Kensington®

Zabezpiecz swoje urządzenie, chroń swoje dane.

W jaki sposób bezpieczeństwo fizyczne może pomóc zapobiec kolejnym naruszeniom danych

Wstęp

Krajobraz bezpieczeństwa ewoluował dramatycznie w ostatnich latach, napędzany transformacyjnymi zmianami w sposobie i miejscu naszej pracy. Ostatecznym motorem napędowym była pandemia COVID-19; przyspieszyła ona przyjęcie hybrydowych i elastycznych modeli pracy oraz fundamentalnie zmieniła priorytety bezpieczeństwa urządzeń.

Firma Kensington sponsorowała badanie przeprowadzone przez niezależnego specjalistę ds. badań rynkowych Vanson Bourne, obejmujące 1000 starszych decydentów IT odpowiedzialnych za bezpieczeństwo sprzętu fizycznego w swoich organizacjach w Stanach Zjednoczonych i regionie EMEA. Prawie wszyscy ankietowani (**92%**) zaostrzyli swoje zasady bezpieczeństwa w odpowiedzi na pandemię, rozpoznając zwiększone ryzyko związane z zdecentralizowanymi środowiskami pracy. Patrząc w przyszłość, w kierunku 2025 r., oczekuje się wzrostu poziomu bardziej elastycznych modeli pracy, co podkreśla, że nadszedł czas na przemyślenie strategii bezpieczeństwa urządzeń.

Naruszenia danych nie są tylko problemem cyfrowym — każde skradzione lub niezabezpieczone urządzenie stanowi potencjalną bramę do nieautoryzowanego dostępu do poufnych informacji, co stwarza poważne ryzyko dla organizacji. Ponieważ ciężar finansowy naruszenia danych wynosi obecnie średnio miliony dolarów, stawka nigdy nie była wyższa. W miarę jak organizacje nadal dostosowują swoje modele pracy, pilna potrzeba zajęcia się bezpieczeństwem urządzeń wzrosła masowo. Bardziej rygorystyczne wymagania dotyczące ochrony danych i wzrost liczby naruszeń danych jeszcze bardziej zwiększyły znaczenie ochrony zarówno urządzeń fizycznych, jak i przechowywanych na nich poufnych informacji. Niniejszy raport podkreśla kluczową rolę, jaką odgrywają blokady bezpieczeństwa w łagodzeniu tych ryzyk, i zwraca uwagę na to, dlaczego podjęcie działań teraz jest niezbędne, aby wyprzedzić pojawiające się wyzwania.

Dzięki tym odkryciom zbadamy namacalne skutki kradzieży urządzeń, pokażemy, jak proste, ale skuteczne rozwiązania, takie jak blokady bezpieczeństwa, mogą pomóc w łagodzeniu ryzyka i podkreślimy, jak bezpieczeństwo fizyczne zapewnia spokój ducha w świecie, w którym modele pracy nieustannie ewoluują. Od zrozumienia oszałamiających konsekwencji kradzieży urządzeń po zademonstrowanie opłacalności i pewności blokad, raport ten dostarcza praktycznych spostrzeżeń dla organizacji poruszających się po dzisiejszym złożonym krajobrazie bezpieczeństwa.

Najważniejsze ustalenia:

76% respondentów twierdzi, że ich organizacja została dotknięta incydentami kradzieży w ciągu ostatnich 2 lat, przy czym incydenty te są częstsze w organizacjach o bardziej elastycznych modelach pracy. Na przykład nasze badania wykazały, że (**85%**) organizacji o elastycznych modelach pracy doświadczyło incydentu kradzieży w ciągu ostatnich 2 lat, w porównaniu do **71%** organizacji, których pracownicy są w pełni na miejscu.

Skutki kradzieży urządzeń wykraczają poza utratę sprzętu i obejmują:

- konieczność wzmocnienia istniejących środków bezpieczeństwa (**33%**)
- konsekwencje prawne lub regulacyjne wynikające z naruszenia danych na skradzionych urządzeniach (**33%**)
- zakłócenia w produktywności pracowników spowodowane zgubieniem lub kradzieżą urządzeń (**32%**)

Organizacje stosujące blokady bezpieczeństwa miały o **37%** mniejsze prawdopodobieństwo wystąpienia naruszenia bezpieczeństwa danych spowodowanego przez niezabezpieczone urządzenie (**38%** w porównaniu z **60%** wśród tych, które nie stosują blokad bezpieczeństwa).

Organizacje, które obecnie używają blokad, częściej stosują podwójne podejście do bezpieczeństwa – trzy czwarte (**76%**) korzysta z cyfrowych środków, takich jak odcisk palca lub klucze bezpieczeństwa, w celu uwierzytelniania dwuskładnikowego, podczas gdy odsetek ten wśród tych, które w ogóle nie stosują blokad, wynosi **62%**.

84% uważa, że blokady bezpieczeństwa są opłacalnym rozwiązaniem w ograniczaniu ryzyka naruszeń danych i oferują znaczną wartość przy stosunkowo niskiej inwestycji.

