ZARZĄDZANIE PRZEDSIĘBIORSTWEM

ESG przestaje być dodatkiem do strategii. Staje się sposobem zarządzania ryzykiem

Zrównoważone zarządzanie przedsiębiorstwem coraz rzadziej jest dziś traktowane jako obszar wizerunkowy, a coraz częściej jako element odporności biznesowej. Firmy działają w warunkach rosnącej presji regulacyjnej, kosztowej i środowiskowej, dlatego ESG przestaje być osobnym projektem, a zaczyna wpływać na codzienne decyzje zakupowe, logistyczne i operacyjne.

JAROSŁAW KAMIŃSKI
dyrektor zarządzający
RAJAPACK Polska

Dobrym przykładem jest rynek opakowań. Nadchodzące wymagania PPWR pokazują, że odpowiedzialność środowiskowa nie kończy się na wyborze bardziej ekologicznego materiału. Obejmuje cały cykl życia opakowania: jego projekt, masę, możliwość recyklingu, ponowne użycie, transport, oznakowanie i raportowanie. W praktyce oznacza to konieczność współpracy wielu działów jednocześnie – od zakupów i logistyki po compliance, marketing i operacje.

Efektywność

Firmy, które chcą zarządzać ESG skutecznie, powinny patrzeć na zrównoważony rozwój nie tylko przez pryzmat obowiązków regulacyjnych, ale także efektywności. Ograniczenie nadmiarowych materiałów, lepsze dopasowanie opakowań do produktów, skracanie łańcuchów dostaw czy wybór dostawców działających bliżej rynku mogą jednocześnie zmniejszać wpływ środowiskowy i poprawiać przewidywalność operacyjną. To szczególnie istotne w czasach, w których odporność łańcucha dostaw staje się jednym z kluczowych elementów zarządzania przedsiębiorstwem.

Widać też wyraźnie, że ESG wymaga danych. Deklaracje przestają wystarczać. Coraz większe znaczenie mają identyfikowalność produktów, certyfikaty, informacje o pochodzeniu materiałów, udział surowców z recyklingu czy możliwość udokumentowania zgodności z regulacjami. Dla zarządów oznacza to zmianę podejścia: zrównoważony rozwój nie jest już wyłącznie odpowiedzialnością działów CSR, ale częścią decyzji strategicznych dotyczących kosztów, dostawców i modelu operacyjnego firmy.

Narzędzie lepszego zarządzania

Największą przewagę zyskają te organizacje, które potraktują ESG jako narzędzie lepszego zarządzania, a nie wyłącznie jako obowiązek raportowy. W praktyce oznacza to wybór rozwiązań, które łączą odpowiedzialność środowiskową z efektywnością ekonomiczną – bo tylko wtedy zrównoważony rozwój staje się trwałym elementem strategii biznesowej.

AI i automatyzacja to projekty biznesowe

Sztuczna inteligencja przestała być wizją przyszłości – polskie firmy wdrażają ją jako standard w swojej działalności. Raport Polcom pokazuje, że 60 proc. średnich i dużych przedsiębiorstw już korzysta z AI, 64 proc. zamierza zwiększyć inwestycje w automatyzację, a IT ewoluuje z centrum kosztów w strategiczny motor przewagi konkurencyjnej.

ADAM MATYASZEK
dyrektor Działu Sprzedaży w Polcom

Zmiana nie dotyczy jednak tylko technologii, ale też i sposobu podejmowania decyzji, organizacji pracy i samej roli menedżera. Jak skutecznie zarządzać firmą w świecie, w którym algorytm bywa lepszym analitykiem niż człowiek?

Koniec epoki intuicji. Zaczyna się era danych

Przez dekady zarządzanie przedsiębiorstwem opierało się na doświadczeniu, instynkcie i hierarchicznym przepływie informacji. Menedżer był przede wszystkim tym, który wiedział więcej – o rynku, o procesach, o ludziach. Dziś ta przewaga systematycznie się kurczy. Nie dlatego, że doświadczenie straciło na wartości, ale dlatego, że pojawiło się narzędzie, które analizuje tysiące zmiennych w czasie rzeczywistym, nie popełnia błędów przy powtarzalnych zadaniach i nie potrzebuje przerwy na lunch.

Polskie firmy doskonale to rozumieją – i działają. Z raport Polcom „Barometr cyfrowej transformacji polskiego biznesu 2025-2026" wynika, że już 60 proc. średnich i dużych przedsiębiorstw korzysta z mechanizmów sztucznej inteligencji w jakiejś formie. 52 proc. wykorzystuje AI do automatyzacji procesów operacyjnych, a kolejne 37 proc. przygląda się tym rozwiązaniom z dużym zainteresowaniem. Nie jesteśmy już na etapie fascynacji technologią. Jesteśmy na etapie jej wdrażania – z konkretnymi oczekiwaniami biznesowymi i mierzalnymi efektami.

Cztery silniki, jeden ekosystem

Żeby zrozumieć, jak AI i automatyzacja zmieniają zarządzanie, trzeba spojrzeć na szerszy kontekst. Polskie firmy myślą o transformacji cyfrowej nie przez pryzmat pojedynczych narzędzi, lecz jako o spójnym ekosystemie czterech wzajemnie wzmacniających się technologii: chmury obliczeniowej, sztucznej inteligencji, automatyzacji i cyberbezpieczeństwa. Aż 72 proc. firm jest przekonanych, że korzystanie z wielu komplementarnych rozwiązań – a nie wdrażanie ich w izolacji – realnie zwiększa wydajność i innowacyjność.

Widać to wyraźnie w danych budżetowych. Na lata 2025-2026 aż 64 proc. firm planuje zwiększyć wydatki na automatyzację, 58 proc. na AI, 56 proc. na chmurę obliczeniową. IT przestaje być kosztem operacyjnym – staje się strategicznym filarem budowania przewagi konkurencyjnej.

AI w gabinecie prezesa

Najciekawszym – i chyba najbardziej niedocenianym – zjawiskiem jest przesunięcie AI w górę hierarchii organizacyjnej. Przez długi czas kojarzyła się głównie z automatyzacją operacyjną: chatbotami, sortowaniem faktur, kontrolą jakości. To wciąż ważne zastosowania, ale nowe dane wskazują na wyraźną zmianę.

Już 63 proc. firm korzysta z AI do wspomagania procesów poznawczych i dostępu do wiedzy, w tym z modeli językowych. 37 proc. firm już dziś używa AI do przekształcania procesów decyzyjnych i personalizacji usług, a kolejne 41 proc. poważnie to rozważa – łącznie blisko 80 proc. rynku.

Dział finansowy, który wcześniej „rejestrował zdarzenia", dziś dzięki analityce predykcyjnej może być partnerem strategicznym zarządu – wyprzedzającym problemy, zanim pojawią się w rachunku wyników. CFO bez narzędzi AI podejmuje gorsze decyzje niż jego konkurenci. To już nie kwestia nowoczesności – to kwestia przetrwania na rynku.

Automatyzacja: od fabryki do back-office

Gdy mówi się o automatyzacji, myśl nieuchronnie wędruje ku halom produkcyjnym i robotycznym ramionom. Tymczasem prawdziwa rewolucja dzieje się w biurach: automatyzacja procesów księgowych, obsługa klienta przez chatboty, selekcja CV w HR, analiza umów prawnych – to działające systemy, które dziś oszczędzają godziny pracy tam, gdzie wcześniej ktoś siedział z arkuszem kalkulacyjnym.

Dane są jednoznaczne: 84 proc. firm uważa, że automatyzacja wspierana przez AI optymalizuje koszty. 70 proc. dostrzega wzrost efektywności dzięki eliminacji rutynowych zadań. 68 proc. wskazuje na poprawę jakości procesów i redukcję błędów. Co szczególnie ważne – 72 proc. zauważa pozytywny wpływ automatyzacji na obsługę klienta. W dobie, gdy doświadczenie klienta staje się głównym polem konkurencji, to liczby, których nie można ignorować.

> Obawy pracowników i kadry zarządzającej przed technologiami cyfrowymi to realna bariera – dostrzega ją 61 proc. firm.

Organizacja pracy: co naprawdę się zmienia?

Automatyzacja i AI nie tylko optymalizują procesy – zmieniają samą naturę pracy. Z jednej strony korzyści są oczywiste: wyeliminowanie powtarzalnych zadań pozwala pracownikom skupić się na tym, do czego ludzki umysł jest naprawdę potrzebny – kreatywności, relacjach, ocenie kontekstu. Z drugiej – pojawia się lęk. I to lęk, którego nie należy bagatelizować.

Obawy pracowników i kadry zarządzającej przed technologiami cyfrowymi to realna bariera – dostrzega ją 61 proc. firm, a w sektorze przemysłowym aż 67 proc. Technologia sama w sobie nie wystarczy. Potrzebne jest zarządzanie zmianą: komunikacja, edukacja, włączanie ludzi w proces transformacji zamiast informowania ich o jej efektach po fakcie. Brak kompetencji cyfrowych to drugi co do wielkości hamulec transformacji – wskazuje na niego 71 proc. ankietowanych. Paradoks polega na tym, że im bardziej zaawansowane stają się narzędzia, tym bardziej zaawansowani muszą być ludzie, którzy je stosują i nadzorują.

