

TECHNIKI IDENTYFIKACJI I ANALIZY ZAGROŻEŃ

Przypomnę iż identyfikacja ryzyka ma na celu ujawnienie pełnej „ekspozycji” przedsiębiorstwa na zjawiska niepewności. Należy tutaj zaznaczyć, że w praktyce pracy risk managera bardzo często rozmywa się granica, kiedy prowadzone przez niego działania są jeszcze „identyfikacją” ryzyka, a kiedy już jego opisywaniem – wielokrotnie następuje jednocześnie „odkrywanie” zagrożenia i zbieranie informacji pozwalające na jego opisanie i oszacowanie. Co na temat identyfikacji ryzyka mówi Risk Management Standard? Poprawne wykonanie tego zadania wymaga dogłębnej znajomości przedsiębiorstwa, rynku na jakim funkcjonuje, oraz środowiska gospodarczego, politycznego i społecznego. Ponadto osoba przeprowadzająca identyfikację zagrożeń powinna „czuć” strategiczne i operacyjne cele jakie sobie firma stawia, a także znać wynik analizy SWOT dla przedsiębiorstwa i rynku.

Gdzie zagrożenia?

Identyfikacja ryzyka powinna zostać przeprowadzona w sposób systemowy i polegać na metodycznym przeglądzie wszystkich bez wyjątków aspektów funkcjonowania firmy i jej otoczenia biznesowego. Zidentyfikowane zagrożenia sugeruje się sklasyfikować w następujących grupach:

- strategiczne (długoterminowe cele firmy),
- operacyjne (codzienne funkcjonowanie firmy),
- finansowe (kontrola finansów i wykorzystanie kapitału przedsiębiorstwa),
- knowledge management (kontrola nad wiedzą, technologią, przepływem informacji oraz ich bezpieczeństwem),
- zgodność (BHP, środowisko, warunki handlowe, ochrona konsumenta, prawa pracownicze, ochrona danych osobowych ...).

Twórcy Risk Management Standard dopuszczają angażowanie zewnętrznych konsultantów w celu lepszego wykonania tej części procesu zarządzania ryzykiem, jednak podkreślają, iż niezastąpiona będzie wewnętrzna analiza poparta solidną wiedzą i narzędziami analitycznymi.

Ważny skutek

Tyle teoria – a co mówi praktyka ? Należałoby zacząć od zdecydowania, czy zaczynamy od szukania przyczyn zagrożeń, czy ich skutków. Na pierwszy rzut oka wydawałoby się, że pytanie jest nie na miejscu, gdyż zagrożenie samo w sobie jest (może być) przyczyną kataklizmów i niepowodzeń stąd możemy szukać jedynie przyczyn. Nie jest to podejście niewłaściwe - można powiedzieć, że jest charakterystyczne dla towarzystw ubezpieczeniowych, które ubezpieczają od ognia, powodzi, lawiny, kradzieży, wybuchu – czyli wydawałoby się zjawisk będących początkiem łańcucha przyczynowo-skutkowego. Jednak ta droga obciążona jest dużym ryzykiem, iż nie będziemy w stanie wymienić wszystkich „przyczyn” (cudzystłów dlatego, iż wymienione zjawiska w większości jednak nie są same w sobie przyczynami, również z ubezpieczeniowego punktu widzenia), a tym bardziej wszystkich konsekwencji biznesowych, do których mogą prowadzić. Zgadzam się więc z Marcinem Z. Brodą, który szerzej pisał o tym już dość dawno temu (www.ryzyko.pl, Wiadomości Ubezpieczeniowe), iż podejściem właściwym z biznesowego punktu widzenia – gdyż gwarantującym większą kontrolę nad procesem i efektem identyfikacji ryzyka – jest szukanie skutków. Upraszczając: nie interesuje nas więc, czy linię produkcyjną tracimy na skutek działania ognia, powodzi, wybuchu, aktu terroryzmu, czy też zajmuje ją komornik – istotny jest określony (niepożądany) skutek.

