WRZESIEŃ 2025

DFUSION COMMUNICATION

CYBERZAGROŻENIA

A WIZERUNEK ORGANIZACJI

Aleksandra Huścia

Senior Account Manager,
dfusion communication

Cyberkryzys: cisza, która zmienia wszystko

Cyberatak nie przypomina sceny z filmu. Nie ma huku ani alarmów, jest cisza. W tej ciszy zmienia się jednak wszystko — dane zaczynają krążyć w sieci, systemy zostają zablokowane, a reputacja organizacji staje się jedyną walutą, którą można jeszcze obronić.

Dane nie pozostawiają złudzeń. Według Cybersecurity Ventures, **światowe koszty cyberprzestępczości w 2025 roku osiągną 10,5 bln dolarów** – to więcej niż roczne PKB Niemiec i Japonii razem wzięte. Średni koszt pojedynczego wycieku danych w 2024 r. wynosił 4,88 mln dolarów – o 10% więcej niż rok wcześniej (IBM Security, Cost of a Data Breach Report 2024). W sektorze ochrony zdrowia to już ponad 10,9 mln dolarów na incydent, a rosnąca liczba ataków ransomware, które uderzają co 11 sekund, tylko pogarsza tę statystykę. FBI odnotowuje miliardy dolarów rocznych strat wynikających z phishingu, BEC i socjotechniki.

I teraz najważniejsze: Finanse można odzyskać. Dane można odbudować. Ale reputację?

Dlatego dziś mówimy: cyberbezpieczeństwo to nie tylko firewalle – to także komunikacja. A rolą komunikacji jest nie tylko przygotowanie organizacji na incydent, ale przede wszystkim niedopuszczenie do strat wizerunkowych w jego szerokim otoczeniu.

Biorąc pod uwagę skalę zagrożenia, przeprowadziliśmy badanie wśród ekspertek i ekspertów komunikacji i marketingu, w którym zapytaliśmy o poziom przygotowania do sytuacji kryzysowych, świadomość ryzyka i stosowane procedury. Wyniki jasno pokazują, że choć temat staje się coraz bardziej istotny, wiele firm wciąż reaguje wtedy, gdy jest już za późno.

Łukasz Malczewski

Managing Partner,
dfusion communication

Czego uczą nas piloci myśliwców o współczesnych kryzysach?

Pułkownik John Boyd, pilot i weteran wojny koreańskiej, stworzył cykl decyzyjny OODA Loop (Obserwuj, Orientuj się, Decyduj, Działaj). Model ten stał się podstawą zarządzania kryzysowego, szczególnie w dynamicznym otoczeniu – jak podczas pilotowania myśliwca. Poniżej przedstawiamy analizę sytuacji kryzysowej według czterech etapów.

Etap I:

Obserwacja – wszystko zaczyna się od sygnału

Czasem to alert systemu bezpieczeństwa, czasem wpis w mediach społecznościowych albo informacja z dark webu. To jeszcze nie „moment prawdy", lecz chwila, w której można zdobyć przewagę lub ją stracić. Nie każdy incydent kończy się w mediach, ale każdy może – dlatego kluczowe są pierwsze minuty.

Z przeprowadzonego przez nas badania (Cyberzagrożenia a wizerunek organizacji, dfusion communication, czerwiec 2025) wynika,

że 59% organizacji prowadzi stały monitoring reputacyjny, ale tylko 28% regularnie ćwiczy scenariusze. Ponad 70% firm wciąż „uczy się w biegu". Tymczasem właśnie na tym etapie można zatrzymać kryzys. Liczy się czas i świadomość. PR-owiec nie musi znać kodu źródłowego, ale musi rozpoznawać sygnały: skan z darknetu, opinię klienta, dziwny ruch w mediach czy przeciek do redakcji.

Etap II:

Orientacja – czy to już kryzys?

Nie każdy incydent techniczny oznacza kryzys medialny, ale każdy kryzys może zacząć się od incydentu. Kluczowe pytanie brzmi: kiedy sytuacja wymyka się spod kontroli? Z badań wynika, że mamy do czynienia z organizacjami dwóch prędkości. 38% posiada szczegółowy plan komunikacji kryzysowej, 23% działa według ogólnych schematów, a 38% w ogóle nie ma planu lub świadomości jego istnienia.

Faza orientacji to analiza i klasyfikacja: co się wydarzyło, jaka jest skala, czy dane wyciekły, czy media wiedzą, czy trzeba informować klientów i regulatorów. Nie ma tu miejsca na panikę, ale też na zwłokę. Najlepsze firmy podejmują decyzje w kilka minut, nie dni. Brak decyzji to również decyzja – zwykle najgorsza.

Etap III:

Decyzja – plan, który… jest

W kryzysie dobre decyzje rzadko zapadają ad hoc. Muszą wynikać z wcześniej przygotowanych scenariuszy, zasobów i zespołów. Nawet jeśli sytuacja jest rozpoznana, trzeba wiedzieć, co zrobić – a to często pięta achillesowa dużych organizacji.

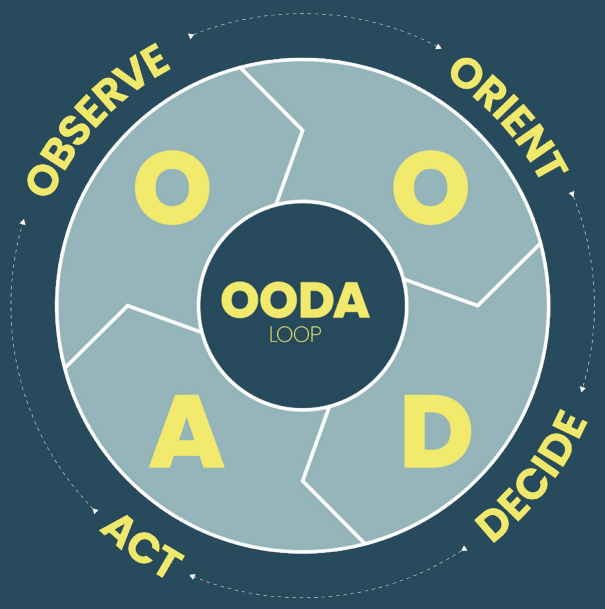
Badanie pokazuje, że największą barierą jest brak szybkiego dostępu do faktów (60%). Inne problemy to brak procedur, obawa o panikę klientów, presja mediów i konflikty między działami. Kryzys pokazuje, czy organizacja naprawdę współpracuje. Jeśli IT nie komunikuje się z PR-em, a compliance z działem prawnym, chaos jest nieunikniony. Dlatego tak ważne są scenariusze – przygotowane, zatwierdzone, przetestowane. W kryzysie nie ma czasu na pisanie planu – można go tylko uruchomić.

