad met diefstalincidenten, waarbij incidenten vaker voorkomen in organisaties met flexibelere werkmodellen. Ons onderzoek onthulde bijvoorbeeld dat (**85%**) van de organisaties met flexibele werkmodellen in de afgelopen 2 jaar te maken heeft gehad met een diefstalincident, vergeleken met **71%** van de organisaties waarvan de werknemers volledig onsite zijn.

De gevolgen van diefstal van apparaten reiken verder dan alleen het verlies van hardware. Ze omvatten:

- de noodzaak om bestaande veiligheidsmaatregelen te verbeteren (**33%**)
- juridische of wettelijke gevolgen als gevolg van gecompromitteerde gegevens op gestolen apparaten (**33%**)
- verstoring van de productiviteit van werknemers door verloren of gestolen apparaten (**32%**)

Organisaties die beveiligingssloten gebruiken, lopen **37%** minder risico op een datalek als gevolg van een onbeveiligd apparaat (**38%** versus **60%** bij organisaties die geen beveiligingssloten gebruiken).

Organisaties die momenteel sloten gebruiken, hanteren vaker een dubbele aanpak voor beveiliging. Driekwart (**76%**) gebruikt digitale maatregelen zoals vingerafdruk- of beveiligingssleutels voor tweefactorauthenticatie, vergeleken met **62%** van de organisaties die helemaal geen sloten gebruiken.

84% is het erover eens dat beveiligingssloten kosteneffectief zijn bij het beperken van potentiële datalekken en dat ze een aanzienlijke waarde bieden voor een relatief lage investering.

- **42%** is van mening dat apparaatvergrendelingen zeer kosteneffectief zijn en een hoge mate van bescherming bieden tegen lage kosten. Het hoogste management erkent de waarde ervan vaker (**56%**) dan het middenmanagement (**36%**).

Bijna alle ondervraagden (**97%**) zijn van mening dat apparaatvergrendelingen diefstal kunnen voorkomen en de kans op ongeautoriseerde toegang tot gevoelige bedrijfsgegevens kunnen verkleinen.

Gestolen apparaten - de impact is enorm

Er gaat zelden een dag voorbij waarop je niets hoort over een beveiligingsincident – of het nu gaat om een grootschalige aanval op een wereldwijd conglomeraat of een meer gerichte exploitatie van kritieke infrastructuur of service. En hoewel die voorbeelden suggereren dat cyberincidenten vaak het meest worden besproken – of in ieder geval worden verondersteld – is het belangrijk om te erkennen dat fysieke beveiligingsbedreigingen net zo kritiek kunnen zijn.

Er is weinig wijdverbreid gesprek over fysieke beveiligingsincidenten, waarbij onbevoegden toegang krijgen tot beveiligde gebieden of activa in gevaar brengen, wat net zulke ernstige gevolgen heeft als de gemiddelde ransomware-aanval. Volgens ons onderzoek zegt meer dan driekwart (**76%**) van de ondervraagden dat hun organisatie de afgelopen twee jaar is getroffen door incidenten van diefstal van apparaten.

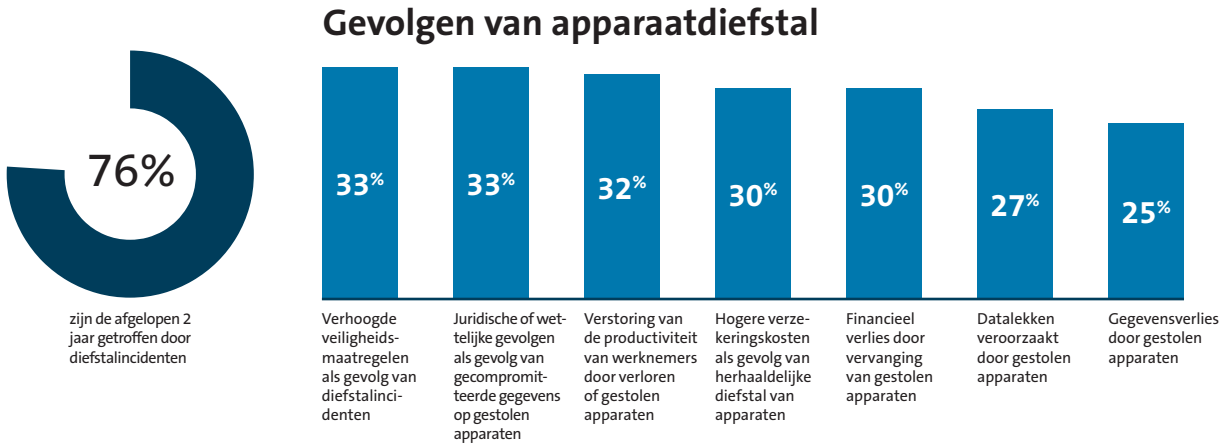


Fig. 1: *Hoe is uw organisatie de afgelopen twee jaar beïnvloed door incidenten van apparaatdiefstal? [Gevraagd aan alle respondenten: 1000]*

