Kensington®

Proteggi il tuo dispositivo, tutela i tuoi dati.

Come la sicurezza fisica può aiutarti a prevenire possibili violazioni dei dati

Introduzione

Il panorama della sicurezza si è evoluto radicalmente negli ultimi anni, guidato da cambiamenti radicali nel modo e nel luogo in cui lavoriamo. Il motore principale di tutto questo è stata la pandemia di COVID-19; ha accelerato l'adozione di modelli di lavoro ibridi e flessibili e ha modificato radicalmente le priorità di sicurezza dei dispositivi.

Kensington ha sponsorizzato uno studio condotto dallo specialista indipendente di ricerche di mercato Vanson Bourne, su 1.000 responsabili delle decisioni IT senior per la sicurezza hardware della propria organizzazione negli Stati Uniti e nell'EMEA. Quasi tutti gli intervistati (**92%**) hanno rafforzato le proprie policy di sicurezza in risposta alla pandemia, riconoscendo i maggiori rischi associati agli ambienti di lavoro decentralizzati. Mentre guardiamo al 2025, si prevede che il livello di modelli di lavoro più flessibili aumenterà, sottolineando che è giunto il momento di ripensare le strategie di sicurezza dei dispositivi.

Le violazioni dei dati non sono solo un problema digitale: ogni dispositivo rubato o non protetto rappresenta un potenziale gateway per l'accesso non autorizzato a informazioni sensibili, ponendo rischi significativi per le organizzazioni. Con l'onere finanziario di una violazione dei dati che ora ammonta in media a milioni di dollari, la posta in gioco non è mai stata così alta. Mentre le organizzazioni continuano ad adattare i loro modelli di lavoro, l'urgenza di affrontare la sicurezza dei dispositivi è cresciuta enormemente. Requisiti di protezione dei dati più rigorosi e un'ondata di violazioni dei dati hanno ulteriormente aumentato l'importanza di salvaguardare sia i dispositivi fisici sia le informazioni sensibili in essi contenute. Questo rapporto evidenzia il ruolo fondamentale che i cavi di sicurezza svolgono nell'attenuazione di questi rischi e sottolinea perché agire ora è essenziale per rimanere al passo con le sfide emergenti.

Attraverso queste scoperte, esamineremo gli impatti tangibili del furto di dispositivi, mostreremo come soluzioni semplici ma efficaci come i cavi di sicurezza possano aiutare a mitigare i rischi e metteremo in evidenza come la sicurezza fisica fornisca tranquillità in un mondo in cui i modelli di lavoro sono in continua evoluzione. Dalla comprensione delle sconvolgenti conseguenze del furto di dispositivi alla dimostrazione dell'economicità e della efficienza dei lucchetti, questo rapporto fornisce spunti pratici per le organizzazioni che navigano nel complesso panorama della sicurezza odierno.

Risultati principali:

Il **76%** degli intervistati afferma che la propria organizzazione è stata colpita da incidenti di furto negli ultimi 2 anni, soprattutto nelle organizzazioni con modelli di lavoro più flessibili. Ad esempio, la nostra ricerca ha rivelato che (l'**85%**) delle organizzazioni con modelli di lavoro flessibili ha subito un incidente di furto negli ultimi 2 anni, rispetto al **71%** delle organizzazioni i cui dipendenti sono completamente in sede.

L'impatto del furto va oltre la perdita dell'hardware, tra cui:

- la necessità di potenziare le misure di sicurezza esistenti (**33%**)
- conseguenze legali o normative dovute a dati compromessi su dispositivi rubati (**33%**)
- interruzione della produttività dei dipendenti dovuta a dispositivi smarriti o rubati (**32%**)

Le organizzazioni che utilizzano cavi di sicurezza hanno avuto il **37%** di probabilità in meno di subire una violazione dei dati causata da un dispositivo non protetto (il **38%** rispetto al **60%** tra quelle che non utilizzano cavi di sicurezza).

Le organizzazioni che attualmente utilizzano i lucchetti sono anche più propense ad adottare un duplice approccio alla sicurezza: tre quarti (**76%**) utilizzano misure digitali come chiavette biometriche per l'autenticazione a due fattori, rispetto al **62%** di quelle che non utilizzano affatto lucchetti di sicurezza.

L'**84%** concorda sul fatto che i cavi di sicurezza siano convenienti per mitigare potenziali violazioni dei dati, offrendo un valore significativo a fronte di un investimento relativamente basso.

- Il **42%** ritiene che siano estremamente convenienti, in quanto forniscono un'elevata protezione a costi contenuti; i dirigenti più anziani sono più propensi a riconoscerne il valore (**56%**) rispetto ai dirigenti di medio livello (**36%**).

Quasi tutti gli intervistati (**97%**) ritengono che i cavi dei dispositivi possano prevenire i furti, riducendo la probabilità di accessi non autorizzati ai dati aziendali sensibili.

Dispositivi rubati, conseguenze sconvolgenti

Raramente passa un giorno in cui non si senta parlare di qualche tipo di incidente di sicurezza, che si tratti di un attacco su larga scala a un conglomerato globale o di uno sfruttamento più mirato di infrastrutture o servizi critici. E mentre questi esempi suggeriscono che gli incidenti informatici sono spesso i più ampiamente discussi, è importante riconoscere che le minacce alla sicurezza fisica possono essere altrettanto critiche.

Si parla poco di incidenti di sicurezza fisica, in cui persone non autorizzate accedono ad aree protette o compromettono dispositivi, con conseguenze altrettanto disastrose di un normale attacco ransomware. Secondo la nostra ricerca, oltre tre quarti (**76%**) degli intervistati affermano che la propria organizzazione è stata colpita da incidenti di furto di dispositivi negli ultimi due anni.

