Raport z badania

Dezinformacja jako ryzyko dla polskiego biznesu

Badanie wśród przedstawicieli firm

Zrealizowano dla:

GRUPA PTWP

Kwiecień 2026

Metodologia

Czas realizacji: Kwiecień 2026 roku

Jednostka badania:
- Badanie ilościowe – osoby zarządzające oraz pracownicy firm
- Badanie jakościowe – eksperci z zakresu dezinformacji, monitoringu mediów i treści internetowych, przedstawiciele przedsiębiorców

Wielkość próby : N=205 (badanie ilościowe CAWI)
N=4 IDI (eksperci z zakresu dezinformacji, monitoringu mediów i treści internetowych)
N=5 IDI (przedstawiciele przedsiębiorców)

Technika badawcza: CAWI, IDI

Oznaczenia stosowane w raporcie: Badanie ilościowe Badanie jakościowe

Definicja dezinformacji użyta w badaniu ilościowym

Definicja dezinformacji, która została zaprezentowana ankietowanym w badaniu ilościowym

Dezinformacja: celowo rozpowszechniane nieprawdziwe lub zmanipulowane informacje. Mogą to być m.in. fałszywe opinie w mediach, podszywanie się pod przedstawicieli spółki, zmanipulowane materiały audio/wideo, treści generowane przez AI, w tym deepfake, fałszywe komunikaty dotyczące wyników, kontraktów czy decyzji zarządu.

Definicja była wyświetlana po odpowiedzi na pytania o subiektywny poziom wiedzy na temat dezinformacji.

Podsumowanie

- Subiektywna ocena respondentów na temat swojej wiedzy o dezinformacji jest przeważnie dobra, jednak odpowiedzi zdecydowane stanowiły około 20 proc.

- **Badani pracownicy są świadomi, że dezinformacja stanowi realne zagrożenie dla funkcjonowania polskich firm** (86 proc.). Zdecydowana większość uważa, że to niebezpiecznie narzędzie do wpływania na wartość firmy i jej finanse, a zjawisko *fake news* wpływa na postawy konsumentów, co może zagrażać biznesowi. Uczestnicy badania przeważnie uważają, że dezinformacja wiąże się z przynajmniej umiarkowanym ryzykiem dla poszczególnych aspektów działalności ich firm, ale przede wszystkim dla reputacji, a później dla relacji z inwestorami i liczby klientów/obrotów.

- Chociaż deklaratywna świadomość badanych jest wysoka, to dominuje opinia, że polski biznes nie nadąża w zakresie działań prewencyjnych – dwóch na trzech badanych zgadza się z opinią, że polski biznes myśli o zagrożeniach jak w 2020 roku, gdy dezinformacja jest już w roku 2030. Według badanych to właśnie brak świadomości zagrożenia i brak odpowiednich procedur stanowią największe bariery w skutecznym reagowaniu na dezinformację. Z danych wynika, że szkolenia z zakresu rozpoznawania i przeciwdziałania dezinformacji nie są powszechnie stosowaną praktyką.

- **Niemal 40 proc. badanych przyznało, że ich firma była ofiarą ataku dezinformacyjnego** (w tym 29 proc. – wielokrotnie). Głównie były to fałszywe lub częściowo nieprawdziwe (zmanipulowane) informacje na temat firmy. Problem dotyczy najczęściej dużych przedsiębiorstw.

- O powszechności zjawiska dezinformacji świadczy fakt, że większość badanych miała styczność z różnymi formami działań dezinformacyjnych w odniesieniu do działalności biznesowej firm funkcjonujących na polskim rynku. Najczęściej były to fałszywe lub zmanipulowane informacje na temat przedsiębiorstwa, ale też fałszywe teksty generowane przez AI podszywające się pod wiarygodne źródła, fałszywe grafiki, fałszywe strony podszywające się pod firmę.

01

PERCEPCJA ZJAWISKA DEZINFORMACJI

Dezinformacja to nie tylko fałsz

Dezinformacja jest rozumiana przede wszystkim jako celowe wpływanie na sposób postrzegania firmy, marki, projektu lub branży.

Eksperci podkreślają, że o dezinformacji nie decyduje wyłącznie to, czy dana treść jest całkowicie fałszywa. Równie, albo nawet bardziej, skuteczne może być wykorzystanie informacji prawdziwej, ale osadzonej w mylącym kontekście, celowe pominięcie części faktów, przesunięcie akcentów interpretacyjnych albo nadanie przekazowi takiej formy, która wzmacnia określoną ocenę firmy, marki lub branży. W tym ujęciu dezinformacja jest działaniem intencjonalnym, ukierunkowanym na wywołanie konkretnego skutku: osłabienie reputacji, wzbudzenie niepokoju, podważenie wiarygodności albo zmianę zachowań odbiorców.

Osoby zarządzające opisują dezinformację w bardzo podobny sposób, ale mocniej osadzają ją w realiach funkcjonowania organizacji. W ich wypowiedziach wyraźnie widać, że dezinformacja nie jest rozumiana jako pojedyncza nieprawdziwa wiadomość, lecz jako zjawisko wpływające na sposób postrzegania firmy, projektu lub całego sektora. Respondenci zwracają uwagę, że może ona osłabiać zaufanie, wywoływać błędne oceny, uruchamiać emocjonalne reakcje i prowadzić do decyzji opartych na niepełnym albo zniekształconym obrazie sytuacji. W praktyce oznacza to, że stawką nie jest sama „prawda informacji", ale to, jaki obraz organizacji utrwala się w otoczeniu.

Dezinformacja jest ujmowana przede wszystkim jako świadome sterowanie percepcją firmy, a nie jedynie rozpowszechnianie nieprawdziwych treści.

Co decyduje o skuteczności dezinformacji?

Dezinformacja nie wygrywa dlatego, że jest najbardziej wiarygodna, lecz dlatego, że trafia w emocje, wcześniejsze przekonania i sposób działania platform cyfrowych.

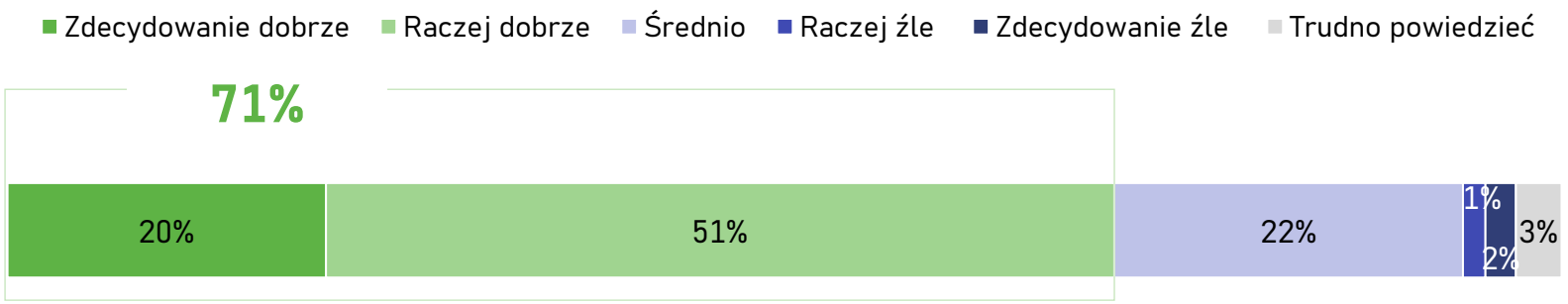
Eksperci wskazują, że dezinformacja działa przede wszystkim dlatego, że odwołuje się do silnych emocji: strachu, niepewności, oburzenia, troski o zdrowie, dzieci, bezpieczeństwo lub przyszłość. Duże znaczenie ma przy tym nie tylko sama treść, ale także jej „opakowanie": powtarzalność przekazu, pozór eksperckości, autorytet nadawcy, realistyczny format i algorytmiczne wzmacnianie treści angażujących emocjonalnie. W badaniu wyraźnie wybrzmiewa też teza, że podatność nie zależy w prosty sposób od poziomu wykształcenia, lecz raczej od kontekstu, poziomu stresu, deficytu wiedzy w danym obszarze oraz funkcjonowania odbiorcy w określonej bańce informacyjnej.