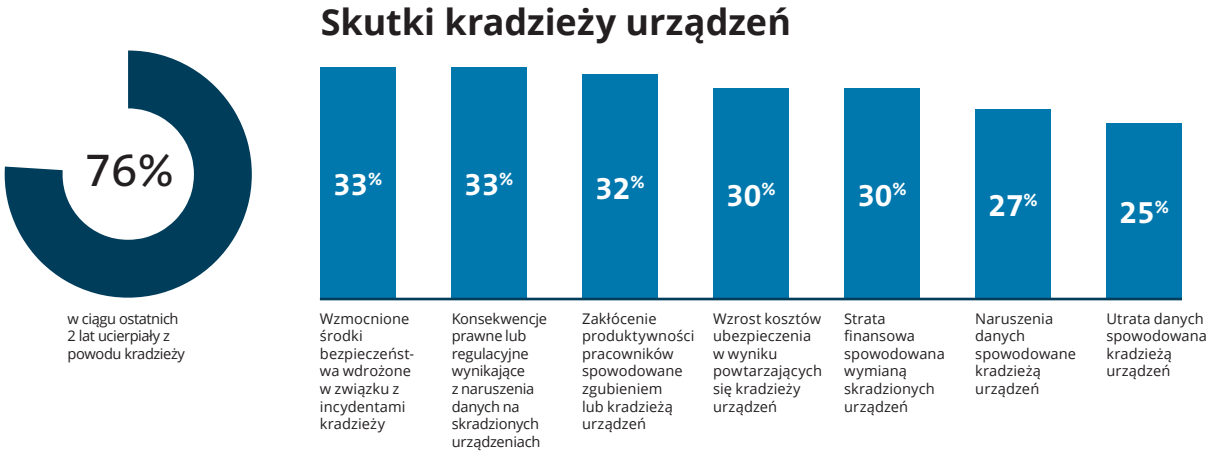
- **42%** ankietowanych uważa, że blokady urządzeń są niezwykle opłacalne, zapewniają wysoką ochronę przy niskich kosztach, przy czym najwyżsi rangą kierownicy częściej dostrzegają ich wartość (**56%**) niż kadra zarządzająca średniego szczebla (**36%**).

Prawie wszyscy ankietowani (**97%**) uważają, że blokady urządzeń mogą zapobiegać kradzieży, zmniejszając prawdopodobieństwo nieautoryzowanego dostępu do poufnych danych firmy.

Skradzione urządzenia, szokujące konsekwencje

Nie ma dnia, w którym nie słyszy się o jakimś incydencie bezpieczeństwa – czy to o ataku na dużą skalę na globalny konglomerat, czy o bardziej ukierunkowanym wykorzystaniu krytycznej infrastruktury lub usługi. I chociaż te przykłady sugerują, że cyberincydenty są często najszerzej omawiane – lub przynajmniej zakłada się, że są – ważne jest, aby zdać sobie sprawę, że zagrożenia bezpieczeństwa fizycznego mogą być równie krytyczne.

Niewiele mówi się o incydentach związanych z bezpieczeństwem fizycznym, w których osoby nieupoważnione uzyskują dostęp do zabezpieczonych obszarów lub narażają zasoby, co ma równie poważne konsekwencje jak przeciętny atak ransomware. Według naszych badań ponad trzy czwarte (**76%**) ankietowanych twierdzi, że ich organizacja została dotknięta incydentami kradzieży urządzeń w ciągu ostatnich dwóch lat.



Ryc. 1: *Jak incydenty kradzieży urządzeń wpłynęły na Twoją organizację w ciągu ostatnich dwóch lat? [Zapytano wszystkich respondentów: 1000]*

Nie chodzi tylko o oczywisty koszt wymiany urządzenia, z którym muszą się zmierzyć organizacje (**30%**). Do najczęstszych skutków należą wzrost środków bezpieczeństwa wdrożonych w wyniku (**33%**) lub konsekwencje prawne lub regulacyjne z powodu naruszeń danych (**33%**), przy czym te ostatnie są często wyraźnie opisane. Na przykład GDPR[1] grzywny mogą sięgać nawet 20 milionów euro lub 4% globalnego obrotu organizacji, a nawet mniej poważne naruszenia kosztują do 10 milionów euro, stwarzając znaczne ryzyko finansowe w przypadku braku zgodności. Do skutków finansowych dochodzą również koszty zakłóceń w produktywności pracowników z powodu zgubionych lub skradzionych urządzeń (**32%**). Po każdym z tych skutków istnieje wyraźny wpływ finansowy lub czasowy na wynik finansowy organizacji. Tak więc nie tylko incydenty związane z bezpieczeństwem cyfrowym wymagają uwagi — zagrożenia fizyczne również stwarzają znaczne ryzyko. Pogłębiając zrozumienie tych luk, organizacje mogą podjąć proste, opłacalne kroki w celu zabezpieczenia swoich urządzeń. Ponieważ środki bezpieczeństwa fizycznego są zarówno niedrogie, jak i łatwe do wdrożenia (jak omówimy później), stanowią one praktyczny pierwszy krok w kierunku wzmocnienia ogólnego bezpieczeństwa.

"Oprócz środków cyberbezpieczeństwa **równie ważne jest bezpieczeństwo fizyczne.** Bezpieczne kable są częścią silniejszej strategii cyberbezpieczeństwa."

Kadra zarządzająca wyższego szczebla; Produkcja i wytwarzanie; Ponad 1000 pracowników; Całkowicie stacjonarny model pracy; Francja

1 Kary/grzywny za naruszenie RODO, Intersoft Consulting, https://gdpr-info.eu/issues/fines-penalties/

W dzisiejszych czasach nie chodzi o to, czy dojdzie do naruszenia danych, ale kiedy. W rzeczywistości każda kradzież urządzenia to naruszenie danych, które czeka, aby się wydarzyć, a konsekwencje finansowe dla organizacji są oszałamiające. Według najnowszego raportu IBM na temat kosztów naruszenia danych[2], średni globalny koszt naruszenia danych w 2024 r. wynosi 4,88 mln USD; wzrost o **10%** w ciągu roku w porównaniu ze średnią 4,45 mln USD w 2023 r. Ta liczba różni się w zależności od branży i wielkości organizacji, więc niektóre organizacje mogą ponieść jeszcze wyższe koszty.