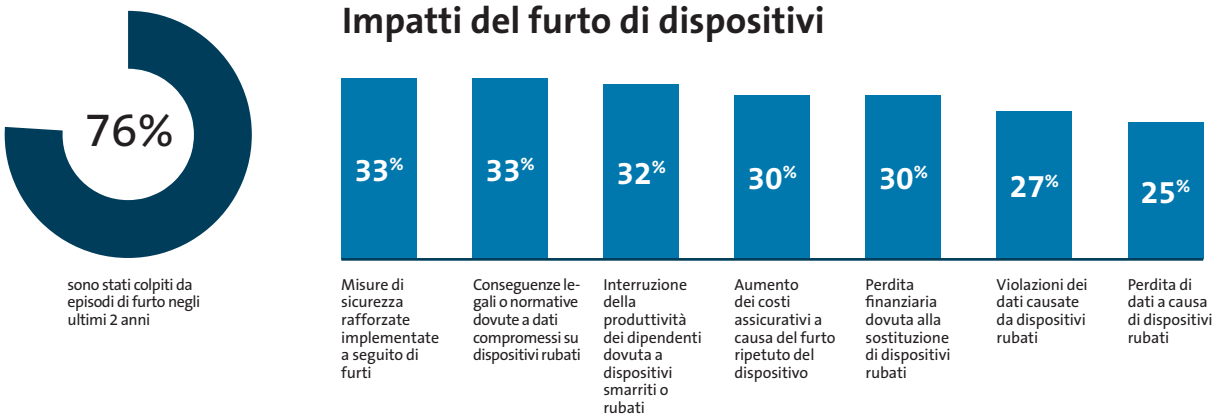


Fig. 1: *In che modo la tua organizzazione è stata influenzata dagli incidenti di furto di dispositivi negli ultimi due anni? [Domanda rivolta a tutti gli intervistati: 1000]*

Non è solo l'evidente costo di sostituzione di un dispositivo che le organizzazioni devono affrontare (**30%**). Gli impatti più comuni includono un aumento delle misure di sicurezza implementate come (**33%**) o conseguenze legali o normative dovute a dati compromessi (**33%**), dove queste ultime sono spesso chiaramente delineate. Ad esempio, multe GDPR[1] possono arrivare fino a 20 milioni di euro o al 4% del fatturato globale di un'organizzazione. Anche le violazioni meno gravi possono costare fino a 10 milioni di euro, ponendo significativi rischi finanziari per la non conformità. Agli impatti finanziari si aggiunge anche il costo dell'interruzione della produttività dei dipendenti a causa di dispositivi persi o rubati (**32%**). Sulla base di uno qualsiasi di questi impatti, c'è una chiara implicazione finanziaria o di tempo sui profitti dell'organizzazione. Quindi, non sono solo gli incidenti di sicurezza digitale a richiedere attenzione: anche le minacce fisiche presentano rischi significativi. Approfondendo la loro comprensione di queste vulnerabilità, le organizzazioni possono adottare misure semplici ed economiche per salvaguardare i propri dispositivi. Poiché le misure di sicurezza fisica sono sia convenienti che facili da implementare (come esploreremo più avanti), rappresentano un primo passo pratico per rafforzare la sicurezza complessiva.

"Oltre alle misure di sicurezza informatica, **la sicurezza fisica è altrettanto importante.** I cavi di sicurezza sono parte di una strategia più forte."

Alta dirigenza; produzione; 1.000 o più dipendenti; modello di lavoro completamente in loco; Francia

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

Al giorno d'oggi, non è questione di se si verifica una violazione dei dati, ma di quando. Infatti, ogni singolo furto di dispositivo è una violazione dei dati in attesa di verificarsi e le implicazioni finanziarie sono sbalorditive per le organizzazioni. Secondo il più recente rapporto IBM sui costi delle violazioni dei dati[2], il costo medio globale di una violazione dei dati nel 2024 si attesta a 4,88 milioni di dollari USA; un aumento del **10%** in un anno rispetto alla media di 4,45 milioni di dollari USA nel 2023. Questa cifra varia a seconda del settore e delle dimensioni dell'organizzazione, quindi alcune organizzazioni potrebbero dover affrontare costi ancora più elevati.

I dati in primo piano:

- **Settore:** le organizzazioni nei settori dei servizi al consumatore (**95%)**, energia, petrolio/gas e servizi di pubblica utilità (**90%**) e edilizia e proprietà (**89%**) sono quelle con maggiori probabilità di essere state colpite dal furto di dispositivi. La maggiore mobilità di dipendenti e dispositivi in queste attività li espone a un rischio maggiore di furto.
- **Dimensioni:** la probabilità di furto di dispositivi nelle organizzazioni più piccole (100-249 dipendenti) è aumentata di più (**82%**) rispetto alle organizzazioni più grandi con più di 1.000 dipendenti (**69%**), evidenziando l'impatto relativo sulle organizzazioni più piccole in cui le risorse sono più limitate, gli impatti potrebbero essere più pronunciati.
- **Anzianità:** coloro che ricoprono posizioni più elevate hanno molte più probabilità di segnalare di essere stati colpiti da incidenti di furto (**87%**) rispetto ai manager di medio livello (**67%**). È probabile che coloro che sono responsabili della gestione quotidiana di un'azienda siano poco informati sulle potenziali minacce che i dispositivi non sicuri devono affrontare. Aumentare la loro consapevolezza delle minacce e delle relative ripercussioni aiuterà a incoraggiare le aziende a integrare i cavi di sicurezza nelle loro esigenze culturali e ad allineare le prospettive a tutti i livelli per supportare una strategia di sicurezza completa.

Che ruolo hanno in questo contesto i modelli di lavoro?

