Raport z badania

Prewencja szkodowa w polskich przedsiębiorstwach

HOWDEN

Podziękowania

Autorzy pragną podziękować wszystkim respondentom, którzy wzięli udział w badaniu, dzieląc się swoim doświadczeniem i wiedzą na temat prewencji szkodowej.

Szczególne podziękowania kierujemy do przedstawicieli firm produkcyjnych, usługowych oraz handlowych, którzy poświęcili swój czas na wypełnienie ankiety.

Dziękujemy również partnerom projektu:
- Howden Polska S.A.
- Akademii Leona Koźmińskiego w Warszawie

Za wsparcie w realizacji badania i cenną wymianę doświadczeń dziękujemy ekspertom z wiodących firm ubezpieczeniowych oraz towarzystw reasekuracyjnych działających na polskim rynku.

Zaangażowanie wszystkich stron nie oznacza automatycznej akceptacji wszystkich wniosków i rekomendacji zawartych w niniejszym raporcie.

Dziękujemy także recenzentom: Mec. Annie Tarasiuk, Marcinowi Janickiemu i Dariuszowi Fuchs za bezcenne uwagi, które przyczyniły się do wartości merytorycznej Raportu.

Dr hab. Katarzyna Malinowska, Profesor ALK
Jarosław Sepioło, Howden Polska

Streszczenie

Główne obserwacje

Wyniki badania wskazują na rosnące zainteresowanie prewencją szkodową w polskich przedsiębiorstwach, jednocześnie ujawniając istotne luki między świadomością a systematycznym wdrażaniem najlepszych praktyk.

Świadomość i podejście strategiczne

Pozytywny sygnał: Zdecydowana większość badanych firm (81%) uznaje prewencję za część strategii zarządzania ryzykiem. To znacząca zmiana w porównaniu z dekadą temu, kiedy prewencja była często postrzegana jako opcjonalny dodatek do ubezpieczenia.

Obszar do poprawy: Mimo wysokiej świadomości, tylko 52% firm posiada dedykowany budżet na prewencję, a 48% analizuje skuteczność podejmowanych działań w sposób cykliczny. Oznacza to, że deklaracje strategiczne nie zawsze przekładają się na systematyczne działania operacyjne.

Obszary prewencji – priorytety polskich firm

Ranking kluczowych obszarów prewencji wyraźnie wskazuje na zmieniający się krajobraz ryzyka:

- **Cyberbezpieczeństwo (81%)** – bezsprzecznie dominujący obszar zainteresowania
- **Prewencja pożarowa (67%)** – tradycyjnie istotna, wciąż wysoko na liście priorytetów
- **Zgodność z wymogami prawnymi (67%)** – rosnące znaczenie compliance
- **BHP (57%)** – fundamentalny obszar odpowiedzialności pracodawcy
- **Awarie techniczne (48%)** – ważne szczególnie dla sektora produkcyjnego

Interesujące jest, że odpowiedzialność cywilna jako obszar prewencji została wymieniona stosunkowo rzadko (10%), mimo że stanowi jeden z najważniejszych obszarów ubezpieczeniowych. Może to sugerować, że firmy traktują OC bardziej jako konieczność prawną niż obszar do aktywnego zarządzania ryzykiem.

Percepcja kosztów vs korzyści prewencji szkód

- 57% respondentów zdecydowanie zgadza się, że prewencja się opłaca, a tylko 5% wyraża wątpliwości. To bardzo pozytywny sygnał wskazujący na dojrzałość rynku.
- Jednocześnie:
- 43% firm traktuje prewencję jako element budowania przewagi konkurencyjnej
- 38% firm podejmuje decyzje o zaprzestaniu prewencji z powodu kosztów
- 33% zauważa tendencję do przechodzenia od szkód spektakularnych do częstych, mniejszych incydentów

To pokazuje, że chociaż korzyści są dostrzegane, presja kosztowa wciąż stanowi istotną barierę.

Kluczowe bariery wdrażania prewencji

Respondenci wskazali następujące główne przeszkody:

- **Brak świadomości** (38%) – mimo ogólnego zrozumienia wartości prewencji, szczegółowa wiedza o dostępnych rozwiązaniach jest ograniczona
- **Brak czasu** (24%) – operacyjne wyzwania przysłaniają działania długoterminowe
- **Brak danych** (24%) – trudność w udowodnieniu ROI bez rzetelnej analityki
- **Brak budżetu** (14%) – choć nie jest to główna bariera, wciąż stanowi istotne ograniczenie

Współpraca z ubezpieczycielami – niewykorzystany potencjał

Wyniki badania ujawniają znaczącą lukę między ofertą a wykorzystaniem wsparcia ubezpieczycieli:

- 67% brokerów deklaruje możliwość wsparcia w działaniach prewencyjnych
- 71% ubezpieczycieli twierdzi, że może uczestniczyć w doradztwie prewencyjnym
- Ale tylko 48% firm faktycznie korzysta z takiego wsparcia

To pokazuje, że komunikacja między ubezpieczycielami, a klientami wymaga poprawy. Firmy nie zawsze wiedzą, jakiego wsparcia mogą oczekiwać, a ubezpieczyciele nie zawsze skutecznie promują swoje możliwości analityczne i doradcze.

Pozytywny sygnał: 52% firm uważa, że ubezpieczyciele mogliby w większym stopniu wspierać działania prewencyjne, co wskazuje na otwartość na głębszą współpracę.

Pomiar skuteczności – kluczowa luka

- Jedynie 48% firm prowadzi cykliczne analizy skuteczności prewencji, co oznacza, że ponad połowa organizacji działa "po omacku", bez systematycznej oceny efektywności podejmowanych działań.

Firmy, które regularnie mierzą skuteczność, wykorzystują różne podejścia:

- Liczba szkód/incydentów (36%) – najpopularniejsza metryka
- Przestoje (13%) – szczególnie istotne w produkcji
- Wpływ na wyniki finansowe (23%) – próba bezpośredniego powiązania z cash-flow lub EBITDA
- Składka ubezpieczeniowa (23%) – używana jako proxy efektywności prewencji

Brak systematycznego pomiaru utrudnia uzasadnienie dalszych inwestycji w prewencję i przekonanie zarządu o jej wartości.

Odpowiedzialność i zasoby

Kluczowym czynnikiem skutecznej prewencji jest jasno określona odpowiedzialność:
- 39% firm wskazuje zarząd jako odpowiedzialny za planowanie prewencji
- 32% firm przypisuje tę rolę działom operacyjnym
- 21% firm wskazuje dział finansowy

Interesujące, że tylko 7% firm ma zewnętrznego doradcę odpowiedzialnego za prewencję, co sugeruje, że większość organizacji woli zarządzać tym obszarem wewnętrznie.

Wprowadzenie: Prewencja ryzyka jako funkcja ubezpieczeń

Ubezpieczenia są tradycyjnie formą zarządzania ryzykiem, ale ich funkcja zawsze wykraczała poza aspekty czysto kompensacyjne. Jedną z pomocniczych, ale ważną funkcji ubezpieczeń było zawsze także zapobieganie ryzyku, Jest to bez wątpienia najbardziej racjonalna metoda kontroli strat.

Nowoczesne podejście do ubezpieczeń kładzie nacisk na prewencję, tj. działania mające na celu:
- Zmniejszenie prawdopodobieństwa wystąpienia zdarzenia
- Ograniczenie potencjalnej wielkości skali szkody
- Przyspieszenie powrotu do normalnego funkcjonowania
- Nauka ubezpieczeniowa wskazuje nawet na dwie podstawowe, ale równorzędne funkcje ubezpieczeń - kompensacyjną i prewencyjną.

Funkcja prewencyjna ubezpieczeń zależy od kultury ubezpieczeniowej, warunków społeczno-gospodarczych, czy też wymogów prawnych. Staje się ona również czynnikiem walki konkurencyjnej na rynku ubezpieczeniowym.

Zdaniem ekspertów prowadzenie działalności ubezpieczeniowej bez prewencji byłoby nieopłacalne, a ponadto dzięki prewencji proces likwidacji szkód przez ubezpieczyciela może stać się bardziej zrównoważony.

Znaczenie funkcji prewencyjnej wynika jednak nie tylko z czynników konkurencyjnych, rynkowych, ale także ze społecznej roli, jaką odgrywają ubezpieczenia. Mogą one uzupełniać społeczną i organizacyjną rolę, jaką odgrywają państwa, zwłaszcza w zakresie ryzyk katastroficznych. I choć prewencja ubezpieczeniowa przynosi potencjalnie oczywiste korzyści dla samych ubezpieczonych, to jednak istniejące ubezpieczenie potencjalnie wpływa na pokusę nadużycia.

Działania prewencyjne ubezpieczyciela mają ją eliminować lub ograniczać. Prowadzi to do przekonania, że aspekt prewencji w działalności ubezpieczycieli powinien być obowiązkowy, a nie tylko wynikać z dobrej woli ubezpieczyciela, czy opłacalności danego modelu biznesowego.

Przez prewencję możemy rozumieć zarówno środki, które mają na celu uniknięcie materializacji ryzyka, które nazywane są również "środkami ostrożności", jak i zapobieganie lub zmniejszanie skutków wypadku ubezpieczeniowego (łagodzenie strat).

Prewencja ryzyka ma na celu systematyczne zmniejszanie prawdopodobieństwa wystąpienia ryzyka, przy czym mając na uwadze definicję ryzyka, może ona działać na oba elementy ryzyka, tj. prawdopodobieństwo i skutki zdarzenia.
Metody zapobiegania ryzyku obejmują wszystkie techniki i praktyki zarządzania, które pomagają zapobiegać wystąpieniu zdarzenia losowego.

Skutki prewencyjne można osiągnąć za pomocą kształtowania prawa, tak aby zawierało ono normy zachęcające społeczeństwo, w tym przedsiębiorców do zapobiegania zdarzeniom losowym i ograniczania strat. Może to odbywać się poprzez nakładanie konsekwencji prawnych w przypadku, gdy określone zachowanie prowadzi do powstania lub zwiększenia szkody lub zaniechania zapobiegania zdarzeniom losowym. Do ogólnych form prewencji należą warunki ubezpieczenia zawierające różnego rodzaju zapewnienia, wyłączenia odpowiedzialności ubezpieczyciela, czy też przewidujące regres ubezpieczeniowy, franszyzy lub systemy malus-bonus.

Dla kogo prewencja ma znaczenie?

Skuteczna prewencja szkodowa przynosi wymierne korzyści nie tylko pojedynczym organizacjom, ale całemu ekosystemowi gospodarczemu i społecznemu. Jej wartość można rozpatrywać z perspektywy trzech kluczowych grup interesariuszy.

Dla przedsiębiorstw prewencja stanowi źródło bezpośrednich korzyści finansowych i strategicznych. Po pierwsze, systematyczne działania prewencyjne przekładają się na niższe składki ubezpieczeniowe lub ubezpieczalność – ubezpieczyciele coraz częściej nagradzają proaktywne podejście do zarządzania ryzykiem rabatami sięgającymi nawet 20-30% wartości polisy.

Po drugie, mniejsze straty operacyjne wynikające z rzadszych i mniej dotkliwych incydentów bezpośrednio poprawiają rentowność działalności.

Po trzecie, firmy znane z wysokich standardów bezpieczeństwa budują lepszą reputację i wiarygodność w oczach klientów, partnerów biznesowych oraz instytucji finansowych.

Coraz częściej certyfikaty bezpieczeństwa stają się warunkiem dostępu do przetargów publicznych czy kredytów na preferencyjnych warunkach.

Po czwarte, dojrzałe podejście do prewencji staje się wymierną przewagą konkurencyjną – pozwala wyróżnić się na tle konkurencji i zdobyć zaufanie wymagających klientów.

Wreszcie, skuteczna prewencja zapewnia ciągłość działania nawet w obliczu kryzysów, co w dzisiejszym turbulentnym środowisku biznesowym może decydować o przetrwaniu firmy.

Z perspektywy ubezpieczycieli prewencja jest fundamentem zrównoważonego modelu biznesowego. Klienci inwestujący w prewencję generują niższy współczynnik szkodowości, co bezpośrednio przekłada się na rentowność portfela ubezpieczeniowego. Stabilniejsze portfele, w których przewidywalność ryzyka jest wyższa, pozwalają ubezpieczycielom na lepsze zarządzanie kapitałem własnym i wymogami solwencyjnymi.

Współpraca w zakresie prewencji buduje długoterminowe relacje z klientami oparte na partnerstwie, a nie jedynie transakcyjnej sprzedaży polis – tacy klienci rzadziej zmieniają ubezpieczycieli i są mniej wrażliwi cenowo.

Wreszcie, niższa szkodowość w portfelu daje ubezpieczycielom możliwość oferowania konkurencyjnych stawek, co zwiększa ich atrakcyjność rynkową i pozwala pozyskiwać nowych klientów bez prowadzenia wojny cenowej osłabiającej wyniki finansowe.

Dla społeczeństwa jako całości prewencja generuje pozytywne efekty zewnętrzne o fundamentalnym znaczeniu.

Bezpieczniejsze miejsca pracy oznaczają mniej wypadków, chorób zawodowych i związanych z nimi tragedii osobistych oraz kosztów społecznych. Skuteczna prewencja środowiskowa – od zabezpieczeń przed wyciekami substancji niebezpiecznych po systemy wczesnego ostrzegania przed pożarami – chroni ekosystemy i zdrowie publiczne.

Stabilność ekonomiczna całych regionów i sektorów zależy od odporności kluczowych przedsiębiorstw – ich zdolność do uniknięcia katastrof lub szybkiego powrotu do działalności chroni miejsca pracy i lokalne gospodarki.