Dane w centrum uwagi:

- **Sektor:** organizacje z branży usług konsumenckich (**95%**), energetyki, ropy naftowej/gazu i usług komunalnych (**90%**) oraz budownictwa i nieruchomości (**89%**) są najbardziej narażone na kradzież urządzeń. Większa mobilność pracowników i urządzeń w tych firmach naraża je na większe ryzyko kradzieży
- **Wielkość:** prawdopodobieństwo kradzieży urządzeń w mniejszych organizacjach (100–249 pracowników) wzrosło bardziej (**82%**) niż w większych organizacjach zatrudniających ponad 1000 pracowników (**69%**), co podkreśla względny wpływ na mniejsze organizacje, w których zasoby są bardziej ograniczone, a skutki mogą być bardziej widoczne
- **Stanowisko:** Osoby na wyższych stanowiskach znacznie częściej zgłaszają, że miały do czynienia z incydentami kradzieży (**87%**) niż kierownicy średniego szczebla (**67%**). Jest prawdopodobne, że osoby odpowiedzialne za codzienne prowadzenie firmy są słabo poinformowane o potencjalnych zagrożeniach, którym stawiają czoła niezabezpieczone urządzenia. Zwiększenie ich świadomości zagrożeń i związanych z nimi reperkusji pomoże zachęcić firmy do wbudowania blokad bezpieczeństwa w ich potrzeby kulturowe i dostosowania perspektyw na wszystkich szczeblach w celu wsparcia kompleksowej strategii bezpieczeństwa.

Jaką rolę odgrywają tu modele pracy?

Przedstawiając niniejsze badanie, zwróciliśmy uwagę na ogromną zmianę, jaka zaszła w ostatnich latach w sposobach pracy, a pandemia COVID-19 przyspieszyła przyjmowanie bardziej elastycznych modeli pracy, wykraczających poza stałe miejsce pracy.

Ponad trzy czwarte (**76%**) wszystkich ankietowanych zgłosiło, że w ciągu ostatnich 2 lat ich organizacja ucierpiała z powodu kradzieży urządzeń. Staje się to bardziej widoczne tam, gdzie modele pracy są bardziej elastyczne – odsetek ten wzrasta do ponad 9 na 10 (**94%**) pracowników pracujących całkowicie zdalnie.

Powszechność kradzieży urządzeń w ciągu ostatnich dwóch lat według obecnego modelu działania

Rys. 2: *Odsetek respondentów, których organizacja została dotknięta incydentami kradzieży urządzeń w ciągu ostatnich dwóch lat [Zadano to wszystkim respondentom, pokazano dane podzielone według aktualnie działającego modelu, liczby bazowe na wykresie]*

2 Raport o kosztach naruszeń danych 2024, IBM, lipiec 2024 r., https://www.ibm.com/reports/data-breach

Chociaż dla każdej organizacji ważne jest dbanie o bezpieczeństwo urządzeń fizycznych i obawianie się skutków ich kradzieży, elastyczne i zdalne modele pracy znacznie zwiększają ryzyko kradzieży urządzeń, przez co solidne środki bezpieczeństwa są ważniejsze niż kiedykolwiek wcześniej.

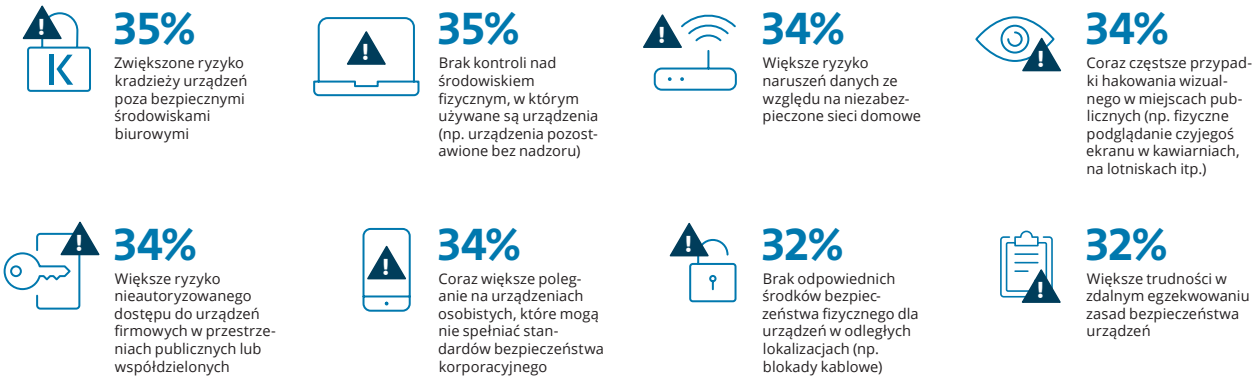
Ważne jest, aby zauważyć, że poziom kradzieży urządzeń jest ogólnie wysoki, nawet gdy pracownicy są w pełni na miejscu – organizacje nie mogą być zadowolone, niezależnie od tego, gdzie pracują ich pracownicy. Zagrożenie kradzieżą urządzeń nie jest nowe i nie pojawiło się dopiero jako część tego postpandemicznego świata. Nasze badania z 2016[3] zbadały zagrożenia bezpieczeństwa spowodowane kradzieżą IT w przedsiębiorstwie. Ankietowani specjaliści IT ocenili ryzyko kradzieży urządzeń w biurze (**23%**) jako prawie tak wysokie, jak kradzieży w samochodach i transporcie (**25%**) oraz wyższe niż kradzieży na lotniskach i w hotelach (**15%**) lub restauracjach (**12%**). Pokazuje to, że kradzież urządzeń pozostaje uporczywym zagrożeniem, nawet w środowiskach w pełni na miejscu, podkreślając potrzebę czujności i proaktywnych środków bezpieczeństwa fizycznego niezależnie od miejsca pracy.

To wyzwanie zostało jeszcze bardziej wzmocnione w świecie po COVID-19, gdzie **93%** organizacji zgłosiło wzrost ryzyka bezpieczeństwa z powodu przejścia na elastyczne i hybrydowe modele pracy. Ryzyko to wykracza poza kradzież urządzeń fizycznych, obejmując zwiększone podatności na ochronę danych, nieautoryzowany dostęp i naruszenia spowodowane przez niezabezpieczone sieci domowe i zdecentralizowane środowiska pracy.