Uwaga na informacje

Drugą zasadą logiczną, pomagającą risk managerowi nie popełnić „samobójstwa informacyjnego” (tzn. nie zginąć w ogromnych ilościach skondensowanych informacji, jakie będzie musiał samodzielnie gromadzić i przetwarzać), to zasada: od ogółu do szczegółu. Wymaga sporo trudu oparcie się pokusie

Risk Management Consulting Rafał Rudnicki

skr. poczt. 70, 62-035 Kórnik, tel. 501 449 889, e-mail rafal@rudnicki.com.pl

przyjęcia atrakcyjnej informacji, zbędnej w początkowym etapie zarządzania ryzykiem. Podczas choćby wstępnych rozmów z menedżerami różnych szczebli risk manager zwykle jest zarzucany różnymi „gardłowymi” dla firmy problemami czy też „cudownymi” pomysłami na jej uzdrowienie, których innym nie udało się wprowadzić w życie, lub pytając na przykład o szacunkową wartość budynków w lokalizacji X otrzymuje on bardzo szczegółową listę środków trwałych dla wszystkich lokalizacji firmy na świecie - „bo może mu się przydać”. Sztuka selekcjonowania i „dozowania” informacji decyduje jednak o powodzeniu i sprawności pierwszych etapów pracy risk managera i pomaga uchronić się przed „zmęczeniem informacją”.

Metody uniwersalne

Każda branża jest inna, działa na innym rynku, nawet firmy z tej samej branży korzystają z innych technologii czy też mają inne struktury zarządzania. Stąd każde przedsiębiorstwo wymaga generalnie zindywidualizowanego podejścia, choć wierzę, że poniższe metody, zasługują na miano uniwersalnych i należałoby od nich zacząć. Każdy risk manager powinien zacząć od poznania swojej firmy, lub od spojrzenia na nią zupełnie od nowa, w pełni obiektywnie, jak na „obcy” twór. To zadanie dla osób związanych od lat z firmą jest niezwykle trudne. Przede wszystkim należy:

- zadawać **fundamentalne pytania**: jakie są cele strategiczne firmy na najbliższe 5-10 lat? Niezbędny jest przegląd wyników analizy SWOT (Strengths, Weaknesses, Opportunities and Threats, czyli silnych i słabych stron firmy oraz szans i zagrożeń przed nią stojących) a jeśli nie daj Boże takiej analizy nie ma, należy doprowadzić do jej wykonania.

- dokonać gruntownego przeglądu tzw. KPI (Key Performance Indicators, czyli kluczowych wskaźników sprawności firmy, ustalanych w zależności od jej priorytetów i branży jako np. rentowność sprzedaży, terminowość dostaw, ilość reklamacji, rotacja klientów itp) oraz zastanowić się, czy od czasu ich opracowania firma nie zmieniła się na tyle, że KPI należałoby również „przekalibrować”?

Jak Państwo widzą, „wejście” risk managera do firmy jest bardzo zaakcentowane, gdyż zaczyna od zastanawiania się nad poprawnością typowo strategicznych elementów przedsiębiorstwa. Jest to moment prawdy - okazuje się, czy zarząd przedsiębiorstwa jest zdeterminowany do wprowadzenia kultury zarządzania ryzykiem, czy jest przygotowany na zmiany i czego po tym procesie rzeczywiście oczekuje.

Zza biurka

Po tym efektywnym wstępie przychodzi czas na okres żmudnej pracy:

- przeprowadzenie „zza biurka” analizy działów i funkcji firmy pod kątem współzależności i koncentracji lub rozproszenia decyzji, procesów i zasobów

- poznanie głównych technologii użytkowanych w przedsiębiorstwie od strony technicznej, ich specyfiki, słabych punktów, itp. oraz odniesienie ich do technologii konkurencyjnych

- przegląd alokacji zasobów firmy w różnych oddziałach geograficznych, działach operacyjnych czy funkcjonalnych i miejsc ich koncentracji (przykładowa lista zasobów: objętość budynków, wartość budynków, wartość maszyn i wyposażenia, wartość średniego i maksymalnego stanu magazynowego, ilość pracowników, koszt siły roboczej, przepływy (wejście/wyjście) materiałów i środków (w tonach, litrach itp.), przychody jednostek/działów, udział głównego Klienta w przychodach oddziałów/jednostek, zyski oddziałów / jednostek i ich udział w całej firmie, dotychczasowe szkody oddziałów / jednostek).

Na tym etapie można sobie już pozwolić na pierwsze wnioski dotyczące identyfikacji zagrożeń: które zasoby przedsiębiorstwa są krytyczne, gdzie są one najbardziej skoncentrowane (miejsce najbardziej dotkliwego dla firmy uderzenia), potencjalne zjawiska uruchamiające zdarzenie. Jeśli wcześniej popełniono błędy lub niedoskonałości zarządczo-organizacyjne, lub dopuszczono się znacznych niedopatrzeń (np. technologicznych), to teraz możemy je już choćby intuicyjnie zlokalizować.