Wreszcie, systematyczna prewencja ogranicza skutki katastrof naturalnych i technologicznych, które mogłyby w przeciwnym razie pochłonąć ogromne środki publiczne przeznaczone na pomoc poszkodowanym i odbudowę infrastruktury.

W ten sposób inwestycje prywatne w prewencję chronią finanse publiczne i umożliwiają lepsze wykorzystanie ograniczonych zasobów państwa.

Prewencja tworzy zatem pozytywne sprzężenie zwrotne: przedsiębiorstwa zyskują konkurencyjność, ubezpieczyciele stabilność, a społeczeństwo bezpieczeństwo i dobrobyt. To sytuacja win-win-win, która uzasadnia wspólne zaangażowanie wszystkich stron w budowanie kultury proaktywnego zarządzania ryzykiem.

Korzyści prewencji:
wielowymiarowa wartość dla organizacji

Korzyści finansowe

- Niższe składki ubezpieczeniowe
- Lepsze warunki ubezpieczenia
- Łatwiejszy dostęp do finansowania

Korzyści strategiczne

- Lepsza reputacja i zaufanie
- Przewaga w przetargach
- Wyższa wycena firmy
- Łatwiejsze spełnianie wymogów ESG

Korzyści operacyjne

- Mniejsze przerwy w produkcji
- Wyższa efektywność (OEE)
- Wyższe morale pracowników
- Łatwiejsze zarządzanie łańcuchem dostaw

Kluczowy wniosek

Prewencja to nie koszt, lecz inwestycja o wielowymiarowym zwrocie – od bezpośrednich oszczędności finansowych, przez poprawę efektywności operacyjnej, aż po strategiczne korzyści reputacyjne i dostęp do kapitału.

Organizacje rozumiejące tę kompleksową wartość są lepiej przygotowane do konkurowania w niepewnym otoczeniu biznesowym.

Nowe technologie a prewencja

Wiele ryzyk, które jeszcze dekadę temu były nieubezpieczalne lub ekstremalnie drogie, stało się dostępne dzięki przełomowym technologiom prewencyjnym. Technologia umożliwia demokratyzację zaawansowanej prewencji – to, co jeszcze 5 lat temu było dostępne tylko dla korporacji, dziś może mieć mała firma. Organizacje, które zainwestują w ten ekosystem dziś, będą liderami jutro.

Obszar ryzyka	Technologia umożliwiająca	Efekt
Cyberbezpieczeństwo	SIEM, AI/ML, threat intelligence	Wykrywanie zagrożeń w czasie rzeczywistym
Mienie i nieruchomości	IoT (czujniki wycieku, smart smoke detectors)	Natychmiastowe alerty, automatyczna reakcja
Ryzyko klimatyczne i rolnicze	Dane satelitarne, geolokalizacja, prognozy pogody	Precyzyjne przewidywanie i ostrzeganie
Zdrowie i życie	Wearables, telemedicine, AI diagnostics	Profilaktyka zamiast leczenia

Od aplikacji do ekosystemów prewencyjnych. Nowa generacja narzędzi komunikacyjnych zmienia relację ubezpieczyciel-klient:

Wczoraj

- Statyczna polisa wystawiona raz w roku
- Kontakt tylko przy szkodzie
- Brak informacji zwrotnej o ryzyku

Dziś

- Aplikacje mobilne z real-time alertami o zagrożeniach
- Smart devices monitorujące ryzyko 24/7 (czujniki wody, dymu, temperatury)
- Pakiety prewencyjne – ubezpieczyciele dostarczają urządzenia IoT jako część polisy
- Zniżki składki – za instalację smart devices i udostępnienie danych

Przyszłość: Od składki do abonamentu za bezpieczeństwo

Tradycyjny model

Klient płaci składkę → otrzymuje odszkodowanie po szkodzie

Nowy model (Prevention-as-a-Service):

Klient płaci abonament → otrzymuje:

- Ochronę ubezpieczeniową
- Monitoring ryzyka w czasie rzeczywistym
- Przewidywanie zagrożeń (AI/ML)
- Wsparcie w zapobieganiu (konsultacje, audyty, narzędzia)
- Technologie prewencyjne (IoT, aplikacje)

Kluczowy wniosek

Przyszłość ubezpieczeń to nie pytanie "ile zapłacisz za odszkodowanie", ale "jak razem zapobiegniemy szkodzie".

Filary skutecznej prewencji

Opierając się na najlepszych praktykach globalnych oraz doświadczeniach sektora ubezpieczeniowego, wyróżniamy cztery kluczowe filary, które łącznie determinują skuteczność programów prewencyjnych, który opiera się o model drabiny Hudsona, który rozpoczął swoją karierę w obszarze bezpieczeństwa po katastrofie platformy Piper Alpha w 1988 roku, stworzył teoretyczny model znany jako Drabina Bezpieczeństwa Hudsona (Hudson Safety Ladder), który obrazuje ewolucyjną ścieżkę rozwoju kultury bezpieczeństwa w organizacji.

Opierając się na najlepszych praktykach globalnych oraz doświadczeniach sektora ubezpieczeniowego, wyróżniamy cztery kluczowe filary, które łącznie determinują skuteczność programów prewencyjnych, który opiera się o model drabiny Hudsona, który rozpoczął swoją karierę w obszarze bezpieczeństwa po katastrofie platformy Piper Alpha w 1988 roku, stworzył teoretyczny model znany jako Drabina Bezpieczeństwa Hudsona (Hudson Safety Ladder), który obrazuje ewolucyjną ścieżkę rozwoju kultury bezpieczeństwa w organizacji.

Model Hudsona powstał w odpowiedzi na powtarzające się pytanie: dlaczego dochodzi do poważnych wypadków przemysłowych, mimo istnienia przepisów, procedur i systemów zarządzania bezpieczeństwem? Analiza katastrof takich jak wybuch platformy Piper Alpha (167 ofiar śmiertelnych w 1988 roku) czy późniejszych incydentów w przemyśle naftowym, chemicznym i morskim doprowadziła Hudsona do kluczowego wniosku: niewłaściwa kultura bezpieczeństwa jest zawsze podstawową przyczyną wypadków.

Pięć wymiarów kultury bezpieczeństwa według Hudsona

Przywództwo

- Silne przywództwo wyznacza ton dla całej organizacji
- Liderzy przewodzą własnym przykładem
- Demonstrowanie zaangażowania w bezpieczeństwo
- Nie wystarczą deklaracje – pracownicy obserwują, czy menedżerowie sami przestrzegają zasad

Szacunek

- Wszyscy traktowani z szacunkiem przy zgłaszaniu kwestii bezpieczeństwa
- Kultura zaufania bez lęku przed karami
- Komfortowe zgłaszanie błędów i near-miss niezależnie od pozycji w hierarchii

Uważność

- Świadomość potencjalnych zagrożeń
- Ciągła czujność i gotowość na nieoczekiwane
- Przeciwdziałanie rutynie usypiającej uwagę
- Aktywne poszukiwanie sygnałów ostrzegawczych

Sprawiedliwość

- Jasne granice między zachowaniem akceptowalnym a nieakceptowalnym
- Kultura odpowiedzialności
- Kluczowe rozróżnienie:
  Błędy z omylności = okazja do nauki i świadome lekceważenie = konsekwencje

Uczenie się

- Gotowość do adaptacji i reform
- Zachęta do zgłaszania błędów i incydentów
- Wykorzystanie zdarzeń jako okazji do nauki
- Ciągłe doskonalenie systemów

Pięć szczebli Drabiny Bezpieczeństwa

Model Hudsona przedstawia rozwój kultury bezpieczeństwa jako ewolucyjną drabinę składającą się z pięciu poziomów. Kluczowym założeniem jest, że im wyżej na drabinie, tym większe zaufanie i dzielenie się informacją w organizacji. Poziomy te można bezpośrednio przełożyć na kontekst prewencji szkodowej w ubezpieczeniach:

Poziom	Charakterystyka	Prewencja szkodowa
PATOLOGICZNY **"Kogo to obchodzi, dopóki nas nie złapią"**	• Brak inwestycji w bezpieczeństwo • Ignorowanie lub ukrywanie problemów • Bezpieczeństwo jako przeszkoda w biznesie • Regulacje = uciążliwy obowiązek	• Całkowity brak prewencji • Reakcja tylko pod presją (kontrola, kara) • Brak działań wyprzedzających
REAKTYWNY **"Bezpieczeństwo jest ważne, robimy dużo po każdym wypadku"**	• Tryb "gaszenia pożarów" • Działania dopiero po incydencie • Dochodzenia i wnioski post factum • Brak systematycznego podejścia	• Prewencja po szkodzie • Ubezpieczenie kupowane po pierwszej stracie • Limity zwiększane po ich wyczerpaniu
KALKULATYWNY **"Mamy systemy do zarządzania wszystkimi zagrożeniami"**	• Formalne systemy (ISO, procedury) • Szkolenia i audyty • Motywacja: unikanie kar, niższe składki • Kontrola i egzekwowanie • Brak głębokiego zaangażowania	• Programy prewencyjne istnieją • Postrzegane jako oddzielna funkcja • Niezintegrowane z operacjami • Driven by compliance
PROAKTYWNY **"Pracujemy nad problemami, które wciąż znajdujemy"**	• Wysoki priorytet bezpieczeństwa • Aktywne poszukiwanie zagrożeń • Zachęta do zgłaszania near-miss • Analiza trendów i benchmarking • Ciągłe ulepszenia	• Zaawansowana prewencja • Predykcyjna analityka • Predykcyjne utrzymanie ruchu • Współpraca z ubezpieczycielem • Każdy incident = lekcja
GENERATYWNY **"Bezpieczeństwo to sposób, w jaki prowadzimy biznes"**	• Pełna integracja z operacjami • Zakorzenione w zachowaniach • Nie kontrola, lecz przekonanie • Odpowiedzialność za siebie i innych • Źródło dumy i tożsamości	• Kultura prewencyjna • Każdy myśli kategoriami ryzyka • Innowacje "od dołu" • Prewencja w każdej decyzji • Spontaniczne, nie narzucane

Gdzie są polskie firmy?

Wyniki badania:
większość firm na poziomie 2-3,
z potencjałem do poziom 4.

Poziom 2 (reaktywny)

- 48% bez budżetu, działania post factum

Poziom 3 (kalkulatywny)

- 81% deklaruje strategię, ale tylko 48% mierzy skuteczność

Poziom 4 (proaktywny)

- 52% z budżetem i systematyczną analizą

Im wyżej na drabinie → tym większe zaufanie i przepływ informacji → tym skuteczniejsza prewencja.

Studium przypadku:

Skuteczna prewencja w praktyce zarządzania ryzykiem pożarowym w przedsiębiorstwach produkcyjnych

Autor: Damian Mikułan, Kierownik Działu Bezpieczeństwa Procesów, Tanne Sp. z o.o.

Wprowadzenie

W zakładach produkcyjnych, szczególnie tam, gdzie procesy są szybkie, a instalacje skomplikowane, prewencja przeciwpożarowa jest jednym z kluczowych elementów bezpieczeństwa. Choć często mówi się, że trudno ją zmierzyć lub policzyć jej realny zwrot z inwestycji, praktyka pokazuje coś odwrotnego. Analizy zdarzeń i doświadczenie zawodowe jasno dowodzą, że istnieje jeden czynnik wspólny dla wszystkich działań prewencyjnych: czas reakcji. To właśnie czas decyduje o tym, jak rozwinie się zagrożenie, ile będzie kosztować przestój i czy szkoda w ogóle powstanie. W tej części Raportu przedstawiamy trzy etapy reakcji na zagrożenie pożarem oraz to, jak ich właściwe zarządzanie może radykalnie ograniczyć skutki niebezpiecznych zdarzeń.

Czas jako główny czynnik prewencyjny

Jednym z najważniejszych wniosków wynikających z doświadczeń operacyjnych jest to, że skuteczność ochrony przeciwpożarowej można realnie mierzyć poprzez czas reakcji – zarówno systemów technicznych, jak i ludzi. To parametr wpływający bezpośrednio na:

- Możliwość wykrycia zagrożenia na jego najwcześniejszym etapie,
- Tempo i skuteczność podjętych działań,
- Ograniczenie energii pożaru, skali wybuchu lub zasięgu szkody,
- Czas postoju produkcji oraz jego koszty.
- W analizie prewencyjnej czas reakcji można wyróżnić w trzech kluczowych kategoriach:
- Czas reakcji systemów przeciwpożarowych i automatyki przemysłowej,
- Czas reakcji operatora maszyny / linii produkcyjnej,
- Czas reakcji służb ratowniczych.

Każdy z tych etapów wpływa na kolejny, a ich efektywna konfiguracja i współdziałanie decydują o tym, czy zdarzenie zostanie zatrzymane w zarodku, czy rozwinie się w poważną szkodę.

1. Reakcja systemów przeciwpożarowych i automatyki przemysłowej

Systemy automatycznego wykrywania i przeciwdziałania zagrożeniom stanowią pierwszą i najszybszą linię obrony. Ich przewagą jest działanie w milisekundach, a więc w czasie, w którym człowiek nie ma możliwości podjęcia decyzji ani reakcji.

Kluczowe przykłady systemów:

- Monitoring np. temperatury, ciśnienia – umożliwia szybkie wykrywanie odchyleń od wartości dopuszczalnych;
- Sterowanie maszyną – wykorzystuje zaprogramowane scenariusze reakcji, takie jak zatrzymanie procesu, odcięcie medium czy kontrolowany wyrzut materiału;
- Systemy wykrywania i gaszenia iskier;
- Systemy tłumienia lub izolacji wybuchu.