"**To najłatwiejszy sposób,** aby upewnić się, że nasze urządzenia są dosłownie pod kluczem! Dzięki temu **wiemy, że wszystko jest bezpieczne**"

Członek zarządu/C-level; IT, technologia i telekomunikacja; 100-249 pracowników; elastyczny model pracy; USA

Ryzyko związane z bezpieczeństwem wzrasta w wyniku hybrydowych lub zdalnych środowisk pracy



Rys. 3: *Twoim zdaniem, jakie zagrożenia bezpieczeństwa wzrosły w wyniku hybrydowych lub zdalnych środowisk pracy po pandemii COVID-19? [Zapytano respondentów, których organizacje odnotowały przejście na pracę hybrydową/zdalną po pandemii COVID-19: 494]*

Mając to na uwadze, najlepszym podejściem do kwestii bezpieczeństwa jest połączenie solidnych środków fizycznych z zaawansowanymi zabezpieczeniami cyfrowymi, co gwarantuje kompleksową ochronę zarówno urządzeń, jak i danych w coraz bardziej zdecentralizowanym świecie.

3 Badanie dotyczące bezpieczeństwa IT i kradzieży laptopów, Kensington, sierpień 2016 r., 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=AfmBOooRTMdZ4gjmcNB3viXIJclL4GY47XxO5I08AldLhLEB5LjnH0Ts

Blokady, które zapobiegają stratom i oszczędzają koszty

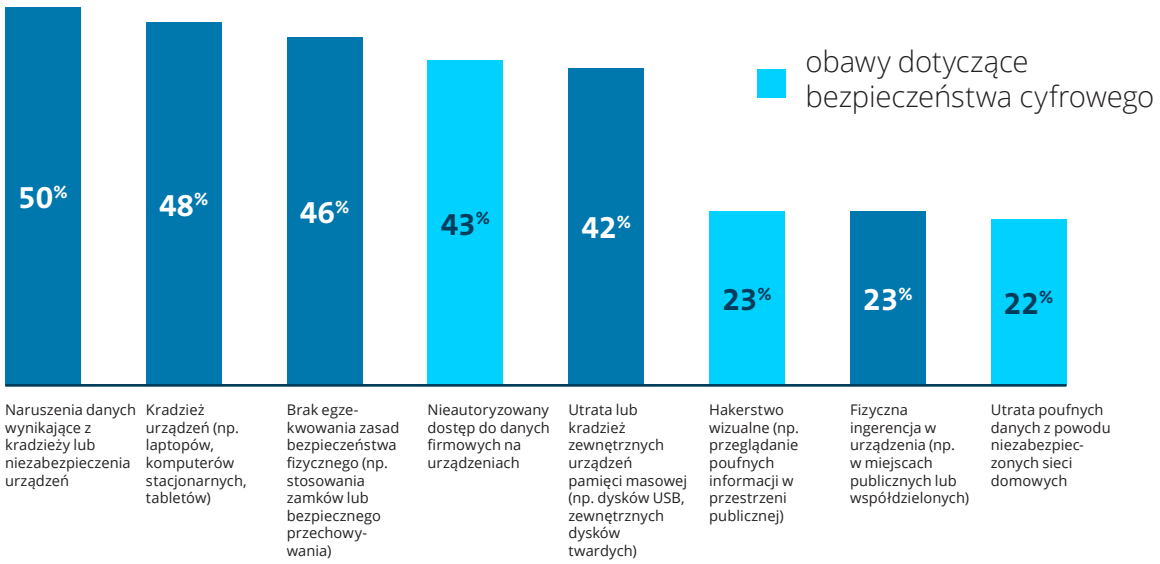
"Brak blokady bezpieczeństwa w sprzęcie doprowadził do naruszenia bezpieczeństwa danych, **co spowodowało znaczne straty dla firmy.**"

Kadra zarządzająca średniego szczebla; IT, technologia i telekomunikacja; 1000 lub więcej pracowników; Elastyczny model pracy; USA

Do tej pory odkryliśmy konsekwencje kradzieży urządzeń i jak powszechne może być to zjawisko niezależnie od środowiska pracy. Jednak nie jest to jedyne zmartwienie naszych ankietowanych decydentów IT. Istnieje szeroki zakres aspektów, o które się martwią, jeśli chodzi o bezpieczeństwo, zarówno w obszarach fizycznych, jak i cyfrowych.

Niektóre z tych obaw przedstawiają nowe czynniki dotyczące bezpieczeństwa fizycznego. Na przykład prawie jedna czwarta (**23%**) jest zaniepokojona hakowaniem wizualnym, gdzie poufne dane są na łasce kogokolwiek, jeśli czyjś ekran jest widoczny w miejscu publicznym – w kawiarni lub w transporcie publicznym. W rzeczywistości osoby pracujące elastycznie (**48%**) częściej niż osoby pracujące w pełni zdalnie (**36%**) lub w środowisku hybrydowym (**33%**) zgłaszają hakowanie wizualne jako problem. Podkreśla to, że hakowanie wizualne nie jest związane tylko z pracą zdalną, ale raczej z przyznawaniem nadmiernych swobód, które są trudniejsze do kontrolowania. Organizacje będą musiały wziąć pod uwagę ochronę swoich danych, gdy pracownicy są poza domem, poprzez dodatkowe środki ochronne, takie jak filtry prywatyzujące.

Najbardziej niepokojące obszary bezpieczeństwa urządzeń

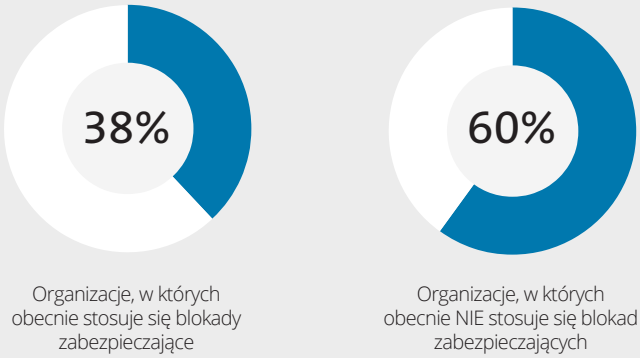


Rys. 4: *Które obszary bezpieczeństwa urządzeń w Twojej organizacji najbardziej Cię niepokoją? [Zadano wszystkim respondentom: 1000, pokazując kombinację odpowiedzi na pierwszym, drugim i trzecim miejscu]*

Największym zmartwieniem są jednak naruszenia bezpieczeństwa danych, co jest uzasadnione, ponieważ znaczny odsetek (**46%**) doświadczył naruszenia bezpieczeństwa danych jako bezpośredniej konsekwencji niezabezpieczonego urządzenia .