Jak spowiednik

Po wykonaniu takich prac wstępnych przychodzi czas na bardziej konkretne i dociekliwe narzędzia umożliwiające szczegółowe wniknięcie w materię zagrożeń. Przede wszystkim są to **indywidualne rozmowy (wywiady)** z kluczowymi pracownikami przedsiębiorstwa, między innymi:

- menedżerami i kierownikami niższych szczebli operacyjnych, zarządzającymi HR, łańcuchem dostaw i logistyką,
- inżynierami i technologami,
- specjalistą BHP.

Lista ta jest otwarta i risk manager powinien przejawiać mnóstwo twórczej (odkrywczej) inicjatywy w elastycznym uzupełnianiu tej listy o nowe, niezbędne jego zdaniem funkcje. Niekoniecznie muszą to być wysokie funkcje zarządcze – niejednokrotnie kierownicy liniowi będą mieli najwięcej swoich własnych, bardzo ciekawych spostrzeżeń, o które nikt ich po prostu nigdy nie zapytał. Niezwykle interesujące może być zderzenie opinii dotyczących tych samych obszarów a artykułowanych przez osoby piastujące skrajnie różne funkcje: np. jak kierownik zmiany w zespole obsługującym linię technologiczną (produkcja) usprawniłby proces supply chain (dostawy/zakupy), lub jakie wprowadziłby metody motywacji pracowników (HR) albo jakie zaproponowałby ulepszenia w procedurze doboru firm serwisujących kluczowe maszyny w firmie (dział jakości)? Dobrze poprowadzony ten etap rozpoznania może uczynić z risk managera zaufanego spowiednika.

Bardziej zaawansowanym narzędziem zmierzającym do tych samych efektów jest **sesja burzy mózgów**, w której uczestniczą zwykle kierownicy liniowi (operacyjni) lub średniego szczebla, piastujący różnorakie (możliwie wszystkie) funkcje. Na takiej sesji – której celem jest wyłonienie pełnej listy zagrożeń - nie ma pomysłów zakazanych; nawet śmierć prezesa jest dozwolona.

Kolejne źródło doskonałych informacji na temat zagrożeń to **analiza szkód**: własnych i znanych na rynku, dokonywana przez przegląd i kompilację własnych baz danych i raportów na temat szkód, a także lustrację dostępnych archiwów firmy oraz prasy pod kątem zdarzeń krytycznych np. u konkurentów. Jeśli do tej pory analiza szkód była prowadzona przez firmę (lub jej brokera, ubezpieczycieli) w sposób sensowny, risk manager ma do dyspozycji naprawdę potężne narzędzie.

Czas podsumowania

Po drugiej fazie dociekań risk manager powinien być już w stanie wskazać – przynajmniej orientacyjnie – na słabe punkty: niedostatki zasobów lub złą ich alokację, wąskie gardła w organizacji procesów, obszary niezgodności praktyki z istniejącymi procedurami lub niemożność prawidłowego wypełnienia tych procedur, obszary najmniejszych rezerw na margines błędu ludzkiego lub obszary największego uzależnienia od podmiotów zewnętrznych. Dalej, może wskazać jednoznacznie na powiązania i zależności pomiędzy działami, procesami i zasobami. Wszelkie hipotezy i przypuszczenia będą mogły zostać potem zweryfikowane metodami analitycznymi np. „fault tree” lub „flow chart” – o czym będzie mowa później.

W terenie

Wszystkie dotychczasowe działania są w przeważającej części czasu wykonywane w biurze, a jedynie sporadycznie (maksymalnie do 20% czasu) wymagają wizyty w magazynach, halach produkcyjnych, warsztatach itp. Powalają wyrobić sobie opinię na temat, jak w firmie powinno być lub jak kierownictwo sądzi, że w niej jest. Kolejny etap to wyjście risk managera w teren, w którym powinien teraz spędzać coraz więcej czasu i wyrabiać w sobie coraz ściślejszy kontakt z codzienną rzeczywistością firmy, jakakolwiek ona by nie była. Mowa oczywiście o odbyciu wizji lokalnych lub **audytów obiektów**, linii technologicznych i przebiegających w nich procesów. Wynikiem takich audytów mogą być raporty opisowe, odnotowujące np. następujące informacje:

- obiekt/urządzenie,
- funkcja, wiek, stan,
- zaobserwowane błędy/wady,
- wpływ obiektu/urządzenia na procesy lub zasoby,
- proponowane działania naprawcze.