Trzy wnioski dla zarządzających

AI i automatyzacja to projekty biznesowe, nie IT. Powinny być inicjowane i rozliczane na poziomie zarządu. Lider, który nie rozumie narzędzi AI wspierających jego branżę, traci zdolność zarządzania własną przewagą konkurencyjną.

Ludzie są ważniejsi niż algorytmy. Najlepszy system AI nie przyniesie rezultatów, jeśli pracownicy nie będą chcieli lub umieli z niego korzystać. Inwestycja w kompetencje cyfrowe i zarządzanie zmianą to warunek zwrotu z całej reszty.

Synergia jest ważniejsza niż doskonałość jednego narzędzia. Chmura, AI, automatyzacja i cyberbezpieczeństwo wzajemnie się wzmacniają. Organizacje zarządzające tymi obszarami spójnie zyskują przewagę niemożliwą do zreplikowania pojedynczym zakupem.

Zarządzanie w erze AI nie polega na zastępowaniu ludzi maszynami. Polega na budowaniu organizacji, w której ludzie i technologia razem robią to, czego żadne z nich nie potrafi zrobić osobno.

AI przyspiesza biznes, ale najpierw trzeba uporządkować fundamenty systemów IT

Z Krystianem Baranem, Project Management Lead w Ideo, o presji wdrażania AI, długu technologicznym i bezpiecznej modernizacji systemów legacy, rozmawiała Justyna Szymańska.

Firmy coraz mocniej czują, że automatyzacja i sztuczna inteligencja przestały być ciekawostką – dziś są jednym z warunków utrzymania konkurencyjności. Jednocześnie wiele organizacji nadal opiera kluczowe procesy na systemach tworzonych lata temu – trudnych w utrzymaniu, słabo udokumentowanych i nieprzygotowanych do integracji z nowoczesnymi narzędziami.

Jakie najważniejsze zmiany zachodzą obecnie na rynku IT?

Rozmawiając z naszymi klientami, zauważam, że dziś rośnie presja związana z wykorzystaniem AI i to jest największa zmiana, jaką obserwujemy. Firmy widzą, że sztuczna inteligencja może znacząco zwiększyć produktywność, przyspieszyć procesy i ograniczyć koszty operacyjne. Jednocześnie rośnie obawa, że konkurencja wdroży te rozwiązania szybciej i zyska przewagę trudną do nadrobienia.

Firmy nie rywalizują dziś o to, czy wdrożą AI, ale o to, czy zrobią to szybciej niż konkurencja.

W praktyce okazuje się jednak, że sama decyzja o wdrożeniu AI nie wystarcza. Organizacje mają ambitne plany, ale ich środowisko IT nie jest na to gotowe. Dane są rozproszone, procesy nie są ustandaryzowane, a kluczowe systemy działają w oparciu o przestarzałe technologie.

Z jednej strony mamy więc ogromną szansę: automatyzację, przyspieszenie procesów i lepsze decyzje. Z drugiej jednak realne ograniczenia wynikające z długu technologicznego.

Rynek oczekuje dziś szybszego dostarczania rozwiązań i krótszego time-to-market. AI tylko wzmacnia tę presję, ale żeby jej sprostać, trzeba najpierw uporządkować fundamenty: dane, integracje i stabilność systemów.

Jakie konsekwencje ma odkładanie modernizacji systemów IT?

Zmiany w IT bardzo przyspieszyły. Nowe rozwiązania powstają znacznie szybciej niż kiedyś, a systemy budowane lata temu coraz częściej zaczynają ograniczać rozwój organizacji.

Największe ryzyka dotyczą bezpieczeństwa, kosztów i dostępności kompetencji. Stare systemy działają na niewspieranych technologiach, mają luki bezpieczeństwa i wymagają specjalistów, których coraz trudniej znaleźć. Coraz częściej ich utrzymanie pochłania większą część budżetu IT niż rozwój.

Do tego dochodzi problem wiedzy ukrytej. System zna jedna osoba albo niewielki zespół, a dokumentacja jest niepełna lub przestarzała. W wielu organizacjach przekłada się to wprost na ryzyko operacyjne.

Największym ograniczeniem dla rozwoju i wdrożeń AI w wielu firmach nie jest brak technologii, ale stare systemy i dane.

Wiele systemów, często kluczowych dla działania firmy, było projektowanych w czasach, gdy nie myślano o API, integracjach czy AI (tzw. systemy legacy). Dziś oznacza to, że ich rozwój, integracja czy rozbudowa są kosztowne i obarczone dużym ryzykiem.

Dług technologiczny nie znika – on narasta. Im dłużej firma odkłada modernizację, tym bardziej złożonym i kosztownym przedsięwzięciem staje się późniejsza zmiana.

Które problemy najczęściej rozwiązuje dobrze wdrożone IT?

Najczęściej są to problemy z przepływem informacji, ręczną pracą i brakiem kontroli nad procesami. W wielu firmach dane istnieją, ale są rozproszone. Zespoły przepisują je między systemami, porównują arkusze i tworzą obejścia.

To działa do pewnej skali. Później zaczyna generować błędy, opóźnienia i realne koszty.

Dobrze wdrożony system porządkuje procesy, automatyzuje powtarzalne działania i łączy dane w jedno środowisko. Firma zyskuje dostęp do aktualnych informacji, ogranicza błędy i może szybciej podejmować decyzje.

> Największym ograniczeniem dla rozwoju i wdrożeń AI w wielu firmach nie jest brak technologii, ale stare systemy i dane

W kontekście systemów legacy równie ważne jest odzyskanie kontroli nad kodem, dokumentacją, bezpieczeństwem i dalszym rozwojem.

Jak dopasować technologię do potrzeb firmy?

Kluczowe jest to, aby nie zaczynać od mody na konkretną technologię. AI, chmura czy mikroserwisy mogą dawać ogromną wartość, ale tylko wtedy, gdy odpowiadają na realny problem biznesowy.

Technologia powinna wynikać z procesu, skali organizacji i celu, który firma chce osiągnąć.

Nie każde przedsiębiorstwo potrzebuje dużej transformacji. Czasem większą wartość daje modernizacja jednego systemu, uporządkowanie danych albo integracja istniejących narzędzi. W innych przypadkach potrzebna jest głębsza przebudowa.

Najważniejsze jest dopasowanie skali wdrożenia bez „przewymiarowania", ale z uwzględnieniem przyszłego rozwoju.

Jak zarządzać zmianą, aby nie zaburzyć działania firmy?

Kluczowe jest założenie, że firma musi działać także w trakcie zmiany. W przypadku systemów krytycznych nie można po prostu wyłączyć starego rozwiązania i przełączyć się na nowe.

Najbezpieczniejsze jest podejście ewolucyjne. Najpierw stabilizujemy obecny system, następnie go analizujemy, a dopiero później planujemy zmiany.

Często optymalna ścieżka polega na równoległym działaniu starego i nowego systemu. Dzięki temu można porównywać dane, testować procesy i przeprowadzić tzw. soft launch.

Bardzo ważne jest skracanie pętli informacji zwrotnej: testy, walidacja danych i szybkie iteracje. To zmniejsza ryzyko błędów i skraca czas wdrożeń.

Najlepsze efekty daje sytuacja, w której jeden partner odpowiada zarówno za utrzymanie obecnych systemów, jak i wdrożenie nowych rozwiązań. To zwiększa kontrolę i minimalizuje ryzyko przestojów.

Co jest dziś największym wyzwaniem dla firm?

Największym wyzwaniem nie jest samo wdrożenie AI. Prawdziwe wyzwanie polega na tym, aby wykorzystać AI tam, gdzie przynosi realną wartość, a jednocześnie utrzymać stabilność systemów.

W praktyce oznacza to stopniową modernizację starszych systemów, uporządkowanie danych i przygotowanie środowiska IT na przyszłość.

Firmy, które podejdą do tego etapowo, nie będą musiały wybierać między innowacją a bezpieczeństwem. Mogą rozwijać się bez destabilizacji operacji.

Jakie trendy będą miały największy wpływ na zarządzanie firmami?

AI pozostaje głównym trendem, ale jego skuteczność zależy od sposobu wdrożenia. Wykorzystanie sztucznej inteligencji w sposób ogólny i nieprzemyślany nie przynosi oczekiwanych efektów.

Najbliższe lata to rozwój agentów AI, którzy nie tylko przejmą część powtarzalnych procesów, ale otrzymają możliwość podejmowania określonych decyzji. Człowiek coraz częściej będzie pełnił rolę nadzorcy i menedżera.

Równolegle rośnie znaczenie danych – bez ich uporządkowania AI nie przyniesie realnej wartości.

Istotnym trendem będzie także FinOps. Wykorzystanie AI i danych w czasie rzeczywistym powoduje wzrost kosztów infrastruktury, dlatego firmy będą szukały optymalizacji m.in. poprzez środowiska hybrydowe i lokalne modele AI.

Przedsiębiorstwo przyszłości – elastyczność, innowacje, skalowanie

PAULINA GROCHOWSKA
radczyni prawna, członkini zarządu Systemu Gazociągów Tranzytowych Europol Gaz

Przyszłość przedsiębiorstw jeszcze nigdy wcześniej nie była tak mocno powiązana z technologią i elastycznymi formami zatrudnienia. Firmy budowane przez ostatnie dwie dekady, oparte na powtarzalności procesów i hierarchicznym zarządzaniu, coraz częściej przegrywają z organizacjami, które potrafią działać zwinnie i nie boją się eksperymentować. Jaki zatem model zarządzania sprawdzi się najlepiej w przyszłości?