Het zijn niet alleen de voor de hand liggende kosten van het vervangen van een apparaat waar organisaties mee te maken krijgen (**30%**). De meest voorkomende gevolgen zijn onder meer een toename van de geïmplementeerde beveiligingsmaatregelen als gevolg daarvan (**33%**) of juridische of regelgevende gevolgen vanwege gecompromitteerde gegevens (**33%**), waarbij het laatste vaak duidelijk wordt beschreven. Bijvoorbeeld GSGVO[1] boetes kunnen oplopen tot 20 miljoen euro of **4%** van de wereldwijde omzet van een organisatie, waarbij zelfs minder ernstige overtredingen tot 10 miljoen euro kosten, wat aanzienlijke financiële risico's met zich meebrengt voor niet-naleving. Naast de financiële gevolgen zijn er ook kosten van verstoring van de productiviteit van werknemers door verloren of gestolen apparaten (**32%**). Als gevolg van al deze gevolgen is er een duidelijke financiële of tijdsimpact op de winstgevendheid van de organisatie. Het zijn dus niet alleen digitale beveiligingsincidenten die aandacht vereisen, maar ook fysieke bedreigingen vormen aanzienlijke risico's. Door hun begrip van deze kwetsbaarheden te verdiepen, kunnen organisaties eenvoudige, kosteneffectieve stappen ondernemen om hun apparaten te beschermen. Omdat fysieke beveiligingsmaatregelen zowel betaalbaar als eenvoudig te implementeren zijn (zoals we later zullen onderzoeken), vormen ze een praktische eerste stap in het versterken van de algehele beveiliging.

"Naast cybersecuritymaatregelen **is fysieke beveiliging net zo belangrijk** Beveiligingskabels zijn onderdeel van een sterkere cybersecuritystrategie."

Senior management; Productie en fabricage; 1.000 of meer werknemers; Volledig on-site werkmodel; Frankrijk

1 AVG-boetes/straffen, Intersoft Consulting, https://gdpr-info.eu/issues/fines-penalties/

Tegenwoordig is het niet de vraag of er een datalek optreedt, maar wanneer. Sterker nog, elke diefstal van een apparaat is een datalek dat staat te gebeuren, en de financiële gevolgen zijn verbijsterend voor organisaties. Volgens het meest recente rapport van IBM over de kosten van datalekken[2], bedragen de wereldwijde gemiddelde kosten van een datalek in 2024 $ 4,88 miljoen USD; een stijging van **10%** in een jaar ten opzichte van het gemiddelde van $ 4,45 miljoen USD in 2023. Dit cijfer verschilt per branche en organisatiegrootte, dus sommige organisaties kunnen met nog hogere kosten te maken krijgen.

Spotlight op de data:

- **Sector:** organisaties in de consumenten dienstverlening(**95%**), energie, olie/gas en nutsbedrijven (**90%**) en bouw en onroerend goed (**89%**) zijn het meest waarschijnlijk getroffen door diefstal van apparaten. De hogere mobiliteit van werknemers en apparaten in deze bedrijven stelt hen bloot aan een groter risico op diefstal
- **Grootte:** de kans op diefstal van apparaten in kleinere organisaties (100-249 werknemers) is meer toegenomen (**82%**) dan in grotere organisaties met meer dan 1.000 werknemers (**69%**), wat de relatieve impact op kleinere organisaties benadrukt, waar de middelen beperkter zijn, de gevolgen kunnen groter zijn
- **Senioriteit:** Mensen in hogere functies melden veel vaker dat ze te maken hebben gehad met diefstalincidenten (**87%**) dan managers op middenniveau (**67%**). Het is waarschijnlijk dat degenen die verantwoordelijk zijn voor de dagelijkse gang van zaken in een bedrijf slecht op de hoogte zijn van de potentiële bedreigingen waarmee onveilige apparaten worden geconfronteerd. Door hun bewustzijn van de bedreigingen en de bijbehorende gevolgen te vergroten, worden bedrijven aangemoedigd om beveiligingssloten in hun culturele behoeften te integreren en perspectieven op alle niveaus op elkaar af te stemmen om een uitgebreide beveiligingsstrategie te ondersteunen

Welke rol spelen werkmodellen hierbij?

Toen we dit onderzoek introduceerden, merkten we op dat de manieren van werken de afgelopen jaren enorm zijn veranderd. De invoering van flexibelere werkmodellen, los van een vaste werkplek, is door de COVID-19-pandemie versneld.

Uit een onderzoek blijkt dat meer dan driekwart (**76%**) van alle ondervraagden aangeeft dat hun organisatie de afgelopen twee jaar te maken heeft gehad met diefstal van apparaten. Dit wordt nog duidelijker als de werkmodellen flexibeler zijn: bij werknemers die volledig op afstand werken, is dit zelfs meer dan 9 op de 10 (**94%**).

Wijdverbreidheid van apparaatdiefstal in de afgelopen twee jaar, volgens het huidige werkmodel

Fig. 2: *Percentage respondenten wiens organisatie de afgelopen twee jaar te maken heeft gehad met incidenten van diefstal van apparaten [Gevraagd aan alle respondenten, met gegevens opgesplitst naar huidig werkend model, basisnummers in grafiek]*

2 Rapport over de kosten van datalekken 2024, IBM, juli 2024, https://www.ibm.com/reports/data-breach

Hoewel het voor elke organisatie belangrijk is om rekening te houden met de fysieke beveiliging van apparaten en zich bewust te zijn van de gevolgen van diefstal van apparaten, vergroten flexibele en op afstand werkende modellen het risico op diefstal van apparaten aanzienlijk. Robuuste beveiligingsmaatregelen zijn daarom belangrijker dan ooit.