Nell'introdurre questa ricerca abbiamo notato il radicale cambiamento nei metodi di lavoro degli ultimi anni, con l'adozione di modelli di lavoro più flessibili, lontani da un posto di lavoro fisso, accelerato dalla pandemia di COVID-19.

Mentre oltre tre quarti (**76%**) di tutti gli intervistati segnalano che la propria organizzazione è stata colpita dal furto di dispositivi negli ultimi 2 anni, questo diventa più evidente laddove i modelli di lavoro sono più flessibili, salendo a oltre 9 su 10 (**94%**) dove i dipendenti lavorano completamente da remoto.

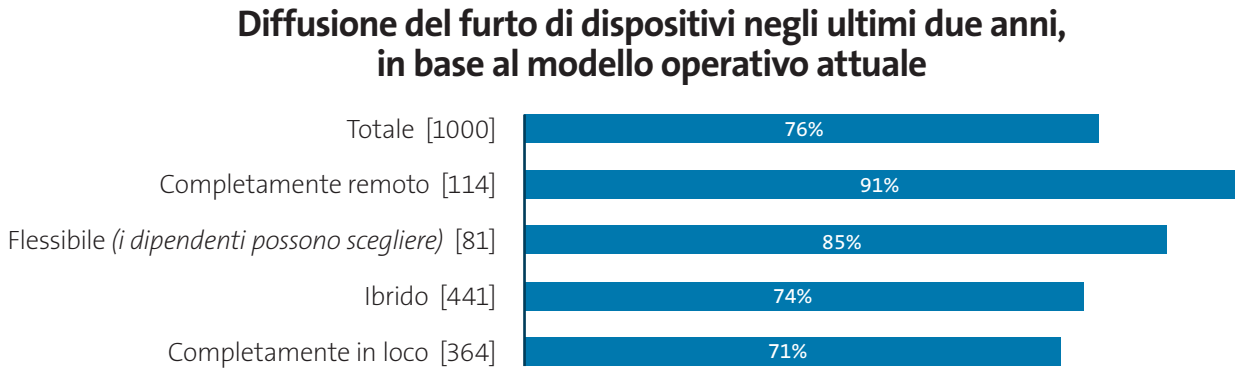


Fig. 2: *Percentuale di intervistati la cui organizzazione è stata colpita da incidenti di furto di dispositivi negli ultimi due anni [Domanda rivolta a tutti gli intervistati, con dati suddivisi in base al modello di lavoro attuale, numeri di base nel grafico]*

2 Report sui costi delle violazioni dei dati 2024, IBM, luglio 2024, https://www.ibm.com/reports/data-breach

Sebbene sia importante per qualsiasi organizzazione prestare attenzione alla sicurezza dei dispositivi fisici e alle conseguenze del furto di tali dispositivi, i modelli di lavoro flessibili e da remoto amplificano notevolmente il rischio di furto di dispositivi, rendendo più che mai fondamentali misure di sicurezza efficaci.

È importante notare che il livello di furto di dispositivi è generalmente elevato, anche quando i dipendenti sono completamente in sede: le organizzazioni non hanno spazio per essere compiacenti, indipendentemente da dove lavorino i loro dipendenti. La minaccia del furto di dispositivi non è una novità e non è nemmeno appena apparsa come parte di questo mondo post-pandemia. La nostra ricerca del 2016[3] ha esaminato i rischi per la sicurezza creati dal furto IT in azienda. I professionisti IT intervistati hanno classificato il rischio di furto di dispositivi in ufficio (**23%**) quasi alto quanto il furto in auto e nei trasporti (**25%**) e più alto del furto in aeroporti e hotel (**15%**) o ristoranti (**12%**). Ciò dimostra come il furto di dispositivi rimanga una minaccia persistente, anche in ambienti completamente in sede, sottolineando la necessità di vigilanza e misure di sicurezza fisica proattive.

Questa sfida è stata ulteriormente amplificata nel mondo post-COVID-19, con il **93%** delle organizzazioni che segnala un aumento dei rischi per la sicurezza dovuto al passaggio a modelli di lavoro flessibili e ibridi. Questi rischi si estendono oltre il furto di dispositivi fisici per includere maggiori vulnerabilità nella protezione dei dati, accessi non autorizzati e violazioni causate da reti domestiche non protette e ambienti di lavoro decentralizzati.

"**È il modo più semplice** per assicurarci che i nostri dispositivi siano letteralmente sotto chiave! **Ci fa sapere che tutto è sicuro e protetto.**"

Membro del consiglio di amministrazione/livello C; IT, tecnologia e telecomunicazioni; 100-249 dipendenti; modello di lavoro flessibile; USA

Il rischio per la sicurezza aumenta a causa degli ambienti di lavoro ibridi o remoti

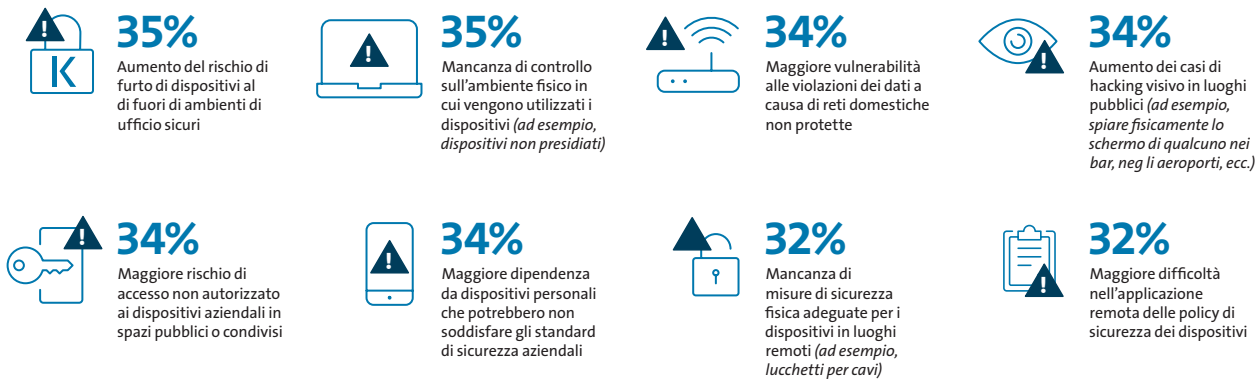


Fig. 3: *Secondo lei, quali rischi per la sicurezza sono aumentati a causa degli ambienti di lavoro ibridi o da remoto a seguito alla pandemia di COVID-19? [Domanda rivolta agli intervistati la cui organizzazione ha assistito a un passaggio al lavoro ibrido/da remoto a seguito della pandemia di COVID-19: 494]*

