Sylwia Konecka

Zarządzanie ryzykiem dotyczącym przepływu informacji w łańcuchach dostaw

Ekonomiczne Problemy Usług nr 35, cz. 2, 109-119

2009

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 544 EKONOMICZNE PROBLEMY USŁUG NR 35 2009

SYLWIA KONECKA
Wyższa Szkoła Logistyki w Poznaniu

ZARZĄDZANIE RYZYKIEM DOTYCZĄCYM PRZEPŁYWU INFORMACJI W ŁAŃCUCHACH DOSTAW

Posiadanie, właściwy obieg i wykorzystanie informacji jest między innymi warunkiem sprawnego i racjonalnego przepływu dóbr między punktem nadania a punktem odbioru – przedmiotu zainteresowania logistyki. W ujęciu wewnętrznym przepływy informacyjne służą komunikacji między grupami roboczymi i poszczególnymi pracownikami w przedsiębiorstwie, zespalają wszystkie sfery działalności przedsiębiorstwa, umożliwiając integrację np. zaopatrzenia z produkcją i dystrybucją. Wagę informacji podkreśla fakt, iż traktuje się ją jako czynnik produkcji, na równi z siłą roboczą, ziemią i kapitałem. Przepływy informacyjne w relacjach zewnętrznych tworzą połączenia między klientem a dostawcą, łączą w ten sposób ogniwa łańcucha dostaw. Zapewnienie dostępu do wielu źródeł danych oraz integracji systemów informacyjnych przedsiębiorstwa i łańcucha dostaw możliwe jest wyłącznie przy wykorzystaniu systemów informatycznych.

Obecnie uważa się, że systemy informacyjne i informatyczne są jedną z głównych przyczyn zmian zachodzących w warunkach prowadzenia działalności gospodarczej. Światowej sławy profesor Michael Hammer przyrównuje wprowadzenie Internetu, do przełomu równoznacznego w swojej skali z odkryciem ognia. Rozwój technologii informacyjnych, komunikacyjnych i informatycznych wraz z obniżeniem poziomu barier wejścia na rynki to czynniki, które zwiększyły ekspozycję przedsiębiorstw na ryzyko. W najnowszych publika-

cjach wskazuje się na potrzebę zarządzania ryzykiem w skali łańcuchów dostaw, jedną z kategorii jest ryzyko związane z przepływem informacji.

Ryzyko dotyczące informacji może być zdefiniowane jako ”prawdopodobieństwo wystąpienia straty spowodowanej nieprawidłową, niekompletną informacją bądź nielegalnym dostępem do informacji”. Natomiast zarządzanie ryzykiem dotyczącym informacji w łańcuchu dostaw jako ”skoordynowane lub wspólne zarządzanie ryzykiem związanym z przepływem informacji przez partnerów wzdłuż łańcucha dostaw w celu zwiększenia zyskowności i poprawy ciągłości działania”[1].

Ryzyko dotyczące przepływu informacji w łańcuchu dostaw można podzielić na cztery grupy, za kryterium podziału przyjęto skutek jaki poszczególne kategorie ryzyka wywierają na łańcuch dostaw. Należą do nich[2]:

- ryzyko dotyczące bezpieczeństwa bądź przerwania przepływu informacji,
- ryzyko związane z prognozami popytu,
- ryzyko nieprzestrzegania praw wynikających z własności intelektualnej,
- ryzyko outsourcingu systemów informacyjnych i technologii informatycznych.

Przerwanie bądź naruszenie bezpieczeństwa systemu informatycznego może mieć istotne znaczenie dla całej sieci, gdyż dzielenie się informacjami między partnerami w łańcuchu dostaw jest jednym z kluczowych elementów umożliwiających osiąganie przewagi konkurencyjnej. Z tego typu zdarzeniami wiążą się różnego rodzaju straty np. sprzedaży, koszty odzyskania danych i długoterminowe koszty związane ze stratą przychylności klientów. Najpopularniejsze typy ryzyka w tej grupie to:

- zagrożenia powodowane przez hakerów, wirusy, robaki. Tego typu ryzyko najczęściej pojawia się wśród dostawców drugiego i trzeciego rzędu, którzy jako małe bądź średnie przedsiębiorstwa nie dysponują funduszami zdolnymi zapewnić odpowiednią ochronę informacji. Dodatkowo w tego typu firmach zazwyczaj brakuje polityki bezpieczeń-

[1] M. Nishat Faisal, D.K. Banwet and R. Shankar, *Information risks management in supply chains: an assessment and mitigation framework*, Journal of Enterprise Information Management, Vol. 20 No. 6 2007, s. 679.