Het is belangrijk om op te merken dat het niveau van diefstal van apparaten over het algemeen hoog is, zelfs wanneer werknemers volledig op locatie zijn. Organisaties hebben geen ruimte om zelfgenoegzaam te zijn, ongeacht waar hun werknemers werken. De dreiging van diefstal van apparaten is niet nieuw en is ook niet zomaar ontstaan als onderdeel van deze post-pandemische wereld. Ons onderzoek in 2016[3] onderzocht de beveiligingsrisico's die IT-diefstal in het bedrijf creëert. Ondervraagde IT-professionals rangschikten het risico van diefstal van apparaten op kantoor (**23%**) bijna net zo hoog als diefstal in auto 's en vervoer (**25%**), en hoger dan diefstal op luchthavens en in hotels (**15%**) of restaurants (**12%**). Dit laat zien hoe diefstal van apparaten een voortdurende dreiging blijft, zelfs in volledig on-site omgevingen, wat de noodzaak van waakzaamheid en proactieve fysieke beveiligingsmaatregelen onderstreept, ongeacht de werkplek.

Deze uitdaging is nog groter geworden in de post-COVID-19-wereld, waarbij **93%** van de organisaties een toename van beveiligingsrisico's meldt vanwege de verschuiving naar flexibele en hybride werkmodellen. Deze risico's gaan verder dan diefstal van fysieke apparaten en omvatten verhoogde kwetsbaarheden in gegevensbescherming, ongeautoriseerde toegang en inbreuken veroorzaakt door onbeveiligde thuisnetwerken en gedecentraliseerde werkomgevingen.

"**Het is de makkelijkste manier** om ervoor te zorgen dat onze apparaten letterlijk op slot zitten! Het zorgt ervoor dat **we weten dat alles veilig en beveiligd is**"

Bestuurslid/C-level; IT, technologie en telecom; 100-249 medewerkers; Flexibel werkmodel; VS

Toename van het beveiligingsrisico door hybride of remote werkomgevingen

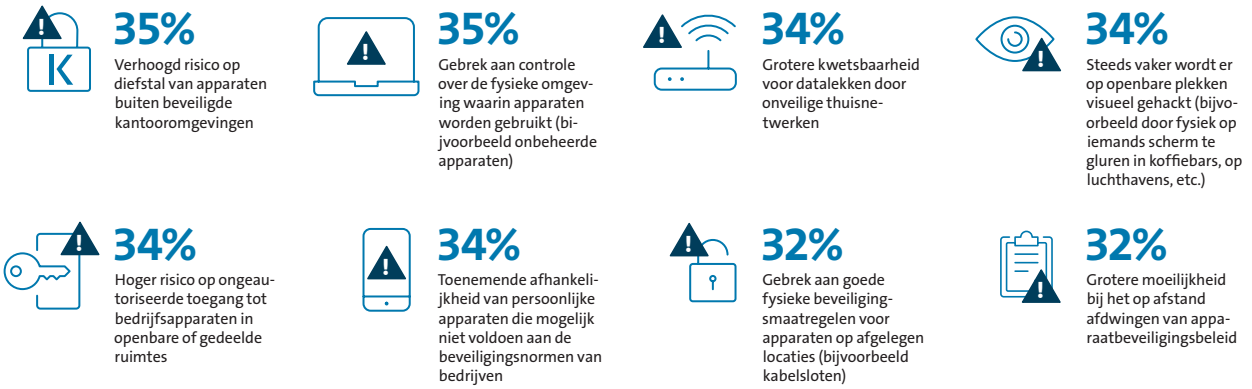


Fig. 3: *Welke veiligheidsrisico's zijn volgens u toegenomen als gevolg van hybride of op afstand werkende omgevingen na de COVID-19-pandemie? [Gevraagd aan respondenten wiens organisatie een verschuiving naar hybride/op afstand werken zag na de COVID-19-pandemie: 494]*

Met dit in gedachten ligt de beste aanpak voor beveiliging in het combineren van robuuste fysieke maatregelen met geavanceerde digitale beveiligingen. Zo wordt volledige bescherming van zowel apparaten als gegevens gegarandeerd in een steeds meer gedecentraliseerde wereld.

3 Enquête naar IT-beveiliging en diefstal van laptops, Kensington, augustus 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

Sloten die verlies voorkomen - en kosten besparen

"Het ontbreken van een beveiligingsslot op de apparatuur leidde tot een datalek, **wat resulteerde in aanzienlijke verliezen voor het bedrijf.**"

Middenkader; IT, technologie en telecom; 1.000 of meer werknemers; Flexibel werkmodel; VS

Tot nu toe hebben we de gevolgen van diefstal van apparaten blootgelegd en hoe wijdverbreid dit kan zijn, ongeacht de werkomgeving. Toch is dit niet de enige zorg voor onze ondervraagde senior IT-besluitvormers. Er is een breed scala aan aspecten waar ze zich zorgen over maken als het gaat om beveiliging, zowel fysiek als digitaal.