Materiał z wywiadów z **osobami zarządzającymi** pokazuje, że najsilniej działają te narracje, które dotyczą tematów szczególnie wrażliwych społecznie i biznesowo. W sektorze żywnościowym są to kwestie bezpieczeństwa produktów, jakości i etyki produkcji. W ochronie zdrowia najłatwiej eskalują przekazy dotyczące bezpieczeństwa pacjentów, jakości leczenia, cen i dostępności usług. W energetyce szczególnie podatne na manipulację okazują się zagadnienia związane z kosztami inwestycji, stabilnością technologii, zależnością od warunków pogodowych i znaczeniem sektora dla bezpieczeństwa energetycznego. To właśnie w tych obszarach informacja szybko zamienia się w emocjonalną ocenę firmy lub branży.

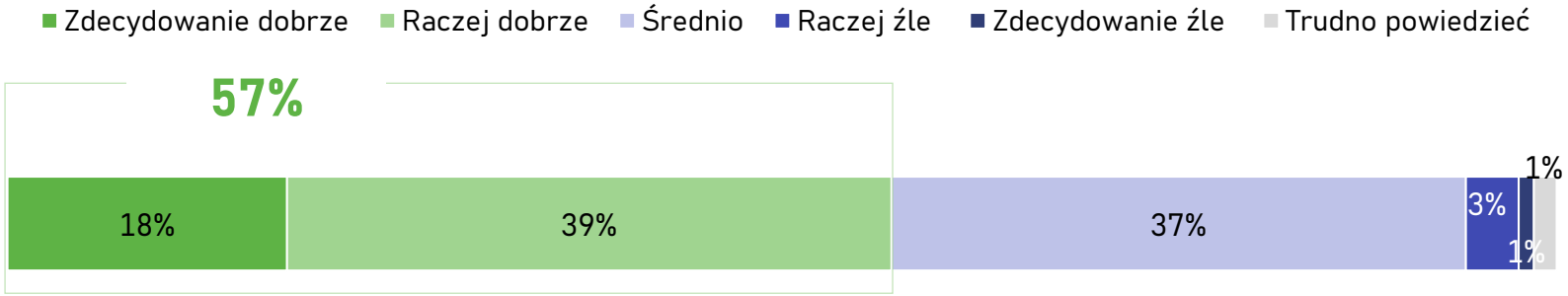
Największą siłą dezinformacji jest zdolność do uruchamiania emocji w obszarach, które odbiorcy uznają za osobiste, ważne i ryzykowne.

Subiektywna ocena wiedzy na temat dezinformacji

Q: Jak ocenia Pan/i swoją ogólną wiedzę na temat **zjawiska dezinformacji**?



Q: Jak ocenia Pan/i swoją wiedzę na temat **zjawiska dezinformacji w biznesie?**



Subiektywnie respondenci dobrze oceniali swoją wiedzę na temat ogólnego zjawiska dezinformacji, ale tylko co piąty określił ją jako zdecydowanie dobrą. W przypadku dezinformacji rozumianej w kontekście biznesowym odpowiedzi są mniej jednoznaczne. Swoją wiedzę jako dobrą oceniło 57 proc. zapytanych, ale już prawie czterech na dziesięciu jako średnią. Podobnie jak w przypadku pierwszego pytania odpowiedzi zdecydowane stanowiły około 20 proc.

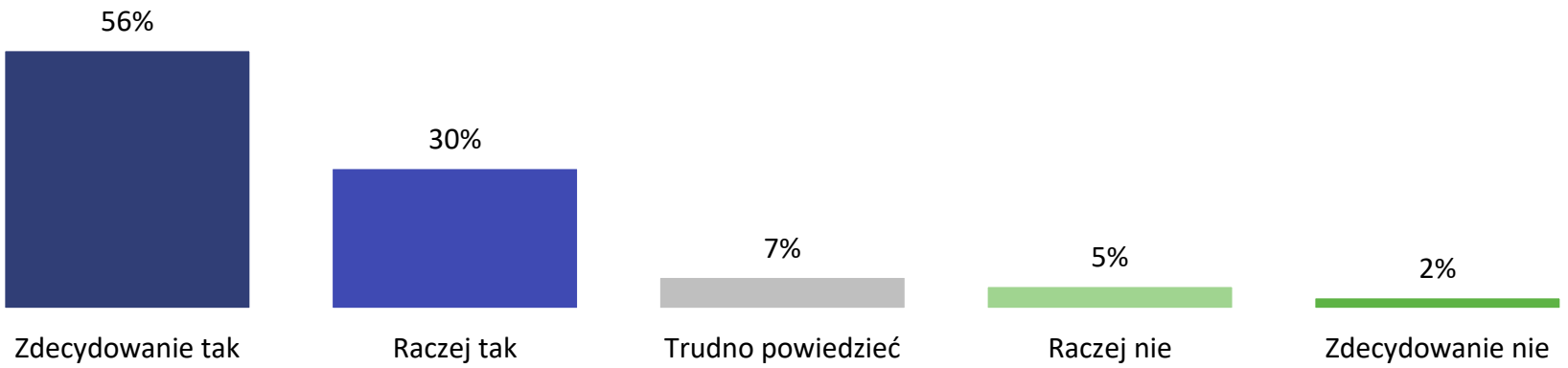
Dezinformacja jako zagrożenie dla firm

Ogólna ocena

Q: Czy Pana/i zdaniem dezinformacja stanowi obecnie **realne zagrożenie dla funkcjonowania polskich firm?**

86%

badanych postrzega dezinformację jako **realne zagrożenie** dla funkcjonowania polskich firm



Dezinformacja w opiniach pytanych stanowi obecnie realne zagrożenie dla funkcjonowania polskich firm, ponad połowa respondentów taką opinię wyraziła w sposób zdecydowany.

Samo zjawisko nie jest niczym nowym

Dezinformacja jest dziś szybsza, tańsza i bardziej ciągła niż jeszcze kilka lat temu, a firmy nadal zbyt często traktują ją bardziej jako problem komunikacyjny niż strategiczne ryzyko.

Eksperci są zgodni, że sama logika dezinformacji nie jest nowa, natomiast zasadniczo zmieniły się warunki jej funkcjonowania. Dziś treści powstają szybciej, ich produkcja jest prostsza i tańsza, a ich rozpowszechnianie odbywa się niemal równocześnie w wielu kanałach. W wywiadach pojawia się mocna teza, że jeszcze niedawno przenikanie narracji między platformami można było mierzyć w dniach, podczas gdy obecnie ten proces częściej przebiega w minutach. Dla biznesu oznacza to skrócenie czasu reakcji, większą presję operacyjną i wyraźny wzrost kosztu bezczynności.

Osoby zarządzające potwierdzają, że ryzyko jest istotne, ale w wielu organizacjach nie przekłada się jeszcze na działania wyprzedzające. Dezinformacja pozostaje często klasyfikowana jako problem wizerunkowy, uruchamiający reakcję dopiero wtedy, gdy staje się głośny lub widoczny na zewnątrz. Tymczasem z ich wypowiedzi wynika, że skutki mogą wykraczać daleko poza reputację: dotyczyć relacji z inwestorami i partnerami, decyzji instytucji finansowych, sprzedaży, oceny projektów inwestycyjnych czy ogólnego postrzegania całej branży. Problem polega więc nie tylko na rosnącej sile zjawiska, ale także na tym, że organizacyjna waga tego ryzyka wciąż bywa niedoszacowana.