Odpowiedź nie brzmi „agile" ani „lean". Model, który dziś wygrywa, jest hybrydowy i warstwowy: łączy świadomy dobór metodyki projektowej, nową architekturę organizacji opartą na ludziach i agentach AI oraz elastyczną, lecz zgodną z prawem strukturę zatrudnienia. To te trzy warstwy decydują, czy firma jest jednocześnie elastyczna, innowacyjna i zdolna do skalowania.

Warstwa pierwsza: od kaskady przez agile do asynchroniczności

Klasyczny model kaskadowy, z harmonogramem Gantta i odgórnie wyznaczonymi kamieniami milowymi, był odpowiedzią na świat, w którym wymagania klienta nie zmieniają się i są możliwe do precyzyjnego zdefiniowania. Tam, gdzie projekt ma jasno określony cel, budżet i konkretny rezultat (budowa, produkcja, infrastruktura), dobry Gantt wciąż nie ma sobie równych. Z kolei filozofia Agile powstała w 2001 r. jako reakcja na te sztywne, ciężkie i kaskadowe procesy, które nie nadążały za zmieniającymi się wymaganiami i tempem ery internetu. Iteracyjne sprinty i ciągły feedback od klienta pozwala dostarczać działające oprogramowanie krok po kroku, bez czekania miesiącami na ogromne wdrożenia. Następnie metodyka Lean dołożyła do tego dyscyplinę i efektywność. Aktualnie, coraz częściej mówi się o kolejnym etapie: asynchronous agile. Zespoły rezygnują ze standardowej kultury spotkań i pracują w trybie, gdzie pracownicy sami określają swój czas pracy. Oznacza to, że komunikują się przez współdzielone dokumenty, tablice zadań i komunikatory. Zespoły nie organizują regularnych spotkań, zamiast tego dowożą wyniki i gotowe projekty. Praktycy tego podejścia (m.in. rozproszone zespoły Atlassian i Loom) wskazują, że lepiej skaluje się ono w zespołach międzynarodowych i sprzyja głębokiej pracy.

Co istotne, nowe modele nie zastępują starych, a działają równolegle. Ten sam projekt może mieć kaskadowy plan finansowy, agile'owy backlog produktowy i asynchroniczny tryb komunikacji. Najlepszym modelem zarządzania nie jest więc jedna metodyka, lecz umiejętność dobrania jej do kontekstu.

Warstwa druga: koniczynka Handy'ego w wersji 2.0

W 1989 r. Charles Handy opisał shamrock organisation, czyli organizację-koniczynę o trzech listkach: pierwszy to stały rdzeń, odpowiedzialny za ciągłość działania i najistotniejsze zadania. Drugi to sieć wyspecjalizowanych podwykonawców zatrudnianych projektowo oraz trzeci, najbardziej elastyczny, składający się z freelancerów wykonujących zadania dorywcze. Przedstawiony przez Handy'ego model okazał się proroczy, dziś działa w nim praktycznie każdy z branży kreatywnej, IT, czy konsultingowej. Ponad trzydzieści lat później liście koniczyny zmieniają się. W erze agentów sztucznej inteligencji, druga i trzecia warstwa organizacji nie musi już być w całości złożona z ludzi. Specjalistyczne zadania, kodowanie, prototypowanie, obsługę klienta, research, analizy, nie zleca się już wyłącznie freelancerom, lecz rosnącej armii agentów. Firma Gartner odnotował w 2025 r. wzrost zapytań korporacyjnych o orkiestrację wieloagentowych systemów AI o 1 445 proc. rok do roku.

Konsekwencje wdrażania agentów AI stają się szybko widoczne. Ludzki rdzeń kurczy się, ale jego waga rośnie. Człowiek odpowiada za strategię, relacje z klientem i decyzje, których agent nie powinien podejmować samodzielnie. Wbrew powszechnej narracji „AI zastępuje ludzi" trafniej będzie powiedzieć: sztuczna inteligencja zastępuje procesy, a ludzi przesuwa wyżej w łańcuchu wartości, do analizy i odpowiedzialności.

Dowodem są dane o przychodzie na pracownika. Firma Midjourney wygenerowało w 2025 r. ok. 500 mln dol. przy ok. 107 zatrudnionych osobach, to blisko 4,7 mln dol. na osobę. Cursor uzyskał ok. 3,3 mln dol. przychodu na osobę. Tradycyjne firmy uznawały poziom 200-300 tys. dol. na osobę za świetny wynik. Rośnie także rola pojedynczych founderów. Coraz częściej przedsiębiorstwo to wąski zespół kilku osób, uzupełniony stosem agentów i siecią kontraktorów, dostarczający zakres prac do niedawna wymagający kilkudziesięciu etatów.

Warstwa trzecia: elastyczne zatrudnienie i nowa rama prawna

Trzecim filarem jest rynek pracy. Elastyczne formy zatrudnienia, zwłaszcza freelancing, przestają być alternatywą dla etatu i stają się jednym z głównych kierunków jego rozwoju, szczególnie w młodszych pokoleniach. Od 8 lipca 2026 r. obowiązuje w Polsce nowelizacja ustawy o PIP, która daje inspekcji prawo do administracyjnego stwierdzenia istnienia stosunku pracy, jeśli współpraca B2B faktycznie spełnia warunki etatu z art. 22 Kodeksu pracy. Reforma nie likwiduje B2B. likwiduje „fikcyjne B2B". Dla przedsiębiorstwa przyszłości oznacza to konieczność uczciwego podejścia do stosunku pracy ze swoimi podwykonawcami.

Jaki model wygrywa

Jeden model nigdy nie będzie odpowiedzią na wszystkie problemy. Najważniejszy jest świadomy dobór metodyki do projektu (np. Gantt dla wdrożeń, scrum dla rozwoju, async-first dla pracy koncepcyjnej) oraz elastyczna warstwa kontraktorów i agentów, którą można powiększać i zmniejszać w rytmie projektów. Innowacyjność rodzi się z małego, silnego rdzenia decyzyjnego, który szybko eksperymentuje i iteruje, zamiast czekać tygodniami na decyzje przełożonych. Skalowanie zapewniają agenci AI pozwalając na większą efektywność, bez proporcjonalnego wzrostu zatrudnienia.

Wygrywać będą więc organizacje, które potrafią jednocześnie utrzymać silny rdzeń decydentów, zarządzać flotą agentów i otoczyć się siecią ludzkich ekspertów. Zwiększanie skali bez zwiększania zatrudnienia, elastyczność bez chaosu, innowacja bez przestojów, to to, co będzie cechowało przedsiębiorstwa przyszłości.

Większa skala to nie zawsze najlepszy model biznesowy

Dziś bardzo dużo mówi się o sztucznej inteligencji i automatyzacji – i słusznie, bo to jedna z największych zmian technologicznych, jakie obserwujemy od lat.

GRZEGORZ GACEK
prezes HSP Management

W mojej ocenie jednak AI powinno być przede wszystkim narzędziem wspierającym człowieka, a nie próbą zastępowania relacji międzyludzkich. Szczególnie w hotelarstwie, które z natury opiera się na kontakcie, rozmowie i umiejętności rozumienia potrzeb drugiego człowieka.

Nowoczesne technologie mają ogromne znaczenie w obszarach operacyjnych. W naszych obiektach korzystamy z systemów, które pomagają zarządzać energią, temperaturą czy wentylacją w sposób bardziej efektywny i dostosowany do rzeczywistego wykorzystania przestrzeni. Dzięki analizie danych możemy ograniczać zużycie mediów, poprawiać komfort gości i jednocześnie działać w sposób bardziej odpowiedzialny środowiskowo. Są to rozwiązania, które realnie zwiększają efektywność organizacji, choć często wymagają dużych inwestycji na początku.

Jednocześnie uważam, że w branży hospitality technologia nigdy nie zastąpi człowieka. Goście nadal oczekują uważności, rozmowy, indywidualnego podejścia i poczucia, że ktoś naprawdę rozumie ich potrzeby. Można zautomatyzować wiele procesów, ale nie da się zastąpić atmosfery tworzonej przez ludzi.

W warunkach ciągłej zmiany

Współczesny biznes funkcjonuje w warunkach ciągłej zmiany. Zmieniają się technologie, modele komunikacji i oczekiwania klientów. W hotelarstwie widzimy to bardzo wyraźnie – od sposobu projektowania przestrzeni po sam sposób odpoczynku i podróżowania. Dlatego firmy muszą być elastyczne i gotowe do ciągłego rozwoju, ale bez utraty własnej tożsamości.

Nie zawsze największa skala oznacza również najlepszy model biznesowy. Coraz częściej przewagę budują organizacje, które potrafią szybko reagować na zmiany, zachowując jednocześnie wysoką jakość i autentyczność. W moim przekonaniu właśnie to będzie jednym z najważniejszych wyzwań dla przedsiębiorstw przyszłości.

Wspierać decyzje biznesowe

88 proc. firm eksperymentuje dziś ze sztuczną inteligencją, ale aż 81 proc. organizacji nie widzi realnego wpływu tych działań na wynik finansowy. Mimo to rynek przyspiesza.