In quest'ottica, l'approccio migliore alla sicurezza consiste nel combinare solide misure fisiche con misure di sicurezza digitali avanzate, garantendo una protezione completa sia per i dispositivi sia per i dati in un mondo sempre più decentralizzato.

3 Sondaggio sulla sicurezza informatica e sui furti di laptop, Kensington, agosto 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=AfmBOooRTMdZ4gjmcNB3viXlJcIL4GY47XxO5I08AId-LhLEB5LjnH0Ts

Cavi di sicurezza che impediscono le perdite e riducono i costi

"La mancanza di un cavo di sicurezza sull'apparecchiatura ha portato a una violazione dei dati, **con conseguenti perdite significative per l'azienda.**"

Dirigenti di medio livello; IT, tecnologia e telecomunicazioni; 1.000 o più dipendenti; Modello di lavoro flessibile; USA

Finora abbiamo scoperto le conseguenze del furto di dispositivi e quanto questo possa essere pervasivo indipendentemente dall'ambiente di lavoro. Tuttavia, questa non è l'unica preoccupazione per i decisori IT senior da noi intervistati. C'è un'ampia gamma di aspetti di cui sono preoccupati quando si tratta di sicurezza, sia nelle aree fisiche che in quelle digitali.

Alcune di queste preoccupazioni presentano nuovi fattori di sicurezza fisica. Ad esempio, quasi un quarto (**23%**) è preoccupato per l'hacking visivo, in cui i dati sensibili sono alla mercé di chiunque se lo schermo di qualcuno è esposto in un luogo pubblico, come in una caffetteria o su un treno. Infatti, coloro che lavorano in modo flessibile (**48%**) hanno maggiori probabilità di coloro che lavorano in modalità completamente remota (**36%**) o ibrida (**33%**) di segnalare l'hacking visivo come una preoccupazione. Ciò evidenzia che l'hacking visivo non è solo associato al lavoro da casa, ma piuttosto alla concessione di libertà che sono più difficili da controllare. Le organizzazioni dovranno prendere in considerazione la protezione dei propri dati quando i dipendenti sono fuori casa, attraverso deterrenti aggiuntivi come gli schermi per la privacy.

Le aree più critiche per la sicurezza dei dispositivi

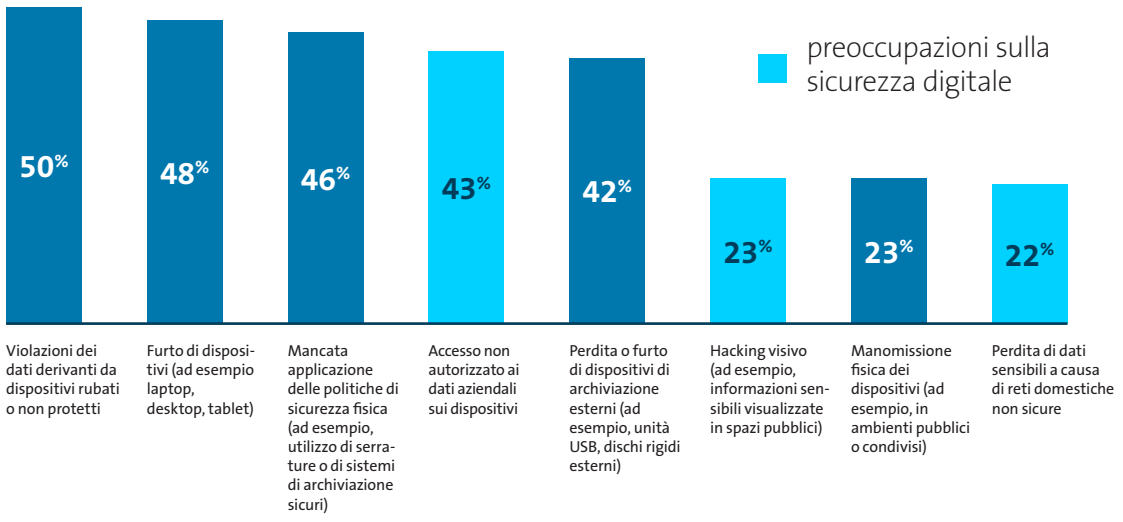


Fig. 4: *Quali aree della sicurezza dei dispositivi nella tua organizzazione ti preoccupano di più? [Domanda rivolta a tutti gli intervistati: 1000, che mostra la combinazione delle risposte classificate al primo, secondo e terzo posto]*

Le violazioni dei dati restano la principale preoccupazione, dato che una percentuale notevole (**46%**) ha subito un furto di dati come conseguenza diretta di un dispositivo non assicurato.

Ecco dove un cavo di sicurezza può aiutare. Le organizzazioni che utilizzano cavi di sicurezza hanno il **37%** di probabilità in meno di aver subito una violazione dei dati a causa di un dispositivo non protetto rispetto a quelle che non utilizzano affatto cavi di sicurezza.