Punkt po punkcie

W firmie może występować nawet grubo ponad sto wstępnie zidentyfikowanych zagrożeń, z których najczęściej pozostaje około 25% zagrożeń strategicznych – co przekłada się na liczbę ok. 25-40 ważnych dla firmy zjawisk. W ich identyfikacji pomagają specjalistyczne metody analityczne.

Pierwsza z nich polega na stworzeniu „**Check listy**” czyli dokumentów zawierających spis standardowych pytań lub parametrów do sprawdzenia i pozwalające na uproszczoną, ale dość kompletną ocenę obiektu lub funkcji (procesu) pod kątem jej wrażliwości na zagrożenia. Jest to bardzo elastyczne narzędzie: możemy konstruować je w wielu wariantach, począwszy od prostych dokumentów na 2-3 strony, gdzie dopuszcza się odpowiedzi jedynie „tak/nie” aż po kilkudziesięciostronicowe opracowania, dające strukturalną ocenę kilkudziesięciu obszarów i setek parametrów, gdzie zwykle odpowiedzi mogą się mieścić na wielostopniowej skali.

Generalnie wykonywanie samej wizji lokalnej za pomocą check listy nie jest takie trudne jak konstruowania samej check listy – należy liczyć się z koniecznością skonstruowania jej od zera, z wielogodzinnymi konsultacjami z własnymi specjalistami oraz ekspertami z zewnątrz firmy. Każda próba pójścia na skróty może skończyć się pominięciem jakiegoś zagrożenia lub skonstruowaniem systemu wskaźników, który nie oddaje wiernie rzeczywistości.

Mapa risk menedżera

Niezwykle przydatnym narzędziem, pomagającym zaatakować każdy problem „od zera” i bez sugerowania się swoimi ewentualnymi uprzedzeniami jest **mapowanie procesów** przydatne głównie w usługach, i w niektórych przedsiębiorstwach produkcyjnych. Dla każdego procesu (funkcji, działalności) firmy należy przeprowadzić analizę:

- wartości „wejściowych” (materiały, energia, pieniądze, czas pracowników – środki, które podlegają zużyciu)
- wartości „wyjściowe” (usługi, produkty, odpady)
- zasoby i mechanizmy (nie podlegające zużyciu np. maszyny i ludzie)
- narzędzia kontroli (determinują przebieg procesu bądź funkcji i jego skutek: procedury, normy, budżet, prawo ...).

Przepływ w tabeli

Flow charts (analiza przepływu) służy ogólnej i szerokiej analizie zagrożeń, bez wchodzenia w szczegóły (do czego służą inne narzędzia). Analiza flow charts może dotyczyć:

- materiałów i mediów (głównie przedsiębiorstwa o profilu produkcyjnym, ale nie tylko)
- produktów (lub usług) oraz procesów (funkcji) generujących przychody (wartość dodaną).

Przedmiotem tego badania jest analiza ilości i rodzaju (jakości) przepływających przez infrastrukturę firmy materiałów pod kątem wzajemnego wpływu na wynik (sprawność) produkcji i wąskich gardeł. Jej podsumowaniem jest tabelaryczne przedstawienie zależności:

zdarzenia krytyczne -> potencjalne przyczyny -> potencjalne skutki.

Najczęściej są to stosunkowo skomplikowane struktury nie mieszczące się na kartce formatu A4. Badanie zależności pomiędzy tymi wartościami przedstawionymi w formie graficznej (analitycznej) może być niezwykle odkrywczą przygodą dla niejednego menedżera od lat zarządzającego firmą.

Po przeprowadzeniu powyższych analiz i badań, risk manager może już sformułować stosunkowo szczegółowe i ostateczne wnioski, które zagrożenia mogą mieć największe przełożenie na KPI (krytyczne zasoby, procesy, przepływy materiałów i mediów).

Jakość ryzyka

Ostatnią ze specjalistycznych technik, służących identyfikacji zagrożeń, jaką chciałbym – nieco szerzej – omówić, jest metoda **HAZOP (Hazard and Operability Studies)** będąca analizą jakościową. Nie znam dobrego tłumaczenia tej nazwy na język polski, stąd będę się posługiwał skrótem HAZOP. Ta metoda analityczna służy szczegółowej analizie urządzeń lub procesów technologicznych, które wcześniejszymi metodami zostały wyłonione jako szczególnie zagrożone. Jest to przykład zaawansowanego narzędzia, który da Państwu pogląd, na ile pracochłonnym zadaniem może być dogłębna identyfikacja i analiza zagrożeń.