Etap IV:

Działaj – komunikacja jako narzędzie

Na tym etapie marka ma dwa wyjścia: mówić własnym głosem albo pozwolić innym przejąć narrację. Liczy się nie perfekcja, lecz prędkość, empatia i autentyczność. Zamiast mówić „analizujemy sytuację", trzeba jasno komunikować: „zostaliśmy zaatakowani, działamy, jesteśmy".

Najczęstsze błędy organizacji to milczenie, nadmiar technicznego żargonu i lakoniczne oświadczenia. Tymczasem właśnie teraz reputacja może zyskać – jeśli reakcja będzie szybka i wiarygodna. 94,9% respondentów badania podkreśla wagę współpracy między działami, a 87% – konieczność transparentności i szybkiej reakcji.



Postrzeganie ryzyka i przygotowanie organizacji

PYTANIE NR 1

Jak oceniasz ogólny poziom ryzyka reputacyjnego, który organizacja może ponieść w wyniku cyberzagrożeń (ataków hakerskich, wycieków danych, cyberprzestępczości)?

46% Bardzo wysokie

41% Wysokie

5% Średnie

Wniosek: Specjaliści i specjalistki ds. PR są świadomi istotnego wpływu cyberzagrożeń na wizerunek organizacji. Wynika to zarówno z rosnącej aktywności cyberprzestępców w przestrzeni wirtualnej, jak i z wysokiej wrażliwości mediów na tego rodzaju incydenty. Jednocześnie zwracają oni uwagę, że cyberzagrożenia wciąż pozostają stosunkowo nieprzebadanym obszarem wśród ryzyk wizerunkowych. W konsekwencji konieczne jest doskonalenie komunikacji między działami, wdrażanie skuteczniejszych procedur oraz systematyczne podnoszenie kompetencji poprzez szkolenia.

PYTANIE NR 2

Czy Twoja organizacja posiada scenariusz i plan zarządzania komunikacją kryzysową w kontekście cyberzagrożeń?

- **38%** Tak, posiadamy szczegółowy plan
- **23%** Tak, posiadamy plan ogólny, ale nie uwzględnia cyberzagrożeń
- **21%** Nie wiem
- **13%** Nie posiadamy planu, ale planujemy wprowadzić
- **5%** Nie posiadamy planu

Jakie cyberzagrożenia budzą największe obawy w kontekście reputacji organizacji?

Pytanie z wielokrotnym wyborem odpowiedzi

87,2%

Wyciek danych

Np. dane klientów, pracowników, dane finansowe

61,5%

Phishing

Próby wyłudzenia informacji w celu uzyskania dostępu do systemów

53,8%

Atak ransomware

Blokowanie dostępu do danych i żądanie okupu

48,7%

Ataki DDoS

Zakłócenie działalności organizacji poprzez zalanie systemów dużą ilością danych

43,6%

Deepfake

Fałszywe wideo lub audio przedstawiające organizację lub jej przedstawicieli

41%

Fake leaks

Np. rozpowszechnianie fałszywych informacji lub szkalowanie reputacji

Case study:

W marcu 2025 r. pojawiła się w darknecie baza rzekomo zawierająca dane 24 mln klientów Empiku, co wywołało falę nagłówków w największych mediach w Polsce. Empik szybko zareagował, analizując sprawę z CERT-em i jasno zakomunikował, że nie doszło do żadnego wycieku z jego systemów – ogłoszenie o sprzedaży „bazy Empiku" okazało się spreparowaną mieszanką starych i publicznych danych, a **żadnego włamania do systemów nie było.**

Case study:

W maju 2024 roku brytyjska firma inżynieryjna Arup padła ofiarą **oszustwa z wykorzystaniem technologii deepfake.** Pracownik biura w Hongkongu przekonany, że uczestniczy w wideokonferencji z członkami zarządu firmy, przelał łącznie 20 milionów funtów na konta przestępców. W rzeczywistości spotkanie zostało sfabrykowane – zarówno twarze, jak i głosy „uczestników" wygenerowano za pomocą sztucznej inteligencji. Arup zapewnia, że sytuacja nie wpłynęła na stabilność finansową firmy, a jej systemy informatyczne nie zostały naruszone. Mimo to przypadek ten wywołał ogromne poruszenie w branży – nie tylko ze względu na skalę strat, ale też zaawansowanie technologiczne przestępstwa.

Adam Sanocki

Członek Zarządu
Polskie Porty Lotnicze S.A.

Wyniki badania „Cyberzagrożenia a wizerunek organizacji" są potwierdzeniem obserwowanych trendów i sygnałem ostrzegawczym dla rynku. Cyberataki przestały być domeną IT – dziś to wyzwanie strategiczne i komunikacyjne. Obrona przed utratą zaufania wymaga nie tylko technologii, ale i jasno określonych procedur, treningów oraz kultury transparentności.

W Grupie PPL, strategicznej dla polskiego lotnictwa, gdzie pracuje 7500 osób, cyberbezpieczeństwo ma znaczenie kluczowe. Zmiany prawne zobowiążą zarządzających lotniskami i przewoźników do najwyższych standardów ochrony. Odpowiedzialność za infrastrukturę krytyczną nie pozostawia miejsca na błędy w ochronie danych czy zarządzaniu kryzysem.

W Polsce notuje się od kilku do kilkudziesięciu prób ataków na godzinę, zależnie od instytucji i aktywności cyberprzestępców. W takich warunkach kompromisy są niemożliwe.

Dziś już nie pytamy „czy", ale „kiedy" nasza organizacja stanie się celem ataku.

Aż 87% respondentów uznaje wyciek danych za poważne zagrożenie reputacyjne, a 46% ocenia poziom ryzyka jako bardzo wysoki. Nowym polem niepokoju są także deepfake (44%) i fake leaks (41%). W świecie, gdzie łatwo zmanipulować obraz i dźwięk, jeden materiał może wywołać spiralę kryzysową i zniszczyć zaufanie.