Znaczenie projektowania prewencji już na etapie inwestycji

Najlepszą praktyką jest projektowanie zabezpieczeń równolegle z planowaniem zakupu nowych maszyn. W przedsiębiorstwach o wysokiej świadomości ryzyka zespoły inwestycyjne pracują wspólnie z operatorami, technologami oraz służbami odpowiedzialnymi za bezpieczeństwo, aby wypracować optymalny zestaw zabezpieczeń. Czasami jednak doposażenie parku maszynowego po okresie eksploatacji pozwala w pełni zidentyfikować zagrożenia wynikające z jego użytkowania.

Przykłady dobrych praktyk:

- Analiza potencjalnych ryzyk oraz podejmowanie działań zapobiegawczych już na etapie projektowania parku maszynowego.
- Uzgadnianie optymalnych rozwiązań technicznych z producentem maszyny na etapie inwestycji, z wykorzystaniem jego wiedzy o krytycznych punktach procesu.
- Rozszerzanie logiki sterowania maszyn o funkcje wspomagające decyzje operatorów, a w przypadkach jednoznacznych – automatyzowanie reakcji, gdy udział człowieka nie wnosi dodatkowej wartości lub może być zbyt wolny.
- Przeprowadzanie okresowej, ponownej analizy ryzyka procesu po określonym czasie eksploatacji, w celu weryfikacji skuteczności zastosowanych środków ochronnych oraz uzasadnienia doposażenia instalacji w dodatkowe systemy bezpieczeństwa, w tym redundancję istniejących systemów.

2. Reakcja operatora – kluczowy, ale najbardziej nieprzewidywalny element

Czynnik ludzki pozostaje najbardziej zmienną częścią systemu prewencji. Operatorzy różnią się doświadczeniem, poziomem tolerancji na stres, znajomością procedur i zdolnością koncentracji. Dlatego konieczne jest traktowanie ich roli jako elementu, który można wzmacniać poprzez kulturę organizacyjną, szkolenia i właściwe procedury.

Czynniki wpływające na skuteczność reakcji operatora:

- doświadczenie na zajmowanym stanowisku oraz rotacja personelu,
- regularne ćwiczenia praktyczne (obsługa maszyn, reakcje scenariuszowe oraz najprostsze tj. właściwy dobór i użycie gaśnic),
- liczba urządzeń nadzorowanych jednocześnie,
- dostępność procedur i materiałów szkoleniowych,
- czytelność alarmów i komunikatów systemowych.

Praktyczne znaczenie szkoleń i kultury bezpieczeństwa

Zdarzenia pożarowe często rozwijają się dynamicznie, a czas od wykrycia do eskalacji może wynosić sekundy. Kluczowe jest, aby operator:

- wiedział, jak zareagować,
- miał niezbędne narzędzia dostępne „pod ręką",
- nie bał się podjąć działania.

Dobrym przykładem znaczenia właściwego przeszkolenia personelu oraz ergonomicznego rozmieszczenia wyposażenia jest zdarzenie, w którym operator widząc zarzewie ognia zareagował natychmiast, wykorzystując podręczną gaśnicę. Gaśnicę umieszczono w tym miejscu kilka lat wcześniej na podstawie przeprowadzonego audytu oraz wyciągniętych wniosków. Szybka interwencja pozwoliła ograniczyć skutki incydentu do około dziesięciominutowego przestoju instalacji.

W przypadku, gdyby najbliższa gaśnica znajdowała się w odległości kilkudziesięciu metrów, czas reakcji mógłby ulec wydłużeniu, co znacząco zwiększyłoby skalę strat.

Kultura „no blame" – fundament skutecznej prewencji

Prowadzenie szczegółowych analiz każdego zdarzenia, dokumentowanie faktów, wyciąganie wniosków i udostępnianie je wszystkim pracownikom to podstawy skutecznego zarządzania prewencją. Warunkiem koniecznym jest brak obwiniania pracowników – tylko wtedy można liczyć na rzetelny opis sytuacji i prawdziwe dane do analizy.

3. Reakcja służb ratowniczych – ostatnia bariera

Jeśli dwa wcześniejsze etapy nie zadziałały lub nie wystarczyły, do gry wchodzą służby wewnętrzne i zewnętrzne. Ich czas reakcji jest jednak znacznie dłuższy – w przypadku jednostek państwowych zwykle wynosi od kilku do kilkudziesięciu minut, co przy dynamice pożaru jest czasem bardzo długim.

Etap wewnętrzny: służby zakładowe

W wielu nowoczesnych zakładach działają wewnętrzne zespoły reagowania złożone z pracowników posiadających przeszkolenie z zakresu ochrony przeciwpożarowej . Dysponują sprzętem, środkami gaśniczymi i są w stanie rozpocząć działania natychmiast po przyjęciu zgłoszenia.

Etap zewnętrzny: Państwowa Straż Pożarna

Straż pożarna dociera zwykle w czasie około kilkunastu minut – to moment, w którym pożar często ma już znaczną energię i wymaga zaawansowanych działań. Dlatego PSP nie powinna być traktowana jako podstawowy środek ochrony, lecz jako element interwencji zewnętrznej, uruchamiany po wyczerpaniu środków prewencji i ochrony wewnętrznej.

Znaczenie prewencji szkodowej w strategii zarządzania ryzykiem

Skuteczny system prewencyjny zmniejsza nie tylko ryzyko pożaru, ale przede wszystkim:

- minimalizuje przestoje produkcyjne,
- ogranicza ryzyko szkód majątkowych,
- poprawia ciągłość działania (business continuity),
- zmniejsza koszty ubezpieczenia i ryzyko regresów,
- buduje kulturę organizacyjną opartą na odpowiedzialności.

Z perspektywy zarządzania ryzykiem prewencja nie jest kosztem, lecz inwestycją w stabilność operacyjną. Każda sytuacja, w której zdarzenie zostaje zatrzymane na wczesnym etapie, oznacza krótszy przestój, mniejsze straty i realną ochronę wyniku finansowego.

Podsumowanie

Skuteczna prewencja pożarowa to nie zbiór pojedynczych działań, lecz spójny system oparty na trzech kluczowych obszarach: automatyzacji, kompetencjach pracowników i gotowości służb. Czas reakcji jest głównym parametrem wpływającym na rozwój każdego zdarzenia. Krótszy czas oznacza mniejsze szkody, szybszy powrót do produkcji i realne oszczędności.

Wdrażanie prewencji nie jest efektem jednorazowego działania, lecz ciągłego doskonalenia procesów. Organizacje, które potrafią zharmonizować działania systemów, ludzi i służb, osiągają najwyższy poziom bezpieczeństwa operacyjnego.

Podsumowanie dobrych praktyk:

01 **Projektuj prewencję na etapie inwestycji**
Współpraca działu inwestycji, operatorów i służb bezpieczeństwa jest kluczowa.
To wtedy można najefektywniej zaplanować system detekcji, gaszenia
i logikę zachowania maszyn.

02 **Zwiększ automatyzację reakcji tam, gdzie człowiek nie wnosi wartości**
Jeśli reakcja/decyzja operatora nie jest konieczna lub jej spowolnienie może pogorszyć sytuację, funkcje te powinny być realizowane automatycznie.

03 **Zapewnij operatorom stałe szkolenia i ćwiczenia praktyczne**
Szkolenia powinny być powtarzane cyklicznie, z elementami praktycznymi i symulacjami scenariuszy.

04 **Buduj kulturę bezpieczeństwa opartą na zaufaniu**
Kultura "no blame" zwiększa jakość analiz powypadkowych i umożliwia realne wnioski.

05 **Wyposaż stanowiska w podręczny sprzęt gaśniczy**
Gaśnice powinny znajdować się bliżej niż wymagane minimum – kilka dodatkowych urządzeń może zdecydować o losie całej linii produkcyjnej.

06 **Dokumentuj wszystkie zdarzenia i analizuj je z zespołem**
Transparentność i dzielenie się wiedzą zwiększają świadomość pracowników i wpływają na ich reakcje w przyszłości.

Badanie
wyniki i analiza

Cele badania: Paradoks prewencji w Polsce

Polskie przedsiębiorstwa stoją przed paradoksem: rosnąca świadomość znaczenia prewencji nie zawsze przekłada się na systematyczne działania.

Niniejsze badanie ma na celu:

- **Zdiagnozować stan faktyczny** – jak polskie firmy podchodzą do prewencji
- **Zidentyfikować bariery** – co powstrzymuje przed wdrażaniem rozwiązań prewencyjnych
- 3 które działania przynoszą największe efekty
- **Zaproponować rekomendacje** – jak zwiększyć skuteczność prewencji

Adresaci badania: wielokrotne studium przypadku
Badanie zostało przeprowadzone w grudniu 2024 roku wśród 21 przedstawicieli polskich przedsiębiorstw reprezentujących różne branże i wielkości organizacji:

- **Sektory:**
  produkcja (38%), usługi (52%), handel (5%), logistyka i inne (5%)
- **Wielkość firm:**
  od małych (<50 pracowników) do dużych (>1000 pracowników)

Respondenci reprezentowali najwyższe szczeble zarządzania, w tym CFO (19%), CEO (19%), COO (10%), dyrektorów ds. bezpieczeństwa (10%) oraz innych członków kadry zarządzającej (52%).

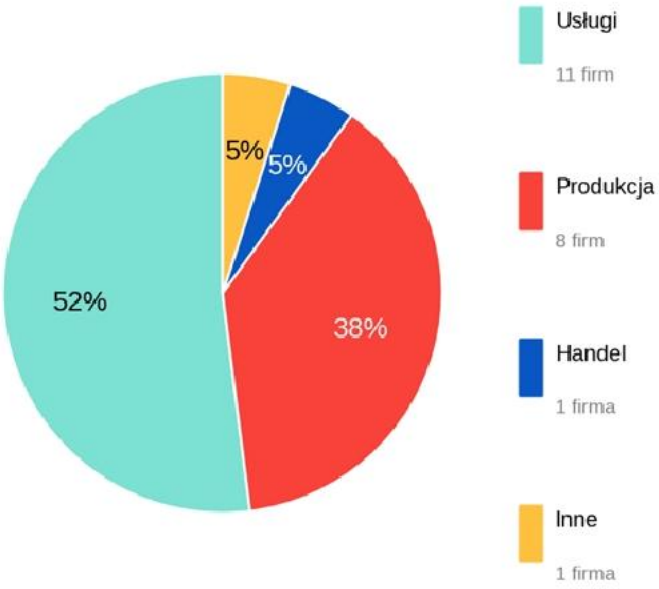
Badanie zostało dokonane metodą wielokrotnych przypadków (multiple-case study lub collective case study) na próbie około dwudziestu przedsiębiorstw.

Metoda ta umożliwiła porównanie podejścia do prewencji w badanych przedsiębiorstwach, zidentyfikowanie ich wzorców zachowania i podejścia wobec prewencji.

Badanie umożliwiło także pogłębioną analizę wybranych przypadków.

Cele badania: Paradoks prewencji w Polsce

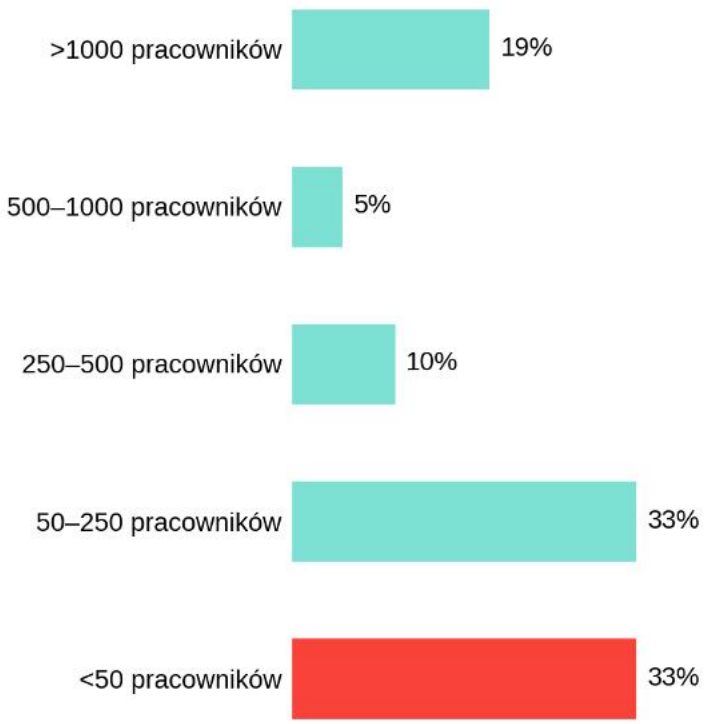
Wykres 1: Struktura branżowa respondentów



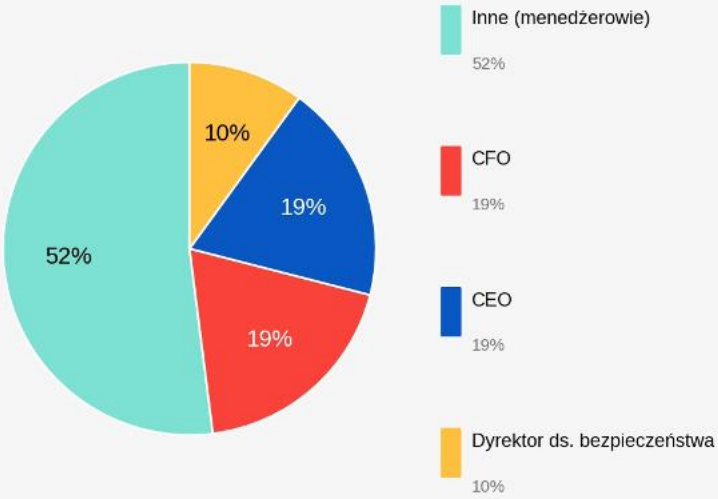
Badanie objęło przekrój polskiej gospodarki z dominacją sektora usługowego (52%), co odzwierciedla strukturę współczesnej ekonomii.
Znaczący udział produkcji (38%) zapewnia wgląd w praktyki prewencyjne w branży szczególnie narażonej na ryzyka techniczne i operacyjne.
Natomiast zróżnicowanie sektorowe pozwala na identyfikację uniwersalnych wyzwań prewencyjnych niezależnie od charakteru działalności.