Sommige van deze zorgen brengen nieuwe factoren rondom fysieke beveiliging met zich mee. Bijna een kwart (**23%**) maakt zich bijvoorbeeld zorgen over visueel hacken, waarbij gevoelige gegevens aan iedereen zijn overgeleverd als iemands scherm op een openbare plek wordt getoond – in een koffiezaak of in het openbaar vervoer. Sterker nog, mensen die flexibel werken (**48%**) melden visueel hacken vaker als een zorg dan mensen die volledig op afstand (**36%**) of in een hybride (**33%**) opstelling werken. Dit benadrukt dat visueel hacken niet alleen wordt geassocieerd met thuiswerken, maar eerder met het verlenen van buitensporige vrijheden die moeilijker te controleren zijn. Organisaties zullen rekening moeten houden met het beschermen van hun gegevens wanneer werknemers buitenshuis zijn, door middel van extra afschrikmiddelen zoals privacy filters.

De meest zorgwekkende gebieden van apparaatbeveiliging

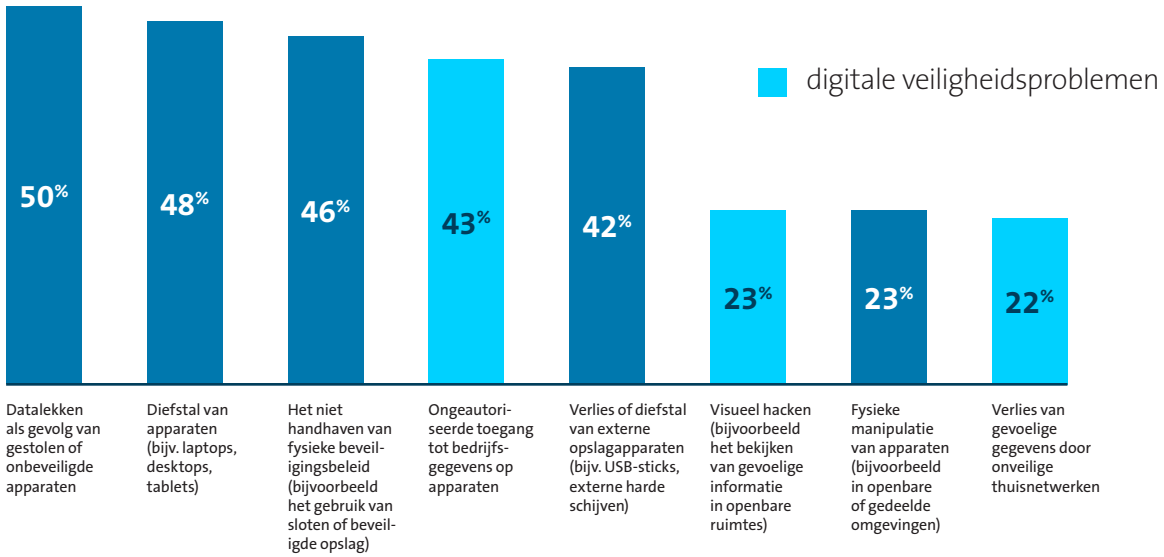


Fig. 4: *Welke aspecten van apparaatbeveiliging in uw organisatie baren u het de meeste zorgen? [Gevraagd aan alle respondenten: 1000, waarbij de combinatie van antwoorden op de eerste, tweede en derde plaats wordt weergegeven]*

Datalekken vormen echter de grootste zorg. Dit is terecht, aangezien een aanzienlijk deel (**46%**) te maken heeft gehad met een datalek als direct gevolg van een onbeveiligd apparaat.

Dit is waar een beveiligingsslot kan helpen. Organisaties die beveiligingssloten gebruiken, hebben **37%** minder kans op een datalek vanwege een onbeveiligd apparaat dan organisaties die helemaal geen beveiligingssloten gebruiken.

Organisaties die te maken hebben gehad met een datalek of verlies van gevoelige gegevens vanwege een onbeveiligd apparaat

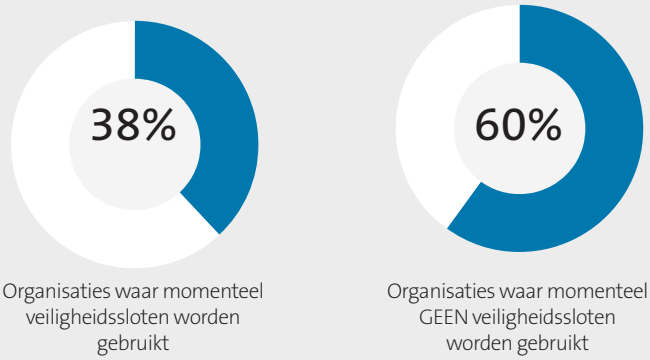


Fig. 5: *Heeft uw organisatie te maken gehad met een datalek of verlies van gevoelige gegevens als direct gevolg van het onbeveiligd achterlaten van een apparaat? [Gevraagd aan alle respondenten, gesplitst in degenen die momenteel beveiligingssloten gebruiken: 629; en degenen die momenteel geen beveiligingssloten gebruiken: 371]*

De uitkomst is duidelijk: het aantonen van een meetbare vermindering van datalekken of dataverlies versterkt de waarde van beveiligingssloten als een cruciaal onderdeel van uitgebreide apparaatbeveiliging. Dit overtuigende bewijs benadrukt hoe beveiligingssloten direct risico's beperken, en positioneert ze als een essentiële investering voor organisaties die zich inzetten voor het beschermen van hun gegevens en het minimaliseren van beveiligingskwetsbaarheden.