Tutaj blokada bezpieczeństwa może pomóc. Organizacje korzystające z blokad bezpieczeństwa są o **37%** mniej narażone na naruszenie danych z powodu niezabezpieczonego urządzenia w porównaniu z tymi, które w ogóle nie korzystają z blokad bezpieczeństwa.

Organizacje, które doświadczyły naruszenia bezpieczeństwa danych lub utraty poufnych danych z powodu niezabezpieczonego urządzenia



Rys. 5: *Czy Twoja organizacja doświadczyła naruszenia danych lub utraty poufnych danych jako bezpośredniej konsekwencji pozostawienia urządzenia bez zabezpieczeń? [Zapytano wszystkich respondentów, podzielonych na tych, którzy obecnie używają blokad bezpieczeństwa: 629; i tych, którzy obecnie nie używają blokad bezpieczeństwa: 371]*

Wynik jest jasny: wykazanie mierzalnej redukcji naruszeń danych lub utraty danych wzmacnia wartość blokad bezpieczeństwa jako krytycznego elementu kompleksowej ochrony urządzeń. Ten przekonujący dowód podkreśla, w jaki sposób blokady bezpieczeństwa bezpośrednio łagodzą ryzyko, pozycjonując je jako niezbędną inwestycję dla organizacji zobowiązanych do ochrony swoich danych i minimalizowania luk w zabezpieczeniach.

Dane w centrum uwagi:

- **Sektor:** na podstawie wyników ankiety organizacje z branży usług konsumenckich (**65%**) i publicznej/prywatnej opieki zdrowotnej (**57%**) częściej doświadczały naruszenia danych w wyniku niezabezpieczonego urządzenia. Pierwszy z nich był jednym z najbardziej narażonych na kradzież urządzeń. W przypadku drugiego może to podkreślać większe obawy dotyczące zdecentralizowanej natury placówek opieki zdrowotnej i bliższego kontaktu członków społeczeństwa z urządzeniami. Posiadanie tak dużej ilości poufnych danych naraża ten sektor na większe ryzyko
- **Rozmiar:** dodatkowo podkreślając ograniczone zasoby mniejszych organizacji, są one bardziej narażone (**59%**) niż ich większe odpowiedniki (**40%**) na naruszenie danych z powodu niezabezpieczonego urządzenia. Nie tylko zmagają się z początkowymi środkami odstraszającymi, ale także z efektem kuli śnieżnej, który następuje
- **Stanowisko:** młodsi ankietowani rzadziej zgłaszają naruszenie danych lub utratę poufnych danych z powodu niezabezpieczonego urządzenia (**30%**) niż ich koledzy z zarządu/C-level (**59%**). Istnieje wyraźne rozbieżności w firmach, jeśli chodzi o prawdziwe zrozumienie bezpieczeństwa urządzeń fizycznych i konsekwencji jego braku – apel o szerszą edukację i dzielenie się wiedzą

"Niewielka początkowa inwestycja w środki bezpieczeństwa (blokady) może **znacznie zmniejszyć prawdopodobieństwo kosztownej wymiany urządzeń** lub dłuższego przestoju."

Kadra zarządzająca wyższego szczebla Edukacja – zapewniona przez rząd/państwo; 1000 lub więcej pracowników; Hybrydowy model pracy; USA

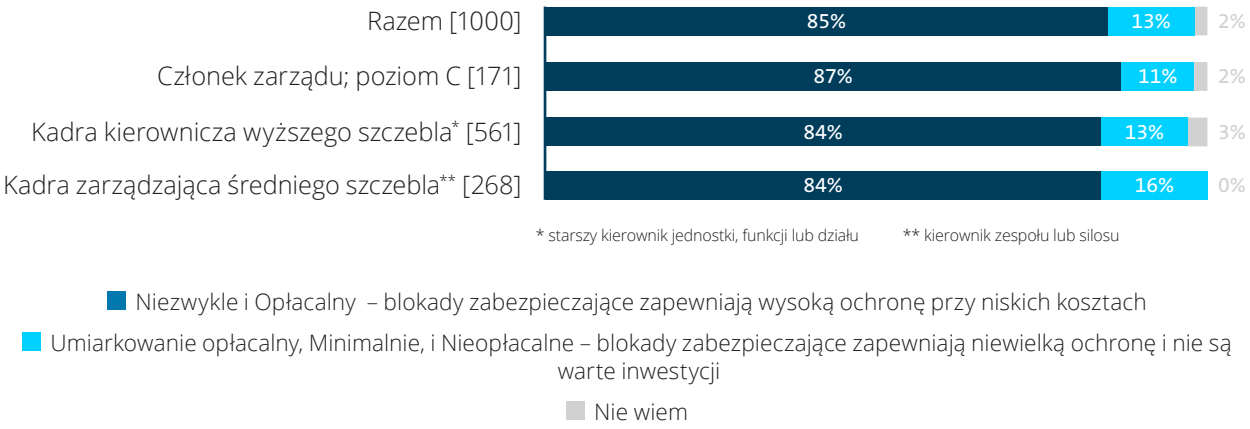
Jak zatem organizacje powinny przezwyciężyć tę przeszkodę?

Organizacje borykają się z wieloma problemami bezpieczeństwa cyfrowego i fizycznego, a skutki kradzieży urządzeń są oszałamiające dla organizacji i ich wyników finansowych. Powinny szukać najbardziej opłacalnego rozwiązania. A dzięki ich udowodnionemu sukcesowi, może to być prosta blokada bezpieczeństwa.

Większość (**84%**) naszych ankietowanych decydentów ds. IT wyższego szczebla twierdzi, że blokady bezpieczeństwa są opłacalne w ograniczaniu potencjalnych naruszeń danych –oferują znaczną wartość w zapobieganiu kradzieży i naruszeniom. Co więcej, **42%** uważa, że są niezwykle opłacalne.