Przygotowanie do analizy polega na:

- wyodrębnieniu (wyizolowaniu) pewnego zespołu lub mechanizmu z bardziej złożonej linii technologicznej
- zdefiniowaniu celu, jakiemu służy element (mechanizm) całego urządzenia bądź procesu
- zdefiniowaniu wszystkich możliwych odchyłeń poza dopuszczalne minimum i maksimum dla zachowania czy też kluczowych parametrów pracy tego elementu
- zdefiniowaniu przyczyn oraz skutków takiego odchylenia.

Posłużę się tu bardzo prostym przykładem: instalacja ciepłej wody w hotelu oraz kończący ją kran z ciepłą wodą. Analizowanym działaniem będzie wypływ wody pod ciśnieniem, a kluczowym parametrem będzie temperatura wody.

Charakterystyczne dla metody jest użycie „słów kluczy” prowadzących przez analizę logiczną:

- brak/zaden = zamierzona czynność/działanie nie występuje (woda nie leci po odkręceniu kranu)
- więcej/mniej = wzrost lub spadek jednego z parametrów czynności/działania poza dopuszczone minimum lub maksimum (leci wrzątek zamiast wody o temperaturze 40-50 stopni)
- oraz/dodatkowo = oprócz pożądanego działania otrzymujemy inne, niepożądane (po odkręceniu kurka leci ciepła woda ale również słychać głośny bulgot i wydobywa się powietrze pod wysokim ciśnieniem)
- częściowo = jedynie częściowo (niekompletnie) osiągnięto zamierzony cel/czynność (woda „częściowo” podgrzana, tzn jedynie letnia, nie ciepła)
- odwrotnie = następuje odwrócenie oczekiwanej czynności/procesu (po odkręceniu kurka pojawia się podciśnienie: kurek zasysa powietrze)
- inny niż/inaczej = efekt/czynność spodziewana została zastąpiona czymś zupełnie odmiennym (po odkręceniu kurka leci z niego olej napędowy).

Analiza (pojedynczego elementu całego systemu lub procesu) polega na przypisaniu do każdego słowa-klucza interpretacji wg kategorii: klucz, odpowiadające mu zjawisko, przyczyna, skutek, działanie zapobiegawcze. Przykładowo:

- klucz = więcej/mniej
- zjawisko = wrzątek zamiast temperatury 40-50 stopni
- przyczyna = zbyt wysoka temperatura kotła

Risk Management Consulting Rafał Rudnicki

skr. poczt. 70, 62-035 Kórnik, tel. 501 449 889, e-mail rafal@rudnicki.com.pl

- skutek = gość hotelowy zostaje poparzony
- działania = założyć termostat w instalacji kotła.

Zakładając, że instalacja wodociągowa może mieć np. piętnaście zespołów lub odcinków kluczowych, a każdy z nich podlega ocenie wg sześciu słów kluczy, z kolei każde zjawisko odnoszące się do słowa klucza może mieć np. 3 przyczyny oraz 2 skutki, otrzymujemy 540 możliwych przypadków do rozpatrzenia i przeanalizowania. Proszę również wziąć pod uwagę, że większość instalacji lub urządzeń (systemów) przemysłowych musi spełniać więcej niż jeden parametr (jak temperatura wody w naszym przykładzie). W rezultacie, wielość ocenianych parametrów to kolejny mnożnik zwiększający ilość możliwych kombinacji, idących niejednokrotnie w tysiące.

Zagrożenia: jakie i ile?