Spotlight op de data:

- **Sector:** op basis van de resultaten van het onderzoek is de kans groter dat organisaties in de consumenten dienstverlening (**65%**) en de publieke/private gezondheidszorg (**57%**) een datalek hebben ondervonden als gevolg van een onbeveiligd apparaat. De eerste was een van de sectoren die het meest waarschijnlijk te maken kreeg met diefstal van apparaten. Met de laatste benadrukt dit misschien grotere zorgen over de gedecentraliseerde aard van zorginstellingen en het feit dat leden van het publiek nauwer in contact staan met apparaten. Het hebben van zo'n overvloed aan gevoelige gegevens brengt een groter risico voor deze sector.
- **Grootte:** om de beperkte middelen van kleinere organisaties verder te benadrukken, is de kans groter (**59%**) dan bij hun grotere tegenhangers (**40%**) dat ze een datalek hebben ervaren vanwege een onbeveiligd apparaat. Ze worstelen niet alleen met de eerste afschrikmiddelen, maar ook met het sneeuwbaleffect dat volgt.
- **Senioriteit:** de meer junior personen onder de ondervraagden melden minder snel een datalek of verlies van gevoelige gegevens vanwege een onbeveiligd apparaat (**30%**) dan hun bestuurs-/C-levelcollega's (**59%**). Er is een duidelijke misalignment binnen bedrijven als het gaat om een echt begrip van fysieke apparaatbeveiliging en de gevolgen van het ontbreken hiervan - een oproep voor bredere educatie en kennisdeling.

"Een kleine initiële investering in veiligheidsmaatregelen (sloten) kan **de kans op kostbare vervangingen van apparaten** of langdurige uitvaltijd aanzienlijk verkleinen."

Senior management; Onderwijs – door de overheid/staat verstrekt; 1.000 of meer werknemers; Hybride werkmodel; VS

Hoe kunnen organisaties dit probleem aanpakken?

Organisaties worden geconfronteerd met zoveel digitale en fysieke beveiligingsproblemen, en de impact van diefstal van apparaten is verbijsterend voor organisaties en hun winstcijfers. Ze zouden op zoek moeten gaan naar de meest kosteneffectieve oplossing. En met hun bewezen succes zou dat kunnen passen bij het simpele beveiligingsslot.

De meerderheid (**84%**) van onze ondervraagde senior IT-besluitvormers zegt dat beveiligingssloten kosteneffectief zijn bij het beperken van potentiële datalekken – dat ze een aanzienlijke waarde bieden bij het voorkomen van diefstal en inbreuken. Bovendien gelooft **42%** dat ze extreem kosteneffectief zijn.

Dit is een universele mening die wordt gedeeld door degenen die al beveiligingssloten gebruiken en zelfs degenen die dat niet doen - wat de vraag oproept, waarom niet? Organisaties zien sloten misschien als een logistieke uitdaging voor apparaatbeheer of misschien leidt een sterkere focus op digitale dan op fysieke beveiliging tot een onderschatting van de waarde van sloten, waardoor de acceptatie wordt belemmerd. Maar vergeleken met de duizelingwekkende financiële gevolgen van apparaatdiefstal, vertegenwoordigen de kosten van een beveiligingsslot - doorgaans gemiddeld slechts $ 30 tot $ 50 per apparaat - een minimale investering voor het verminderen van risico's. Als we hier dieper op ingaan, zien we een duidelijk verschil in mening binnen de organisatorische hiërarchie.

Waargenomen kosteneffectiviteit van veiligheidssloten

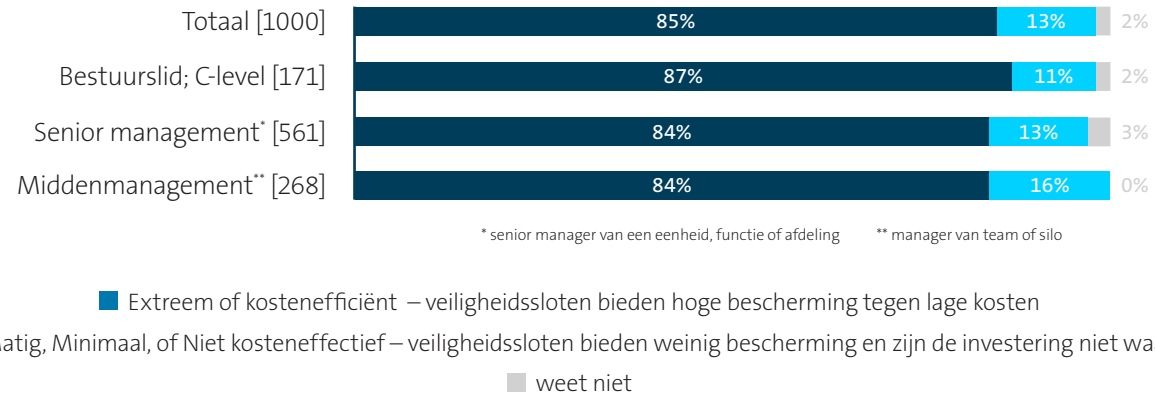


Fig. 6: *Wat betreft kosteneffectiviteit, hoe ziet u de rol van fysieke beveiligingssloten bij het beperken van potentiële datalekken of diefstal? [Gevraagd aan alle respondenten, met gegevens opgesplitst naar anciënniteit, basisnummers in grafiek]*

Deze bevindingen benadrukken de cruciale noodzaak om de grondoorzaken van diefstal van apparaten en de bredere impact ervan binnen een organisatie aan te pakken. Hoewel senior leiders beveiligingssloten eerder als extreem kosteneffectief beschouwen (**56%**), neemt dit geloof af op lagere niveaus van de hiërarchie. Uiteindelijk zullen senior leiders zich altijd meer richten op bredere implicaties (bijv. wettelijke boetes, reputatie), terwijl managers op lager niveau zich richten op de dagelijkse impact (bijv. productiviteitsverlies).