Jest to powszechna opinia podzielana przez tych, którzy już używają blokad bezpieczeństwa, a nawet przez tych, którzy ich nie używają – co rodzi pytanie, dlaczego nie? Organizacje mogą postrzegać blokady jako dodatkowe wyzwania logistyczne w zarządzaniu urządzeniami lub być może silniejsze skupienie się na bezpieczeństwie cyfrowym nad fizycznym prowadzi do niedoceniania wartości blokad, co utrudnia adopcję. Jednak w porównaniu do oszałamiających konsekwencji finansowych kradzieży urządzeń, koszt blokady bezpieczeństwa – zwykle wynoszący średnio zaledwie 30–50 USD za urządzenie – stanowi minimalną inwestycję w celu zmniejszenia ryzyka. Zagłębiając się w to dalej, widzimy wyraźną różnicę w opiniach w całej hierarchii organizacyjnej.

Organizacje, w których obecnie NIE stosuje się blokad zabezpieczających



Rys. 6: *Jak oceniasz rolę fizycznych blokad zabezpieczających w ograniczaniu potencjalnych naruszeń danych lub kradzieży pod kątem opłacalności? [Zapytano wszystkich respondentów, pokazując dane podzielone według starszeństwa, liczby bazowe na wykresie]*

Te ustalenia podkreślają krytyczną potrzebę zajęcia się podstawowymi przyczynami kradzieży urządzeń i ich szerszym wpływem na całą organizację. Podczas gdy starsi liderzy częściej postrzegają blokady bezpieczeństwa jako niezwykle opłacalne (**56%**), przekonanie to słabnie na niższych szczeblach hierarchii. Ostatecznie starsi liderzy zawsze będą bardziej skupieni na szerszych implikacjach (np. grzywny regulacyjne, reputacja), podczas gdy menedżerowie niższego szczebla na codziennych skutkach (np. utrata produktywności).

To rozłączenie podkreśla znaczenie dostosowania organizacyjnego i edukacji na temat wartości blokad bezpieczeństwa - nie tylko jako opłacalnego narzędzia, ale jako proaktywnego rozwiązania zapobiegającego znacznym stratom, zanim one wystąpią. Zniwelowanie tych luk w postrzeganiu zapewni ujednolicone i skuteczne podejście do łagodzenia ryzyka kradzieży urządzeń i ochrony poufnych danych.

"Gdy raz zostanie utracone, spowoduje znaczne straty. Musimy **rozwiązać ten problem u źródła.**"

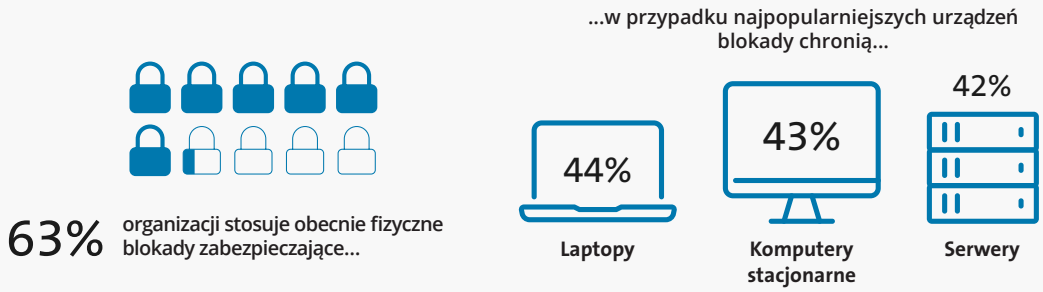
Kadra zarządzająca średniego szczebla Ochrona zdrowia – własność prywatna; 1000 lub więcej pracowników; Hybrydowy model pracy; USA

Blokady służą do zabezpieczania i zapewniania bezpieczeństwa

Kontynuowaliśmy badanie, w jaki sposób blokady zabezpieczające są nie tylko skuteczne w ograniczaniu kradzieży, ale także oferują ekonomiczne rozwiązanie w celu złagodzenia szerszych zagrożeń bezpieczeństwa. Ich różnorodne zastosowania podkreślają ich wszechstronność w rozwiązywaniu problemów bezpieczeństwa w różnych środowiskach — korzyść, którą wiele organizacji już dostrzega.

Wiele osób już używa blokad bezpieczeństwa, aby zabezpieczyć urządzenia elektroniczne w swojej organizacji. Najczęściej zabezpieczane urządzenia to laptopy (**44%**), komputery stacjonarne (**43%**) i serwery (**42%**), co odzwierciedla priorytet nadany zabezpieczeniu krytycznego sprzętu, który często przechowuje poufne dane. Ta powszechna adopcja podkreśla uznanie blokad za kluczowe narzędzie w ochronie przed kradzieżą i nieautoryzowanym dostępem.

Postrzegana opłacalność blokad zabezpieczających



Rys. 7: *W przypadku których z poniższych urządzeń elektronicznych w Twojej organizacji stosowane są fizyczne blokady zabezpieczające? [Zapytano wszystkich respondentów: 1000]*

Jednak fakt, że prawie 4 na 10 ankietowanych stwierdziło, że ich organizacje nie stosują blokad, budzi obawy o luki w strategiach bezpieczeństwa urządzeń, zwłaszcza w przypadku urządzeń często używanych w mobilnych lub hybrydowych środowiskach pracy.

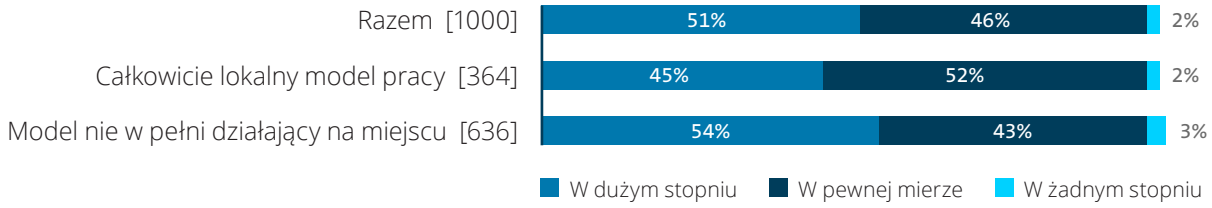
Dla organizacji dane te podkreślają potrzebę kompleksowej oceny obecnych środków bezpieczeństwa. Podczas gdy blokady są zaufanym i szeroko stosowanym rozwiązaniem, rozszerzenie ich zastosowania na szerszy zakres urządzeń i połączenie ich z uzupełniającymi zabezpieczeniami cyfrowymi może pomóc zamknąć istniejące luki w zabezpieczeniach i skuteczniej ograniczyć ryzyko.