Równomierna reprezentacja małych (33%) i średnich przedsiębiorstw (33%) wraz ze znaczącym udziałem dużych korporacji (19%) pozwala na analizę porównawczą praktyk prewencyjnych w zależności od skali działalności.
Wnioski wskazują, że wyzwania prewencyjne są uniwersalne – zarówno małe firmy borykające się z ograniczonymi zasobami, jak i duże korporacje z kompleksową strukturą organizacyjną identyfikują podobne bariery i potrzeby w zakresie prewencji szkodowej.

Wykres 2: Wielkość organizacji

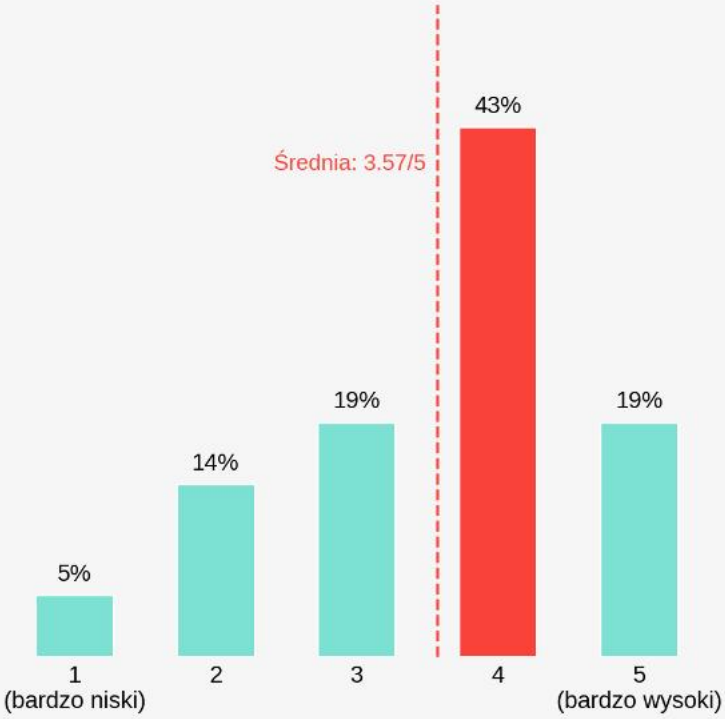


Wykres 3: Stanowiska respondentów



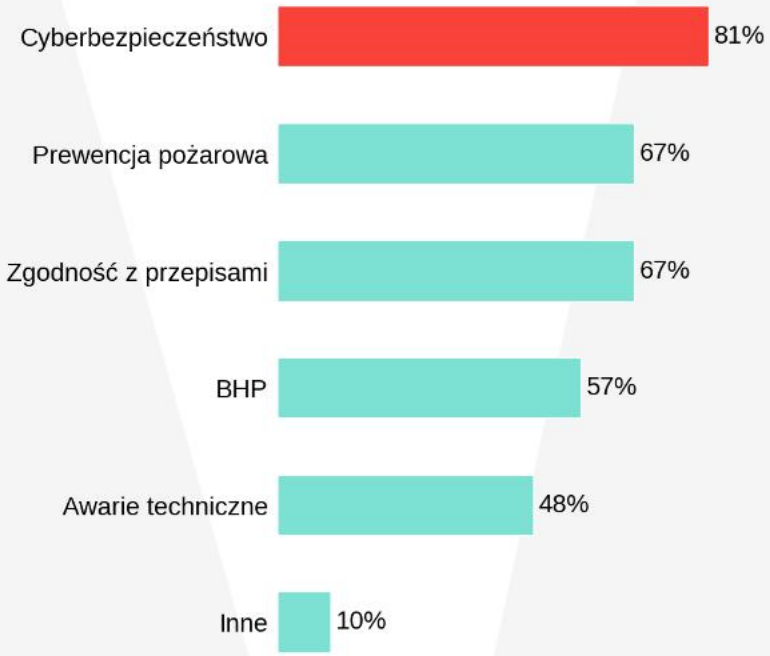
Jednym z kluczowych wskaźników jakości badania był dla autorów profil uczestników badania wyznaczony przez przedsiębiorstwa jako najbardziej kompetentny do zarządzania działaniami prewencyjnymi.
Łącznie 38% respondentów to członkowie najwyższego kierownictwa (CEO i CFO), co potwierdza, że zebrane odpowiedzi odzwierciedlają perspektywę decydentów strategicznych odpowiedzialnych za alokację zasobów i kształtowanie kultury organizacyjnej.
Stosunkowo niski udział dedykowanych dyrektorów ds. bezpieczeństwa (10%) może sugerować, że w polskich firmach odpowiedzialność za prewencję jest rozproszona, a nie skoncentrowana w wyspecjalizowanej roli.

Wykres 4: Poziom wiedzy o prewencji w organizacji (skala 1–5)



Jak wynika z tej sekcji badania, ponad 62% firm ocenia swoją wiedzę o prewencji na poziomie dobrym lub bardzo dobrym (4-5), co wskazuje na rosnącą dojrzałość rynku.
Jednocześnie prawie co piąta firma (19%) ocenia swoją wiedzę poniżej średniej, co ujawnia znaczne zróżnicowanie w poziomie świadomości prewencyjnej między organizacjami.
Przyczynę takiego podejścia można upatrywać w tym, że przedsiębiorstwa z wyższą samooceną wiedzy częściej posiadają dedykowany budżet na prewencję (korelacja: r=0.68) i osobę odpowiedzialną za ten obszar, co potwierdza, że wiedza przekłada się na działanie.

Wykres 5: Obszary zastosowania prewencji (wielokrotny wybór)

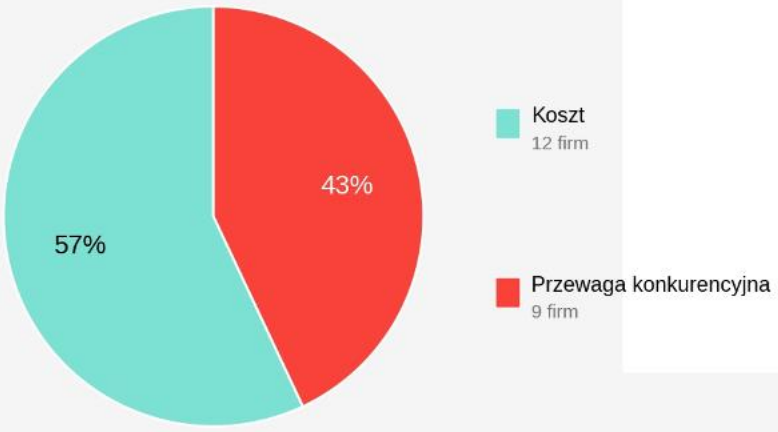


* Respondenci mogli wskazać więcej niż jedną odpowiedź

W badaniu zaobserwowano wyraźną dominację cyberbezpieczeństwa: Cyberryzko jest bezapelacyjnym liderem (81%), co odzwierciedla globalny trend rosnących zagrożeń cybernetycznych. Jednocześnie firmy nie zaniedbują tradycyjnych obszarów – dwie trzecie inwestuje w prewencję pożarową i compliance

W tym kontekście zidentyfikowano też obszary niedoceniane, wśród których wyróżnić możemy odpowiedzialność cywilna (praktycznie nieobecna), ryzyka ESG i klimatyczne (zero wskazań), ciągłość działania (business continuity). Sugeruje to w naszej ocenie ewidentną potrzebę edukacji o szerszym spektrum ryzyk wykraczających poza najbardziej widoczne zagrożenia.

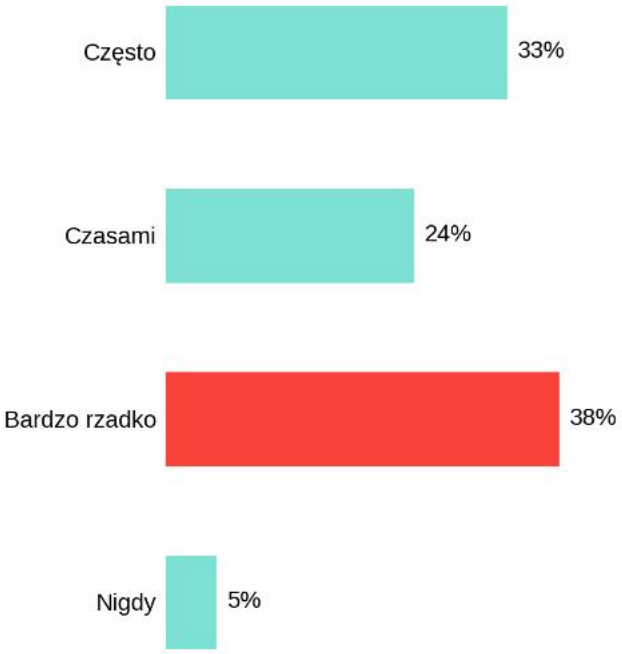
Wykres 6: Postrzeganie prewencji – koszt vs przewaga konkurencyjna



Możemy stwierdzić, że jesteśmy w fazie przełomu w postrzeganiu prewencji. Niemal połowa firm (43%) dostrzega już strategiczną wartość prewencji jako elementu budowania przewagi konkurencyjnej. To fundamentalna zmiana w porównaniu z dekadą temu, kiedy prewencja była powszechnie postrzegana wyłącznie jako koszt konieczny.

Za paradoks można uznać, to, że firmy postrzegające prewencję jako przewagę konkurencyjną częściej mierzą jej skuteczność (67% vs 38% w grupie postrzegającej ją jako koszt) i wykazują lepsze wyniki finansowe. Można więc na tej podstawie sformułować rekomendację: Kluczowe jest komunikowanie ROI prewencji – niższe składki, mniej przestojów, lepsza reputacja, dostęp do finansowania.

Wykres 7: Częstotliwość podejmowania decyzji prewencyjnych



Jak wynika z powyższego mamy do czynienia z luką w systematyczności działań. Tylko jedna trzecia firm bowiem podejmuje decyzje prewencyjne regularnie. Dla pozostałych 62% są to działania sporadyczne lub bardzo rzadkie, co wskazuje na brak systematycznego, zinstytucjonalizowanego podejścia do prewencji.

W tym względzie widoczna jest wyraźna korelacja wyników badania; Firmy regularnie podejmujące decyzje prewencyjne:

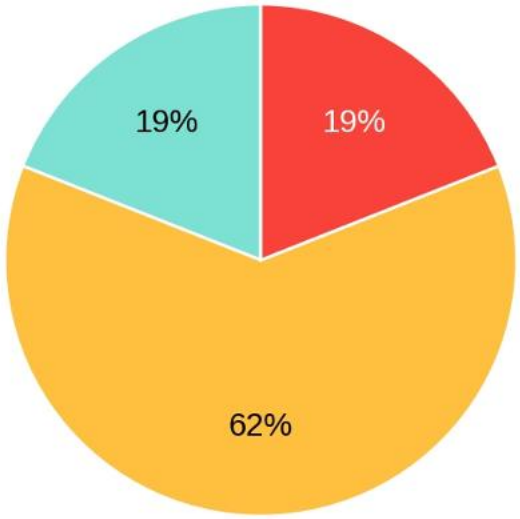
- Mają średnio o 1.2 punktu wyższą ocenę znaczenia prewencji (4.8 vs 3.6)
- 4x częściej posiadają dedykowany budżet (83% vs 21%)
- 3x częściej mierzą skuteczność działań

Wykres 8: Przecenianie zdarzeń spektakularnych vs szkód częstych

Na przykładzie powyższych odpowiedzi możemy wywnioskować racjonalność poznawczą. Dwie trzecie respondentów (67%) deklaruje, że nie przecenia ryzyka spektakularnych, ale rzadkich szkód (pożary, eksplozje) kosztem częstszych, ale mniej dramatycznych incydentów.

Na tym tle można zasugerować rekomendację, że systematyczne raportowanie danych o faktycznej częstotliwości i wartości różnych typów szkód może pomóc w przeciwdziałaniu zniekształceniom poznawczym.

Wykres 9: Preferencja oszczędności krótkoterminowych vs bezpieczeństwa długoterminowego



Zdecydowanie nie
19%

Raczej nie
62%

Raczej tak
19%

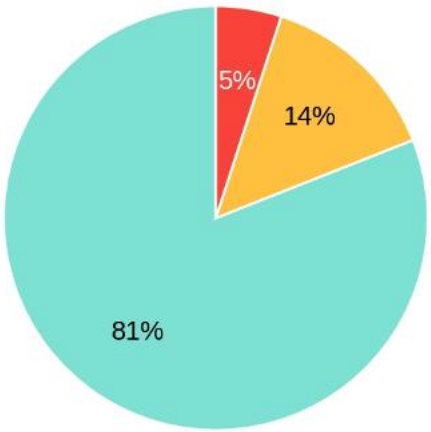
Badanie w powyższym zakresie pokazuje podejście do długoterminowego myślenia. Zdecydowana większość przedsiębiorstw (81%) deklaruje, że nie faworyzuje oszczędności krótkoterminowych kosztem bezpieczeństwa długoterminowego. To bardzo pozytywny sygnał wskazujący na dojrzałość strategiczną polskich menedżerów.
Jednakże wyniki odpowiedzi na inne pytania (odpowiedzi na Q25 pokazują, że 38% firm musiało zaprzestać działań prewencyjnych pod presją kosztową) sugerują, że w praktyce presja na wyniki krótkoterminowe bywa silniejsza niż deklaracje.