Aziende che hanno subito violazioni o perdite di dati sensibili a causa di un dispositivo non assicurato

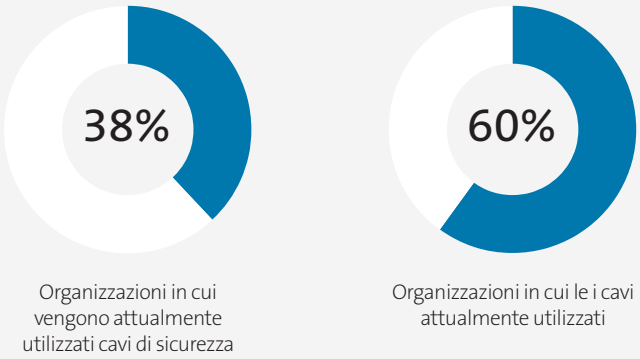


Fig. 5: *La tua organizzazione ha subito una violazione dei dati o una perdita di dati sensibili come conseguenza diretta di un dispositivo non protetto? [Domanda rivolta a tutti gli intervistati, suddivisi tra coloro che attualmente utilizzano cavi di sicurezza: 629; e coloro che attualmente non li usano: 371]*

Il risultato è chiaro: dimostrare una riduzione misurabile delle violazioni o perdite di dati rafforza il valore dei cavi di sicurezza come componente fondamentale della protezione completa dei dispositivi. Questa prova convincente evidenzia come i cavi di sicurezza riducano direttamente il rischio, posizionandoli come un investimento essenziale per le organizzazioni impegnate a salvaguardare i propri dati e ridurre al minimo la vulnerabilità.

I dati in primo piano:

- **Settore:** in base ai risultati del sondaggio, le organizzazioni nei settori dei servizi al consumatore (**65%**) e dell'assistenza sanitaria pubblica/privata (**57%**) hanno maggiori probabilità di aver subito una violazione dei dati come conseguenza di un dispositivo non protetto. Le prime sono state tra le più propense a essere colpite dal furto di dispositivi in generale. Nel caso delle seconde, si evidenzia forse una preoccupazione maggiore per la natura decentralizzata delle istituzioni sanitarie e per i membri del pubblico che sono a più stretto contatto con i dispositivi. Avere una tale ricchezza di dati sensibili espone questo settore a un rischio maggiore.
- **Dimensioni:** evidenziando ulteriormente le risorse limitate delle organizzazioni più piccole, è più probabile (**59%**) rispetto alle loro controparti più grandi (**40%**) che abbiano subito una violazione dei dati a causa di un dispositivo non protetto. Non solo hanno difficoltà con i deterrenti iniziali, ma anche con l'effetto valanga che ne consegue.
- **Anzianità:** i più giovani tra gli intervistati hanno meno probabilità di segnalare una violazione dei dati o una perdita di dati sensibili a causa di un dispositivo non protetto (**30%**) rispetto ai colleghi del consiglio di amministrazione/di livello C (**59%**). C'è un chiaro disallineamento all'interno delle aziende quando si tratta di una vera comprensione della sicurezza dei dispositivi fisici e delle conseguenze della sua mancata implementazione: una richiesta di istruzione più ampia e condivisione delle conoscenze.

"Un piccolo investimento iniziale in misure di sicurezza può **ridurre notevolmente la possibilità di costose sostituzioni dei dispositivi** o di tempi di inattività prolungati."

Alta dirigenza; istruzione – fornita dal governo/stato; 1.000 o più dipendenti; modello di lavoro ibrido; USA

Quindi, come dovrebbero agire le organizzazioni per superare questa situazione?

Le organizzazioni devono affrontare così tante preoccupazioni sulla sicurezza digitale e fisica, e gli impatti del furto di dispositivi sono sconvolgenti per le organizzazioni e i loro profitti. Dovrebbero cercare la soluzione più conveniente. E con il loro comprovato successo, questa potrebbe questa potrebbe essere rappresentata da un semplice cavi di sicurezza.

La maggioranza (**84%**) dei decisori IT senior da noi intervistati afferma che le cavi di sicurezza sono convenienti per mitigare potenziali violazioni dei dati, ovvero offrono un valore significativo nella prevenzione di furti e violazioni. A ciò si aggiunge il fatto che il **42%** ritiene che siano estremamente convenienti.

Questa è un'opinione universale condivisa da coloro che già utilizzano le serrature di sicurezza e anche da coloro che non le utilizzano, il che solleva la domanda: perché no? Le organizzazioni potrebbero considerare le serrature come un'aggiunta di sfide logistiche alla gestione dei dispositivi o forse una maggiore attenzione alla sicurezza digitale rispetto a quella fisica porta a una sottostima del valore delle serrature, ostacolandone quindi l'adozione. Tuttavia , se confrontato con le sconvolgenti conseguenze finanziarie del furto di dispositivi, il costo di una serratura di sicurezza, in genere pari a una media di soli $ 30-50 per dispositivo, rappresenta un investimento minimo per ridurre i rischi. Approfondendo ulteriormente la questione, vediamo una netta differenza di opinioni all'interno della gerarchia organizzativa.