Organizacje najczęściej inwestują w procedury prawne i audyty (<50%). Tymczasem tylko 38% ma szczegółowy plan komunikacji kryzysowej, a zaledwie 28% regularnie prowadzi symulacje. To za mało, by mówić o odporności. Techniczne zabezpieczenia są fundamentem, ale o reputacji decyduje komunikacja. Każda złotówka na szkolenia i ćwiczenia to inwestycja w bezpieczeństwo.

Cyberbezpieczeństwo to dziś zadanie całej organizacji – od zarządu po pracowników. Skuteczna obrona wymaga technologii, procedur, treningów i kultury otwartości. Potrzebna jest współpraca IT, prawa i komunikacji, a także proaktywne podejście w świetle nowych regulacji (KSC, NIS2, DORA).

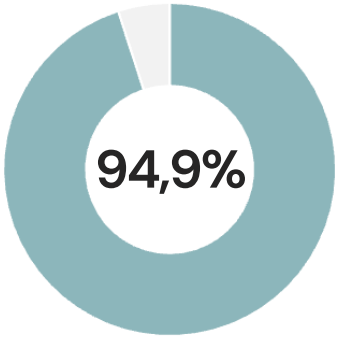
W Grupie PPL inwestujemy w technologię, procedury, szkolenia i monitoring. Cyberbezpieczeństwo i ochrona danych są filarami odpowiedzialnej cyfryzacji. Bo w erze cyfrowej nie istnieje podział na kryzysy technologiczne i wizerunkowe – to dwie strony tego samego medalu. Pytanie brzmi: czy jesteśmy gotowi na cyberkryzys nie tylko technicznie, ale i komunikacyjnie? Jeśli nie, czas najwyższy to zmienić.

Reakcja, komunikacja i doświadczenia organizacji

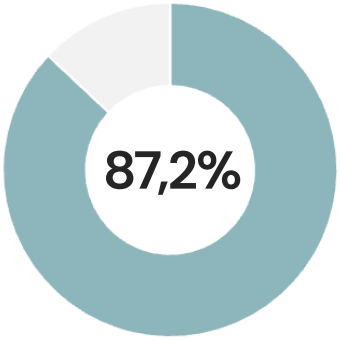
PYTANIE NR 4

Jakie aspekty komunikacji są kluczowe, gdy organizacja jest narażona na cyberzagrożenie lub atak?

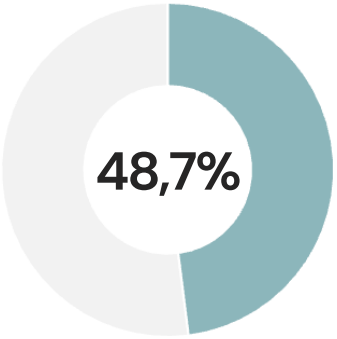
Pytanie z wielokrotnym wyborem odpowiedzi



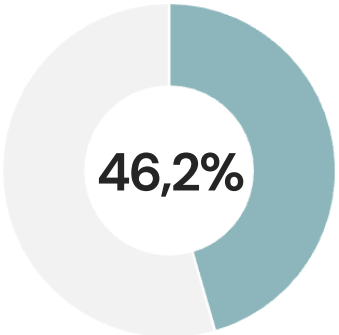
Współpraca wewnętrzna



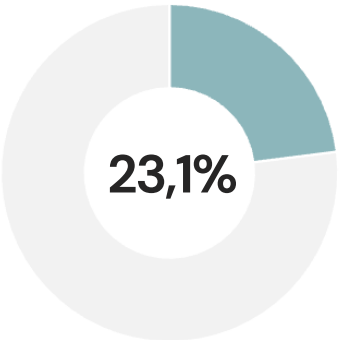
Transparentność



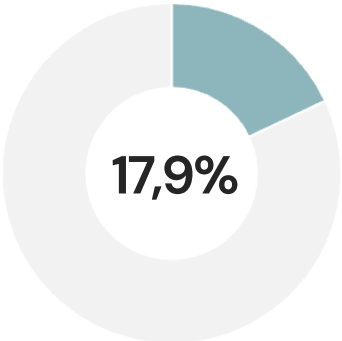
Wyznaczenie ekspertów



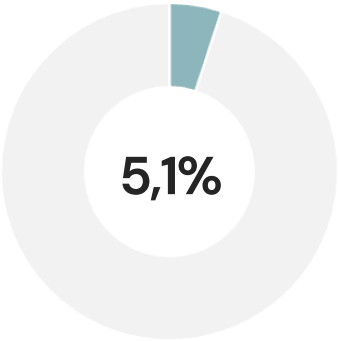
Aktualne informacje



Współpraca z mediami



Przeprosiny

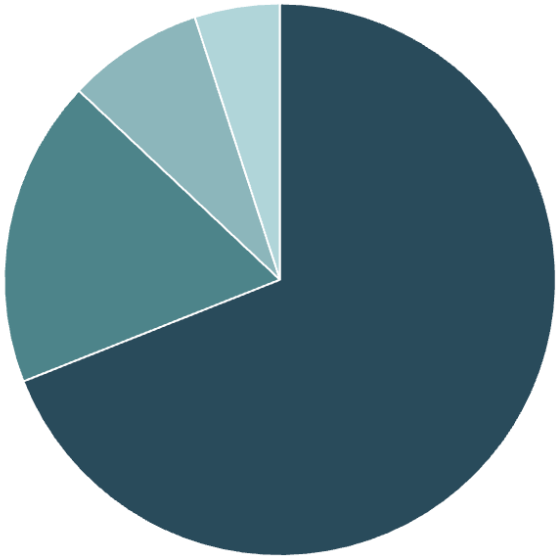


Inne

Wniosek: Cyberkryzysy charakteryzują się wysokim stopniem nieprzewidywalności – zarówno w zakresie momentu wystąpienia, skali konsekwencji, jak i potencjału dezinformacyjnego. W obliczu takich zagrożeń specjaliści PR podkreślają kluczową rolę współpracy wewnętrznej, transparentnej komunikacji oraz wsparcia ekspertów. Jakość przekazywanych informacji zależy przede wszystkim od zaangażowania odpowiednich osób i skutecznej koordynacji działań. Wąskim gardłem nie są same media, lecz wewnętrzne procesy organizacyjne i sposób ich funkcjonowania w sytuacjach kryzysowych.

