BEZPIECZEŃSTWO OBIEKTÓW HANDLOWYCH:

PROGNOZA ZAGROŻEŃ I NOWE TRENDY W REAGOWANIU

Instytut RESCON

Collegium Civitas

CENTRUM BADAŃ NAD TERRORYZMEM

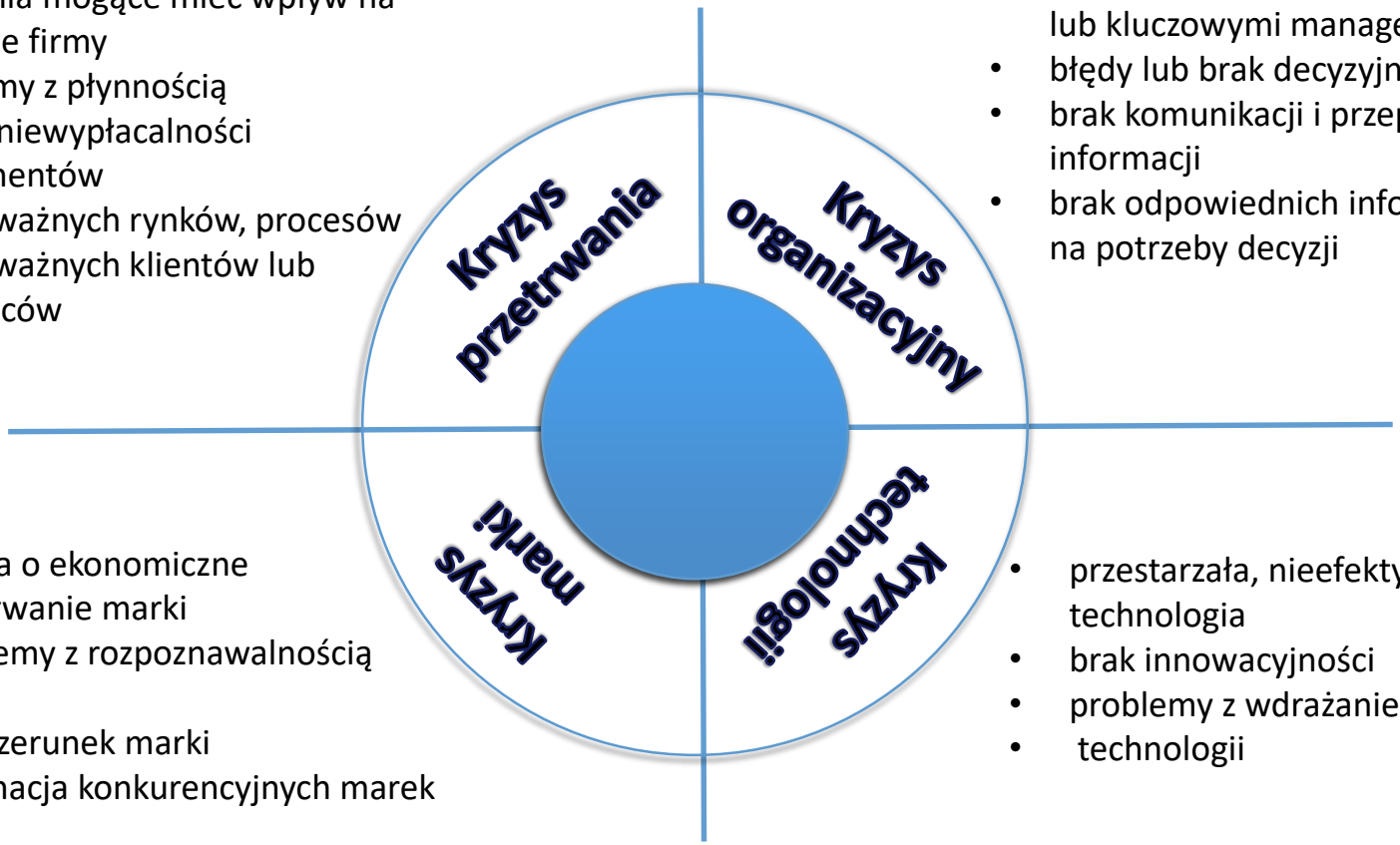
Sytuacja kryzysowa jako sytuacja systemowa