Deze discrepantie benadrukt het belang van organisatorische afstemming en educatie rond de waarde van beveiligingssloten - niet alleen als een kosteneffectieve tool, maar als een proactieve oplossing om significante verliezen te voorkomen voordat ze optreden. Het overbruggen van deze verschillen in perceptie zal zorgen voor een uniforme en effectieve aanpak om de risico's van diefstal van apparaten te beperken en gevoelige gegevens te beschermen.

"Eenmaal verloren, zal het aanzienlijke verliezen veroorzaken. We moeten **dit probleem bij de wortel aanpakken.**"

Middenkader ; Gezondheidszorg - particulier bezit; 1.000 of meer werknemers; Hybride werkmodel; VS

Sloten werken om te beveiligen en gerust te stellen

We zijn blijven onderzoeken hoe beveiligingssloten niet alleen effectief zijn in het verminderen van diefstal, maar ook een kostenefficiënte oplossing bieden om bredere beveiligingsrisico's te beperken. Hun diverse toepassingen benadrukken hun veelzijdigheid in het aanpakken van beveiligingsuitdagingen in verschillende omgevingen - een voordeel dat veel organisaties al beseffen.

Velen gebruiken al beveiligingssloten om elektronische apparaten in hun organisatie te beveiligen. De meest beveiligde apparaten zijn laptops (**44%**), desktops (**43%**) en servers (**42%**), wat de prioriteit weerspiegelt die wordt gegeven aan het beschermen van kritieke hardware die vaak gevoelige gegevens bevat. Deze wijdverbreide acceptatie benadrukt de erkenning van sloten als een essentieel hulpmiddel bij het beschermen tegen diefstal en ongeautoriseerde toegang.

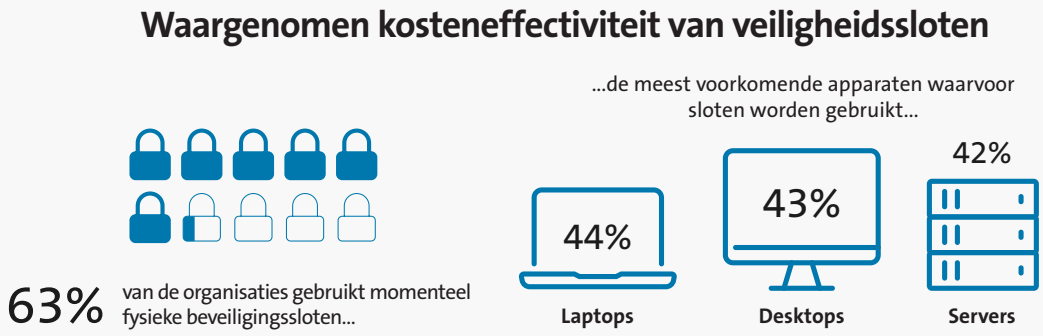


Fig. 7: *Voor welke van de volgende elektronische apparaten worden fysieke beveiligingssloten gebruikt in uw organisatie? [Gevraagd aan alle respondenten: 1000]*

Het feit dat bijna 4 op de 10 ondervraagden aangeeft dat hun organisatie geen sloten gebruikt, roept echter zorgen op over kwetsbaarheden in strategieën voor apparaatbeveiliging, met name voor apparaten die vaak worden gebruikt in mobiele of hybride werkomgevingen.

Voor organisaties onderstreept deze data de noodzaak om hun huidige beveiligingsmaatregelen uitgebreid te evalueren. Hoewel sloten een vertrouwde en veelgebruikte oplossing zijn, kan het uitbreiden van het gebruik ervan naar een breder scala aan apparaten en het koppelen ervan aan aanvullende digitale beschermingen helpen om bestaande beveiligingslekken te dichten en risico's effectiever te beperken.

Bijna alle ondervraagden (**97%**) erkennen de cruciale rol die beveiligingssloten spelen bij het voorkomen van diefstal en de ongeautoriseerde toegang die daar vaak op volgt. Deze brede erkenning weerspiegelt het vertrouwen dat organisaties stellen in fysieke beveiliging als fundamentele maatregel om apparaten en gevoelige gegevens te beschermen. Sloten fungeren als een frontlinieverdediging, waardoor de kans op diefstal wordt verkleind en de risico's die samenhangen met gecompromitteerde hardware worden beperkt.