Wykres 10: Prewencja jako część strategii zarządzania ryzykiem

Na podstawie powyższego wykresu możemy pokazać prewencję jako jeden z kluczowych wskaźników dojrzałości przedsiębiorstwa. Ponad cztery piąte firm (81%) uznaje prewencję za integralną część strategii zarządzania ryzykiem.

To fundamentalna zmiana w porównaniu z dekadą temu, kiedy prewencja była traktowana jako opcjonalny dodatek do ubezpieczenia.

Jednak duży odsetek, bo aż 14% niepewności ("nie wiem") może sugerować brak formalnej, udokumentowanej strategii zarządzania ryzykiem lub niewystarczającą komunikację strategii w organizacji.

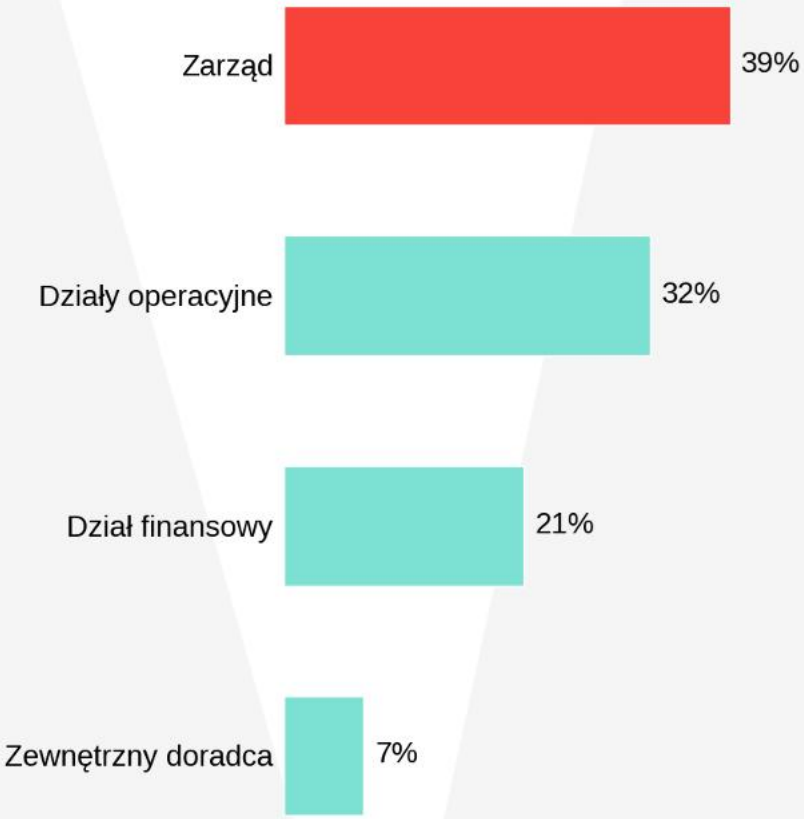


Tak
17 firm

Nie wiem
3 firmy

Nie
1 firma

Wykres 11: Odpowiedzialność za planowanie prewencji

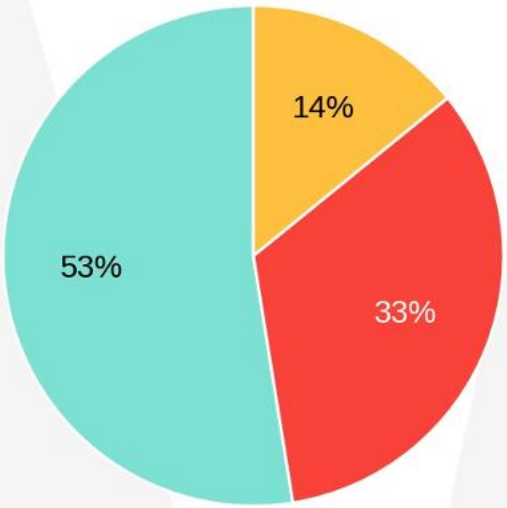


Pozytywnym sygnałem wynikającym z powyższych odpowiedzi jest, że to zarząd najczęściej (39%) ponosi odpowiedzialność za planowanie prewencji, co potwierdza uznanie jej strategicznej wagi.

Stosunkowo wysoka rola działów operacyjnych (32%) świadczy o tym, że prewencja jest w tych organizacjach postrzegana jako integralna część codziennego zarządzania operacyjnego, a nie wyłącznie jako funkcja strategiczna zarezerwowana dla najwyższego kierownictwa. Niska rola zewnętrznych doradców (7%) może wskazywać na kilka równoległych zjawisk: po pierwsze, preferowanie rozwiązań wewnętrznych wynikające z przekonania, że wewnętrzne zespoły lepiej rozumieją specyfikę organizacji; po drugie, niedostateczną świadomość dostępnych usług konsultingowych i ich potencjalnej wartości dodanej; oraz po trzecie, postrzeganie kosztów usług doradczych jako istotnej bariery, szczególnie w kontekście ograniczonych budżetów na prewencję.

Dla porównania, benchmark międzynarodowy pokazuje znacząco odmienną sytuację – w krajach zachodnich odsetek firm korzystających z zewnętrznych konsultantów ds. ryzyka regularnie przekracza 30%, co sugeruje, że polski rynek może nie w pełni wykorzystywać potencjał specjalistycznej ekspertyzy zewnętrznej w budowaniu dojrzałych programów prewencyjnych.

Wykres 12: Posiadanie dedykowanego budżetu na prewencję



Tak
11 firm

Nie
7 firm

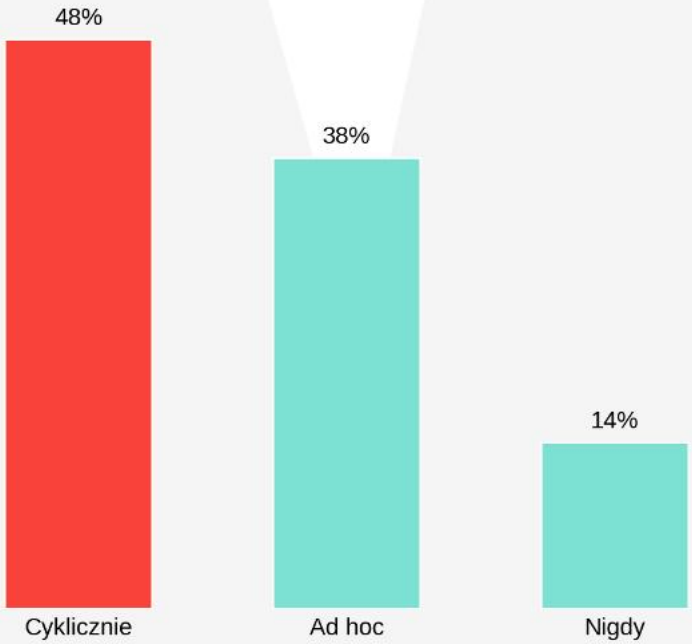
Nie wiem
3 firmy

GAP ANALYSIS:
LUKA MIĘDZY DEKLARACJĄ A DZIAŁANIEM:

81% deklaruje, że prewencja jest częścią strategii
Ale tylko 52% ma dedykowany budżet
Gap = 29 punktów procentowych

Bez dedykowanych środków finansowych trudno o systematyczne, długoterminowe działania prewencyjne. Luka wskazuje, że deklaracje strategiczne nie zawsze przekładają się na konkretne zasoby operacyjne.

Wykres 13: Częstotliwość analizy skuteczności prewencji

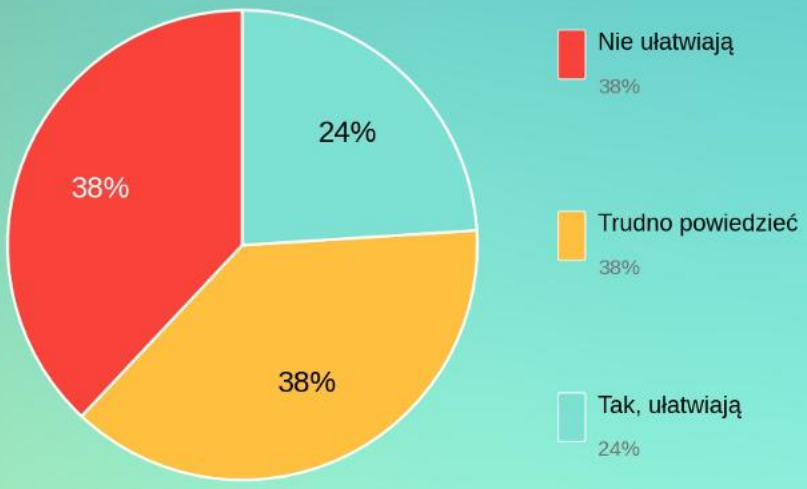


Wyniki badania ujawniają krytyczną lukę w pomiarze skuteczności prewencji – tylko niecała połowa firm (48%) regularnie mierzy efektywność swoich działań prewencyjnych, co ma daleko idące konsekwencje dla jakości zarządzania ryzykiem w tych organizacjach. Po pierwsze, brak systematycznego pomiaru oznacza brak możliwości optymalizacji, ponieważ bez rzetelnych danych organizacje nie są w stanie określić, które działania faktycznie przynoszą wymierne efekty, a które pochłaniają zasoby bez odpowiedniego zwrotu. Po drugie, trudność w uzasadnieniu dalszych inwestycji w prewencję staje się istotną barierą rozwoju – bez wykazania zwrotu z inwestycji (ROI) przekonanie zarządu do alokacji dodatkowych środków na programy prewencyjne graniczy z niemożliwością, szczególnie w sytuacji konkurencji o budżet z innymi projektami biznesowymi. Po trzecie, brak pomiaru prowadzi do braku odpowiedzialności za wyniki, ponieważ nie można efektywnie rozliczać osób i zespołów z rezultatów w obszarze, którego skuteczności się nie kwantyfikuje.

Dla kontrastu, najlepsze praktyki obserwowane w organizacjach na poziomie 4-5 drabiny Hudsona pokazują, że dojrzałe podejście do prewencji wymaga zbalansowanego systemu pomiaru obejmującego zarówno wskaźniki wyprzedzające, jak i wskaźniki opóźnione, takie jak liczba rzeczywistych szkód, roczna średnia strata czy wysokość składek ubezpieczeniowych, co pozwala na pełny obraz skuteczności działań prewencyjnych zarówno w perspektywie predykcyjnej, jak i retrospektywnej.

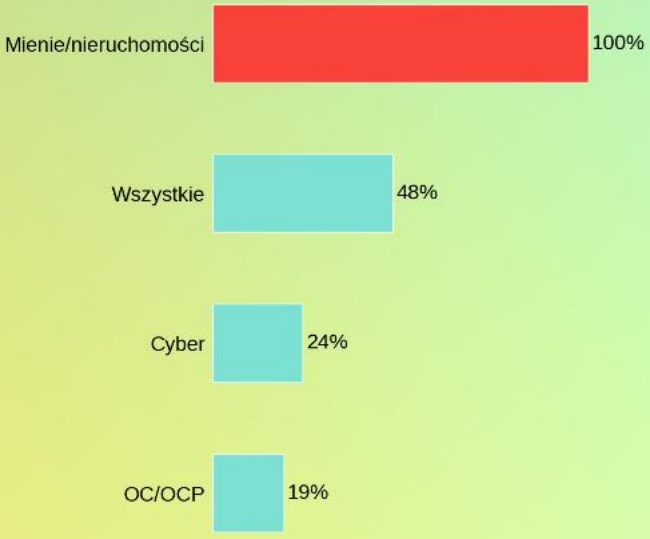
Wykres 14: Wpływ nowych technologii na prewencję

Wyniki badania ujawniają paradoks technologiczny – mimo że inwestycje w cyberbezpieczeństwo, będące z definicji domeną technologiczną, stanowią priorytet dla 81% firm, tylko jedna czwarta respondentów (24%) potwierdza, że nowe technologie faktycznie ułatwiają działania prewencyjne w ich organizacjach. Możliwe przyczyny tego zjawiska obejmują niedostateczne wykorzystanie dostępnych narzędzi takich jak Internet Rzeczy, sztuczna inteligencja czy predykcyjna analityka, brak świadomości możliwości technologicznych wykraczających poza wąski obszar cyberbezpieczeństwa, problemy z integracją systemów prowadzące do funkcjonowania technologii w izolowanych silosach organizacyjnych, oraz lukę kompetencyjną przejawiającą się brakiem umiejętności efektywnego wykorzystania zaawansowanej analityki danych.



Jednocześnie wyniki wskazują na ogromny, niewykorzystany potencjał – technologie takie jak czujniki IoT umożliwiające predykcyjne utrzymanie ruchu, algorytmy uczenia maszynowego wykrywające anomalie zapowiadające awarie, czy cyfrowe bliźniaki pozwalające na symulację różnych scenariuszy ryzyka, mogą radykalnie poprawić skuteczność prewencji, pod warunkiem strategicznego, zintegrowanego podejścia do ich wdrażania, które wykracza poza doraźne reakcje na pojedyncze zagrożenia.