Największa zmiana polega na tym, że dezinformacja stała się stałym elementem otoczenia informacyjnego firm, a nie incydentalnym zakłóceniem.

Kto za tym stoi?

Za tego typu działaniami mogą stać zarówno zewnętrzne operacje wpływu, jak i podmioty nastawione na zysk, przewagę konkurencyjną albo wzmacnianie określonych narracji.

Możliwi sprawcy…

Materiał ekspercki pokazuje, że za działaniami dezinformacyjnymi mogą stać różne grupy. Wśród nich pojawiają się aktorzy państwowi i operacje wpływu zewnętrznego, nieuczciwa konkurencja, grupy przestępcze i oszuści, a także środowiska ideologiczne lub spiskowe. Eksperci zwracają też uwagę, że część przekazów jest następnie wzmacniana przez zwykłych użytkowników i grupy konsumenckie, które nie muszą być inicjatorami działań, ale zwiększają ich zasięg i wiarygodność.

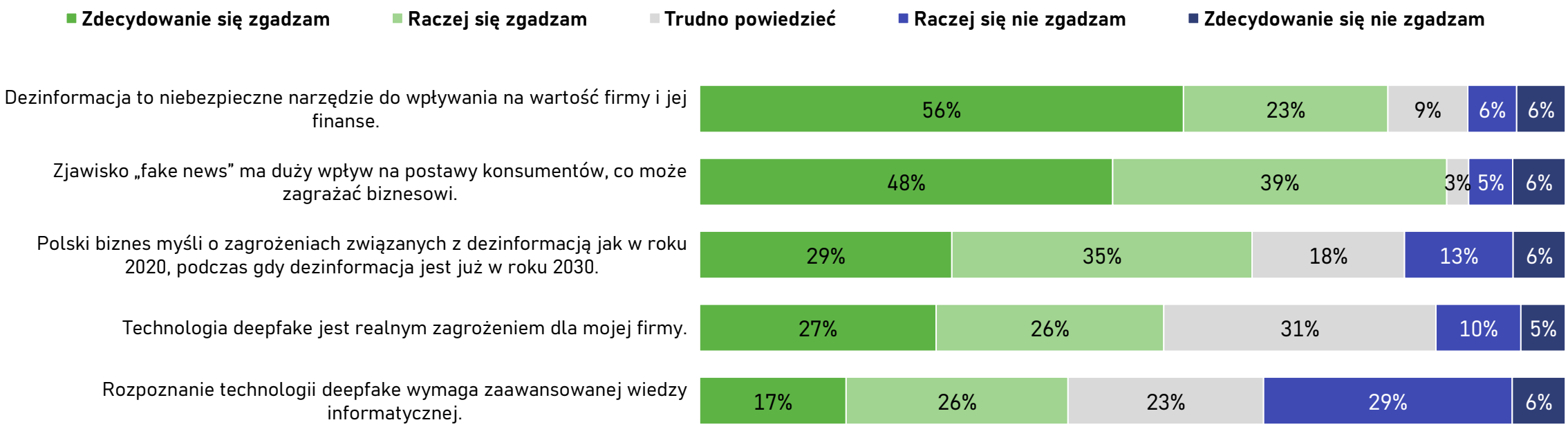
… i ich możliwe motywy

Cele takich działań są zróżnicowane, ale najczęściej sprowadzają się do wywołania konkretnego skutku biznesowego lub społecznego. Może to być osłabienie reputacji firmy, spadek sprzedaży, wywołanie paniki, obniżenie wartości rynkowej, destabilizacja całego sektora, a także wyłudzenie danych lub pieniędzy. Z perspektywy firm najważniejsze jest więc nie tylko to, że pojawia się fałszywy przekaz, ale też to, że często stoi za nim określony interes: polityczny, ekonomiczny, konkurencyjny albo przestępczy.

Dezinformacja wobec firm rzadko jest przypadkowym zakłóceniem. Znacznie częściej stanowi narzędzie realizacji konkretnego interesu — politycznego, ekonomicznego, konkurencyjnego lub przestępczego.

Dezinformacja jako zagrożenie dla firm
Szczegółowe opinie

Q: Na ile zgadza się Pan/i lub nie zgadza z poniższymi stwierdzeniami?



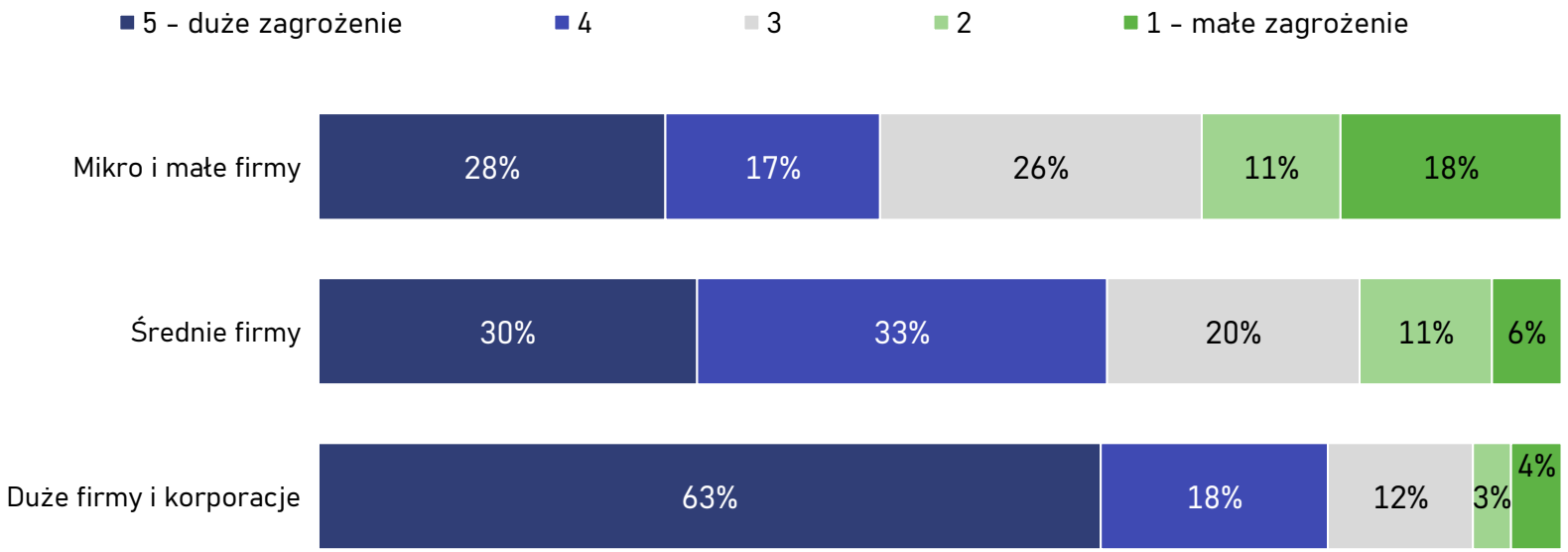
Większa część badanych w zdecydowanym stopniu zgodziła się z twierdzeniem, że dezinformacja jest niebezpiecznym narzędziem wpływu na firmę. Podobnie wysoki poziom jednomyślności wystąpił w przypadku twierdzenia o wpływie *fake news* na postawy konsumentów.

Jednocześnie ponad 60 proc. badanych zgodziło się z twierdzeniem, że polski biznes myśli o dezinformacji *która już była*, jednak badanie pokazuje, że respondenci przykładają do tego problemu dużą uwagę.