"Het hebben van sloten in open kantoren, co-workingruimtes of andere ruimtes waar meerdere mensen aanwezig kunnen zijn, **vermindert het risico op diefstal.**"

Bestuurslid/C-level; Onderwijs – particulier bezit; 100-249 werknemers; VS

Geloof dat fysieke beveiligingsmaatregelen bijdragen aan het voorkomen van diefstal van apparaten

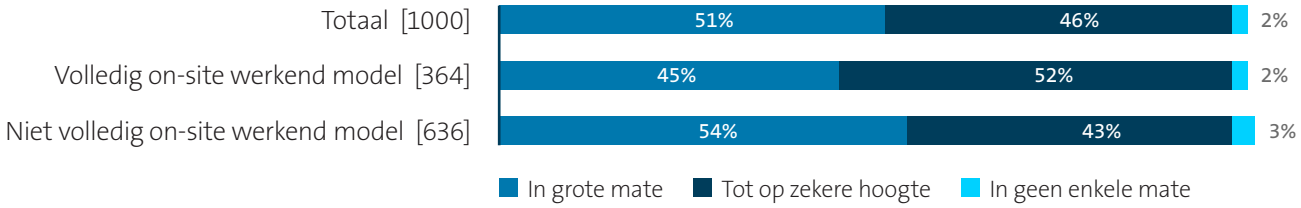


Fig. 8: *In welke mate denkt u dat fysieke beveiligingsmaatregelen zoals veiligheidssloten bijdragen aan het voorkomen van diefstal van apparaten, wat kan leiden tot ongeautoriseerde toegang tot bedrijfsgegevens? [Gevraagd aan alle respondenten, waarbij de gegevens zijn uitgesplitst naar type werkmodel, basisnummers in de grafiek]*

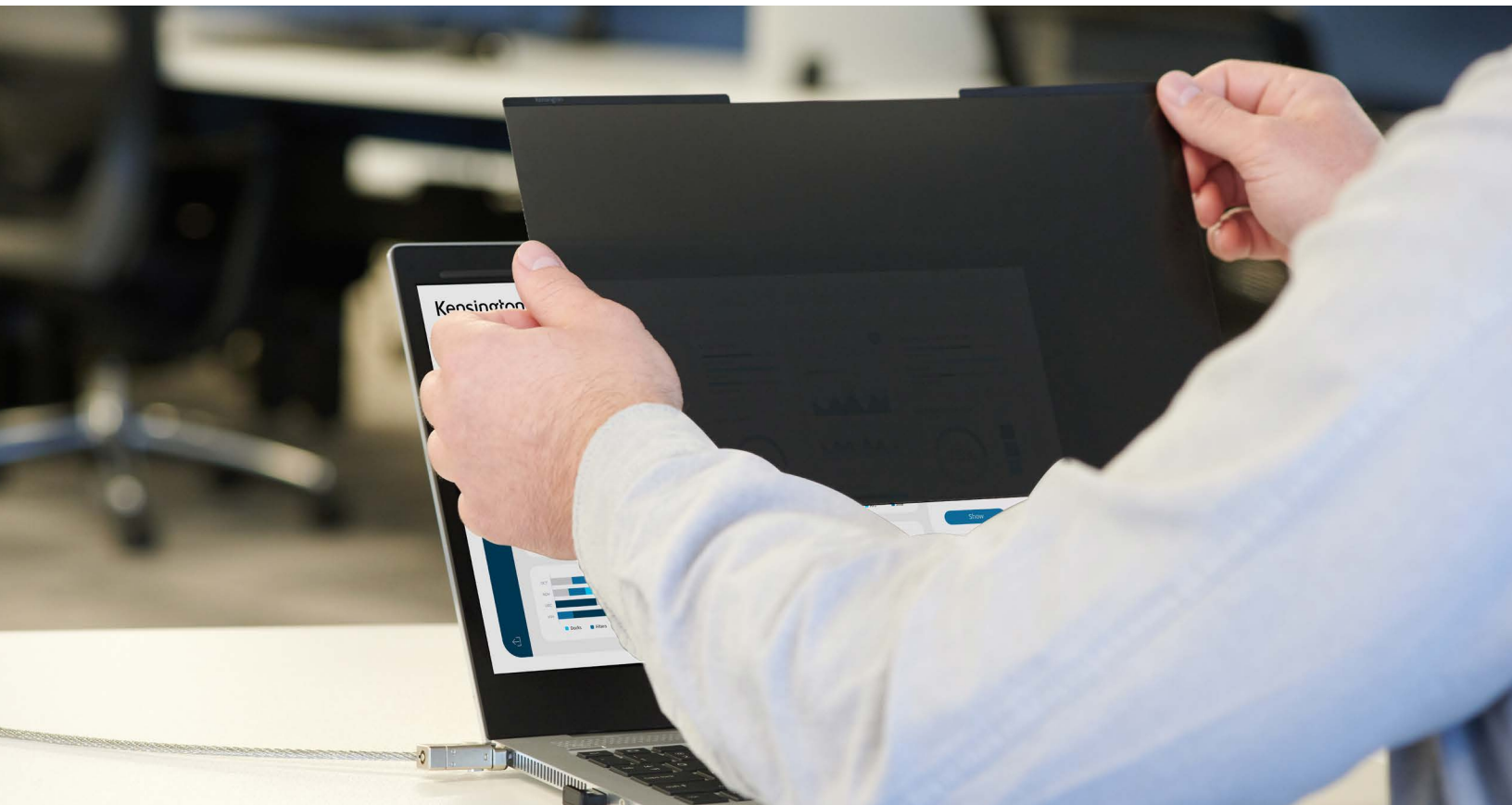
Deze erkenning wordt prominenter wanneer organisaties flexibele en hybride werkmodellen hebben aangenomen. In deze gedecentraliseerde omgevingen worden apparaten steeds vaker gebruikt op onbeveiligde locaties, zoals thuiskantoren of openbare ruimtes, waardoor het risico op diefstal of onbedoelde blootstelling toeneemt. Datalekken veroorzaakt door onbeveiligde apparaten komen aanzienlijk vaker voor in de flexibelere werkopstellingen (**50%** gecombineerd versus **39%** voor een volledig onsite werkmodel).