SEBASTIAN KOPIEJ
prezes zarządu Commplace

Klienci oczekują natychmiastowych odpowiedzi, dostępności 24/7 i coraz szybszego rozwiązywania problemów, dlatego firmy masowo automatyzują obsługę klienta. Coraz większym zagrożeniem nie jest dziś brak AI, ale powierzchowne korzystanie z niej bez realnej architektury procesów.

Coraz więcej AI, coraz mniej efektu

Wiele organizacji wdraża dziś AI dlatego, że „rynek tego oczekuje", a nie dlatego, że wcześniej zdiagnozowały konkretny problem biznesowy. W praktyce oznacza to, że firmy testują chatboty, generują odpowiedzi, automatyzują formularze i pokazują nowoczesność, ale organizacja nadal nie otrzymuje szybszego rozwiązania swojego problemu. To jeden z największych paradoksów obecnej transformacji: organizacje mają więcej danych i narzędzi niż kiedykolwiek wcześniej, a jednocześnie rośnie liczba błędnych decyzji i nietrafionych wdrożeń. Problem nie leży więc w samej technologii, lecz w sposobie jej wdrażania oraz w myleniu demonstracji AI z realną przewagą operacyjną.

Najpierw proces, potem automatyzacja

Sztuczna inteligencja bardzo dobrze działa tam, gdzie kluczowe są szybkość, powtarzalność, analiza dużych wolumenów danych, porządkowanie informacji i automatyczne klasyfikowanie problemów. Dlatego z powodzeniem wspiera chatboty, segregowanie zgłoszeń, analizę historycznych danych oraz automatyczne podsumowania rozmów.

Największa wartość AI nie polega jednak na zastępowaniu człowieka, ale na zwiększaniu jakości i szybkości podejmowania decyzji. Najlepiej sprawdzają się dziś modele hybrydowe, w których AI odpowiada za analizę i organizację informacji, a człowiek za interpretację i decyzję.

Gdzie firmy wpadają w pułapkę

Największe ryzyko pojawia się wtedy, gdy firmy próbują zautomatyzować obszary wymagające odpowiedzialności, interpretacji kontekstu i empatii, szczególnie w sytuacjach reklamacji, sporów finansowych czy błędów systemowych. W takich momentach klient oczekuje nie tylko odpowiedzi, ale również poczucia bezpieczeństwa i realnego zaangażowania po stronie firmy.

Wiele organizacji wpada dziś w pułapkę pozornej optymalizacji: klient otrzymuje odpowiedź szybko, ale nie otrzymuje rozwiązania, trafia między kolejnymi formularzami, nie może porozmawiać z człowiekiem i musi wielokrotnie tłumaczyć ten sam problem. Technicznie system działa poprawnie, ale relacyjnie organizacja zaczyna przegrywać.

„Pytanie czata" to nie transformacja

Firmy, które ograniczają się do zadawania pytań w ogólnych narzędziach AI, zwykle przyspieszają jedynie pojedyncze zadania, ale nie budują trwałego modelu przewagi. Bez integracji z procesami, standardami jakości, wiedzą organizacji i odpowiedzialnością decyzyjną AI pozostaje tylko warstwą efektownej improwizacji.

Według tego podejścia prawdziwa wartość pojawia się dopiero wtedy, gdy rozwiązania są szyte na miarę: dopasowane do modelu obsługi, logiki sprzedaży, komunikacji marki i realnych scenariuszy klienta. Tylko wtedy AI przestaje być modnym dodatkiem, a zaczyna działać jak wzmacniacz wyników.

> Wiele organizacji wdraża dziś AI dlatego, że „rynek tego oczekuje", a nie dlatego, że wcześniej zdiagnozowały konkretny problem biznesowy.

„Największym błędem nie jest dziś to, że firma wdroży za mało narzędzi opartych na sztucznej inteligencji. Największy błąd pojawia się wtedy, gdy organizacja myli zadawanie pytań w czacie z budowaniem realnej przewagi. AI ma sens tylko wtedy, gdy jest szyta na miarę procesów, ludzi i odpowiedzialności. Inaczej generuje sytuacje kryzysowe, a nie rozwój" – komentuje Sebastian Kopiej, prezes zarządu Commplace.

Zarządzanie firmą w erze AI wymaga dziś czegoś więcej niż wdrożenia narzędzi

Jeszcze kilka lat temu dyskusja o sztucznej inteligencji w biznesie koncentrowała się głównie wokół pytania, czy firmy powinny inwestować w AI i automatyzację. Dziś ten etap właściwie mamy już za sobą. Coraz więcej organizacji korzysta z narzędzi opartych na AI, systemów analitycznych czy automatyzacji procesów. Problem polega jednak na tym, że sama obecność technologii przestaje być wyróżnikiem.

W praktyce rynek zaczyna dzielić się nie na firmy „z AI" i „bez AI", ale na organizacje, które wykorzystują technologię powierzchownie, oraz te, które potrafią realnie przełożyć ją na jakość zarządzania, sprawniejsze procesy i lepsze decyzje biznesowe. To właśnie tutaj sztuczna inteligencja zaczyna najmocniej wpływać na sposób funkcjonowania przedsiębiorstw.

AI i analityka danych coraz częściej wspierają nie tylko działania operacyjne, ale również procesy strategiczne – od prognozowania trendów i analizy ryzyk po zarządzanie zasobami, komunikacją czy doświadczeniem klienta. Firmy zyskują dostęp do ogromnej ilości danych i możliwość podejmowania decyzji szybciej niż kiedykolwiek wcześniej.

Jednocześnie szybko okazuje się, że technologia sama w sobie nie rozwiązuje problemów organizacyjnych. W wielu firmach AI trafia do środowiska, w którym procesy są nieuporządkowane, wiedza rozproszona, a komunikacja między działami działa chaotycznie. W efekcie organizacje posiadają nowoczesne narzędzia, ale nadal funkcjonują w oparciu o przeciążenie pracowników, silosy informacyjne i reaktywne zarządzanie.

Dlatego największą wartością AI nie staje się dziś już samo generowanie treści czy automatyzacja pojedynczych zadań, ale zdolność do porządkowania organizacji i wspierania decyzji biznesowych. Dobrze wdrożona technologia może skracać czas reakcji, ograniczać liczbę błędów, poprawiać przepływ informacji i uwalniać zespoły od powtarzalnej pracy operacyjnej. To z kolei pozwala menedżerom skupiać się bardziej na strategii, rozwoju i relacjach niż na gaszeniu bieżących problemów.

Zarządzanie przedsiębiorstwem w czasach permanentnej zmienności

SZCZEPAN GORBACZ
prezes zarządu Amargo

Jeszcze kilka lat temu wiele firm przemysłowych funkcjonowało w relatywnie przewidywalnym otoczeniu. Można było planować inwestycje w dłuższej perspektywie, zakładać względną stabilność kosztów surowców, energii czy transportu oraz budować strategie rozwoju w oparciu o stopniową optymalizację procesów. Dziś sytuacja wygląda zupełnie inaczej.

Pandemia, kryzys energetyczny, wojna w Ukrainie, problemy z dostępnością surowców, rosnące wymagania regulacyjne, presja związana z ESG i transformacją energetyczną – wszystkie te zjawiska sprawiły, że przedsiębiorstwa funkcjonują obecnie w środowisku permanentnej zmienności. W praktyce oznacza to konieczność zupełnie innego podejścia do zarządzania organizacją niż jeszcze dekadę temu.

Zachować odporność operacyjną

W sektorze przemysłowym coraz wyraźniej widać, że przewagę konkurencyjną budują dziś nie wyłącznie firmy najszybciej rosnące, ale przede wszystkim te, które potrafią zachować odporność operacyjną i elastycznie reagować na zmieniające się warunki rynkowe.

Szczególnie widoczne stało się to po 2022 r. Wiele przedsiębiorstw funkcjonujących w modelu opartym na maksymalnej optymalizacji kosztowej zaczęło mierzyć się z problemami wynikającymi z zaburzeń łańcuchów dostaw, skokowych wzrostów cen energii oraz dużej zmienności rynku surowców. Firmy, które wcześniej koncentrowały się głównie na krótkoterminowej efektywności, zostały zmuszone do szybkiego przebudowania sposobu myślenia o bezpieczeństwie operacyjnym.

W praktyce oznacza to m.in.: dywersyfikację dostawców, zwiększanie odporności infrastruktury technicznej, budowanie rezerw operacyjnych, rozwój kompetencji wewnętrznych, większą kontrolę nad procesami technologicznymi i inwestowanie w monitoring i cyfryzację infrastruktury.

Coraz większe znaczenie ma również zdolność przedsiębiorstwa do funkcjonowania w warunkach wysokiej niepewności regulacyjnej. Dotyczy to szczególnie firm przemysłowych działających na styku energetyki, infrastruktury, ochrony środowiska i gospodarki obiegu zamkniętego.

Transformacja energetyczna, polityka klimatyczna Unii Europejskiej, nowe regulacje dotyczące śladu węglowego czy śladu wodnego powodują, że przedsiębiorstwa muszą dziś uwzględniać w swoich strategiach znacznie więcej czynników niż wyłącznie bieżące koszty działalności.