PYTANIE NR 5

Jakie są najbardziej prawdopodobne konsekwencje dla wizerunku organizacji?



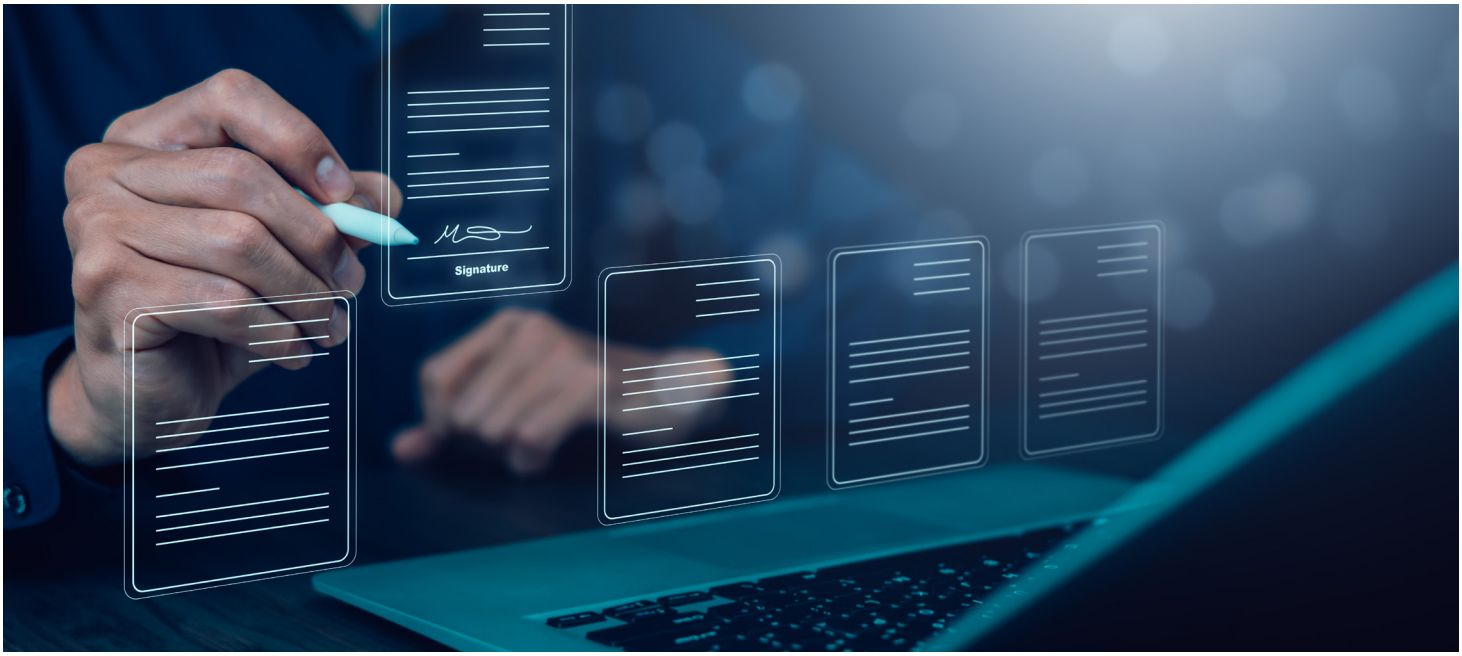
- **69,2%** Utrata zaufania klientów i partnerów biznesowych
- **17,9%** Długotrwałe skutki dla marki i wizerunku organizacji
- **7,7%** Zmniejszenie wartości rynkowej organizacji i spadek akcji
- **5,1%** Złożone problemy organizacyjne

Wniosek:

Z odpowiedzi respondentów wynika, że kluczową konsekwencją cyberkryzysów jest utrata zaufania klientów. Należy jednak pamiętać, że tego typu zdarzenia oddziałują także na szersze otoczenie organizacji – pracowników, dostawców, partnerów biznesowych, a także instytucje rządowe i branżowe. To często niedoceniane grupy interesariuszy, które w praktyce mogą mieć równie istotny, a niekiedy nawet większy wpływ na funkcjonowanie i stabilność organizacji.

Case study:

W styczniu 2025 r. EuroCert, **dostawca usług zaufania, padł ofiarą ataku ransomware** – cyberprzestępcy zaszyfrowali serwery i potencjalnie wykradli aż 65 GB danych klientów, pracowników i kontrahentów – w tym numery PESEL, numery dowodów tożsamości, adresy e-mail, numery telefonów, loginy i hasła. Chociaż EuroCert zapewnił, że sama infrastruktura certyfikatów oferowanych przez Eurocert nie została naruszona, musiał zmierzyć się przede wszystkim z utratą zaufania, czyli kapitału kluczowego w tej branży.



Anna Klimczuk

szefowa komunikacji
Microsoft w Europie Centralnej

Wyniki badania „Cyberzagrożenia a wizerunek organizacji" jednoznacznie pokazują, że zaufanie do marki staje się dziś jednym z najcenniejszych, ale i najbardziej kruchych aktywów organizacji. Aż 69% respondentów wskazuje utratę zaufania klientów i partnerów biznesowych jako najbardziej prawdopodobną konsekwencję cyberzagrożeń dla wizerunku firmy.

To nie przypadek - w świecie, w którym dane są walutą, a reputacja może runąć w ciągu kilku godzin, każda luka w zabezpieczeniach staje się potencjalnym zagrożeniem dla wiarygodności marki.

Specjaliści od cyberbezpieczeństwa mówią wprost – cyberprzestępcy już się nie włamują, oni się logują.

W tym kontekście szczególnie niepokojące jest to, że tylko 38% firm w Polsce posiada szczegółowy plan komunikacji kryzysowej na wypadek incydentu cybernetycznego. Jeszcze mniej – zaledwie 28% - przeprowadza symulacje scenariuszy kryzysowych, które są kluczowe dla sprawdzenia gotowości organizacji w praktyce.