Veiligheidssloten zijn zo ontworpen dat ze geschikt zijn voor uiteenlopende omgevingen en bieden een betrouwbare beveiliging voor apparaten, ongeacht of deze op kantoor, op externe werkplekken of in openbare ruimtes worden gebruikt. Zo kunnen organisaties zich op alle werkmodellen op hun gemak voelen.

De financiële gevolgen van diefstal van apparaten kunnen enorm zijn, waarbij de kosten voor het vervangen van gestolen hardware vaak in het niet vallen bij de bredere impact op productiviteit, naleving van regelgeving en datalekken. Voor organisaties verhoogt elk gestolen of onbeveiligd apparaat het risico, niet alleen voor de bedrijfsvoering, maar ook voor de winstgevendheid. Beveiligingssloten bieden een bewezen en kosteneffectieve oplossing, die door velen al wordt vertrouwd bij het verkleinen van de kans op diefstal en de daaruit voortvloeiende financiële en reputatieschade. Door deze risico's bij de wortel aan te pakken, kunnen organisaties een proactieve houding aannemen bij het beschermen van hun activa en gevoelige gegevens.

Hoewel fysieke beveiligingsmaatregelen zoals sloten effectief zijn, moeten ze deel uitmaken van een bredere strategie om de evoluerende beveiligingsrisico's die samenhangen met hybride werken aan te pakken. Het combineren van sloten met aanvullende digitale bescherming, zoals encryptie en tweefactorauthenticatie, zorgt voor uitgebreide dekking tegen zowel fysieke als digitale bedreigingen. Trainingsprogramma's om werknemers te onderwijzen over het belang van deze geïntegreerde aanpak kunnen de organisatorische beveiliging verder versterken. Voor organisaties die navigeren door de complexiteit van moderne werkmodellen, is het integreren van fysieke en digitale beveiligingsmaatregelen essentieel om risico's te minimaliseren, hun personeel te beschermen en operationele veerkracht te behouden.

Het voorkomen van diefstal van apparaten en de daaruit voortvloeiende datalekken is veel kosteneffectiever dan omgaan met de nasleep. Preventieve maatregelen nemen, zoals het gebruik van laptopsloten, kan uw organisatie beschermen tegen aanzienlijke financiële en operationele gevolgen in de toekomst. Om ervoor te zorgen dat deze maatregelen effectief zijn, is afstemming tussen senior leiderschap, management en teams van cruciaal belang. Een gedeelde toewijding aan beveiligingsprioriteiten zorgt ervoor dat iedereen zijn rol begrijpt bij het beschermen van waardevolle activa en het verminderen van risico's.



Methodologie

Kensington gaf onafhankelijk marktonderzoeksspecialist Vanson Bourne opdracht om het onderzoek uit te voeren waarop dit rapport is gebaseerd. In totaal werden 1.000 senior IT-leiders die betrokken zijn bij of invloed hebben op fysieke IT-hardwarebeveiliging in hun organisatie , geïnterviewd in de herfst van 2024, met vertegenwoordiging in de VS, het VK, Frankrijk en Duitsland.

Respondenten moesten afkomstig zijn uit organisaties met 100 of meer werknemers en uit verschillende particuliere en publieke sectoren.

De interviews werden online afgenomen en werden uitgevoerd met behulp van een rigoureus screeningsproces op meerdere niveaus om ervoor te zorgen dat alleen geschikte kandidaten de kans kregen om deel te nemen. Tenzij anders aangegeven, zijn de besproken resultaten gebaseerd op de totale steekproef.

Over Kensington

Kensington is een toonaangevende leverancier van accessoires voor desktops en mobiele apparaten, vertrouwd door IT, docenten, bedrijven en home-office professionals over de hele wereld voor meer dan 40 jaar. Kensington streeft ernaar om te anticiperen op de behoeften en uitdagingen van de voortdurend veranderende werkplek en professionele prijswinnende oplossingen te creëren voor organisaties die toegewijd zijn om topprofessionals de tools te bieden die ze nodig hebben om te floreren. Het bedrijf is trots op zichzelf als de keuze van professionals en op zijn kernwaarden rondom design, kwaliteit en ondersteuning.

In kantoor- en mobiele omgevingen biedt het uitgebreide portfolio van bekroonde producten van Kensington betrouwbare beveiliging, innovaties op het gebied van desktopproductiviteit, professionele videoconferenties en ergonomisch welzijn.

Kensington, met het hoofdkantoor in Burlingame, Californië, is de uitvinder en een wereldleider in laptopbeveiligheidssloten. Kensington is een divisie van ACCO Brands, de thuisbasis van geweldige merken gebouwd door geweldige mensen, dat consumenten- en eindgebruikersproducten ontwerpt, produceert en op de markt brengt die mensen helpen werken, leren en spelen. Naast Kensington® omvatten de algemeen erkende merken van ACCO Brands AT-A-GLANCE ® , Five Star® , Leitz® , Mead® , PowerA® , Swingline ® , Tilibra en vele anderen. Meer informatie over ACCO Brands Corporation (NYSE:ACCO) is te vinden op www.accobrands.com.

FOR MORE INFORMATION CONTACT: sales@kensington.com

Kensington
The Professionals' Choice™