Dobrym przykładem jest zmienność rynku surowców obserwowana w ostatnich latach. Jeszcze niedawno wiele decyzji inwestycyjnych opierało się przede wszystkim na prostym rachunku ekonomicznym. Obecnie firmy coraz częściej analizują również: dostępność materiałów w długim terminie, odporność łańcucha dostaw, energochłonność procesów, możliwość recyklingu i ponownego wykorzystania surowców i ryzyka regulacyjne związane z ESG i raportowaniem środowiskowym.

To powoduje, że zmienia się także sama rola liderów i osób zarządzających przedsiębiorstwami. Zarządzanie organizacją przemysłową nie polega już wyłącznie na nadzorowaniu produkcji czy sprzedaży. Coraz częściej wymaga łączenia kompetencji technologicznych, finansowych, regulacyjnych i strategicznych.

W praktyce oznacza to konieczność podejmowania decyzji w warunkach ograniczonej przewidywalności rynku. W wielu branżach nie da się już tworzyć strategii wyłącznie w oparciu o historyczne dane i klasyczne modele wzrostu. Kluczowa staje się zdolność szybkiej adaptacji.

> Coraz większą rolę odgrywa bezpieczeństwo infrastruktury technicznej i procesowej.

Bezpieczeństwo infrastruktury technicznej i procesowej

Jednocześnie coraz większą rolę odgrywa bezpieczeństwo infrastruktury technicznej i procesowej. Jeszcze do niedawna kwestie związane z odpornością systemów przemysłowych często traktowano jako obszar stricte techniczny. Dziś stają się one elementem strategicznego zarządzania przedsiębiorstwem.

Dotyczy to m.in.: bezpieczeństwa magazynowania substancji chemicznych, stabilności systemów wodnych, odporności infrastruktury na przerwy energetyczne, bezpieczeństwa nowych technologii energetycznych i cyfrowego monitoringu instalacji i procesów.

Wraz z rozwojem transformacji energetycznej pojawiają się również nowe ryzyka infrastrukturalne, które jeszcze kilka lat temu praktycznie nie występowały w debacie publicznej. Dobrym przykładem są magazyny energii, bezpieczeństwo instalacji opartych na nowych technologiach czy konieczność dostosowania infrastruktury przemysłowej do rosnących wymagań środowiskowych i regulacyjnych.

To powoduje, że firmy przemysłowe coraz częściej muszą patrzeć na inwestycje nie wyłącznie przez pryzmat kosztu początkowego, ale całego cyklu życia infrastruktury oraz jej długoterminowej odporności operacyjnej.

Coraz wyraźniej widać również zmianę podejścia do gospodarki obiegu zamkniętego. Jeszcze kilka lat temu wiele firm traktowało GOZ przede wszystkim jako element polityki wizerunkowej lub wymóg regulacyjny. Dziś coraz częściej staje się ona realnym elementem strategii biznesowej.

W praktyce przedsiębiorstwa zaczynają dostrzegać, że ograniczenie zużycia surowców obniża podatność na wahania rynku, wydłużenie życia infrastruktury zmniejsza koszty inwestycyjne, odzysk materiałów poprawia stabilność operacyjną, a efektywność zasobowa staje się elementem przewagi konkurencyjnej.

Widać to szczególnie w sektorach infrastrukturalnych i przemysłowych, gdzie koszty materiałów, energii oraz utrzymania instalacji mają bezpośredni wpływ na rentowność przedsiębiorstwa.

Zmienia się również podejście do technologii i cyfryzacji. W przemyśle coraz większe znaczenie mają systemy monitoringu infrastruktury, analityka danych oraz rozwiązania umożliwiające predykcyjne zarządzanie utrzymaniem ruchu.

W praktyce oznacza to odejście od modelu reaktywnego, czyli naprawiania problemów dopiero po wystąpieniu awarii, na rzecz modelu predykcyjnego, opartego na analizie danych i bieżącym monitoringu parametrów pracy instalacji.

To szczególnie istotne w przypadku infrastruktury krytycznej oraz systemów, których awaria może powodować poważne skutki operacyjne, środowiskowe lub finansowe. Równocześnie przedsiębiorstwa muszą dziś mierzyć się z coraz większą presją dotyczącą transparentności i raportowania. Klienci, partnerzy biznesowi, instytucje finansowe i regulatorzy oczekują od firm nie tylko efektywności finansowej, ale również odpowiedzialnego podejścia do środowiska, bezpieczeństwa oraz zarządzania ryzykiem.

W takich warunkach kluczowe znaczenie ma długoterminowe myślenie strategiczne. Coraz trudniej budować stabilną organizację wyłącznie w oparciu o krótkoterminową optymalizację kosztową. Znacznie większego znaczenia nabierają: odporność operacyjna, bezpieczeństwo infrastruktury, elastyczność technologiczna, kompetencje zespołów, a także zdolność adaptacji do zmian regulacyjnych i rynkowych.

To właśnie te elementy będą w najbliższych latach decydowały o konkurencyjności przedsiębiorstw przemysłowych funkcjonujących w coraz bardziej wymagającym i nieprzewidywalnym otoczeniu gospodarczym.

Zmiana stałym elementem biznesu

Kryzysy gospodarcze, zakłócenia łańcuchów dostaw, cyberataki czy napięcia geopolityczne sprawiają, że odporność organizacyjna staje się dziś jednym z najważniejszych wyzwań dla firm.

JAKUB KOZAK
Area Sales Director ECE Genetec

Coraz więcej przedsiębiorstw dostrzega, że przewagę konkurencyjną buduje już nie tylko tempo rozwoju, ale przede wszystkim zdolność do utrzymania ciągłości działania i szybkiego reagowania na zmiany.
Współczesne organizacje funkcjonują w permanentnej zmienności. Firmy, które chcą utrzymać stabilność operacyjną, muszą budować odporność wielowymiarowo – zarówno na poziomie technologii, procesów, jak i zarządzania ryzykiem.

Technologia wspiera ciągłość działania
Kluczowe znaczenie ma dziś dostęp do danych w czasie rzeczywistym, możliwość monitorowania wielu lokalizacji jednocześnie oraz automatyzacja procesów bezpieczeństwa.
Szczególnie ważna jest elastyczność infrastruktury technologicznej. Firmy coraz częściej odchodzą od zamkniętych systemów na rzecz rozwiązań otwartych i chmurowych, które pozwalają szybciej dostosowywać się do zmieniających się warunków rynkowych.
Organizacje muszą być przygotowane na sytuacje, w których część procesów zostanie zakłócona praktycznie z dnia na dzień, np. sektor paliwowy. O odporności firmy decyduje dziś m.in. możliwość szybkiego przełączenia operacji, zdalnego zarządzania infrastrukturą oraz integracji danych pochodzących z różnych systemów.
Dlatego, nowoczesne platformy bezpieczeństwa coraz częściej pełnią funkcję nie tylko ochronną, ale również operacyjną i analityczną. Dane zbierane przez systemy monitoringu czy kontroli dostępu mogą wspierać firmy także w optymalizacji procesów i zwiększaniu efektywności operacyjnej.

Cyberbezpieczeństwo i zabezpieczenia techniczne coraz bliżej siebie
Jednym z najważniejszych trendów ostatnich lat jest zacieranie się granicy pomiędzy cyberbezpieczeństwem a zabezpieczeniami technicznymi. Coraz więcej urządzeń wykorzystywanych w organizacjach jest podłączonych do sieci, co sprawia, że potencjalny cyberatak może wpływać również na funkcjonowanie infrastruktury technicznej.
Firmy powinny patrzeć na bezpieczeństwo w sposób holistyczny. Dziś cyberatak może sparaliżować działanie zakładu produkcyjnego czy centrum logistycznego równie skutecznie jak awaria fizyczna. Dlatego konieczna jest integracja kompetencji oraz systemów odpowiedzialnych za oba obszary.
Istotne znaczenie ma także regularna aktualizacja systemów, kontrola dostępu do danych oraz budowanie świadomości pracowników. To właśnie czynnik ludzki nadal pozostaje jednym z najczęstszych źródeł incydentów bezpieczeństwa.

> Odporność biznesowa nie polega wyłącznie na minimalizowaniu ryzyka, ale przede wszystkim na zdolności do szybkiej adaptacji.

Elastyczność ważniejsza niż przewidywanie
Ostatnie lata pokazały, że firmy nie są w stanie przewidzieć wszystkich kryzysów, ale mogą przygotować organizację na szybkie reagowanie.
Odporność biznesowa nie polega wyłącznie na minimalizowaniu ryzyka, ale przede wszystkim na zdolności do szybkiej adaptacji. Możemy przetestować każdy scenariusz, a i tak wydarzy się coś na co nie jesteśmy przygotowani. W tej sytuacji, organizacja i sposób zarządzania kryzysem musi być na tyle elastyczna, aby szybko dostosować się do zagrożenia i je wyeliminować.
Sposobem na przygotowanie firmy, jest zwiększenie inwestycji w rozwiązania oparte na chmurze, automatyzację bezpieczeństwa oraz integrację systemów. Organizacje, które już dziś budują elastyczne środowiska technologiczne i rozwijają kompetencje związane z bezpieczeństwem, będą w przyszłości bardziej odporne na kryzysy gospodarcze i cybernetyczne. Jeśli budujemy rozwiązania tak, by mogły dostosować się do naszych potrzeb biznesowych, organizacja poradzi sobie z każdym kryzysem.