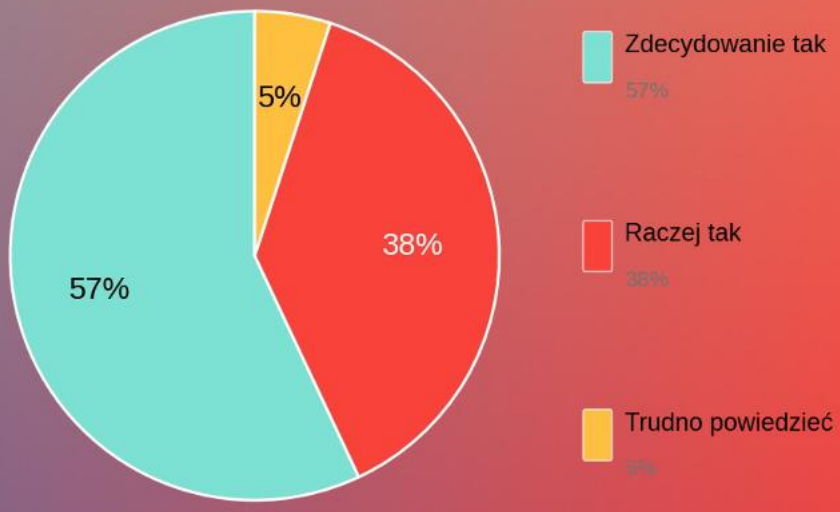
Wykres 15: Typy ubezpieczeń, gdzie prewencja ma największe znaczenie



* Respondenci mogli wskazać więcej niż jedną odpowiedź

Ubezpieczenia majątkowe są jednoznacznie uznawane za najbardziej podatne na działania prewencyjne, ponieważ firmy widzą bezpośredni wpływ zabezpieczeń fizycznych na wysokość składek. Jednocześnie badanie pokazuje, że potencjał prewencji w innych obszarach jest niedoceniany: w cyberubezpieczeniach rzadko łączy się inwestycje w bezpieczeństwo z obniżeniem kosztów ochrony, w ubezpieczeniach OC mało kto dostrzega możliwość redukcji ryzyka poprzez działania zapobiegawcze, a ubezpieczenia ciągłości działania praktycznie nie funkcjonują w świadomości firm jako obszar prewencji. Wskazuje to na potrzebę lepszej edukacji ze strony ubezpieczycieli i brokerów, aby pokazać wpływ systematycznej prewencji na warunki różnych rodzajów ubezpieczeń, nie tylko majątkowych.

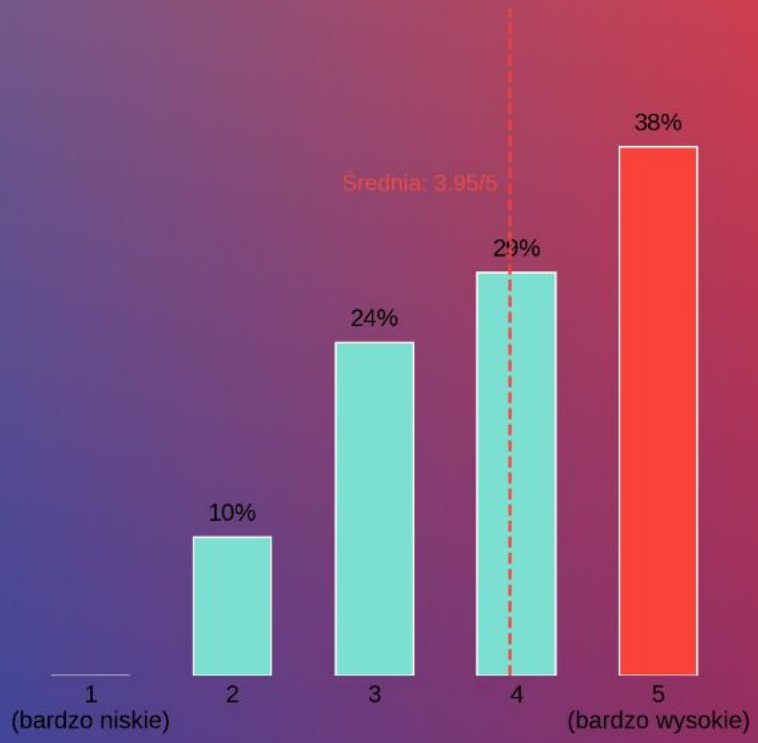
Wykres 16: Przekonanie o opłacalności prewencji



Zdecydowana większość respondentów (95%) wyraża silne przekonanie, że prewencja przynosi wymierne korzyści, co stanowi bardzo pozytywny sygnał gotowości do dalszych inwestycji w tym obszarze. Jednocześnie wyniki ujawniają paradoks wdrażania – chociaż 95% firm wierzy w opłacalność prewencji, tylko 52% posiada dedykowany budżet na działania prewencyjne, a zaledwie 48% systematycznie mierzy ich skuteczność.
Ten znaczący rozdźwięk między deklaracjami a praktyką pokazuje, że przekonanie o wartości prewencji nie przekłada się automatycznie na systematyczne działania operacyjne.

Kluczowe bariery leżą zatem nie w sferze przekonań czy postaw zarządczych, ale w obszarze organizacji wewnętrznej, umiejętności priorytetyzacji konkurujących ze sobą celów biznesowych oraz kompetencji niezbędnych do skutecznego projektowania, wdrażania i monitorowania programów prewencyjnych.

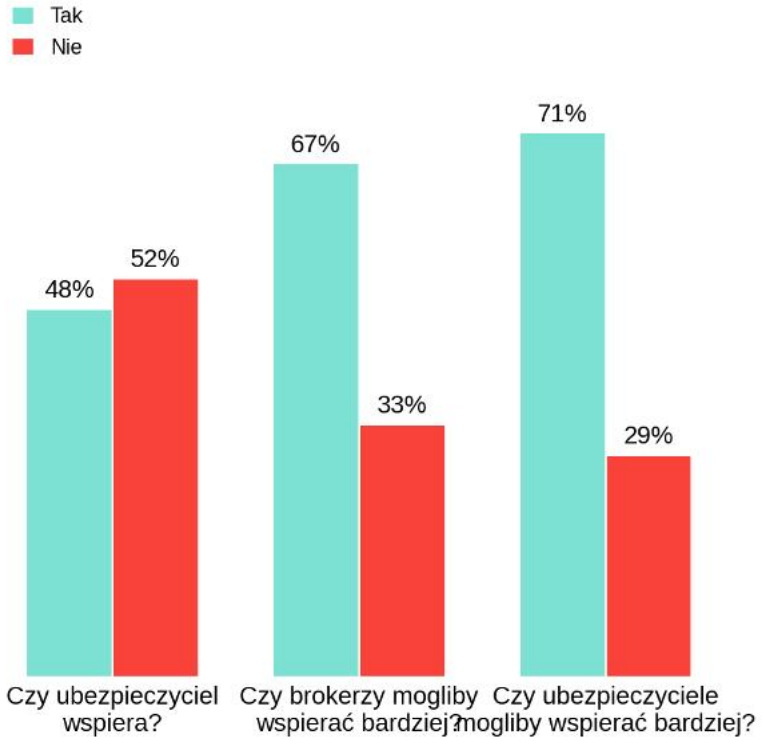
Wykres 17: Znaczenie prewencji dla ochrony majątku i ciągłości działania (skala 1–5)



Średnia ocena znaczenia prewencji na poziomie 3.95 w skali pięciopunktowej potwierdza, że respondenci postrzegają ją jako kluczowy element ochrony wartości przedsiębiorstwa.

Ponadto, 67% firm ocenia znaczenie prewencji na najwyższych poziomach (4-5), co sytuuje ją w jednym szeregu z najważniejszymi funkcjami biznesowymi, takimi jak finanse, sprzedaż czy operacje.

Wykres 18: GAP w wykorzystaniu wsparcia ubezpieczyciela

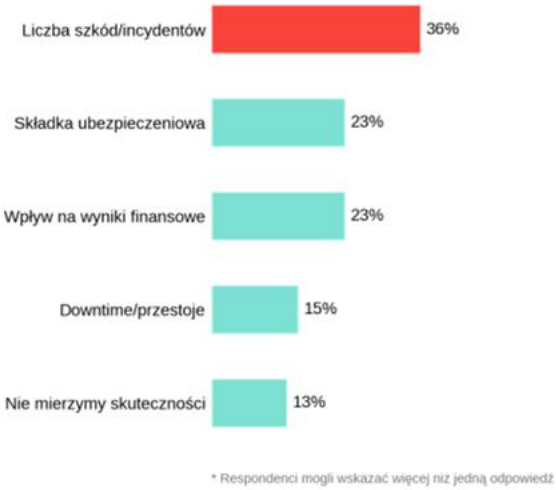


Badanie ujawnia ogromną lukę komunikacyjną między potencjałem wsparcia prewencyjnego a jego rzeczywistym wykorzystaniem – podczas gdy ze strony podażowej brokerzy i ubezpieczyciele deklarują możliwość znacznie większego zaangażowania w doradztwo prewencyjne (odpowiednio 67% i 71%), ze strony popytowej tylko 48% firm faktycznie otrzymuje takie wsparcie, co oznacza gap na poziomie 23 punktów procentowych.

- 4x częściej posiadają dedykowany budżet (83% vs 21%)
- 3x częściej mierzą skuteczność działań

Przyczyny tego zjawiska są wielowymiarowe i obejmują niedostateczną komunikację wartości dodanej oferowanej przez ubezpieczycieli, dominację transakcyjnego, a nie strategicznego modelu relacji, w którym focus koncentruje się na cenie polisy zamiast na partnerstwie w zarządzaniu ryzykiem, brak świadomości klientów o dostępnych usługach takich jak audyty ryzyka, narzędzia analityczne czy specjalistyczne szkolenia, oraz niewystarczające zasoby w obszarze risk engineering po stronie samych ubezpieczycieli. Kluczową rekomendacją wynikającą z tych obserwacji jest fundamentalna zmiana modelu relacji z transakcyjnego na partnerski, w którym ubezpieczyciel pełni rolę doradcy ryzyka aktywnie wspierającego klienta w budowaniu odporności operacyjnej, a nie jedynie sprzedawcy polisy reagującego na zapotrzebowanie po wystąpieniu szkody.

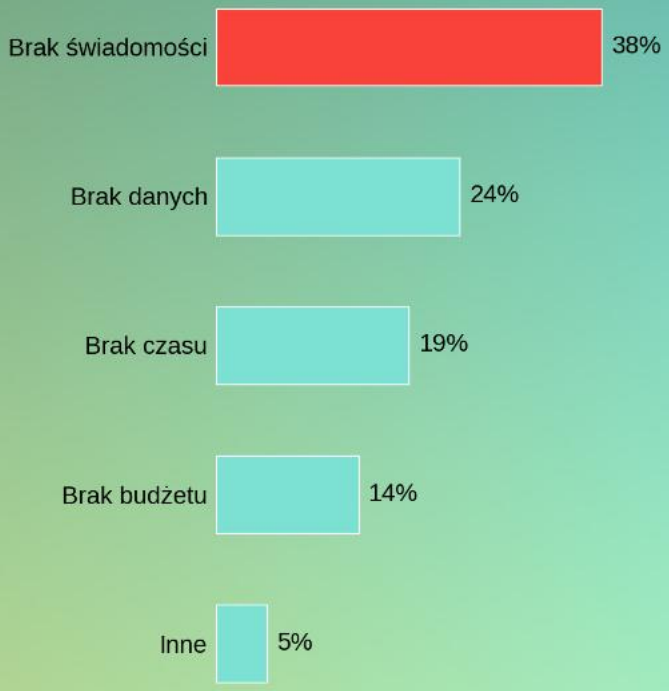
Wykres 19: Wskaźniki oceny skuteczności prewencji (wielokrotny wybór)



* Respondenci mogli wskazać więcej niż jedną odpowiedź

Najpopularniejszym wskaźnikiem oceny skuteczności prewencji jest liczba incydentów (36% wskazań), co choć intuicyjne, jest niewystarczające, ponieważ nie uwzględnia nasilenia i konsekwencji szkód – dziesięć drobnych incydentów ma zupełnie inny wpływ na organizację niż jedna katastrofa o dużej skali. Badanie ujawnia brak zaawansowanych metryk, które są standardem w dojrzałych organizacjach, takich. Co więcej, aż 13% firm w ogóle nie mierzy skuteczności swoich działań prewencyjnych, co oznacza działanie "w ciemno" bez jakiejkolwiek możliwości optymalizacji inwestycji i udoskonalania programów.

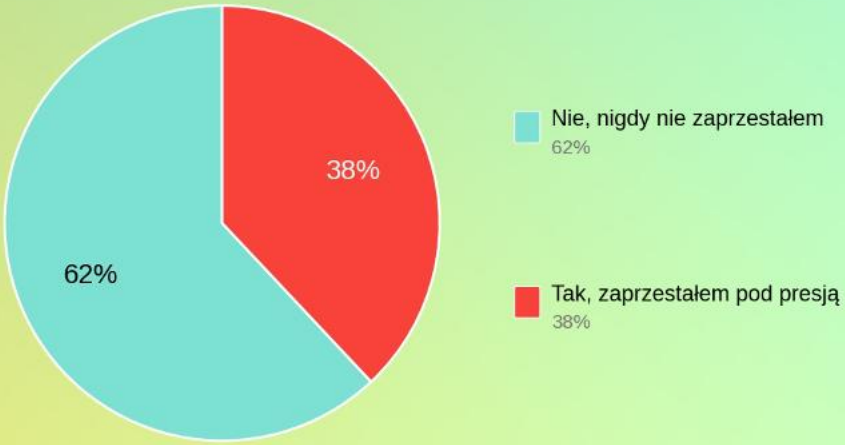
Wykres 20: Główne bariery we wdrażaniu prewencji



Największą przeszkodą we wdrażaniu działań prewencyjnych jest brak świadomości (38%), co wskazuje na kluczową rolę edukacji obejmującej intensywniejsze komunikowanie wartości prewencji, wymianę najlepszych praktyk poprzez case studies i benchmarki branżowe, oraz demonstrację zwrotu z inwestycji na konkretnych, weryfikowalnych przykładach z podobnych organizacji.