Dezinformacja jako zagrożenie dla firm

Kwestia wielkości firmy a ryzyko zagrożeń

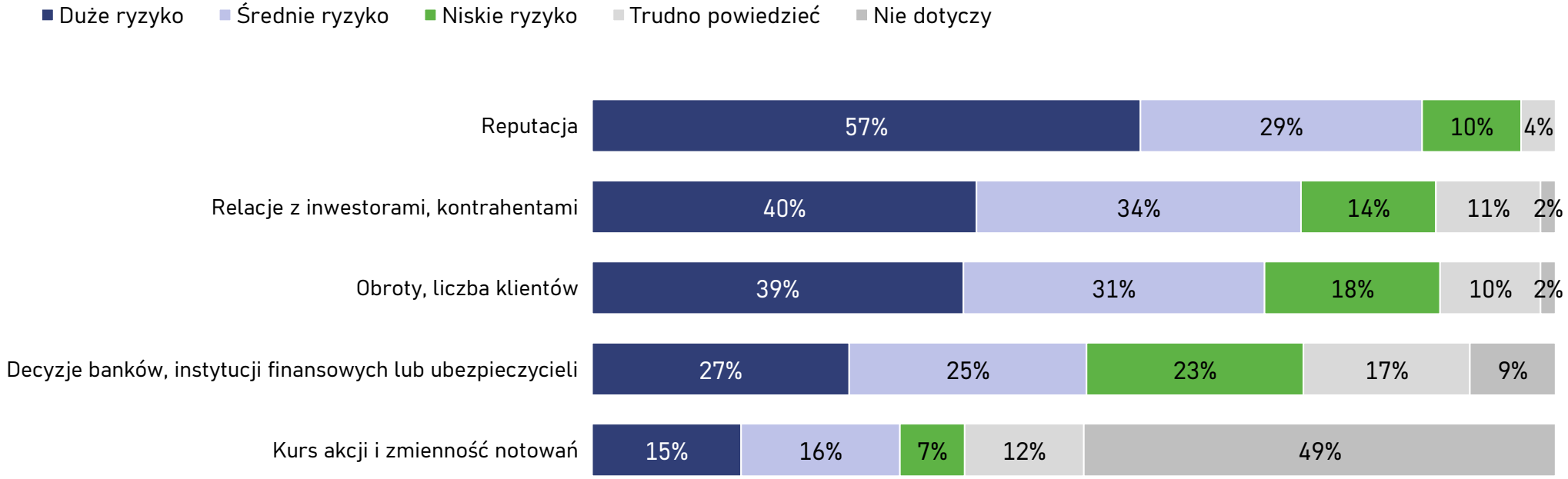
Q: **Na ile firmy różnej wielkości** są Pana/i zdaniem **szczególnie narażone** na działania dezinformacyjne?



Im większa firma tym zdaniem respondentów rośnie zagrożenie narażeniem na działania dezinformacyjne.

Dezinformacja jako zagrożenie dla różnych aspektów działalności firm

Q: Jak dużym **ryzykiem** jest dezinformacja **dla różnych aspektów działalności Państwa firmy**:



Uczestnicy badania przeważnie uważają, że dezinformacja wiąże się z przynajmniej umiarkowanym ryzykiem dla poszczególnych aspektów działalności ich firm, ale przede wszystkim dla reputacji (przeważa ocena, że ryzyko jest duże).

02

STYCZNOŚĆ Z DEZINFORMACJĄ

Dezinformacja przybiera wiele form

Największe ryzyko wynika z połączenia manipulacji treścią i kontekstem z szybkim, wielokanałowym obiegiem informacji oraz rosnącą wiarygodnością syntetycznych formatów.

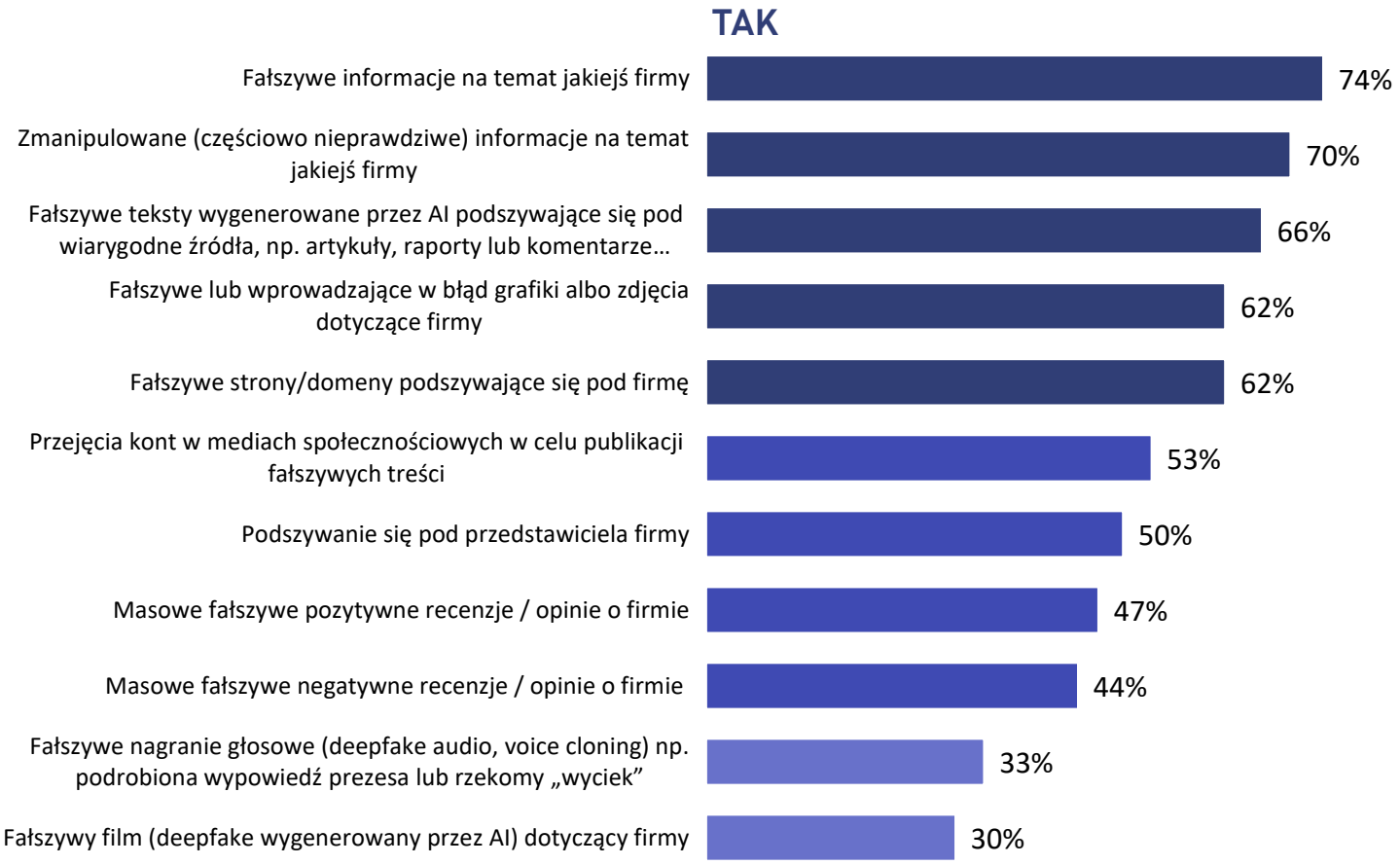
Eksperci opisują szerokie spektrum form dezinformacji: od fałszywych treści o produktach i usługach, przez podszycia pod ekspertów, media i instytucje, po manipulacyjne raporty, treści quasi-analityczne, oszustwa wykorzystujące wizerunek marek oraz materiały audio i wideo generowane przez AI. W ich ocenie technologia nie zmienia podstawowej logiki dezinformacji, ale istotnie zwiększa efektywność całego procesu. AI obniża koszt wytwarzania treści, skraca czas ich przygotowania, umożliwia szybką personalizację przekazu i wzmacnia pozór autentyczności. Szczególnie niebezpieczne stają się formaty, które wyglądają znajomo, profesjonalnie i „prawdziwie", nawet jeśli odbiorca nie potrafi zweryfikować ich źródła.