- działanie systemu zostało trwale zakłócone
- system rzeczywiście lub pozornie utracił zdolność sterowania (zarządzania)
- zagrożone jest osiągnięcie celów strategicznych systemu
- naruszona jest dynamiczna równowaga funkcjonowania systemu
- może zostać zagrożona egzystencja systemu (katastrofa) lub jego podsystemów

Rodzaje kryzysów

- zdarzenia mogące mieć wpływ na istnienie firmy
- problemy z płynnością
- ryzyko niewypłacalności kontrahentów
- utrata ważnych rynków, procesów
- utrata ważnych klientów lub dostawców

- problemy z organizacją firmy lub kluczowymi managerami
- błędy lub brak decyzyjności
- brak komunikacji i przepływu informacji
- brak odpowiednich informacji na potrzeby decyzji



- obawa o ekonomiczne przetrwanie marki
- problemy z rozpoznawalnością marki
- zły wizerunek marki
- dominacja konkurencyjnych marek

- przestarzała, nieefektywna technologia
- brak innowacyjności
- problemy z wdrażaniem
- technologii

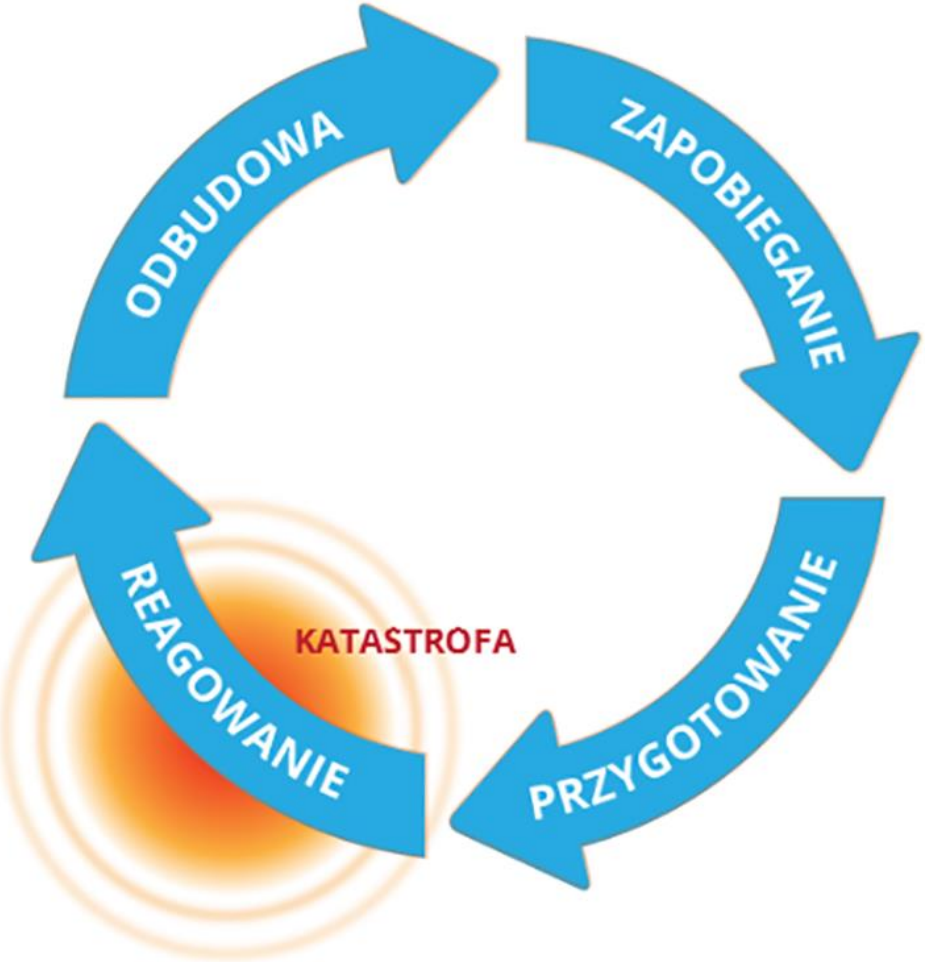
Cechy kryzysu jako sytuacji decyzyjnej

- czas podejmowania decyzji – bardzo krótki
- stopień przewidywalności – bardzo niski (zaskoczenie)
- stopień ryzyka – bardzo wysoki
- obawy wynikające z niepewności – bardzo duże (strach)