Ci, którzy zignorują sztuczną inteligencję, nie odrobią strat

Firmy, także te, w których działam ja, wprowadzają sztuczną inteligencję na różnym poziomie zaangażowania. W wielu miejscach zastąpiła ona copywriterów. Co za tym idzie, osoba, która tworzyła teksty, dalej to robi, ale ze wsparciem sztucznej inteligencji. Taki pracownik otrzymuje także dodatkowe obowiązki.

DAMIAN ABRAMOWICZ
mentor biznesowy i życiowy, trener sprzedaży, biznesmen

Dobrą praktyką jest, aby w związku z wprowadzaniem automatyzacji nie zwalniać ludzi. Szefostwo powinno zadbać o to, by pracownicy stali się multizadaniowi. Na pewno jest to lepsze niż zwalnianie ekspertów i specjalistów na rzecz AI. Już wiadomo, że na ten moment nie przynosi to dobrych efektów, bo do zarządzania AI potrzebny jest człowiek, który się po prostu na tym zna, wie także, jak zadawać pytania. Wszyscy uczymy się sztucznej inteligencji. Róbmy to mądrze.

AI, czyli automatyzacje wspierające człowieka
AI jest w stanie wspierać bardzo wiele zadań w firmach, działać na różnych szczeblach – od księgowości po wysyłki produktów czy kontakt z klientem. My przykładowo mamy wprowadzoną sztuczną inteligencję do wszelkich automatyzacji w firmie, czyli wszystko to, co do tej pory wymagało ręki człowieka, ale też niestety narażało firmę na ryzyko popełnienia błędu, jest zautomatyzowane. W mojej działalności podróżniczej bardzo mocno używamy AI w aplikacji SkyClass.pl, czyli do szukania lotów, wybierania najlepszych propozycji, jeśli chodzi o tanie loty i połączenia. Naturalnie sztuczna inteligencja bardzo nam pomaga w tematach rozliczeń, bilansów wszelkiego rodzaju czy podsumowań. Moduły AI mamy wprowadzone również we wszystkich plikach sprzedażowych, dzięki temu jesteśmy w stanie na bieżąco bardzo precyzyjnie śledzić trendy rynkowe i szybciej reagować.

Sztuczna inteligencja a ryzyko utraty pracy
Osobiście uważam, że AI jest łącznikiem między ludźmi, między działami, jeżeli jest mądrze przez firmę wykorzystywane. Pracownicy powinni być w pierwszej kolejności przeszkoleni z danego zakresu. Bo AI to dla wielu osób jedynie następca przeglądarki, co jest oczywiście wielkim niedopowiedzeniem. Sztuczna inteligencja będzie nas wspierać lub wręcz wyręczać. Przykładowo SI jest w stanie fizycznie wykonywać pewne czynności za nas, np. przygotowywać bilanse, sprawdzać kursy walut czy różnego rodzaju notowania. Rano przychodzimy do pracy i wszystko mamy przygotowane, zaoszczędziliśmy godzinę naszego czasu. Wszystko, co do tej pory robiliśmy ręcznie, mamy dzięki AI zautomatyzowane. Naturalnie człowiek nadal powinien wyników pilnować, ponieważ sztuczna inteligencja popełnia błędy.
Naszych pracowników AI wspiera chociażby przy odpowiadaniu na maile. Dotąd było tak, że jeśli klient zapytał o coś w piątek o 15:00, kiedy firma była już zamknięta, to czekał na odpowiedź do poniedziałku. Pracownik musi przecież „odkopać się" z weekendowych maili, klient czeka, czasami się frustruje. Obecnie AI odpowiada w trybie live i są to odpowiedzi bardzo precyzyjne. Zna naszą ofertę, więc bywa tak, że jest w stanie doprowadzić niemalże do zamknięcia kontraktu sprzedażowego.
Czy sztuczna inteligencja jest zagrożeniem? Na pewno wiele firm zwolni ludzi i zostawi sobie garstkę do obsługi AI. Uważam jednak, że to się po jakimś czasie zemści. Nie jesteśmy na etapie, na którym AI jest praktycznie bezobsługowe. My sobie jasno postawiliśmy, że w każdej dziedzinie, w której pracujemy, i w każdej firmie nie chcemy zwalniać ludzi. Wolimy, aby dzięki AI ich zadania i czas były zoptymalizowane, aby bez problemu mogli spełniać się w pracy i osiągać dobre wyniki bez dodatkowego stresu. To sprzyja efektywności. Każdy jest zadowolony: pracownik, bo nie jest przeciążony, i pracodawca, bo ma lepsze rezultaty oraz pracowników, którzy nie są wypaleni.

Myślisz, że w swojej firmie nie potrzebujesz AI? Mylisz się.
Nie ma chyba takiego obszaru, do którego AI nie można zastosować. Bardzo lubię przekomarzać się z ludźmi, którzy mówią: „w mojej branży to się nie da, bo..." i tu pada wymówka. Prawda jest taka, że praktycznie w każdej działalności występują kwestie prawne, rozliczenia czy kontakt z konsumentem i klientem, a do tego możemy wykorzystać sztuczną inteligencję. Uważam, że wsparcie ze strony sztucznej inteligencji będzie takie, na ile sobie pozwolimy. Na pewno wymaga to dzisiaj elastyczności ze strony zarządów firm oraz pracowników. AI zmienia się bardzo szybko, nie jesteśmy w stanie nauczyć się jej tak jak innych rzeczy z podręcznika. Bardziej chodzi o to, aby nauczyć się ją wykorzystywać w swoim polu działania. Firmy, które to wiedzą, bardzo zyskają. Te, które się wzbraniają, mogą zostać w tyle i już nie nadrobić strat.

Menedżer w czasach permanentnej niepewności gospodarczej i geopolitycznej

JAKUB PAW
Co-Founder & General Partner
w GRUPA FORMA

W czasach permanentnej niepewności gospodarczej i geopolitycznej rola menedżera zmieniła się bardziej niż w poprzednich dwóch dekadach razem wziętych. I będzie zmieniać się dalej.

Jeszcze kilka lat temu organizacje funkcjonowały w rzeczywistości względnej przewidywalności – można było budować kilkuletnie strategie, opierać się na stabilnych założeniach i planować rozwój w uporządkowany sposób. Dziś coraz częściej okazuje się, że turbulencje nie są wyjątkiem między okresami stabilności, lecz nowym środowiskiem działania biznesu.
Na początku lat 20. wszyscy myśleliśmy, że to przejściowy moment. Dziś wygląda na to, że nie była to anomalia tylko początek nowego otoczenia biznesu. I zamiast czekać na „powrót do normalności", trzeba nauczyć się działać skutecznie właśnie w takich warunkach.

Prawdziwy test
Dla firm związanych z branżą retail, hospitality i powierzchni komercyjnych pierwszym prawdziwym testem odporności był okres pandemii. Z dnia na dzień zatrzymały się galerie handlowe, restauracje, hotele i inwestycje. Dla organizacji realizujących przestrzenie komercyjne oznaczało to konieczność całkowitej zmiany sposobu planowania, zarządzania procesami i podejmowania decyzji.

To był moment, kiedy trzeba było poruszać się bez mapy. Nikt nie wiedział, co wydarzy się za tydzień czy miesiąc. Realizowaliśmy wtedy projekty na kilkunastu rynkach jednocześnie. Każdy z nich reagował inaczej i w innym tempie. Obostrzenia zmieniały się dynamicznie, a często były ze sobą sprzeczne. W pewnym momencie wszyscy przeszliśmy ze sterowania strategicznego na sterowanie ręczne.
Właśnie w takich warunkach najmocniej ujawnia się nowa rola menedżera. Nie jako administratora procesów, ale lidera adaptacji, osoby, która potrafi utrzymać kierunek mimo braku pełnej kontroli nad okolicznościami. Coraz większego znaczenia nabiera także odporność psychiczna lidera: jego zdolność do zachowania spokoju, podejmowania decyzji pod presją i budowania poczucia bezpieczeństwa w zespole nawet wtedy, gdy sam funkcjonuje w warunkach wysokiej niepewności. Organizacje bardzo szybko wyczuwają bowiem brak stabilności po stronie zarządzających, jeśli lider zaczyna się chwiać, zespół również przechodzi w tryb defensywny, koncentrując się bardziej na ograniczaniu ryzyka niż na rozwoju i skutecznym działaniu.

Zespół ogromnym aktywem
Jedną z najważniejszych decyzji w czasie kryzysu była ta dotycząca ludzi. Nie zdecydowaliśmy się na redukcję zatrudnienia, mimo ogromnej presji rynkowej i niepewności dotyczącej przyszłości branży. Wiedzieliśmy, że zespół jest naszym ogromnym aktywem i współtworzył to, kim jesteśmy dzisiaj. Uznaliśmy też, że odbudowanie sprawnej i zgranej kadry po pandemii kosztowałoby wielokrotnie więcej niż utrzymanie jej przez nią. Dlatego nie zwolniliśmy nikogo i to bez sięgania po wsparcie publiczne.