Osoby zarządzające wskazują, że w praktyce biznesowej problem rozgrywa się przede wszystkim w mediach społecznościowych, komunikatorach, grupach i na forach internetowych, a następnie bywa wzmacniany przez szerszy obieg medialny. W ich wypowiedziach szczególnie mocno wybrzmiewa rola treści, które wyglądają na eksperckie albo obiektywne, ale w rzeczywistości selektywnie przedstawiają fakty, pomijają metodologię lub nadają prawdziwym informacjom mylące znaczenie. AI jest opisywana jako czynnik, który zwiększa tempo produkcji, skalę dystrybucji i realizm przekazu – zwłaszcza w krótkich treściach wizualnych, trudnych do szybkiego rozpoznania jako nieautentyczne.

To, co dziś najbardziej wzmacnia dezinformację, to połączenie emocjonalnego przekazu z formatem, który wygląda na profesjonalny i wiarygodny.

Styczność z dezinformacją w odniesieniu do biznesu

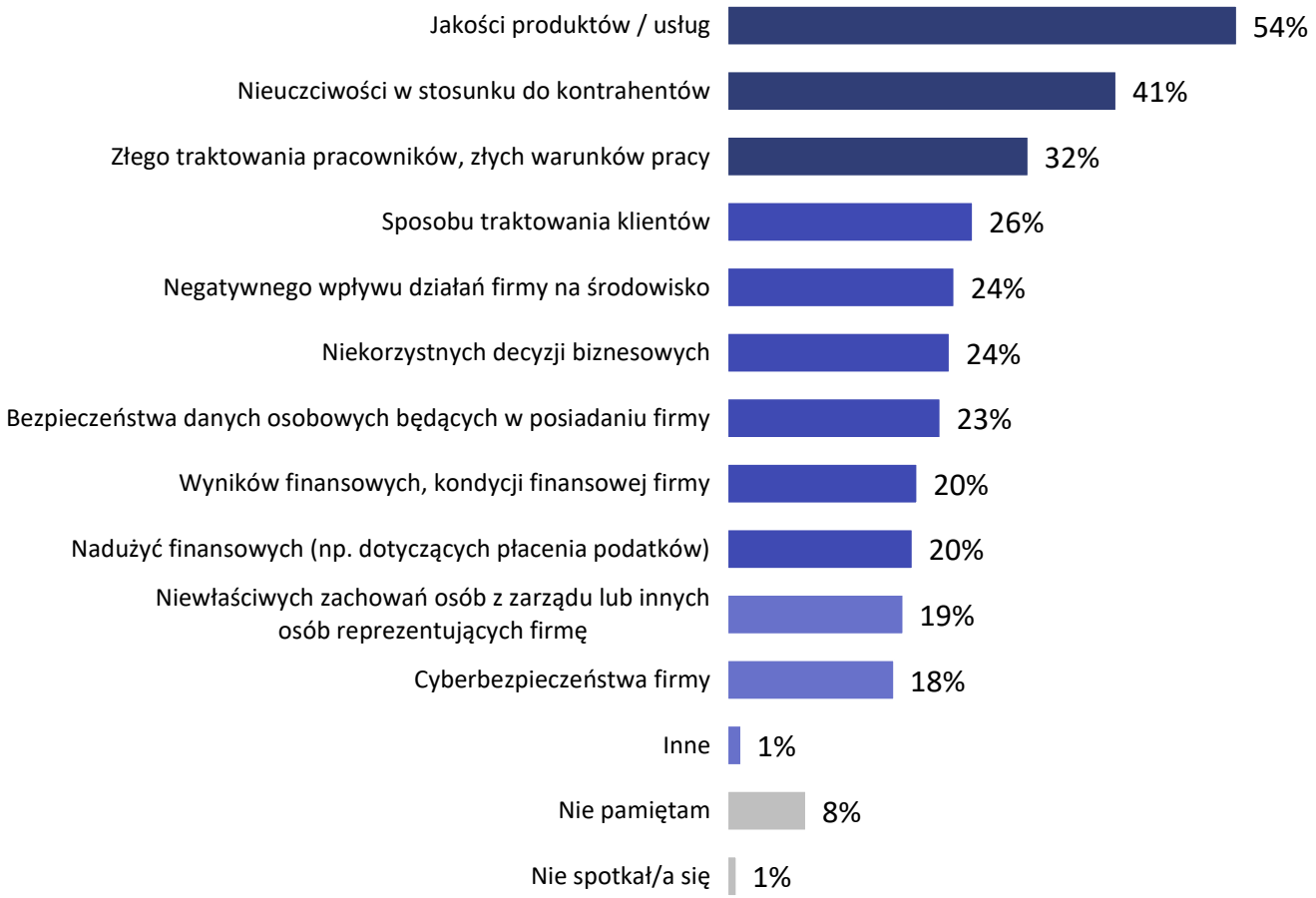
Q: Czy ostatnim roku **spotkał się Pan/i z następującymi zjawiskami w odniesieniu do działalności biznesowej firm** (polskich lub zagranicznych działających na terenie Polski)?
Przedstawiono odsetki odpowiedzi TAK



Respondenci najczęściej spotykali się z fałszywymi lub częściowo nieprawdziwymi informacjami na temat jakiejś firmy. Częste były też generowane przez AI treści podszywające się pod wiarygodne źródła.

Styczność z dezinformacją w odniesieniu do biznesu

Q: Czego dotyczyły działania dezinformacyjne, z którymi się Pan/i spotkał/a?



Działania dezinformacyjne dotyczyły najczęściej jakości dostarczanych produktów i usług, a w drugiej kolejności nieuczciwości w stosunku do kontrahentów. Ankietowani wskazywali także dezinformację na temat złego traktowania pracowników i złych warunków pracy.

03 DOŚWIADCZENIA WŁASNE FIRMY

Dezinformacja jest już codziennością firm

Wypowiedzi osób zarządzających pokazują, że organizacje nie traktują ryzyka hipotetycznie – mają z nim realną styczność, choć nie zawsze w formie spektakularnego kryzysu.

Co mówią firmy…

Dezinformacja nie funkcjonuje w firmach wyłącznie jako spektakularny, łatwy do rozpoznania kryzys. Częściej pojawia się jako rozproszony i stopniowo narastający proces, który zaczyna się od pojedynczych treści, ale z czasem wpływa na zaufanie, obciąża zespoły i zmienia sposób postrzegania firmy lub całego sektora. Różnice między branżami pokazują, że konkretna treść ataku może być różna, ale mechanizm pozostaje podobny: dezinformacja najskuteczniej działa tam, gdzie dotyka tematów budzących silne emocje i łatwo przekłada się na ocenę organizacji. Działania mogą również przyjmować formę skoordynowanej kampanii.

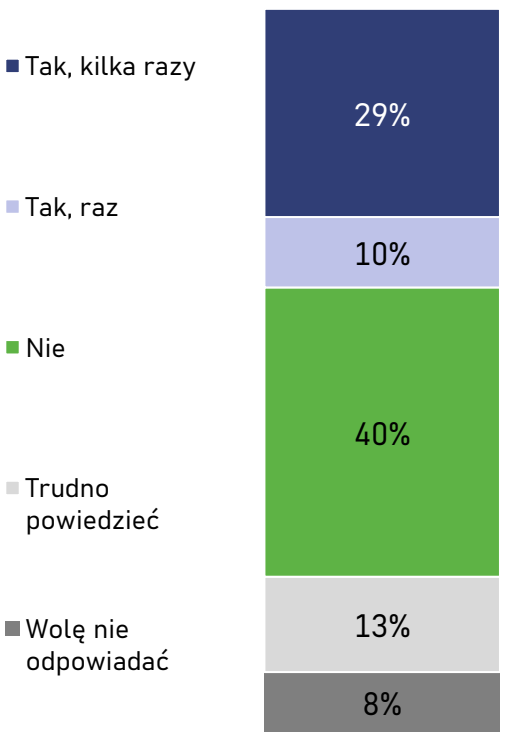
… i co z tego wynika?