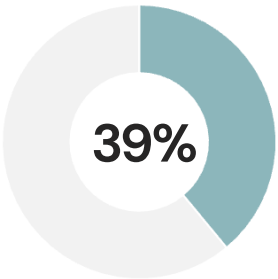
Badanie pokazuje, że skuteczna reakcja na cyberkryzys zaczyna się od wewnętrznej gotowości: jasno określonych ról, procedur, szybkiego dostępu do faktów i sprawnej współpracy między działami. Aż 95% respondentów wskazuje właśnie na współpracę wewnętrzną jako kluczowy aspekt komunikacji w sytuacji kryzysowej, a 87% na transparentność.

To pokazuje, że organizacje rozumieją wagę spójnej i szybkiej komunikacji, ale wciąż zbyt rzadko przekładają tę świadomość na konkretne działania.

W dobie kryzysu nie będzie czasu na improwizację ani miejsca na emocje. Dlatego tak ważne jest nie tylko posiadanie planu, ale także jego regularne ćwiczenie - tak, by w momencie zagrożenia zadziałać według wcześniej wytrenowanego schematu. Tylko wtedy możliwe jest skuteczne zarządzanie reputacją i ochrona zaufania, które - jak pokazuje badanie - jest najcenniejszym kapitałem organizacji.

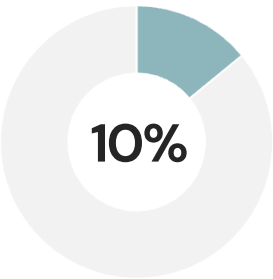
PYTANIE NR 6

Czy organizacja posiada procedury reagowania na przypadki związane z technologiami deepfake (np. fałszywe wideo lub audio wizerunkowe dotyczące firmy lub jej przedstawicieli)?



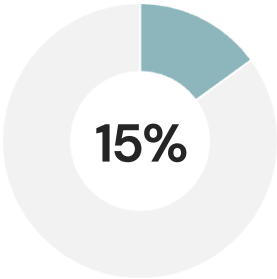
Tak

Posiadamy procedury, narzędzia i ludzi



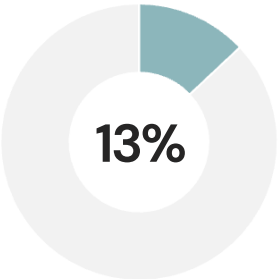
Tak, ale...

Ta procedury są w fazie opracowywania, ale...



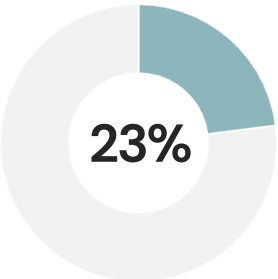
Nie, ale...

Planujemy stworzyć



Nie

...i nie planujemy ich wprowadzać



Nie wiem :(

PYTANIE NR 7

Co Twoim zdaniem najbardziej utrudnia skuteczne zarządzanie komunikacją w sytuacji cyberkryzysu?

Pytanie z wielokrotnym wyborem odpowiedzi

59%	**Brak dostępu do faktów**
43,6%	**Obawa przed paniką klientów**
41%	**Brak jasnych procedur wewnętrznych**
28,2%	**Brak spójności komunikacji między działami**
25,6%	**Presja mediów**
23,1%	**Bariery techniczne – brak narzędzi**
23,1%	**Presja mediów społecznościowych**
10,3%	**Presja prawników**

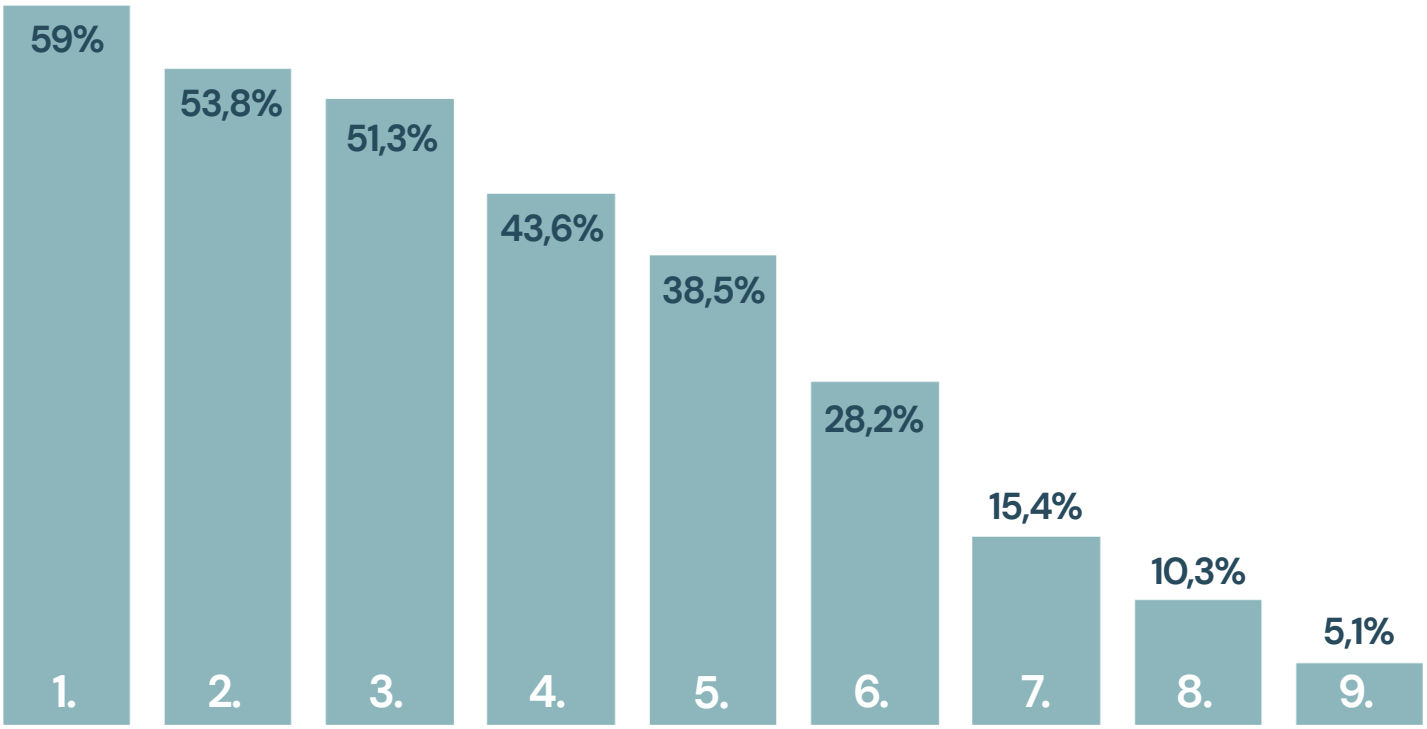
Wniosek:

Skuteczne zarządzanie kryzysem wymaga odpowiedniego przygotowania, obejmującego m.in. jasno określone struktury, zasady przepływu informacji oraz podział odpowiedzialności. Dzięki temu możliwy jest szybki dostęp do rzetelnych danych i właściwych osób, co w konsekwencji przekłada się na sprawność i spójność podejmowanych działań.