Jeśli któryś z czytelników chciałby sam się podjąć identyfikacji zagrożeń we własnym przedsiębiorstwie, pomocne będą przykłady zagrożeń zebrane z kilku różnych źródeł i powszechnie uważane za najważniejsze. Być może pobudzą one wyobraźnię i pomogą Państwu dojść do własnych odkrywczych przemyśleń, czego życzę. W podtytule „Z własnej praktyki” przedstawiłem zagrożenia, które zidentyfikowałem w pewnych firmach, a które nie są zrozumiałe same przez się, choć mogą mieć olbrzymie konsekwencje i siłę rażenia. Warto też zapoznać się z zestawieniami istotnych zagrożeń, które wyłoniły się jako wiodące podczas badań przeprowadzonych na rynku Europejskim przez renomowane firmy konsultingowe. Niestety nie ma jednej odpowiedzi i gotowego przepisu ile takich zagrożeń dotyczy danej firmy. Nie ma wskaźników odnoszących ilość zidentyfikowanych zagrożeń do rodzaju branży, obrotów czy innego czynnika ekonomicznego i pozwalających się upewnić, że prawdopodobnie zidentyfikowaliśmy wszystkie zagrożenia. Przeprowadzane przeze mnie prace z zakresu zarządzania ryzykiem wskazują, że może występować nawet grubo ponad sto wstępnie zidentyfikowanych zagrożeń, z których najczęściej pozostaje około 25% zagrożeń strategicznych – co przekłada się na liczbę ok. 25-40 ważnych dla firmy zjawisk. Moje doświadczenia potwierdzają badania przeprowadzone przez Deloitte & Touche, z których wynika, że dla 30% firm udało się zidentyfikować powyżej 35 zagrożeń, a tylko dla 5% był to przedział 11-15 lub 31-35 zagrożeń. W 10% firm zidentyfikowano od 16 do 20 zagrożeń. Od 21 do 25 i od 26 do 30 zagrożeń zidentyfikowano w 15% firm.

Z własnej praktyki

Na jakie ryzyka warto zwrócić uwagę?

Budowa i remonty (m.in. spawanie wewnątrz magazynu, hali produkcyjnej)

Dostawca gazu, łączy IT, prądu (awaria, odejście, bankructwo, brak mediów)

Dostawcy oprogramowania (odejście, bankructwo, utrata licencji)

Nagle wypowiedzenie umowy najmu (budynek produkcyjny, biurowy, magazyn)

Wadliwe wdrożenia nowych systemów IT i zmiany oprogramowania

Błąd pracownika IT (skasowanie, utrata danych itp.)

Klient (bankructwo, brak płynności, zmiana strategii rynkowej)

Konkurenci (dumping, nowi gracze, nowe usługi i technologie)

Pracownik - stała lub czasowa utrata grupy pracowników (epidemia, wypadek lub zatrucie na imprezie firmowej)

Utrata (śmierć lub odejście) prezesa, członka zarządu

Menedżer/pracownik działa na szkodę firmy, lub odchodzi wraz z wiedzą operacyjną

Zamarzanie paliwa (pojazdy oraz agregaty prądotwórcze)

Produkcja - uwolnienie się mediów technologicznych (sprężone powietrze, acetylen, freon, amoniak) lub innych substancji toksycznych (gazów, cieczy bądź par)

Zewnętrzne - zamach lub działanie terrorystów.



Niektóre istotne zagrożenia wg. Deloitte & Touche

a) zagrożenia wewnętrzne

- samo przetwarzanie danych i zmiany oprzyrządowania/ oprogramowania do tego służącego
- jakość i motywacja pracowników
- zmiany w zakresie odpowiedzialności członków zarządu lub kierownictwa średniego szczebla
- nieefektywny audyt wewnętrzny

b) zagrożenia zewnętrzne

- rozwój technologiczny
- zmieniające się oczekiwania bądź preferencje klientów (ryнку)
- konkurencja
- nowe akty legislacyjne (również te pozostające ciągle w fazie projektu bądź opracowania)
- naturalne katastrofy
- zmiany gospodarcze w skali makro.

Niektóre istotne zagrożenia wg. Ernst & Young oraz FERMA*

- obszar R&D (Badania i Rozwój)
- jakość automatycznych systemów kontroli
- spójność sprzętu i oprogramowania a także (baz) danych
- przestępstwa cybernetyczne i dostęp do internetu
- odpowiedzialność cywilna za produkt
- zarządzanie informacją
- złe zarządzanie relacjami z Klientami

* firmy przeprowadziły badania w Europie w październiku 2002 i wyłoniły obszary szczególnego zainteresowania Risk Managerów.

Istotne zagrożenia wg. AON Risk Consulting

- ośrodki dystrybucji zasobów firmy
- odpowiedzialność pracodawcy, wypadki przy pracy oraz nadmierna rotacja pracowników
- odpowiedzialność kontraktowa
- defraudacja
- terroryzm
- porażka aliansów strategicznych
- nieumiejętne (nieudane) przeprowadzenie zmian w firmie

Uwaga! Opisane powyżej narzędzia analityczne są najczęściej odpowiednie dla jedynie wybranych segmentów biznesu, powinny być stosowane selektywnie, do opisanego (rozwiązania) określonych, szczegółowych problemów.