To podejście pokazuje zmianę w sposobie myślenia współczesnych liderów. Coraz częściej krótkoterminowa optymalizacja ustępuje miejsca decyzjom budującym odporność organizacji w dłuższej perspektywie. Menedżer przyszłości musi umieć działać szybko, ale jednocześnie nie może podejmować decyzji wyłącznie pod wpływem emocji i chwilowego lęku.

Jednocześnie współczesne przywództwo wymaga ogromnej elastyczności decyzyjnej. W realiach ciągłych zmian czekanie na komplet danych staje się coraz rzadziej możliwą strategią działania, w praktyce oznacza bowiem utratę czasu, którego rynek po prostu nie oddaje.
Czekanie na pełny obraz sytuacji często kończy się tym, że pociąg już odjechał. Klucz jest gdzie indziej, w umiejętności szybkiego rozpoznania błędu i korygowania kursu, zanim opóźnienie zacznie kosztować więcej niż sama pomyłka.
Pandemia była jednak dopiero początkiem zmian. Kolejnym przełomowym momentem stała się wojna w Ukrainie, która dla wielu firm oznaczała konieczność redefinicji planów ekspansji i strategii rozwoju.

Kryzysy tworzą nowe możliwości
Byliśmy w trakcie zaawansowanych rozmów o ekspansji na rynki wschodnie. W 2022 r. te rozmowy skończyły się praktycznie z dnia na dzień. Pamiętam moment wybuchu wojny. Byliśmy wtedy na spotkaniu z klientem i nagle wszyscy przestali rozmawiać o biznesie. Nikt nie zadawał już pytań o harmonogramy i budżety. Każdy zadawał sobie pytanie, co będzie dalej.

Jednocześnie doświadczenia ostatnich lat pokazały, że kryzysy, oprócz zagrożeń, tworzą również nowe możliwości dla organizacji potrafiących szybko adaptować się do zmieniających się realiów. Firmy o większej tolerancji na ryzyko i większej zdolności operacyjnej często potrafią wykorzystać moment rynkowego chaosu do dalszego rozwoju.
Nie można patrzeć na takie sytuacje wyłącznie przez pryzmat zagrożeń. Awersja do ryzyka, którą wykazuje większość rynku w trudnych warunkach, dla niektórych firm staje się oknem rozwojowym. Obserwuję to dziś z bliska. Firmy, które nie wycofały się z trudnych rynków, budują tam przewagę, którą konkurencji trudno będzie nadrobić.

Nowoczesny menedżer
Nowoczesny menedżer musi dziś łączyć odporność psychiczną, umiejętność szybkiego reagowania i zdolność prowadzenia organizacji w warunkach ograniczonej przewidywalności. W praktyce oznacza to konieczność podejmowania decyzji nie w oparciu o wieloletnią stabilność rynku, lecz na bazie danych, które są dostępne tu i teraz. W obecnych realiach zarządzanie coraz rzadziej polega na wyznaczaniu odległego, w pełni przewidywalnego scenariusza. Znacznie ważniejsza staje się umiejętność utrzymania właściwego kierunku i reagowania na bieżące sygnały z rynku, zanim pojawią się większe zagrożenia. Rolą lidera nie jest więc tworzenie iluzji pełnej kontroli, ale budowanie w organizacji poczucia stabilności, sprawczości i gotowości do działania nawet w dynamicznie zmieniającym się otoczeniu.
Menedżer nie może paraliżować organizacji własnymi obawami. Ma do nich prawo, ale nie ma prawa nimi zarażać zespołu. Jednocześnie lider musi mieć odwagę przyznać się do błędu, bo dziś transparentność buduje zaufanie bardziej niż pozorna nieomylność.
Zmienia się także sposób planowania biznesu. Wiele firm odchodzi od sztywnego, przywiązania do procedur na rzecz bardziej scenariuszowego podejścia do zarządzania.

Firmy realizujące przestrzenie komercyjne na arenie międzynarodowej muszą równolegle uwzględniać wiele czynników jednocześnie – od sytuacji geopolitycznej i wahań kursów walut, przez dostępność materiałów i komponentów, po dynamicznie zmieniające się koszty logistyki oraz presję czasową po stronie inwestorów. W praktyce oznacza to konieczność ciągłej aktualizacji założeń, szybkiej analizy ryzyk i podejmowania decyzji w czasie rzeczywistym.
To właśnie zdolność do adaptacji staje się dziś jedną z najważniejszych przewag konkurencyjnych organizacji. W świecie permanentnej zmiany wygrywają niekoniecznie największe firmy, lecz te, które potrafią szybciej reagować, podejmować decyzje mimo niepełnych danych i utrzymywać sprawność operacyjną nawet pod silną presją rynku. Dziś rolą menedżera nie jest już zarządzanie przewidywalnością, ale budowanie organizacji gotowej funkcjonować skutecznie również wtedy, gdy przewidywalności po prostu brakuje.

Cyberbezpieczeństwo to warunek stabilnego funkcjonowania biznesu

Jeszcze kilka lat temu cyberbezpieczeństwo było postrzegane głównie jako obszar odpowiedzialności działów IT. Dziś to podejście przestaje być aktualne.

JOANNA CHMIELAK
Enterprise Sales Manager w firmie Fortinet

Rosnąca skala cyberzagrożeń, postępująca cyfryzacja gospodarki oraz coraz większa zależność firm od systemów informatycznych sprawiają, że bezpieczeństwo cyfrowe staje się jednym z kluczowych elementów strategicznego zarządzania przedsiębiorstwem.

Potwierdzają to także dane z raportu Fortinet Cybersecurity Skills Gap Global 2025: aż 95 proc. firm na świecie traktuje cyberbezpieczeństwo jako strategiczny obszar inwestycji. Jednocześnie w ponad połowie organizacji konsekwencje poważnych incydentów cybernetycznych ponoszą również członkowie zarządów, co pokazuje, że cyberodporność jest już nie tylko wyzwaniem technologicznym, ale także odpowiedzialnością na poziomie najwyższego kierownictwa.

Zmienia się nie tylko skala zagrożeń, ale również ich znaczenie dla biznesu Cyberincydenty coraz częściej prowadzą nie tylko do utraty danych, lecz także do przestojów operacyjnych, zakłóceń w łańcuchach dostaw, problemów z realizacją usług czy wielomilionowych strat finansowych. Co druga firma przebadana w raporcie Fortinet poniosła po cyberataku koszty przekraczające milion dolarów, a 59 proc. wracało do pełnej sprawności miesiąc lub dłużej. Cyberatak, który kiedyś był przede wszystkim problemem technologicznym, dziś może bezpośrednio wpływać na stabilność operacyjną firmy, jej reputację i zdolność do utrzymania ciągłości działania.

Każda firma jest dziś cyfrowa

Jednocześnie cyfrowa transformacja objęła dziś praktycznie wszystkie sektory gospodarki. Produkcja, energetyka, logistyka, handel czy sektor finansowy opierają dziś swoje funkcjonowanie na złożonych środowiskach integrujących systemy IT, technologie operacyjne (OT), rozwiązania chmurowe oraz urządzenia Internetu Rzeczy (IoT). Granica między przedsiębiorstwem technologicznym a „tradycyjną" firmą coraz bardziej się zaciera.

Szczególnie wyraźnie widać to w sektorach związanych z infrastrukturą krytyczną. Cyfryzacja przemysłu czy energetyki przynosi ogromne korzyści operacyjne, ale jednocześnie zwiększa poziom zależności od systemów cyfrowych oraz podatność na cyberzagrożenia. W efekcie cyberatak może dziś wpływać nie tylko na pojedynczą firmę, lecz także na funkcjonowanie całych ekosystemów gospodarczych i usług kluczowych dla państwa i społeczeństw. Kluczowe znaczenie zyskują więc odporność operacyjna, zdolność do szybkiego wykrywania incydentów oraz możliwość utrzymania ciągłości działania nawet w przypadku naruszenia bezpieczeństwa.

> Bezpieczeństwo cyfrowe należy postrzegać nie jako projekt technologiczny, lecz jako trwały element strategii biznesowej i zarządzania ryzykiem.

Przyspieszenie w tempie maszynowym

Co ważne, w ostatnich latach także cyberprzestępczość przeszła własną transformację cyfrową. Rozwój sztucznej inteligencji i automatyzacji narzędzi do przeprowadzania cyberataków sprawił, że działania przestępców stały się szybsze, bardziej uporządkowane i prowadzone na niespotykaną wcześniej skalę. Z raportu Fortinet 2026 Global Threat Landscape wynika, że liczba potwierdzonych ofiar ransomware wzrosła rok do roku aż o 389 proc. Jednocześnie czas pomiędzy ujawnieniem podatności a próbą jej wykorzystania skrócił się w wielu przypadkach z kilku dni do zaledwie 24–48 godzin.

To przyspieszone tempo zmienia reguły gry. Firmy nie mogą już opierać bezpieczeństwa na reaktywnym modelu działania, w którym zagrożenia analizuje się dopiero po wystąpieniu incydentu. Współczesna ochrona musi funkcjonować jako ciągły proces obejmujący technologię, ludzi i procedury organizacyjne. Coraz częściej o poziomie cyberdojrzałości przedsiębiorstwa decyduje nie to, czy padnie ono ofiarą ataku, ale jak szybko będzie w stanie odzyskać sprawność operacyjną.