Dezinformacja najłatwiej uderza tam, gdzie organizacja działa wolno, niespójnie i bez jasno ustalonych zasad reagowania. Wiele firm wciąż nie ma gotowości do działania pod presją informacyjną: decyzje są rozproszone, procedury nieprzećwiczone, a odpowiedzialność nieoczywista. To sprawia, że nawet ograniczone zagrożenie może szybko urosnąć do rangi kryzysu. Ostatecznie więc skuteczność dezinformacji zależy nie tylko od jakości samego przekazu, ale także od tego, jak dobrze lub jak słabo przygotowana jest organizacja, przeciwko której ten przekaz jest kierowany.

Najpoważniejszym skutkiem dezinformacji jest długotrwałe podważenie zaufania, które ostatecznie przekłada się na finanse i decyzje rynkowe.

Doświadczenie ataku dezinformacyjnego

Q: **Czy Pana/i firma miała do czynienia z dezinformacją** wymierzoną przeciw Państwa firmie, w okresie ostatnich 3 lat?



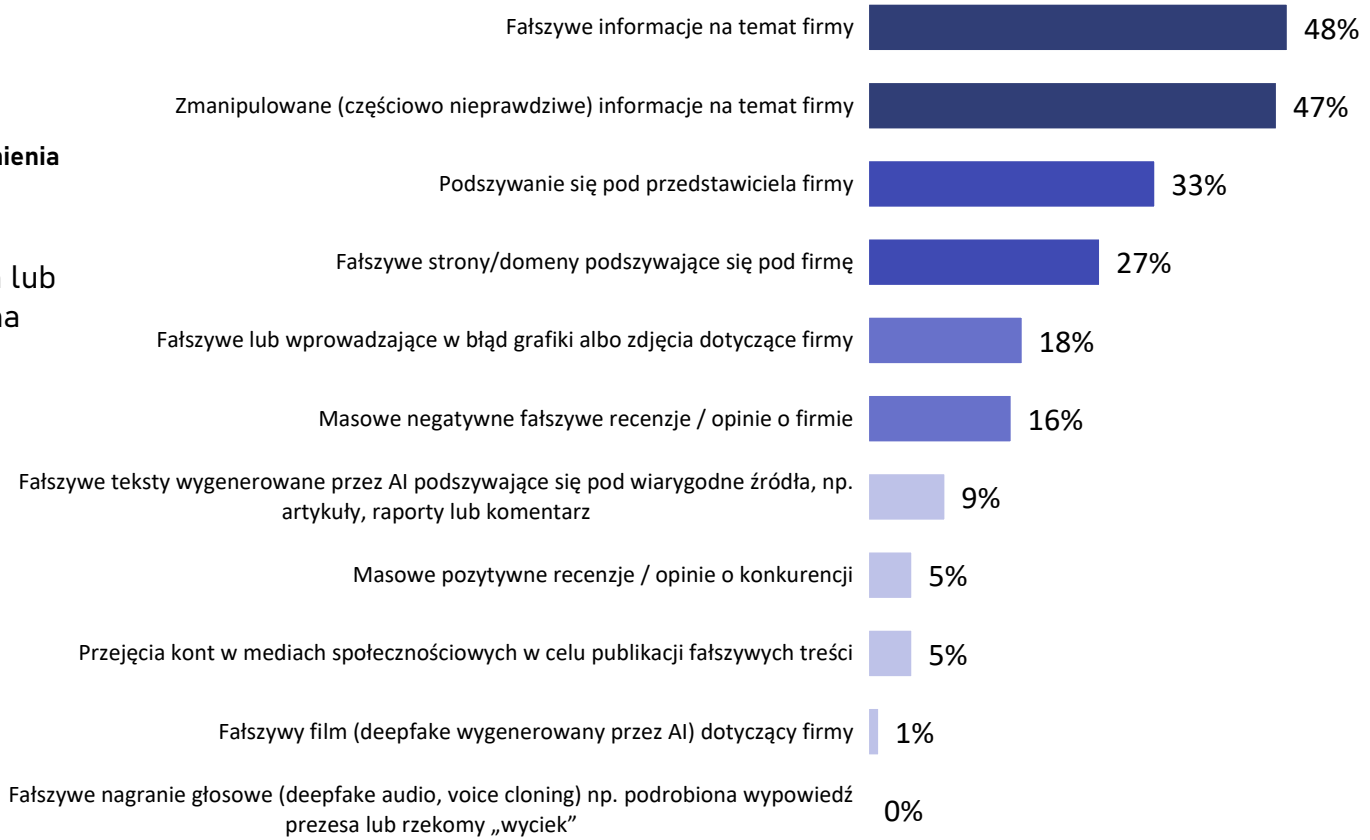
39%

deklaruje, że ich firma miała do czynienia z atakiem dezinformacyjnym.

Najczęstszymi formami było rozprzestrzenianie fałszywych lub zmanipulowanych informacji na temat firmy.

Q: **Jakiej formy użyto** podczas ataku dezinformacyjnego?

Odpowiedzi osób, których firma miała do czynienia z atakiem dezinformacyjnym

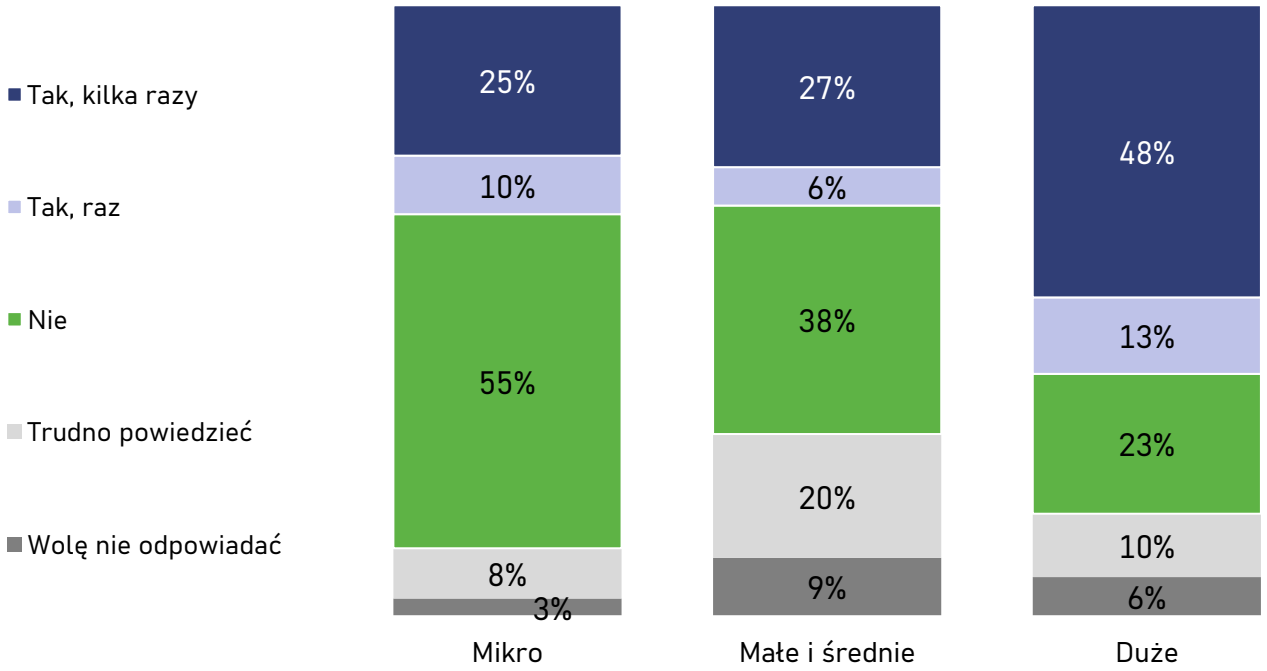


Doświadczenie ataku dezinformacyjnego

Zróżnicowanie ze względu na wielkość przedsiębiorstwa

Q: **Czy Pana/i firma miała do czynienia z dezinformacją** wymierzoną przeciw Państwa firmie, w okresie ostatnich 3 lat?