Prawie wszyscy ankietowani (**97%**) uznają krytyczną rolę blokad zabezpieczających w zapobieganiu kradzieży i nieautoryzowanemu dostępowi, który często następuje po niej. To powszechne uznanie odzwierciedla zaufanie, jakie organizacje pokładają w zabezpieczeniach fizycznych jako podstawowym środku ochrony urządzeń i poufnych danych. Blokady działają jako pierwsza linia obrony, zmniejszając możliwości kradzieży i łagodząc ryzyko związane z naruszonym sprzętem.

"Zamykanie drzwi w biurach typu open space, przestrzeniach coworkingowych lub innych miejscach, w których może przebywać wiele osób, **zmniejsza ryzyko kradzieży.**"

Członek zarządu/C-level; Edukacja – prywatna własność; 100-249 pracowników; USA

Wiara, że środki bezpieczeństwa fizycznego przyczyniają się do zapobiegania kradzieży urządzeń



Rys. 8: *W jakim stopniu Twoim zdaniem środki bezpieczeństwa fizycznego, takie jak blokady bezpieczeństwa, przyczyniają się do zapobiegania kradzieży urządzeń, która mogłaby prowadzić do nieautoryzowanego dostępu do danych firmy? [Zapytano wszystkich respondentów, pokazując dane podzielone według typu modelu roboczego, liczby bazowe na wykresie]*

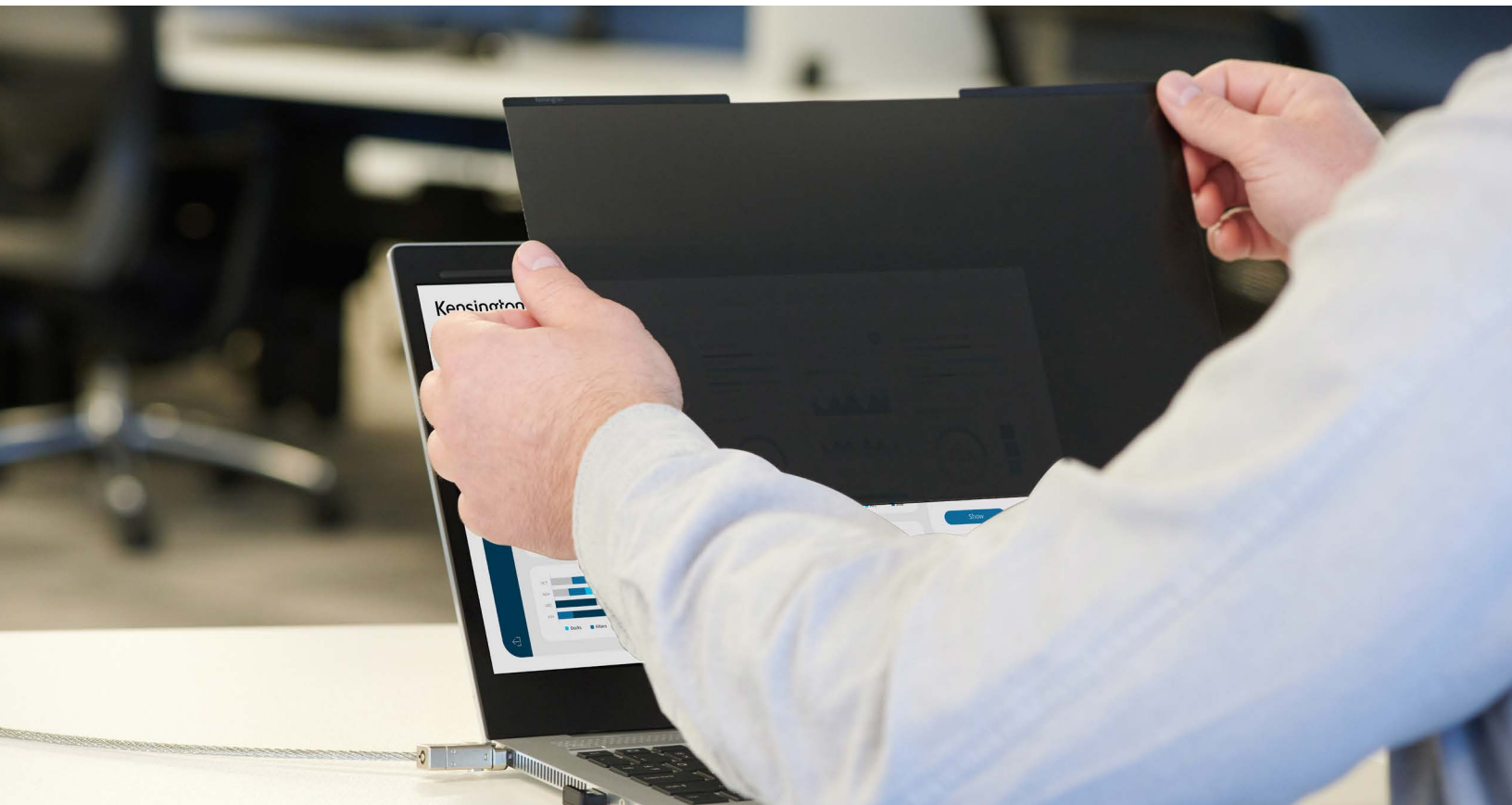
To uznanie staje się bardziej widoczne tam, gdzie organizacje przyjęły elastyczne i hybrydowe modele pracy. W tych zdecentralizowanych środowiskach urządzenia są coraz częściej używane w niezabezpieczonych lokalizacjach, takich jak domowe biura lub przestrzenie publiczne, zwiększając ryzyko kradzieży lub przypadkowego narażenia. Naruszenia danych spowodowane przez niezabezpieczone urządzenia są znacznie częstsze w bardziej elastycznych konfiguracjach pracy (**50%** łącznie w porównaniu z **39%** w przypadku całkowicie lokalnego modelu pracy).