Reagowanie na sytuację kryzysową

- oceń sytuację
- przewiduj rozwój sytuacji
- określ cele i zadania
- zidentyfikuj potrzebne zasoby
- określ plan i strukturę działania
- podejmij działania

Fazy zarządzania kryzysowego



Faza 1 - zapobieganie

- działanie uprzedzające, redukujące lub eliminujące zagrożenie mogące wywołać sytuację kryzysową bądź zmniejszające jej skutki:
  - analiza zagrożeń i ocena wrażliwości
  - wspieranie badań stosowanych i transferu technologii
  - uświadamianie personelu i edukacja w zakresie przeciwdziałania zagrożeniom
  - stworzenie systemu zachęt i restrykcji finansowych oraz właściwe wykorzystanie zasobów
  - zapewnienie przywództwa i koordynacji

Faza 2 - przygotowanie

- opracowanie planów reagowania kryzysowego (kto, co i kiedy będzie robił, za pomocą jakich sił i środków i na jakiej podstawie prawnej – przed w czasie i natychmiast po zdarzeniu kryzysowym):
  - monitorowanie stanu organizacji i możliwości uruchomienia zespołu zarządzania kryzysowego
  - plan reagowania kryzysowego
  - opracowanie zasad wymiany informacji
  - opracowanie baz danych teleadresowych, materiałowo sprzętowych, medycznych itp.
  - szkolenia dla zespołu zarządzania kryzysowego
  - organizowanie i prowadzenie ćwiczeń i gier decyzyjnych
  - określenie oraz zabezpieczenie potrzeb finansowych oraz materiałowo-technicznych

Faza 3 - reagowanie

- działania prewencyjne lub zmniejszające ryzyko strat lub – po ich wystąpieniu – działania ratownicze:
  - uruchomienie zespołu zarządzania kryzysowego
  - uruchomienie działań prewencyjnych
  - wszczęcie procedur i skierowanie sił i środków do działań ratowniczych
  - rozpoczęcie ewakuacji (w razie potrzeby)
  - bieżący monitoring rozwoju sytuacji
  - zewnętrzna komunikacja kryzysowa
  - przewidywanie skutków decyzji

Faza 4 - odbudowa

- końcowa faza zarządzania kryzysowego mająca na celu przywrócenie wszystkich systemów do stanu pierwotnego:
  - szacowanie strat i szkód
  - odtworzenie krytycznej infrastruktury
  - odtworzenie i uzupełnienie zasobów
  - modyfikacja planów i polityk bezpieczeństwa oraz procedur reagowania

Standardy bezpieczeństwa

- przez standardy bezpieczeństwa rozumie się:
  - ustalone rozwiązania organizacyjne i techniczne
  - kompetencje i zachowania człowieka

które spełniają kryteria poprawności
w odniesieniu do zapobiegania stratom

Macierz zagrożeń: przemoc fizyczna

- wykorzystanie materiałów wybuchowych w formie między innymi improwizowanych materiałów wybuchowych (IED), improwizowanych materiałów wybuchowych umieszczanych na pojazdach (VBIED), pasów / kamizelek wypełnionych materiałami wybuchowymi (SVEST)
- broń biała oraz broń palna i ataki w zamkniętych przestrzeniach
- wzięcie zakładników
- porwania, zwłaszcza porwania dla okupu oraz dla efektów propagandowych
- wykorzystanie broni chemicznej i biologicznej
- wykorzystanie zamachowców-samobójców

REAGOWANIE NA ATAK W OBIEKCIE / INSTYTUCJI

- alarm: system alarmowania, odmiennego od funkcjonujących w obiekcie / instytucji systemów alarmowania przeciwpożarowego
- blokada: optymalna organizacja personelu w warunkach zagrożenia ze strony uzbrojonego sprawcy, opracowania techniczne
- ostrzeganie: rola lidera bezpieczeństwa, system komunikowania bez alarmu i podczas alarmu
- aktywna obrona: taktyka reagowania w sytuacji wyższej konieczności, osadzenie rozwiązań w systemie bezpieczeństwa obiektu / instytucji
- pierwsza pomoc: organizacja absorpcji pomocy, w tym szkolenie i opracowanie procedury postępowania na wypadek interwencji Policji lub ochrony

Dziękuję. Pytania?