Percezione del rapporto costo-efficacia dei cavi di sicurezza

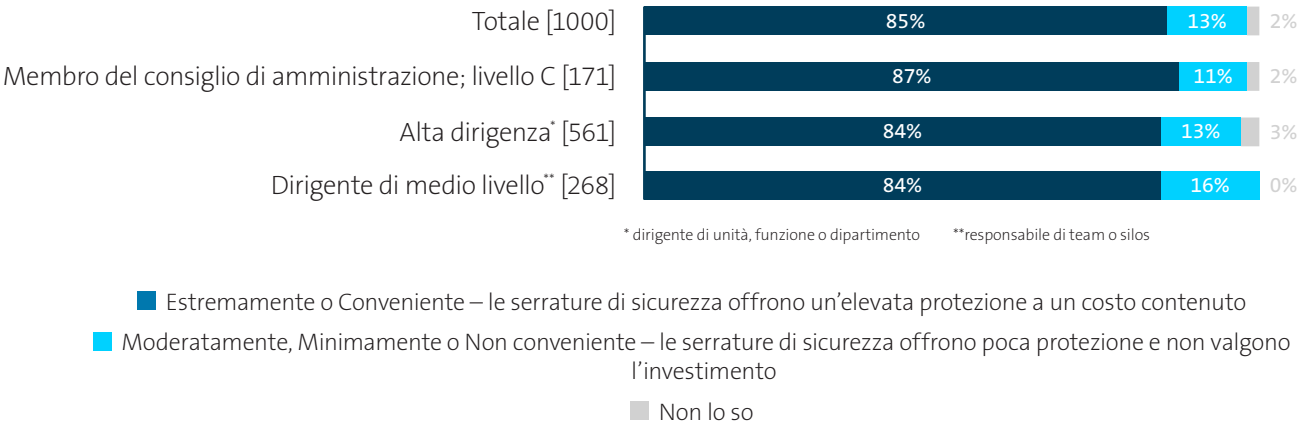


Fig. 6: *In termini di rapporto costo-efficacia, come vede il ruolo dei cavi di sicurezza nella mitigazione di potenziali violazioni o furti di dati? [Domanda rivolta a tutti gli intervistati, con dati suddivisi per anzianità, numeri di base nel grafico]*

Questi risultati sottolineano la necessità critica di affrontare le cause profonde del furto di dispositivi e i suoi impatti più ampi in un'organizzazione. Mentre i dirigenti senior sono più propensi a considerare i cavi di sicurezza come estremamente convenienti (**56%**), questa convinzione diminuisce ai livelli inferiori della gerarchia. In definitiva, i dirigenti senior saranno sempre più concentrati su implicazioni più ampie (ad esempio, sanzioni normative, reputazione), mentre i manager di livello inferiore sugli impatti quotidiani (ad esempio, perdita di produttività).

Questa disconnessione evidenzia l'importanza dell'allineamento organizzativo e della formazione sul valore dei cavi di sicurezza, non solo come strumento conveniente, ma come soluzione proattiva per prevenire perdite significative prima che si verifichino. Colmare queste lacune nella percezione garantirà un approccio unificato ed efficace per mitigare i rischi di furto di dispositivi e proteggere i dati sensibili.

"Una volta persa, causerà perdite significative. Dobbiamo **risolvere questo problema alla radice.**"

Dirigenti di medio livello ; Sanità - di proprietà privata; 1.000 o più dipendenti; Modello di lavoro ibrido; USA

i cavi di sicurezza servono a proteggere e rassicurare

Abbiamo continuato a esplorare come le serrature di sicurezza non solo siano efficaci nel ridurre i furti, ma offrano anche una soluzione conveniente per mitigare rischi più ampi. Le loro diverse applicazioni evidenziano la loro versatilità nell'affrontare le sfide di sicurezza in vari ambienti, un vantaggio che molte organizzazioni stanno già realizzando.

Molti stanno già utilizzando cavi di sicurezza per proteggere i dispositivi elettronici nella loro organizzazione. I dispositivi più comunemente protetti includono laptop (**44%**), desktop (**43%**) e server (**42%**), a dimostrazione della priorità data alla salvaguardia di hardware critici che spesso contengono dati sensibili. Questa adozione diffusa evidenzia il riconoscimento di lucchetti e cavi di sicurezza come uno strumento essenziale per la protezione contro furti e accessi non autorizzati.

Percepita convenienza economica dei lucchetti di sicurezza

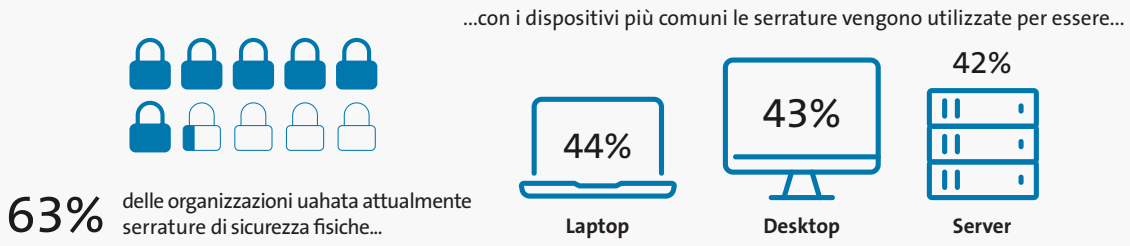


Fig. 7: *Per quali dei seguenti dispositivi elettronici vengono utilizzati cavi di sicurezza fisiche nella vostra organizzazione? [Domanda rivolta a tutti gli intervistati: 1000]*

Tuttavia, il fatto che circa 4 intervistati su 10 affermino che le loro organizzazioni non utilizzino cavi di sicurezza solleva preoccupazioni circa le vulnerabilità dei dispositivi, in particolare per i dispositivi utilizzati frequentemente in ambienti di lavoro mobili o ibridi.

Per le organizzazioni, questi dati sottolineano la necessità di valutare in modo esaustivo le loro attuali misure di sicurezza. Sebbene i lucchetti siano una soluzione affidabile e ampiamente utilizzata, espanderne l'uso su una gamma più ampia di dispositivi e abbinarli a protezioni digitali complementari può aiutare a colmare le lacune di sicurezza esistenti e a mitigare i rischi in modo più efficace.