PYTANIE NR 8

Jakie działania prewencyjne organizacja podejmuje w celu zabezpieczenia się przed cyberzagrożeniami?

Pytanie z wielokrotnym wyborem odpowiedzi



1. **Procedury prawne i organizacyjne**
2. **Regularne audyty bezpieczeństwa i współpraca z ekspertami zewnętrznymi**
3. **Stały monitoring cyberprzestrzeni pod kątem zagrożeń, w tym deepfake**
4. **Szkolenia pracowników w zakresie komunikacji kryzysowej, cyberbezpieczeństwa**
5. **Przygotowanie strategii komunikacyjnych i procedur kryzysowych**
6. **Symulacje scenariuszy kryzysowych**
7. **Współpraca z firmami zajmującymi się weryfikacją tożsamości cyfrowej**
8. **Przekazywanie komunikatów o zabezpieczeniach firmowych w mediach społecznościowych i tradycyjnych**
9. **Brak działań prewencyjnych**

Wniosek:

Organizacje zwracają uwagę na podstawowe wymagania bezpieczeństwa, takie jak procedury prawne, czy audyty. Zdecydowanie mniejszy odsetek osób wskazał na istnienie procedur komunikacyjnych i prowadzenie praktycznych symulacji. Praktyka pokazuje, że to właśnie od procedur komunikacyjnych zależy faktyczna sprawność reakcji na kryzys.

Iwona Kruk

Communications Manager,
Central and Eastern Europe at Uber

Firmy w Polsce są coraz bardziej świadome zagrożeń cybernetycznych i ich natychmiastowych konsekwencji w postaci utraty zaufania do marki. Aż 69,2% ankietowanych uważa, że utrata zaufania klientów i partnerów biznesowych jest najbardziej prawdopodobną konsekwencją cyberzagrożeń. Ten wynik podkreśla, że zaufanie do marki jest postrzegane jako kwestia strategiczna.

Badanie ujawnia jednak znaczącą lukę w przygotowaniu organizacji. Podczas gdy firmy wdrażają podstawowe strategie zabezpieczeń, takie jak procedury prawne (59%) czy regularne audyty bezpieczeństwa (53,8%), to zaledwie 38% respondentów przyznało, że ich organizacje posiadają szczegółowy plan zarządzania komunikacją kryzysową w kontekście cyberzagrożeń. Pokazuje to, że firmy nie rozwijają równolegle strategii komunikacji kryzysowej, które są kluczowe w przypadku cyberkryzysu.

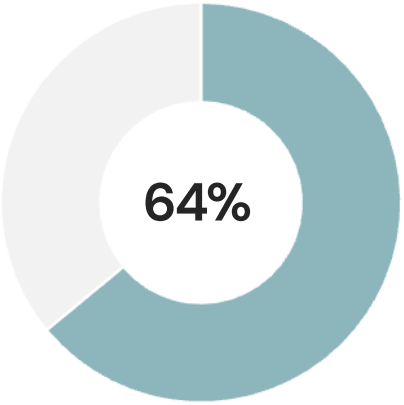
Jak w przypadku każdego kryzysu, transparentność i szybkość działania są kluczem do odbudowania zaufania. W przypadku cyberzagrożeń wiele firm myli brak transparentności z ochroną danych. Tymczasem w aspekcie komunikacyjnym zarówno media, partnerzy biznesowi, jak i odbiorcy końcowi muszą przede wszystkim wiedzieć, w jaki sposób firmy, którym powierzają swoje dane, zabezpieczają je, a w sytuacji kryzysowej – jak zamierzają je chronić. Skuteczne zarządzanie kryzysem komunikacyjnym jest utrudnione przez brak dostępu do faktów (59%) oraz brak jasnych procedur wewnętrznych (41%).

Innym kluczowym aspektem jest sposób komunikacji. Niestety, język często nie nadąża za tempem rozwoju cyberzagrożeń. Dlatego tak ważna jest ścisła współpraca z działami komunikacji, które potrafią przełożyć trudny język branżowy na prosty przekaz.

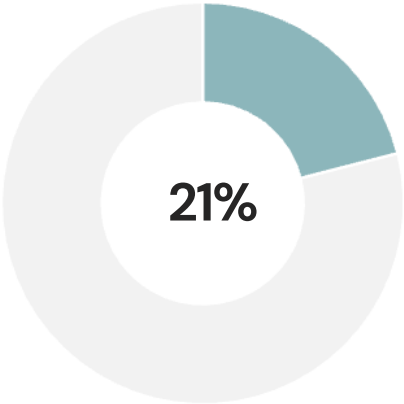
Dzięki temu, odbiorcy zrozumieją, co się wydarzyło, dlaczego jest to ważne i jak konkretna firma zadziałała na ich korzyść.

PYTANIE NR 9

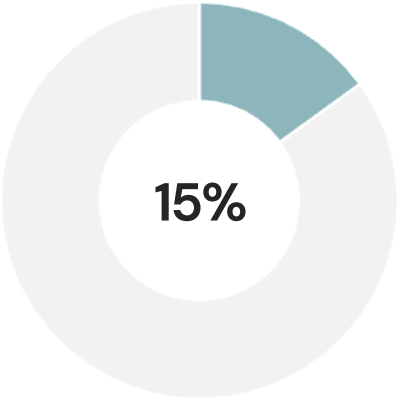
Czy w ostatnich 12 miesiącach Twoja organizacja doświadczyła sytuacji kryzysowej związanej z cyberbezpieczeństwem, która miała wpływ na reputację?