Zróżnicowanie ze względu na wielkość przedsiębiorstwa

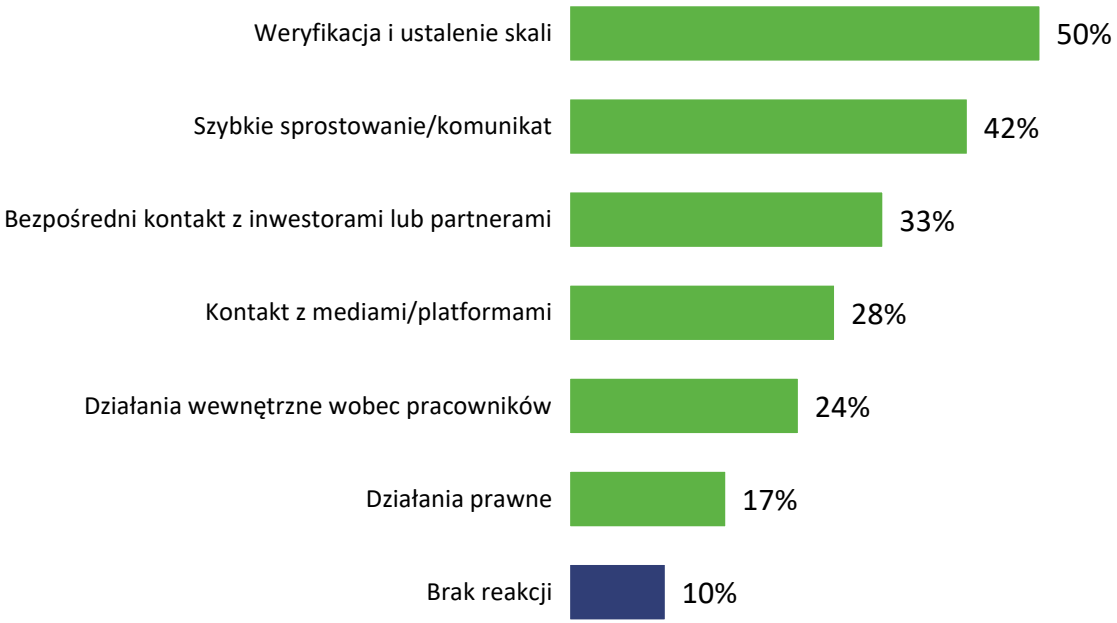


Analiza danych pokazała, że istnieje zróżnicowanie ze względu na wielkość przedsiębiorstwa. Obserwujemy, że **z atakiem dezinformacyjnym najczęściej miały do czynienia duże firmy**. Natomiast pracownicy mikro-przedsiębiorstw częściej niż pozostali badani deklarują brak takich doświadczeń.

Dane potwierdzają ocenę badanych, że na działania dezinformacyjne najbardziej narażone są duże firmy i korporacje.

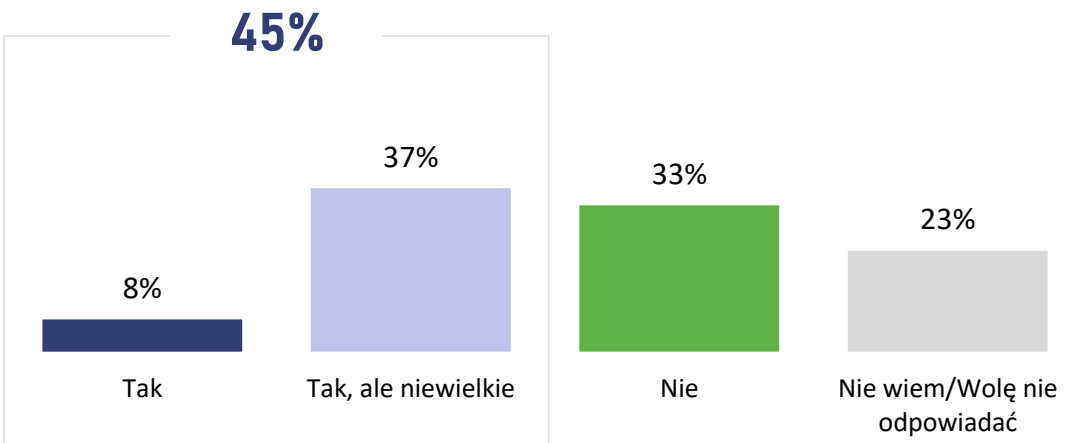
Konsekwencje ataku dezinformacyjnego

Q: **Jak Pana/i firma zareagowała?** (na atak dezinformacyjny – przyp.)



Najczęstszą reakcją na atak była jego weryfikacja i ustalenie jego skali oraz wydanie szybkiego sprostowania i komunikatu. Co dziesiąty respondent deklaruje brak reakcji.

Q: Czy firma odczuła **negatywne skutki biznesowe** tej sytuacji?



Blisko połowa zapytanych przyznaje, że ich firma odczuła negatywne skutki biznesowe ataku dezinformacyjnego, ale zazwyczaj były to niewielkie konsekwencje.

Odpowiedzi osób, których firma miała do czynienia z atakiem dezinformacyjnym

Czym to skutkuje?

Materiał badań jakościowych pokazują, że skutki dezinformacji nie kończą się na komunikacji: obejmują finanse, relacje rynkowe, pracę zespołów i długofalowe zaufanie do firmy lub branży.

Eksperci wskazują na wielopoziomowe skutki dezinformacji. Z jednej strony są to skutki bezpośrednie, takie jak spadek przychodów, koszty obsługi kryzysu, wahania kursu akcji, oszustwa finansowe lub wyłudzenia. Z drugiej strony pojawiają się konsekwencje pośrednie: osłabienie wiarygodności marki, spadek zaufania, pogorszenie marki pracodawcy, trudności w relacjach z partnerami i wyższy koszt odbudowy reputacji. Najgroźniejsze są jednak skutki długoterminowe: trwałe skojarzenie firmy, produktu albo branży z ryzykiem oraz stopniowa erozja zaufania, która przekłada się na realne straty ekonomiczne.

Osoby zarządzające opisują te skutki bardzo konkretnie. Wskazują na wpływ na reputację marki, relacje z inwestorami i partnerami, decyzje banków, instytucji finansowych i ubezpieczycieli, a także na wycenę firmy lub warunki transakcji. W ochronie zdrowia skutki są widziane jako jednocześnie reputacyjne, operacyjne i finansowe: pojawia się więcej pytań, reklamacji, wyjaśnień i obciążenia po stronie zespołów. W energetyce ryzyko jest ujmowane szerzej — jako wpływ na cały ekosystem projektu, łącznie z otoczeniem społecznym, regulacyjnym i inwestycyjnym. Dezinformacja może oddziaływać zarówno bezpośrednio na wynik firmy, jak i pośrednio przez osłabienie zaufania do projektu lub branży.

Najpoważniejszym skutkiem dezinformacji jest długotrwałe podważenie zaufania, które ostatecznie przekłada się na finanse i decyzje rynkowe.

04 ZABEZPIECZENIA I ODPORNOŚĆ ORGANIZACJI

Słabość organizacji to brak gotowości

Respondenci zwracają uwagę na brak procedur, rozproszenie odpowiedzialności, wolne decyzje i traktowanie dezinformacji jako problemu wyłącznie PR-owego.