Quasi tutti gli intervistati (**97%**) riconoscono il ruolo critico che i cavi di sicurezza svolgono nell'aiutare a prevenire i furti e l'accesso non autorizzato che spesso ne consegue. Questo riconoscimento diffuso riflette la fiducia che le organizzazioni ripongono nella sicurezza fisica come misura fondamentale per salvaguardare dispositivi e dati sensibili. I cavi di sicurezza agiscono come una difesa in prima linea, riducendo le opportunità di furto e mitigando i rischi associati all'hardware compromesso.

"LAvere cavi di sicurezza negli uffici aperti, negli spazi di coworking o in altre aree in cui potrebbero essere presenti più persone **riduce il rischio di furto.**"

Membro del consiglio di amministrazione/livello C; Istruzione – di proprietà privata; 100-249 dipendenti; USA

Convinzione che le misure di sicurezza fisica contribuiscano a prevenire il furto del dispositivo

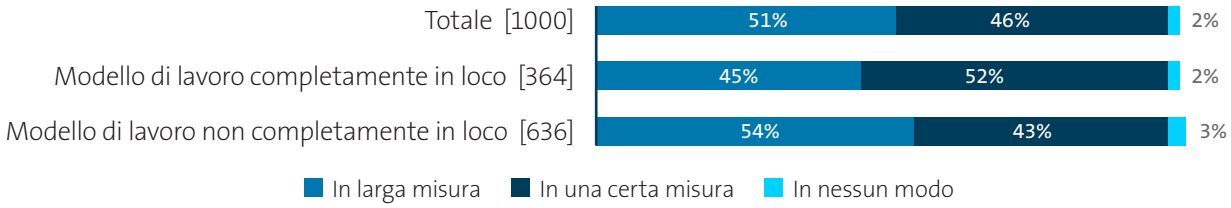


Fig. 8: *In che misura ritieni che le misure di sicurezza fisica, come i cavi di sicurezza, contribuiscano a prevenire il furto di dispositivi che potrebbe portare ad accessi non autorizzati ai dati aziendali? [Domanda rivolta a tutti gli intervistati, con dati suddivisi per tipo di modello di lavoro, numeri di base nel grafico]*

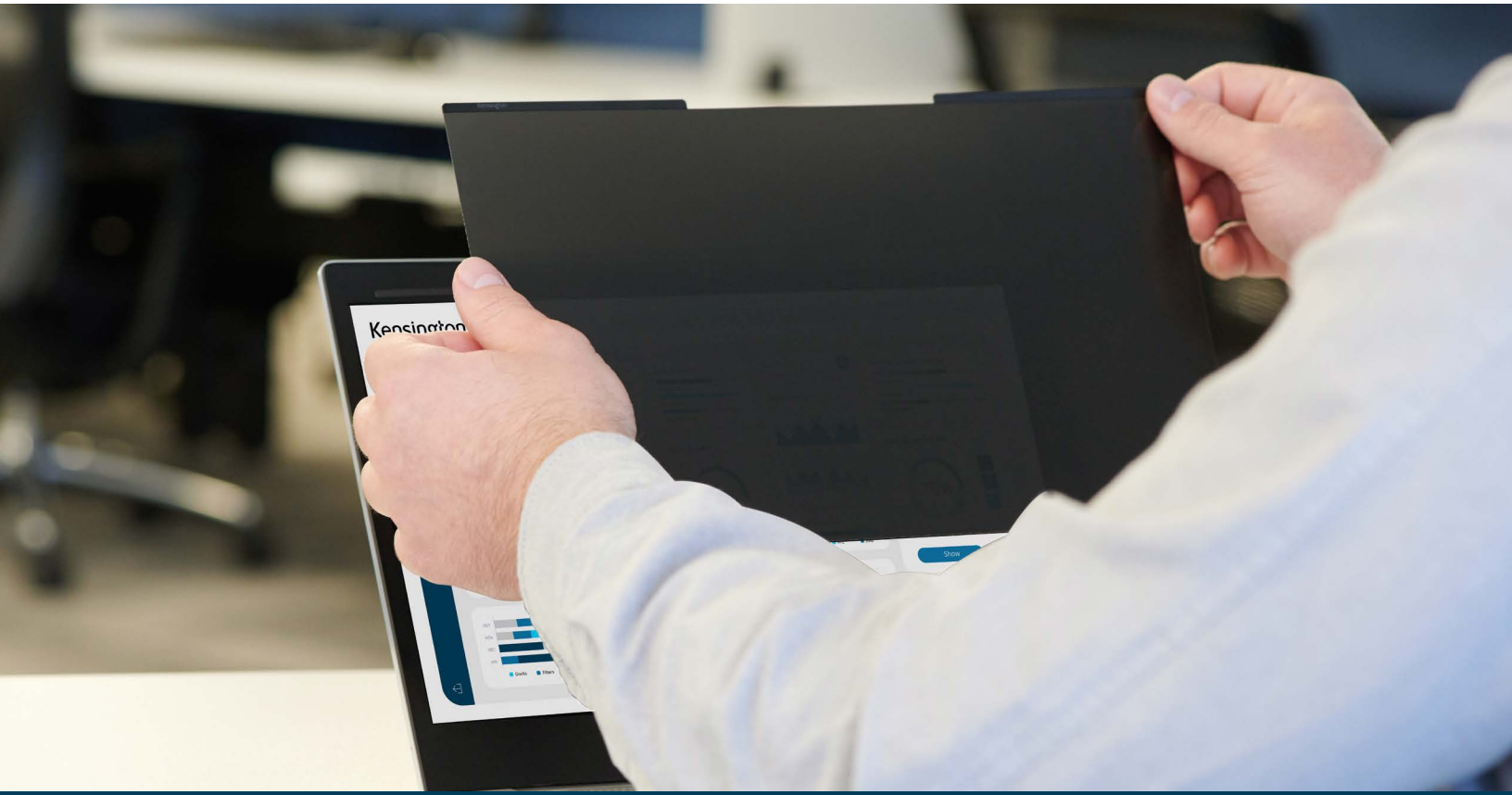
Questo riconoscimento diventa più evidente laddove le organizzazioni hanno adottato modelli di lavoro flessibili e ibridi. In questi ambienti decentralizzati, i dispositivi vengono sempre più utilizzati in luoghi non protetti, come uffici domestici o spazi pubblici, amplificando il rischio di furto o esposizione accidentale. Le violazioni dei dati causate da dispositivi non protetti sono significativamente più comuni nelle configurazioni di lavoro più flessibili (**50%** combinato contro il **39%** per un modello di lavoro completamente in loco).