Nie



Tak



Nie wiem

Case study:

W marcu 2025 roku **szpital MSWiA w Krakowie padł ofiarą ataku ransomware**, który sparaliżował kluczowe systemy elektronicznej dokumentacji medycznej i administracyjnej. Pacjenci musieli być przyjmowani w trybie papierowym, część oddziałów wstrzymała przyjęcia. Dzięki wdrożeniu procedur awaryjnych i uruchomieniu tymczasowej infrastruktury, szpital utrzymał ciągłość działania. W sprawę zaangażowały się krajowe służby – CERT Polska, Centralne Biuro Zwalczania Cyberprzestępczości, Centrum e-Zdrowie, policja, Ministerstwo Zdrowia oraz Ministerstwo Cyfryzacji. Incydent pokazał, jak pilna jest potrzeba wzmocnienia zabezpieczeń w sektorze ochrony zdrowia – zarówno tych technologicznych, jak i proceduralnych.

Anna Olszewska

Dyrektorka Departamentu Komunikacji w KIR

Jeśli – będąc osobą odpowiedzialną za PR w swojej organizacji – myślisz, że kryzys wizerunkowy spowodowany cyberatakiem zagraża przede wszystkim firmom z obszarów powiązanych z technologią – pomyśl jeszcze raz.

Cyberzagrożenia dotyczą dziś każdego podmiotu – niezależnie od branży, profilu działalności, rozmiaru przedsiębiorstwa czy stopnia cyfryzacji. To realne ryzyko - w ciągu ostatnich 5 lat aż 88% firm w Polsce doświadczyło cyberataku lub wycieku danych. W II połowie 2024 r. Polska była drugim najczęściej atakowanym krajem na świecie, a liczba incydentów ransomware wzrosła o 37% (źródło: EY).

Ataki na systemy IT, rozwiązania umożliwiające obsługę procesów pracowniczych, prowadzenie księgowości czy zwykłą pocztę elektroniczną, mogą skutkować wyciekiem danych klientów, kradzieżą tożsamości, utratą krytycznych informacji biznesowych i paraliżem operacyjnym. Z danych publikowanych przez KIR w raporcie „Zaufanie w cyfrowym świecie. Kierunek: wiarygodność." wynika, że co trzeci menedżer w Polsce miał do czynienia z oszustwem dotyczącym dokumentów elektronicznych, otrzymując podrobione faktury, raporty finansowe czy nawet umowy. Celem przestępców są także systemy sterujące fizycznymi procesami (OT - Operational Technology), które mogą prowadzić do zatrzymania produkcji, skażenia leków czy odcięcia dostępu do wody.

Cyberprzestępcy, wykorzystując m.in. sztuczną inteligencję, aktywnie poszukują podmiotów, które mogą być łatwym celem – licząc na słabsze zabezpieczenia i szybszy dostęp do zasobów. Ich działania oznaczają poważne konsekwencje finansowe i reputacyjne, a straty mogą spowodować bankructwo wizerunkowe i rynkowe.

Dlatego odpowiedzialne prowadzenie biznesu w świecie, w którym nie da się pominąć rozwiązań cyfrowych, wymaga nie tylko wyboru sprawdzonych technologii i zaufanych dostawców, ale przede wszystkim świadomego podejścia do budowania odporności organizacji na każdym poziomie.

Zarządzanie wizerunkiem w obszarze cyberbezpieczeństwa jest dziś funkcją strategiczną. Wymaga wielopoziomowej współpracy wewnątrz organizacji, planowania z wyprzedzeniem - w tym opracowania scenariuszy kryzysowych, wdrożenia procedur uwierzytelniania, przeprowadzania symulacji, a także okresowej weryfikacji gotowości. Warto o to zadbać z wyprzedzeniem, bo dla każdej firmy wiarygodność jest kapitałem, który powinien podlegać szczególnej ochronie.

Aleksandra Andreasik-Binkowska

External Communications Leader Europe,
DXC Technology

Wyniki badania nie pozostawiają złudzeń: cyberzagrożenia to dziś jedno z najpoważniejszych wyzwań wizerunkowych, z jakimi mierzą się organizacje. Komunikacja kryzysowa przestaje być „opcją awaryjną" – staje się obowiązkowym elementem strategii reputacyjnej każdej świadomej firmy.

Choć świadomość zagrożeń rośnie, praktyka wciąż pozostaje w tyle. Wiele firm nie posiada gotowego scenariusza działania na wypadek cyberataku. W efekcie reagują dopiero wtedy, gdy sytuacja wymyka się spod kontroli – a w kryzysie informacyjnym czas działa na niekorzyść marki.

Na szczęście coraz więcej organizacji dostrzega znaczenie wewnętrznej współpracy i transparentności. To właśnie te elementy pozwalają zapanować nad chaosem, szybko zebrać fakty i komunikować się w sposób spójny i wiarygodny.

Niepokojące jest natomiast to, jak rzadko przeprowadza się realne ćwiczenia i symulacje. To one odsłaniają słabe punkty, pozwalają usprawnić procedury i przygotować zespół do działania pod presją. Bez takich testów organizacje działają w próżni – a to ryzyko, na które dziś nie można sobie pozwolić.

Cyberkryzys to nie hipotetyczny scenariusz – to kwestia czasu. To również test dojrzałości komunikacyjnej: na szybkość, spójność, odwagę i odpowiedzialność. Ci, którzy są gotowi, nie tylko przetrwają – mogą nawet zyskać. Bo dobrze poprowadzony kryzys buduje reputację równie skutecznie, jak ją ratuje.

Wytyczne dla skutecznej komunikacji w kryzysie

Reputacja stanowi fundament zaufania – zarówno w relacjach z klientami, pracownikami, dostawcami, inwestorami, mediami, jak i szeroko pojętym otoczeniem biznesowo-społecznym. Jak pokazują wyniki badania, w erze cyfrowej sama ochrona technologiczna, taka jak firewall, nie jest wystarczająca. Niezbędne jest także posiadanie planu, zespołu oraz narzędzi umożliwiających bieżącą i skuteczną komunikację. Dlatego kluczowe znaczenie ma przygotowanie organizacji na sytuacje cyberkryzysowe poprzez jasno określone zasady działania, sprawdzoną współpracę między działami oraz wysokie kompetencje zespołów komunikacyjnych.