Blokady bezpieczeństwa zaprojektowano tak, aby mogły być stosowane w różnych środowiskach, oferując niezawodną ochronę urządzeń niezależnie od tego, czy są one używane w biurach, zdalnych przestrzeniach roboczych czy miejscach publicznych, zapewniając organizacjom spokój ducha niezależnie od modelu pracy.

Konsekwencje finansowe kradzieży urządzeń mogą być oszałamiające, a koszty wymiany skradzionego sprzętu często są przyćmione przez szersze skutki dla produktywności, zgodności z przepisami i naruszeń danych. Dla organizacji każde skradzione lub niezabezpieczone urządzenie zwiększa ryzyko — nie tylko dla operacji, ale także dla wyniku finansowego. Blokady zabezpieczające oferują sprawdzone i opłacalne rozwiązanie, któremu wielu już zaufało, jeśli chodzi o zmniejszenie prawdopodobieństwa kradzieży i wynikających z niej finansowych i wizerunkowych skutków. Eliminując te ryzyka u źródła, organizacje mogą przyjąć proaktywne stanowisko w zakresie ochrony swoich aktywów i poufnych danych.

Chociaż środki bezpieczeństwa fizycznego, takie jak blokady, są skuteczne, muszą być częścią szerszej strategii radzenia sobie z ewoluującymi zagrożeniami bezpieczeństwa związanymi z pracą hybrydową. Połączenie blokad z uzupełniającymi zabezpieczeniami cyfrowymi, takimi jak szyfrowanie i uwierzytelnianie dwuskładnikowe, zapewnia kompleksową ochronę przed zagrożeniami fizycznymi i cyfrowymi. Programy szkoleniowe mające na celu edukację pracowników na temat znaczenia tego zintegrowanego podejścia mogą dodatkowo wzmocnić bezpieczeństwo organizacji. Dla organizacji poruszających się po zawiłościach nowoczesnych modeli pracy, integracja środków bezpieczeństwa fizycznego i cyfrowego jest niezbędna do minimalizacji ryzyka, ochrony siły roboczej i utrzymania odporności operacyjnej.

Zapobieganie kradzieży urządzeń i wynikającym z tego naruszeniom danych jest o wiele bardziej opłacalne niż radzenie sobie z następstwami. Podejmowanie środków zapobiegawczych, takich jak używanie blokad laptopów, może chronić Twoją organizację przed znacznymi skutkami finansowymi i operacyjnymi w przyszłości. Aby zapewnić skuteczność tych środków, kluczowe jest dostosowanie się do wyższego kierownictwa, zarządu i zespołów. Wspólne zaangażowanie w priorytety bezpieczeństwa zapewnia, że każdy rozumie swoją rolę w zabezpieczaniu cennych aktywów i ograniczaniu ryzyka.



Metodologia

Firma Kensington zleciła niezależnemu specjaliście ds. badań rynku Vanson Bourne przeprowadzenie badań, na których opiera się niniejszy raport. Jesienią 2024 roku przeprowadzono wywiady z 1000 liderów IT wyższego szczebla zaangażowanych lub mających wpływ na fizyczne bezpieczeństwo sprzętu IT w swoich organizacjach w USA, Wielkiej Brytanii, Francji i Niemczech.

Respondenci musieli pracować w organizacjach zatrudniających co najmniej 100 pracowników i działać w różnych sektorach, zarówno prywatnym jak i publicznym.

Wywiady przeprowadzono online i przeprowadzono je przy użyciu rygorystycznego wielopoziomowego procesu selekcji, aby zapewnić, że tylko odpowiedni kandydaci otrzymali możliwość udziału. O ile nie wskazano inaczej, omawiane wyniki opierają się na całej próbie.

O firmie Kensington

Firma Kensington jest wiodącym dostawcą akcesoriów do komputerów stacjonarnych i urządzeń mobilnych, któremu ufają specjaliści z branży IT, edukatorzy, firmy i profesjonaliści z biur domowych na całym świecie od ponad 40 lat. Kensington stara się przewidywać potrzeby i wyzwania stale ewoluującego miejsca pracy oraz tworzyć nagradzane rozwiązania na poziomie profesjonalnym dla organizacji, które zobowiązały się do zapewnienia najlepszym profesjonalistom narzędzi, których potrzebują do rozwoju. Firma szczyci się tym, że jest wyborem profesjonalistów, a także swoimi podstawowymi wartościami dotyczącymi wzornictwa, jakości i wsparcia.

W środowiskach biurowych i mobilnych szeroka gama nagradzanych produktów firmy Kensington zapewnia niezawodne zabezpieczenia, innowacje zwiększające produktywność pracy na komputerach stacjonarnych, profesjonalne wideokonferencje i ergonomię.

Firma Kensington z siedzibą w Burlingame w Kalifornii jest wynalazcą i światowym liderem w dziedzinie blokad zabezpieczających do laptopów. Firma Kensington jest oddziałem ACCO Brands, która projektuje, produkuje i sprzedaje produkty konsumenckie i dla użytkowników końcowych, które pomagają ludziom pracować, uczyć się i bawić. Oprócz Kensington® , szeroko rozpoznawalne marki ACCO Brands obejmują AT-A-GLANCE® , Five Star®, Leitz®, Mead® , PowerA® , Swingline® , Tilibra i wiele innych. Więcej informacji o ACCO Brands Corporation (NYSE:ACCO) można znaleźć na stronie www.accobrands.com.

FOR MORE INFORMATION CONTACT: sales@kensington.com

Kensington
The Professionals' Choice™