I cavi di sicurezza sono progettati per adattarsi a diversi ambienti, offrendo una protezione affidabile per i dispositivi, indipendentemente dal fatto che vengano utilizzati in uffici, spazi di lavoro remoti o luoghi pubblici, garantendo alle organizzazioni tranquillità in tutti i modelli di lavoro.

Le conseguenze finanziarie del furto di dispositivi possono essere sconvolgenti, con il costo della sostituzione dell'hardware rubato spesso eclissato dagli impatti più ampi sulla produttività, sulla conformità normativa e sulle violazioni dei dati. Per le organizzazioni, ogni dispositivo rubato o non protetto aumenta il rischio, non solo per le operazioni ma anche per i profitti. I cavi di sicurezza offrono una soluzione comprovata ed economica, già utilizzata da molti per ridurre la probabilità di furto e le conseguenti ricadute finanziarie e reputazionali. Affrontando questi rischi alla radice, le organizzazioni possono assumere una posizione proattiva nella salvaguardia dei propri beni e dati sensibili.

Sebbene le misure di sicurezza fisica come i lucchetti siano efficaci, devono essere parte di una strategia più ampia per affrontare i rischi per la sicurezza in evoluzione associati al lavoro ibrido. Combinare i lucchetti con protezioni digitali complementari, come la crittografia e l'autenticazione a due fattori, garantisce una copertura completa contro le minacce sia fisiche che digitali. I programmi di formazione per istruire i dipendenti sull'importanza di questo approccio integrato possono rafforzare ulteriormente la sicurezza organizzativa. Per le organizzazioni che affrontano le complessità dei moderni modelli di lavoro, l'integrazione di misure di sicurezza fisica e digitale è essenziale per ridurre al minimo i rischi, proteggere la propria forza lavoro e mantenere la resilienza operativa.

Prevenire il furto di dispositivi e le conseguenti violazioni dei dati è molto più conveniente che gestire le conseguenze. Adottare misure preventive come l'uso di blocchi per laptop oggi può proteggere la tua organizzazione da impatti finanziari e operativi significativi in futuro. Per garantire che queste misure siano efficaci, è fondamentale l'allineamento tra dirigenti senior, dirigenti e team. Un impegno condiviso per le priorità di sicurezza assicura che tutti comprendano il proprio ruolo nella salvaguardia di asset preziosi e nella riduzione dei rischi.



Metodologia

Kensington ha incaricato Vanson Bourne, specialista indipendente in ricerche di mercato, di intraprendere la ricerca su cui si basa questo rapporto. Un totale di 1.000 dirigenti IT senior coinvolti o che hanno influenza sulla sicurezza hardware IT fisica nella loro organizzazione sono stati intervistati nell'autunno 2024, con rappresentanza negli Stati Uniti, nel Regno Unito, in Francia e in Germania.

Gli intervistati dovevano provenire da organizzazioni con almeno 100 dipendenti e da una vasta gamma di settori pubblico e privato.

Le interviste sono state condotte online e sono state intraprese utilizzando un rigoroso processo di selezione multilivello per garantire che solo i candidati idonei avessero l'opportunità di partecipare. Salvo diversa indicazione, i risultati discussi si basano sul campione totale.

Informazioni su Kensington

Kensington è un fornitore leader di accessori per dispositivi desktop e mobili, a cui si affidano professionisti IT, educatori, aziende e home office in tutto il mondo da oltre 40 anni. Kensington si impegna ad anticipare le esigenze e le sfide del posto di lavoro in continua evoluzione e a creare soluzioni pluripremiate di livello professionale per le organizzazioni impegnate a fornire ai professionisti di punta gli strumenti di cui hanno bisogno per prosperare. L'azienda è orgogliosa di essere la scelta dei professionisti e dei suoi valori fondamentali che circondano design, qualità e supporto.

Negli ambienti d'ufficio e mobili, l'ampio portafoglio di prodotti pluripremiati di Kensington garantisc sicurezza affidabile, innovazioni per la produttività desktop , videoconferenze professionali e benessere ergonomico.

Con sede a Burlingame, California, Kensington è l'inventore e leader mondiale nei lucchetti di sicurezza per laptop. Kensington è una divisione di ACCO Brands, la casa dei grandi marchi costruiti da grandi persone, che progetta, produce e commercializza prodotti per consumatori e utenti finali che aiutano le persone a lavorare, imparare e divertirsi. Oltre a Kensington ® , i marchi ampiamente riconosciuti di ACCO Brands includono AT-A-GLANCE ® , Five Star ® , Leitz ® , Mead ® , PowerA ® , Swingline ® , Tilibra e molti altri. Ulteriori informazioni su ACCO Brands Corporation (NYSE:ACCO) sono disponibili su www.accobrands.com.

Kensington ® è un marchio registrato di ACCO Brands. Tutti gli altri marchi registrati e non registrati sono di proprietà dei rispettivi proprietari.

FOR MORE INFORMATION CONTACT: sales@kensington.com

Kensington
The Professionals' Choice™