Podstawowe wytyczne:

1. Wprowadź system wczesnego ostrzegania przed cyberzagrożeniami.
2. Zintegruj IT i komunikację – ustal jasne procedury przekazywania informacji.
3. Twórz proste i realistyczne plany kryzysowe – aktualizuj je systematycznie.
4. Zapewnij pełną koordynację działań – powołaj zespół kryzysowy, określ jego odpowiedzialności i regularnie testuj procedury.
5. Udrożnij i utrzymuj kanały komunikacji wewnętrznej – sprawdzaj ich skuteczność w symulacjach.
6. Mapuj interesariuszy – komunikuj się nie tylko z mediami, ale także z regulatorami, dostawcami, partnerami i kluczowym otoczeniem.
7. Prowadź regularne szkolenia i ćwiczenia prewencyjne.
8. Monitoruj i neutralizuj dezinformację – nie dopuść do utraty kontroli nad przekazem.
9. Podnoś świadomość całej organizacji – edukuj zespół w zakresie cyberzagrożeń.
10. Analizuj każdy kryzys – wyciągaj wnioski i ucz się przede wszystkim na cudzych błędach.

O dfusion communication

Agencja stworzona w cyfrowych czasach, odpowiadająca na wyzwania komunikacyjne przyszłości.

Innowacyjność stanowi dla nas szczególną wartość. Dotyczy nie tylko kreatywnego podejścia do realizowanych projektów, ale również skutecznego komunikowania nowoczesnych rozwiązań, usług i produktów. Konsultujemy to, by w optymalny sposób łączyć instytucje publiczne w ich skutecznej komunikacji z otoczeniem. Jesteśmy partnerem w kreowaniu i realizacji strategii komunikacyjnych: od działań z zakresu Public Relations, Customer Relations i Digital Communication. Budujemy efektywne relacje, które dają wartość naszym klientom.

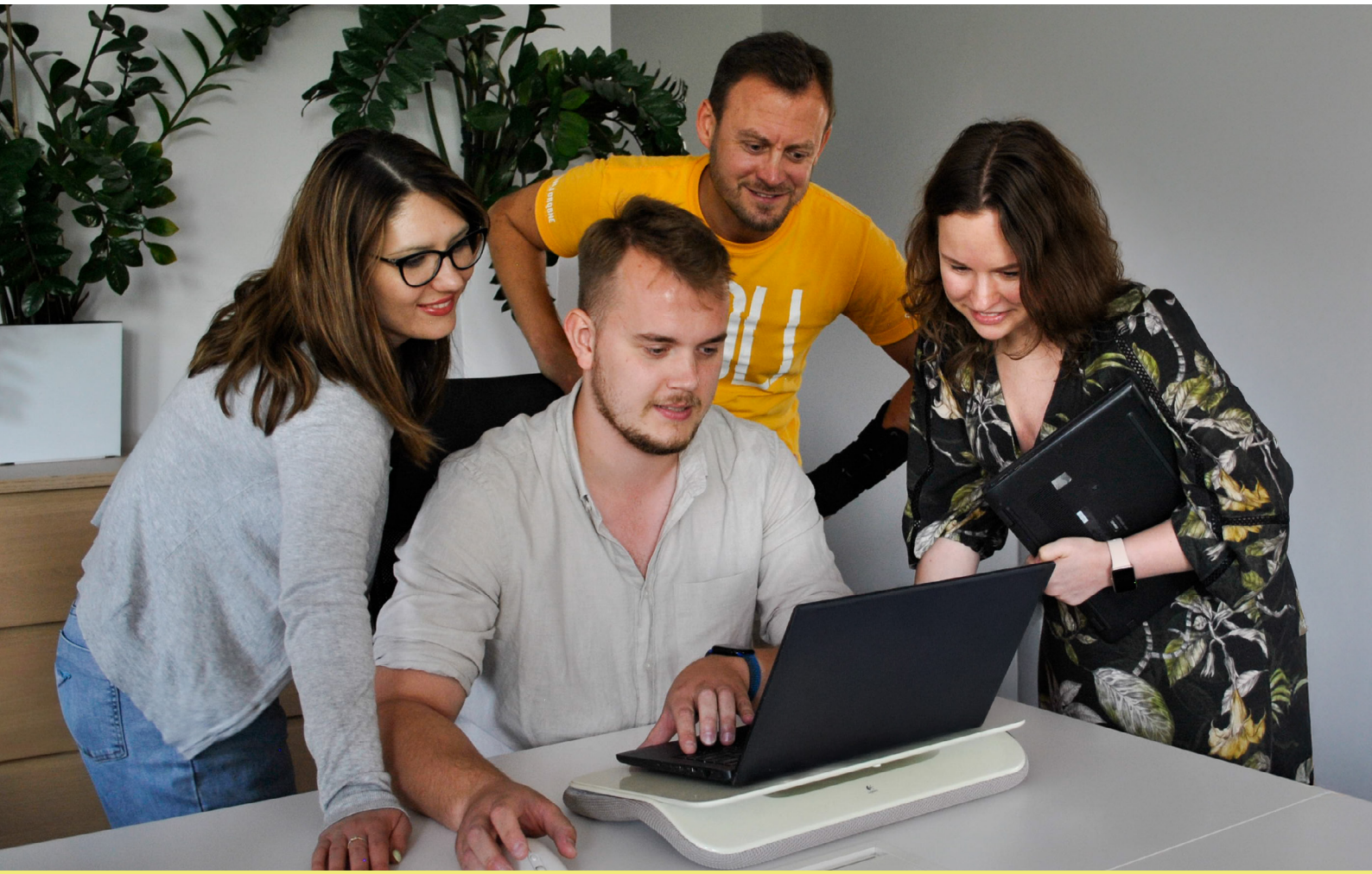
O badaniu

Metodologia badania

Badanie zostało przeprowadzone wśród specjalistek i specjalistów komunikacji oraz marketingu działających na rynku polskim. Wzięło w nim udział 55 respondentów (N=55).

Autorzy raportu

Aleksandra Huścia, Senior Account Manager
Łukasz Malczewski, Managing Partner



Zapraszamy do kontaktu!

e-mail: kontakt@dfusion.pl
tel: 22 403 57 99

www.dfusion.pl