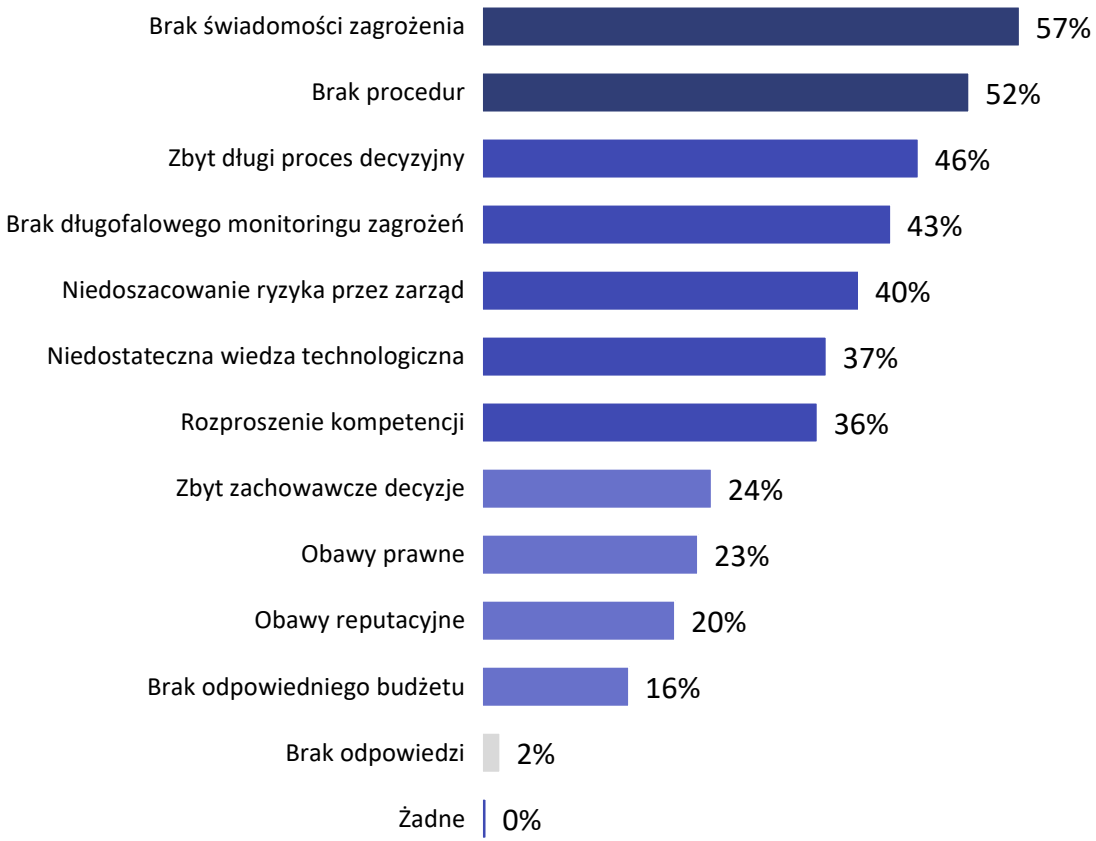
Eksperci oceniają dojrzałość firm w tym obszarze jako ograniczoną. Ich zdaniem organizacje zbyt często reagują dopiero po eskalacji, mylą dezinformację z klasycznym kryzysem komunikacyjnym i nie posiadają trwałego systemu wczesnego ostrzegania. Szczególnie trudne okazuje się rozpoznanie, czy mamy do czynienia z organiczną krytyką, pojedynczym *fejkiem* czy zorganizowaną operacją wpływu. Z tego powodu firmy potrzebują nie tylko narzędzi monitorujących, ale też funkcji bezpieczeństwa informacyjnego, która wykracza poza tradycyjne działania PR.

Osoby zarządzające wskazują na bardzo podobne bariery, ale opisują je bardziej operacyjnie. Najczęściej wymieniają brak procedur, rozproszenie kompetencji, wolne ścieżki decyzyjne, niedoszacowanie ryzyka oraz traktowanie dezinformacji jako problemu reputacyjnego, a nie strategicznego. W ochronie zdrowia dodatkowo wybrzmiewa potrzeba lepszego połączenia komunikacji z obszarami medycznym, prawnym i operacyjnym. W energetyce zwraca się uwagę także na niespójność szerszego otoczenia publicznego i politycznego, które może zwiększać podatność sektora na narracje dezinformacyjne.

Największą słabością firm nie jest brak pojedynczego narzędzia, lecz brak spójnego modelu odpowiedzialności i działania przed eskalacją problemu.

Bariery skutecznej reakcji na dezinformację

Q: Co w Pana/i opinii najbardziej **utrudnia polskim firmom szybką i skuteczną reakcję** na dezinformację?



Brak świadomości zagrożenia oraz **brak procedur** to główne bariery w skutecznym reagowaniu na dezinformację.

Najmniejszą rolę odgrywają obawy prawne lub reputacyjne czy brak odpowiedniego budżetu.

Szkolenia

Q: **Czy w Pana/i firmie były realizowane szkolenia** z zakresu rozpoznawania i przeciwdziałania dezinformacji? Jeśli tak, dla kogo?

33%

badanych potwierdza, że w ich firmie były **realizowane szkolenia** z zakresu rozpoznawania i przeciwdziałania dezinformacji

Ponad połowa respondentów przyznaje, że w ich miejscu pracy nie prowadzono szkoleń z zakresu rozpoznawania i przeciwdziałania dezinformacji.

Co buduje odporność organizacji

Organizacja nie jest w stanie całkowicie zabezpieczyć się przed dezinformacją. Może zwiększać swoją odporność dzięki połączeniu monitoringu, procedur i długofalowego budowania zaufania

1. Monitoring i system wczesnego ostrzegania

Podstawą odporności jest stałe śledzenie wzmianek, narracji i wzorców rozprzestrzeniania się treści. Chodzi nie tylko o rejestrowanie pojedynczych sygnałów, ale o zdolność do wychwytywania zmian tempa, kanałów i sposobów wzmacniania przekazu. Zarówno eksperci, jak i osoby zarządzające wskazują monitoring jako warunek wczesnej reakcji.

2. Jasne procedury i krótkie ścieżki decyzyjne

Organizacja musi wiedzieć, kto odpowiada za ocenę zagrożenia, kto podejmuje decyzję o reakcji i jakie działania mogą zostać uruchomione w różnych scenariuszach. Im szybszy obieg treści, tym większe znaczenie mają proste procedury i gotowe modele postępowania.

3. Współpraca wielu funkcji i przygotowanie ludzi

Skuteczna reakcja nie może być wyłącznie zadaniem komunikacji. Wymaga współpracy z obszarem prawnym, operacyjnym, eksperckim i — w części branż — także z partnerami zewnętrznymi. Ważne jest również przygotowanie liderów i ekspertów do działania pod presją informacyjną.

4. Długofalowe budowanie wiarygodności

Eksperci zwracają uwagę na znaczenie działań uprzedzających, takich jak prebunking, prosta komunikacja, obecność wiarygodnych głosów i budowanie zaufania jeszcze przed kryzysem. Materiał z firm pokazuje z kolei, że w części sektorów równie ważne są edukacja, dialog z otoczeniem i konsekwentne budowanie własnej narracji opartej na danych.

Odporność organizacyjna nie oznacza pełnej kontroli nad informacją, lecz zdolność do szybkiego rozpoznania zagrożenia i zachowania wiarygodności mimo presji.

Dziękujemy
za uwagę

Zostańmy w kontakcie

Tel.: +48 22 266 00 15 E-mail: biuro@ibris.pl www.ibris.pl

AL. Jerozolimskie 96, 00-807 Warszawa