Zaskakującym wnioskiem jest to, że brak budżetu stanowi najmniej istotną barierę (zaledwie 14% wskazań), co sugeruje, że problem leży nie w dostępności środków finansowych, ale w trzech innych obszarach: priorytetyzacji, organizacji, oraz wiedzy operacyjnej. Kluczową rekomendacją jest zatem skoncentrowanie wysiłków na budowaniu zdolności organizacyjnych poprzez rozwój kompetencji, dostarczanie narzędzi i wdrażanie procesów, a nie wyłącznie na zapewnianiu finansowania, które bez odpowiednich umiejętności i struktur organizacyjnych nie zostanie efektywnie wykorzystane.

Wykres 21: Presja kosztowa na decyzje prewencyjne



Chociaż większość firm (62%) nie musiała rezygnować z działań prewencyjnych pod presją kosztową, aż 38% respondentów doświadczyło sytuacji, w której zostali zmuszeni do zaprzestania lub ograniczenia takich działań z powodu reakcji właścicieli lub zarządu na dodatkowe koszty.

To pokazuje istotny rozdźwięk między deklaracjami a praktyką – mimo że 81% respondentów w pytaniu 11 deklarowało, że nie preferuje oszczędności krótkoterminowych kosztem bezpieczeństwa długoterminowego, w rzeczywistości presja na wyniki finansowe mierzone kwartał po kwartale wciąż stanowi poważne wyzwanie dla utrzymania ciągłości programów prewencyjnych. Ryzyko związane z cięciem budżetów prewencyjnych w trudnych czasach jest szczególnie dotkliwe, ponieważ może uruchomić spiralę negatywną – redukcja wydatków na prewencję prowadzi do wzrostu liczby i wartości szkód, co z kolei skutkuje wyższymi składkami ubezpieczeniowymi i dalszym pogorszeniem pozycji finansowej organizacji, ostatecznie generując znacznie większe koszty niż te, które miały zostać zaoszczędzone.

Stan prewencji

w polskich firmach 2024/2025

Świadomość: wysoka

- 81% uznaje prewencję za element strategii

Wdrażanie: średnie

- 52% ma budżet
- 48% mierzy skuteczność

Priorytety

- Cyberbezpieczeństwo (81%)
- Pożar + Compliance (67%)

Współpraca

- Gap 23% między możliwościami a wykorzystaniem wsparcia

Główna bariera

- Brak świadomości (38%)
- NIE brak budżetu (14%)

Kluczowe wnioski

01 Prewencja jako element przewagi konkurencyjnej

Większość firm (81%) postrzega działania prewencyjne jako część strategii zarządzania ryzykiem, co wskazuje na rosnące zrozumienie wartości proaktywnego podejścia do bezpieczeństwa.

Rekomendacje: Integruj prewencję z procesami biznesowymi od etapu planowania. Traktuj inwestycje w prewencję nie jako koszt, ale jako czynnik budujący wartość i odporność organizacji.

02 Luka między świadomością a działaniem

Chociaż 57% firm deklaruje, że prewencja się opłaca, tylko 38% podejmuje decyzje o zaprzestaniu działań prewencyjnych z powodu kosztów, co pokazuje, że wiele organizacji jest świadomych korzyści, ale napotyka bariery we wdrażaniu.

Rekomendacje: Identyfikuj i eliminuj przeszkody organizacyjne.

03 Cyberbezpieczeństwo jako priorytet nr 1

81% respondentów wskazało cyberbezpieczeństwo jako kluczowy obszar prewencji, przewyższając prewencję pożarową (14 wskazań) i awarie techniczne (10 wskazań).

Rekomendacje: Traktuj cyberbezpieczeństwo jako fundamentalny element zarządzania ryzykiem operacyjnym. Inwestuj w systemy wykrywania zagrożeń, szkolenia pracowników oraz plany reakcji na incydenty.

Kluczowe wnioski

04 Niewystarczająca współpraca z ubezpieczycielami

Jedynie 48% firm korzysta ze wsparcia ubezpieczycieli w działaniach prewencyjnych, mimo że 67% brokerów i 71% ubezpieczycieli deklaruje możliwość takiej pomocy.

Rekomendacje: Aktywnie poszukuj wiedzy i doradztwa u partnerów ubezpieczeniowych, posiadających zaawansowane narzędzia analityczne i doświadczenie, które mogą znacząco poprawić skuteczność prewencji.

05 Analityka i pomiar skuteczności wymagają rozwoju

Tylko 48% firm regularnie analizuje skuteczność działań prewencyjnych, a zaledwie 38% stosuje cykliczne przeglądy.

Rekomendacje: Implementuj systemy monitorowania i KPI dla prewencji. Bez pomiaru trudno uzasadnić inwestycje i udowodnić ROI działań prewencyjnych.

06 Rola zarządu w prewencji jest kluczowa

Średnia ocena znaczenia prewencji dla firm wyniosła 3.95/5, przy czym największe zaangażowanie wykazują organizacje z dedykowanym budżetem (52% respondentów) i osobą odpowiedzialną za prewencję.

Rekomendacje: Ustanów jasną odpowiedzialność na poziomie zarządu. Prewencja wymaga lidera, który będzie koordynował działania, budżet i komunikację między działami.

Perspektywy

Czy nadszedł czas na zmianę roli ubezpieczenia z narzędzia transferu ryzyka na zapobieganie ryzyku?

To stwierdzenie przestaje być tylko pytaniem, a zaczyna być koniecznością. Jak wielokrotnie podkreślano "wyjście poza transfer ryzyka na rzecz jego ograniczania i zapobiegania będzie miało kluczowe znaczenie dla ubezpieczycieli, klientów i regulatorów w bardziej ryzykownym świecie".

Ubezpieczenia są zbudowane na fundamencie zaufania pomiędzy ubezpieczycielami a klientami. Ta podstawowa obietnica ochrony i niezawodności nie może zostać naruszona.

Światowa luka w ochronie ubezpieczeniowej jest dobrym punktem wyjścia do wzmacniania tego zaufania.

Opierając się na tym fundamencie, można twierdzić, że obowiązek ubezpieczycieli do aktywnego zaangażowania się w środki zapobiegawcze lub łagodzące wynika z tego fundamentu, a nie jest tylko modelem biznesowym, stosowanym tylko tam, gdzie jest to opłacalne.

Takie podejście faktycznie pomogłoby w wypełnieniu luki ubezpieczeniowej, szczególnie tam, gdzie ryzyka stają się bardziej systemowe i istnieje niebezpieczeństwo ich nieubezpieczalności (jak ma to miejsce na przykład w cyber ryzykach). Środki prewencyjne zaczną odgrywać dominującą rolę w stosunkach ubezpieczeniowych. Stanie się tak jednak, jeśli narzędzie prewencyjne nie będzie oferowane tylko ekskluzywnemu gronu klientów, których będzie stać na korzystanie z narzędzi IoT itp., ale gdy podejście inkluzywne w odniesieniu do zapobiegania ryzyku będzie stosowane jako nieodłączny element ochrony ubezpieczeniowej.

Najważniejszym wyzwaniem dla ubezpieczyciela jest więc przejście z podejścia skoncentrowanego na produkcie na podejście skoncentrowane na kliencie, a także przejście do standardowego oferowania nie tylko produktów ubezpieczeniowych, ale i usług prewencyjnych.

Jak będzie wyglądała prewencja za za 5 lat?

Trend 1: Prewencja jako usługa (Prevention-as-a-Service)

W ciągu najbliższych pięciu lat model zakupu ubezpieczenia jako odrębnego produktu będzie ewoluował w kierunku kompleksowych rozwiązań integrujących ochronę ubezpieczeniową z aktywnym zarządzaniem ryzykiem w formule abonamentowej. Zamiast tradycyjnego schematu, w którym firma najpierw zawiera ubezpieczenie, a następnie osobno buduje program prewencyjny, przedsiębiorstwa będą nabywać pakiety Risk-as-a-Service obejmujące monitoring 24/7 z wykorzystaniem czujników IoT i systemów SIEM dla cyberbezpieczeństwa, automatyczne alerty i rekomendacje działań korygujących generowane przez sztuczną inteligencję analizującą dane w czasie rzeczywistym, dostęp on-demand do ekspertów z różnych dziedzin zarządzania ryzykiem (inżynierowie, prawnicy, specjaliści IT, konsultanci BHP), oraz ubezpieczenie jako integralny element całego ekosystemu, z dynamicznym dostosowywaniem warunków i składki do rzeczywistego poziomu ryzyka. Przykładem może być InsurTech oferujący kompleksowe rozwiązanie dla piekarni, gdzie czujniki temperatury, wilgotności i stężenia CO2 są połączone z platformą analityczną i ubezpieczeniem mienia oraz odpowiedzialności cywilnej – przy przekroczeniu krytycznych parametrów system automatycznie wysyła alert do właściciela i służb ratunkowych, a firma otrzymuje redukcję składki za każdy miesiąc bez incydentów, przy czym cały pakiet jest dostępny w prostej formule miesięcznego abonamentu.

Trend 2: Predykcyjna prewencja oparta na sztucznej inteligencji i big data

Zaawansowane algorytmy uczenia maszynowego umożliwią przewidywanie awarii, cyberataków i przestojów operacyjnych z wyprzedzeniem dni lub tygodni, fundamentalnie zmieniając naturę prewencji z reaktywnej na predykcyjną. Systemy AI będą analizować wzorce z setek podobnych firm, identyfikować anomalie sygnalizujące zbliżające się problemy zanim staną się widoczne dla człowieka, oraz automatycznie rekomendować konkretne działania korygujące z oszacowaniem ich skuteczności i kosztów wdrożenia. Przykładowo, system analizujący logi IT i wzorce ruchu sieciowego wykryje nietypową aktywność charakterystyczną dla wczesnych faz ataku ransomware trzy dni przed jego pełnym uruchomieniem, automatycznie zaizoluje zagrożone segmenty sieci, powiadomi zespół bezpieczeństwa z szczegółową mapą infiltracji i rekomendowanymi krokami naprawczymi, a jednocześnie zaktualizuje profil ryzyka w systemie ubezpieczeniowym. W produkcji, predykcyjna analityka bazująca na danych z czujników wibracji, temperatury i hałasu maszyn będzie przewidywać awarie krytycznych komponentów z dokładnością przekraczającą 85%, pozwalając na planową wymianę części przed ich uszkodzeniem, co eliminuje kosztowne nieplanowane przestoje i szkody wtórne.

Trend 3: Demokratyzacja zaawansowanej prewencji dla małych i średnich przedsiębiorstw

Technologie prewencyjne, które dziś są dostępne tylko dla dużych korporacji dysponujących znacznymi budżetami IT i zespołami specjalistów, staną się powszechnie dostępne dla małych i średnich firm dzięki drastycznemu obniżeniu kosztów, uproszczeniu interfejsów użytkownika i modelom biznesowym opartym na subskrypcji.

Tanie czujniki IoT produkowane masowo będą kosztować dziesiątki, a nie tysiące złotych, cloudowe platformy analityczne dostępne w modelu SaaS wyeliminują potrzebę drogich inwestycji w infrastrukturę IT, a interfejsy no-code/low-code pozwolą małym firmom samodzielnie konfigurować systemy bez angażowania drogich konsultantów.

Przykładowo, mała firma produkcyjna za 200 złotych miesięcznie otrzyma kompletny pakiet obejmujący czujniki wibracji i temperatury zainstalowane na kluczowych maszynach, system predykcyjnego utrzymania ruchu z automatycznymi alertami o zbliżających się awariach, prosty dashboard dostępny przez przeglądarkę internetową pokazujący stan zdrowia" każdej maszyny i rekomendowane działania, oraz ubezpieczenie maszyn ze zniżką 15% w stosunku do stawki standardowej, ponieważ ubezpieczyciel ma dostęp do danych rzeczywistych i widzi, że ryzyko jest aktywnie zarządzane. Ta demokratyzacja technologii prewencyjnych wyrówna szanse między małymi a dużymi graczami, pozwalając MŚP na osiągnięcie poziomu bezpieczeństwa operacyjnego dotychczas zarezerwowanego dla korporacji.

Trend 4: Regulacyjny imperatyw prewencji i rosnące wymogi ESG

Regulatorzy i prawodawcy będą coraz bardziej aktywnie wymuszać proaktywne zarządzanie ryzykiem poprzez rozszerzającą się siatkę dyrektyw, standardów i wymogów raportowania, co uczyni prewencję nie tyle opcją strategiczną, ile warunkiem koniecznym prowadzenia działalności.

Dyrektywa NIS2 dotycząca cyberbezpieczeństwa infrastruktury krytycznej nałoży szczegółowe wymogi na tysiące przedsiębiorstw w całej Unii Europejskiej, włączając obowiązkowe audyty, certyfikacje i raportowanie incydentów pod groźbą dotkliwych kar finansowych.