Dodatkową presję wywierają regulacje. Rozporządzenie DORA czy nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC), wprowadzająca do polskiego porządku przepisy dyrektywy NIS2, formalnie przenoszą odpowiedzialność za cyberodporność na poziom strategicznego zarządzania przedsiębiorstwem. Firmy muszą dziś nie tylko wdrażać rozwiązania ochronne, ale również zarządzać ryzykiem, raportować incydenty, dbać o bezpieczeństwo łańcucha dostaw oraz zapewniać ciągłość działania. Cyberbezpieczeństwo staje się więc jednym z elementów ładu korporacyjnego i obszarem wymagającym aktywnego zaangażowania zarządu.

Cyberodporność zaczyna się od ludzi

To szczególnie istotne w czasie, gdy wiele przedsiębiorstw nadal zmaga się z luką kompetencyjną w obszarze cyberbezpieczeństwa. Z raportu Fortinet Cybersecurity Skills Gap Global 2026 wynika, że 56 proc. liderów IT wskazuje niedobór specjalistów jako jedną z głównych przyczyn poważnych incydentów bezpieczeństwa. Jednocześnie firmy coraz wyraźniej dostrzegają, że budowanie cyberodporności nie może opierać się wyłącznie na inwestycjach technologicznych. Równie ważne stają się edukacja pracowników, rozwój kompetencji oraz budowanie kultury współdzielonej odpowiedzialności za bezpieczeństwo cyfrowe. Dlatego aż 92 proc. firm badanych przez Fortinet planuje w ciągu najbliższych 12 miesięcy inwestować w szkolenia lub certyfikacje związane ze sztuczną inteligencją w obszarze cyberbezpieczeństwa. 59 proc. podmiotów rozwija wewnętrzne programy szkoleniowe lub programy przekwalifikowania pracowników.

W świecie coraz silniej opartym na danych i połączonych systemach IT, cyberbezpieczeństwo przestaje być dodatkiem do transformacji cyfrowej, a staje się jednym z fundamentów stabilnego funkcjonowania przedsiębiorstwa. Firmy konkurują dziś nie tylko jakością usług czy poziomem innowacyjności, ale również zdolnością do utrzymania odporności operacyjnej w środowisku rosnących zagrożeń i cyfrowych zależności. Dlatego bezpieczeństwo cyfrowe należy postrzegać nie jako projekt technologiczny, lecz jako trwały element strategii biznesowej i zarządzania ryzykiem.

NAJDROŻSZE RYZYKO CYBERNETYCZNE? CZŁOWIEK WSPIERANY PRZEZ AI

Choć cyberataki coraz częściej kojarzą się z zaawansowaną sztuczną inteligencją i działalnością grup sponsorowanych przez państwa, rzeczywistość wygląda znacznie bardziej prozaicznie.

ADAM KASSENBERG
kierownik specjalizacji Cybersecurity w Polsko-Japońska Akademia Technik Komputerowych

Największe straty dla firm wciąż powodują podstawowe błędy ludzi: kliknięcie w fałszywy link, otwarcie zainfekowanego załącznika czy przelew wykonany pod presją czasu. Dziś jednak cyberprzestępcy otrzymali nowe narzędzie – AI – które sprawia, że stare metody oszustw stają się szybsze, tańsze i znacznie trudniejsze do wykrycia. To rutynowy phishing, podszywanie się pod przełożonego czy kontrahenta oraz brak aktualizacji oprogramowania odpowiadają za największe szkody. Te zagrożenia wydają się „nudne", dlatego są bagatelizowane – aż do momentu, gdy firma traci dane albo setki tysięcy złotych.

Największe zagrożenie? Człowiek

Według danych przywoływanych przez ekspertów bezpieczeństwa, nawet 70–85 proc. skutecznych cyberataków rozpoczyna się od prostego błędu użytkownika. Fałszywe wiadomości e-mail, linki prowadzące do spreparowanych stron logowania czy prośby o pilny przelew nadal pozostają najskuteczniejszą metodą infiltracji organizacji.

Problem polega na tym, że tradycyjne procedury i systemy ochrony przestają wystarczać, jeśli pracownicy działają automatycznie i pod presją czasu. Cyberprzestępcy doskonale rozumieją psychologię użytkowników – wykorzystują pośpiech, stres i zaufanie do znanych marek czy przełożonych.

W praktyce cyberbezpieczeństwo przegrywa dziś częściej z rutyną niż z wyrafinowanym hakerem.

AI zmienia zasady gry

Sztuczna inteligencja nie stworzyła nowego rodzaju zagrożeń, ale znacząco zwiększyła skuteczność już istniejących metod ataku. Dzięki AI przestępcy mogą dziś przygotowywać perfekcyjnie napisane wiadomości phishingowe, pozbawione błędów językowych i dopasowane do konkretnej osoby lub stanowiska.

Coraz większym problemem stają się również deepfake'i – fałszywe nagrania głosowe i wideo, które mogą imitować członków zarządu, kontrahentów czy klientów. W efekcie oszustwa finansowe stają się bardziej wiarygodne niż kiedykolwiek wcześniej.

Na razie przewagę zyskują atakujący. AI ułatwia phishing, deepfake'i i automatyzację ataków. To oznacza, że kampanie, które kiedyś wymagały tygodni przygotowań, dziś można stworzyć w kilka godzin.

Sztuczna inteligencja obniża także próg wejścia dla cyberprzestępców. Nawet mniej zaawansowane grupy mogą dziś prowadzić skuteczne kampanie phishingowe na ogromną skalę, korzystając z gotowych narzędzi AI.

Wiele incydentów pozostaje niewidocznych

Choć liczba zgłaszanych cyberincydentów rośnie, eksperci ostrzegają, że oficjalne statystyki pokazują jedynie fragment rzeczywistego obrazu zagrożeń.

> Szacuje się, że średni koszt incydentu cyberbezpieczeństwa dla polskiej firmy wynosi obecnie około 30–35 tys. zł.

Z danych CERT Polska wynika, że w 2025 r. zarejestrowano około 658 tys. zgłoszeń dotyczących cyberbezpieczeństwa, a obsłużono około 261 tys. incydentów. To ogromny wzrost względem roku poprzedniego, jednak – jak zaznacza Kassenberg – wynika on głównie z lepszej wykrywalności i większej świadomości organizacji.

Wiele firm żyje w przekonaniu, że skoro niczego nie zauważyły, to nic się nie wydarzyło. Tymczasem brak wykrycia nie oznacza braku incydentu.

Najtrudniejsze do wykrycia są niewielkie wycieki danych oraz sytuacje, w których organizacja staje się nieświadomie pośrednikiem w kolejnych cyberatakach. Tego typu incydenty często wychodzą na jaw dopiero po czasie – gdy pojawiają się problemy u partnerów biznesowych albo dochodzi do utraty danych klientów.

Ataki na łańcuch dostaw rosną w siłę

Coraz większym zagrożeniem są również ataki na łańcuch dostaw. W praktyce oznacza to, że cyberprzestępcy nie atakują bezpośrednio głównego celu, lecz wykorzystują słabszego podwykonawcę lub dostawcę usług. Jeden zhakowany partner może otworzyć drzwi do dziesiątek lub setek organizacji jednocześnie.

Problem dotyczy nie tylko firm IT. Zagrożeniem mogą być również dostawcy usług serwisowych, firmy utrzymujące infrastrukturę czy podmioty posiadające fizyczny dostęp do systemów organizacji.

Wiele przedsiębiorstw nadal nie audytuje bezpieczeństwa swoich partnerów i nie monitoruje dostępu osób trzecich do infrastruktury. Tymczasem właśnie te „niewidoczne" zależności coraz częściej stają się punktem wejścia dla cyberataków.

Jeden procent, który może zatrzymać firmę

Większość prób ataków jest skutecznie blokowana przez systemy bezpieczeństwa. Problemem pozostaje jednak ten niewielki odsetek incydentów, który przełamuje ochronę. Ten przysłowiowy „1 proc." może sparaliżować działalność firmy na tygodnie.

Szacuje się, że średni koszt incydentu cyberbezpieczeństwa dla polskiej firmy wynosi obecnie około 30–35 tys. zł. W przypadku średnich i dużych organizacji realne straty – uwzględniające przestoje, utratę kontraktów, kary oraz odszkodowania – mogą jednak sięgać od kilkuset tysięcy do nawet kilkunastu milionów złotych.

Co istotne, często największym problemem okazują się nie koszty techniczne, ale utrata zaufania klientów oraz zakłócenie działalności operacyjnej.

Cyberbezpieczeństwo to dziś temat dla zarządów

Eksperci coraz częściej podkreślają, że cyberbezpieczeństwo nie może być traktowane wyłącznie jako odpowiedzialność działu IT. To kwestia strategiczna, wpływająca bezpośrednio na ciągłość działania biznesu.

Najczęstsze błędy organizacyjne to m.in. brak obowiązkowego MFA, odkładanie aktualizacji systemów, brak ćwiczeń reagowania na incydenty czy ograniczanie budżetów bezpieczeństwa „w imię optymalizacji".

Cyberbezpieczeństwo nie jest jednorazowym zakupem ani pobocznym tematem technologicznym. To element kultury organizacyjnej. Najtańszą ochroną pozostaje prewencja: regularne szkolenia, symulacje phishingowe i konsekwentne przestrzeganie podstawowych zasad bezpieczeństwa.