Rozporządzenie DORA (Digital Operational Resilience Act) wymusi na sektorze finansowym kompleksowe podejście do odporności operacyjnej, obejmujące zarządzanie ryzykiem stron trzecich, testy penetracyjne i scenariusze kryzysowe.

Dyrektywa CSRD (Corporate Sustainability Reporting Directive) rozszerzy wymogi raportowania ESG na dziesiątki tysięcy firm, przy czym zarządzanie ryzykiem klimatycznym, bezpieczeństwo pracowników i jakość governance staną się obiektywnymi, weryfikowalnymi metrykami wpływającymi na dostęp do kapitału i reputację rynkową. Firmy, które już dziś inwestują w systematyczną prewencję, będą miały znaczącą przewagę compliance i reputacyjną, podczas gdy te opóźniające się będą zmuszone do kosztownego nadrabiania zaległości pod presją regulatorów i rynku.

Trend 5: Prewencja jako fundament strategii ESG i dostępu do kapitału

Inwestorzy instytucjonalni, banki i klienci B2B będą coraz bardziej wymagać od firm transparentności w zarządzaniu ryzykiem, czyniąc dojrzałość prewencyjną kluczowym elementem oceny atrakcyjności inwestycyjnej i wiarygodności kredytowej.

Ratingi ESG, które jeszcze dekadę temu były niszowym narzędziem wykorzystywanym przez nielicznych inwestorów społecznie odpowiedzialnych, staną się mainstream, wpływając na wyceny giełdowe, koszty kredytów i dostęp do funduszy inwestycyjnych.

Agencje ratingowe będą szczegółowo oceniać cyberbezpieczeństwo, zarządzanie BHP, odporność łańcucha dostaw i ciągłość działania jako kluczowe komponenty governance, przy czym firmy z niskimi wynikami w tych obszarach będą karane zarówno przez rynek kapitałowy (niższe wyceny, wyższy koszt kapitału), jak i przez klientów (utrata kontraktów wymagających certyfikacji).

Banki komercyjne już powszechnie stosują zróżnicowane stopy procentowe w zależności od profilu ryzyka ESG, oferując tzw. zielone kredyty lub kredyty zrównoważone rozwojowo (sustainability-linked loans) z preferencyjnym oprocentowaniem dla firm wykazujących wysokie standardy zarządzania ryzykiem.

Klienci B2B, szczególnie duże korporacje zarządzające ryzykiem w całym łańcuchu wartości, będą wymagać od dostawców certyfikatów bezpieczeństwa takich jak ISO 27001 dla cyberbezpieczeństwa czy ISO 45001 dla BHP jako warunku podpisania umowy. W konsekwencji, prewencja przestanie być postrzegana jako funkcja back-office zarządzana przez specjalistów ds. ryzyka, a stanie się elementem front-office, kluczowym dla relacji z klientami, inwestorami i partnerami biznesowymi, bezpośrednio wpływającym na przychody i możliwości rozwoju organizacji.

Konsekwencje

dla polskich przedsiębiorstw

Polska w 2030 roku będzie funkcjonować w radykalnie odmiennym ekosystemie zarządzania ryzykiem, gdzie firmy nieprzygotowane na te trendy znajdą się w dramatycznej niekorzystnej sytuacji konkurencyjnej.

Natomiast te, które będą zwlekać, traktując prewencję jako opcjonalny koszt możliwy do zredukowania w trudnych czasach, znajdą się w spirali negatywnej – rosnące składki ubezpieczeniowe, trudności w uzyskaniu certyfikacji wymaganych przez klientów i regulatorów, wyższe koszty kredytów bankowych, utrata kontraktów na rzecz lepiej zarządzających ryzykiem konkurentów, a ostatecznie marginalizacja rynkowa lub konieczność wyjścia z biznesu.

Przedsiębiorstwa, które już dziś rozpoczną podróż w kierunku dojrzałej kultury prewencyjnej – inwestując w technologie, kompetencje pracowników, systemy pomiarowe i relacje z ubezpieczycielami – będą w 2030 roku liderami swoich branż, osiągającymi niższe koszty ryzyka, lepszy dostęp do kapitału, wyższe marże operacyjne i silniejszą pozycję negocjacyjną wobec klientów i dostawców.

Kluczowe pytanie dla każdego polskiego przedsiębiorcy i menedżera brzmi nie "czy inwestować w prewencję?", lecz "jak szybko możemy rozpocząć transformację, aby w 2030 roku być wśród zwycięzców, a nie przegranych?". Firmy podejmujące działania dziś – nawet małe, stopniowe kroki zgodne z rekomendacjami dla ich wielkości i branży – budują fundament pod przyszłą przewagę konkurencyjną w świecie, gdzie prewencja nie będzie już opcją, lecz warunkiem przetrwania i rozwoju.

Rekomendacje:

Plan działania dla każdego typu organizacji

Dla małej firmy (<50 pracowników)

Priorytet: Podstawy + cyberbezpieczeństwo

Małe przedsiębiorstwa powinny skoncentrować się na budowaniu fundamentów kultury prewencyjnej przy ograniczonych zasobach, według następujących założeń:

Po pierwsze kluczowe jest przeprowadzenie samodzielnej oceny ryzyka z wykorzystaniem dostępnych darmowych narzędzi, takich jak NIST Cybersecurity Framework dla cyberbezpieczeństwa, oraz wdrożenie podstawowych zabezpieczeń cybernetycznych obejmujących uwierzytelnianie wieloskładnikowe (MFA), regularne kopie zapasowe danych i podstawowe szkolenia pracowników z zakresu rozpoznawania zagrożeń phishingowych. Równolegle należy skonsultować się z brokerem ubezpieczeniowym w celu zrozumienia, jakie wymogi prewencyjne mogą wpłynąć na warunki i koszty ubezpieczenia.

Po drugie małe firmy powinny określić jedną osobę odpowiedzialną za bezpieczeństwo, nawet jeśli będzie to zadanie wykonywane w niepełnym wymiarze godzin lub jako dodatkowa odpowiedzialność istniejącego pracownika, wprowadzić prostą procedurę zgłaszania incydentów i sytuacji potencjalnie niebezpiecznych, oraz ustalić bazowy poziom szkodowości, który będzie punktem odniesienia do przyszłych pomiarów skuteczności.

Po trzecie należy wprowadzić systematyczne przeglądy kluczowych wskaźników prewencji, aktywnie poszukiwać prostych, tanich rozwiązań przynoszących szybkie efekty (jak podstawowe zabezpieczenia fizyczne czy poprawione procedury), oraz systematycznie benchmarkować się z podobnymi firmami w branży, wykorzystując stowarzyszenia branżowe i sieci kontaktów.

Kluczowa zasada dla małych firm: lepiej zrobić kilka rzeczy systematycznie i dobrze, niż próbować kompleksowego programu, którego nie da się utrzymać. Wykorzystuj maksymalnie dostępne wsparcie od ubezpieczycieli i brokerów – często oferują bezpłatne audyty i konsultacje dla swoich klientów.

Rekomendacje:

Plan działania dla każdego typu organizacji

Dla średniej firmy (50-500 pracowników)

Priorytet: Systematyzacja + technologia + pomiar

Średnie przedsiębiorstwa dysponują już większymi zasobami, co pozwala na bardziej zaawansowane podejście do prewencji.

Po pierwsze kluczowe jest powołanie międzyfunkcyjnego komitetu ds. ryzyka (risk committee) z przedstawicielami kluczowych działów – operacji, finansów, IT, BHP – zaplanowanie budżetu na prewencję z jasnym podziałem na inwestycje kapitałowe (np. systemy zabezpieczeń) i wydatki operacyjne (szkolenia, utrzymanie), oraz wdrożenie systemu zarządzania ryzykiem, który może w początkowej fazie być nawet prostym narzędziem w Excelu lub SharePoint, o ile jest konsekwentnie stosowany.

Po drugie średnie firmy powinny przeprowadzić profesjonalny audyt ryzyka z partnerem zewnętrznym, którym może być broker ubezpieczeniowy, konsultant lub sam ubezpieczyciel oferujący usługi risk engineering, wdrożyć 2-3 kluczowe technologie prewencyjne dostosowane do specyfiki działalności (np. czujniki IoT do predykcyjnego utrzymania ruchu w produkcji, SIEM dla cyberbezpieczeństwa, systemy monitoringu dla logistyki), oraz rozpocząć systematyczny pomiar skuteczności działań prewencyjnych.

Po trzecie należy przeprowadzić roczny przegląd skuteczności z korektą strategii na podstawie zebranych danych, zorganizować dedykowane szkolenia dla kadry menedżerskiej z zakresu zarządzania ryzykiem i prewencji, oraz przeprowadzić benchmark z rynkiem, wykorzystując dostępne raporty branżowe i wymianę doświadczeń z innymi firmami.

Kluczowa zasada dla średnich firm: prewencja musi być zintegrowana z istniejącymi procesami biznesowymi (planowanie, budżetowanie, rozwój produktów), a nie funkcjonować jako osobny, izolowany program. Inwestycja w odpowiednie narzędzia technologiczne i analityczne na tym etapie zwraca się wielokrotnie poprzez lepszą identyfikację ryzyk i szybszą reakcję.

Rekomendacje:

Plan działania dla każdego typu organizacji

Dla dużej firmy (>500 pracowników)

Priorytet: Integracja + zaawansowana analityka + kultura prewencyjna jako przewaga konkurencyjna

Duże organizacje powinny traktować prewencję jako element strategicznej przewagi. Kluczowe jest jej pełne włączenie w procesy biznesowe oraz wykorzystanie zaawansowanej analityki do świadomego zarządzania ryzykiem.

Po pierwsze – konieczna jest integracja prewencji z decyzjami dotyczącymi zakupów, inwestycji, rozwoju produktów i ekspansji. Obejmuje to wdrożenie modelowania predykcyjnego (AI/ML), analiz scenariuszowych, symulacji Monte Carlo oraz stworzenie real-time dashboardu dla zarządu, który pokazuje ekspozycję na ryzyka i realizację celów prewencyjnych.

Po drugie – duże firmy powinny budować wewnętrzną ekspertyzę poprzez dedykowany zespół risk engineering, rozważyć captive insurance dla wybranych ryzyk oraz zdobyć kluczowe certyfikacje (ISO 31000, 27001, 22301).

Podnosi to standardy i wzmacnia pozycję konkurencyjną w przetargach i relacjach z inwestorami.

Po trzecie – w długim horyzoncie dojrzałość prewencyjna powinna stać się elementem komunikacji ESG i marki korporacyjnej. Dzielenie się wiedzą z partnerami wzmacnia cały łańcuch wartości, a kultura ciągłego doskonalenia sprawia, że pracownicy aktywnie identyfikują i eliminują ryzyka.

Kluczowa zasada: na tym poziomie prewencja staje się sposobem prowadzenia biznesu. Inwestycje w analitykę, technologie i kompetencje pozwalają optymalizować relację ryzyko–zwrot i wpływać na standardy całej branży.

Niezależnie od wielkości każda firma powinna:

01 ·Traktować relację z ubezpiczycielem/brokerem jako strategiczne partnerstwo, nie transakcję – regularne spotkania, wspólne warsztaty ryzyka, wymiana danych i analiz.

02 Mierzyć to, co można zmierzyć – nawet prosta metryka konsekwentnie śledzona jest lepsza niż brak jakiegokolwiek pomiaru.

03 Zacząć od cyberbezpieczeństwa – to uniwersalny priorytet niezależnie od branży i wielkości, z jasnym ROI i rosnącymi wymogami ubezpieczeniowymi.

04 Inwestować w ludzi, nie tylko w systemy – najlepsze technologie są bezużyteczne bez świadomych, przeszkolonych pracowników.

05 Wykorzystywać każdą szkodę i near-miss jako okazję do nauki – systematyczna analiza przyczyn źródłowych (root cause analysis) i wdrażanie działań korygujących zapobiega powtarzaniu się problemów.

Droga do dojrzałej kultury prewencyjnej jest maraton, nie sprint – wymaga cierpliwości, konsekwencji i zaangażowania najwyższego kierownictwa, ale efekty w postaci niższych strat, lepszej reputacji i przewagi konkurencyjnej wielokrotnie przewyższają poniesione nakłady.

Podziękowania i nota końcowa:

Niniejszy raport nie powstałby bez zaangażowania 21 respondentów, którzy poświęcili swój czas na udział w badaniu. Dziękujemy za otwartość w dzieleniu się wyzwaniami i sukcesami w obszarze prewencji szkodowej.
Dziękujemy również partnerom wspierającym projekt:

- Howden Polska S.A. – za finansowanie badania i udostępnienie ekspertyz
- Akademii Leona Koźmińskiego – za wsparcie metodologiczne

Raport ten stanowi punkt wyjścia do dalszej dyskusji o przyszłości prewencji w Polsce.
Zachęcamy do kontaktu i wymiany doświadczeń:

Chcemy usłyszeć Twoją opinię

Czy te wnioski rezonują z Twoim doświadczeniem? Jakie działania prewencyjne przyniosły Twojej firmie największe korzyści?

Podziel się swoją historią – razem budujmy kulturę prewencji w polskich przedsiębiorstwach.

Autorzy
Prof. dr hab. Katarzyna Malinowska
Dyrektor Centrum Ubezpieczeń Gospodarczych
Akademia Leona Koźmińskiego w Warszawie

Kwiecień 2026

Akademia Leona Koźmińskiego, ul. Jagiellońska 59, 03-301 Warszawa
Howden Polska S.A., ul. Słusarska 7, 87-100 Toruń