[2] Ibidem., s. 680.

stwa informacji. Rozpowszechnienie Internetu spowodowało łatwiejszy dostęp do tajnych informacji firmy;

- systemy tzw. *spyware*, które bezwiednie instalowane przez użytkownika umożliwiają osobom trzecim monitorowanie transakcji dokonywanych drogą elektroniczną i wgląd w zawartość dysku twardego;
- oszustwa dokonywane na szkodę firmy przez jej własnych pracowników – jest to jedno z najczęściej występujących zagrożeń. Najczęstszymi przyczynami są: utarczki między pracownikami, zamierzone lub niezamierzone ujawnienie ważnych informacji, a w niektórych przypadkach zemsta wymierzona przeciw firmie;
- ataki uniemożliwiające wykonywanie usług np. przez przerwanie legalnego dostępu do sieci, który może mieć swój efekt w przerwaniu operacji w łańcuchu dostaw;
- katastrofy naturalne takie jak tsunami, huragany np. Katrina, Rita, pożary czy atak na WTC zwróciły uwagę organizacji nie tylko na bezpieczeństwo informacji, ale również konieczność posiadania kopii informacji, aby zapewnić w takich przypadkach nieprzerwany przepływ w łańcuchu dostaw. Przykładowo trzęsienie ziemi na Tajwanie w 2006 roku wywołało chaos komunikacyjny w całej wschodniej Azji, gdyż silne wstrząsy o sile 7,1 stopni w skali Richtera zniszczyły dwa z siedmiu przebiegających tuż obok tajwańskich wybrzeży podmorskich kabli obsługujących połączenia międzynarodowe**.** Doniesienia dotyczące problemów z łącznością dochodziły z instytucji w Chinach, Hongkongu, Japonii, Korei Południowej i na Tajwanie. Tamtejsze banki skarżyły się na jakość zarówno połączeń telefonicznych, jak i internetowych. W znacznym stopniu pogorszyła się łączność z Malezją, Singapurem i Tajlandią. Największy dostawca usług telekomunikacyjnych w Chinach poinformował, że uszkodzone zostały też łącza odpowiadające za połączenia z USA i Europą. Naprawa kabli trwała trzy tygodnie[3].

Ryzyko związane z prognozami wynika z dysproporcji między przewidywaniami firmy a faktycznie zgłaszanym zapotrzebowaniem. Zniekształcenia informacji przepływających przez łańcuch dostaw powodują ryzyko złej prognozy. Głównymi przyczynami zniekształcenia informacji są: promocje prowa-

[3] Tajwan: Trzęsienie ziemi wywołało chaos komunikacyjny w Azji, 2006-12-27, PAP, zab/ kan/

dzące do wykupywania towarów „na zapas", brak wiedzy o popycie występującym u ostatecznego konsumenta prowadzący do nieprawidłowego prognozowania popytu, zamawianie partiami prowadzące do większych zmienności w wielkościach zamówień i fluktuacje cen.

Przykładem chaosu wynikającego ze zniekształcania informacji przebiegających przez łańcuch dostaw jest dobrze znany *bullwhip effect*. Nadreakcja zwiększa koszty i nieefektywności spowodowane zamawianiem zbyt dużych ilości towarów i przetrzymywaniem ich w postaci zapasów. Występowanie *bullwhip effect* zaobserwowano w różnych branżach, np. w sektorze papierniczym, dóbr częstego zakupu, przemyśle samochodowym i hutniczym.[4] Dobrym przykładem jego funkcjonowania są obserwacje dokonane przez kierowników logistycznych firmy Procter & Gamble, w trakcie badania kształtowania się zamówień na jeden z najlepiej sprzedających się produktów tej firmy – Pampersy. Ich sprzedaż w detalicznych sklepach wahała się, ale w sposób umiarkowany. Zamówienia składane przez dystrybutorów cechowało znacznie większe zróżnicowanie. Natomiast jak się okazało największe wahania dotyczyły zamówień na materiały do produkcji. Na pierwszy rzut oka wahania te pozbawione były sensu, bo przecież dzieci zużywają pieluchy w stałych ilościach.[5] Zniekształcona informacja o popycie może również prowadzić do kryzysu spowodowanego nadmiernymi inwestycjami w zapasy, obniżeniem poziomu obsługi klienta, nieefektywnym wykorzystaniem środków transportu, czy utrudnionym procesem planowania produkcji[6].

Aby zredukować ryzyko wynikające ze zniekształcenia informacji w łańcuchu dostaw można wykorzystywać takie koncepcje jak: CPFR *collaborative planning, forecasting and replenishment czyli wspólne planowanie, prognozowanie i uzupełnianie,* ECR – *Efficient Consumer Response czyli Efektywna Obsługa Klienta* i VMI - *Vendor Managed Inventory, Zarządzanie Zapasami przez Dostawcę*. Przedsiębiorstwa np. Dell, Wal Mart dzieląc się informacjami z dostawcami i klientami w celu obniżenia kosztów i zwiększenia poziomu obsługi klientów redukują również ryzyko dotyczące prognozowania.

---

[4] A. Pluta-Zaremba, *Efekt byczego bicza w łańcuchu dostaw,* Gospodarka Materiałowa i Logistyka, nr 5, 2002.

[5] Lee Hau, Padmanabhan V., Whang S., *The Bullwhip Effect in Supply Chains*, Sloan Management Review, spring 1997, s. 93.

[6] K. Rutkowski, *Logistyka dystrybucji*, Wyd. Difin, Warszawa 2001, s. 131.

Ryzyko nieprzestrzegania praw wynikających z własności intelektualnej nabrało szczególnego znaczenia w kontekście łańcucha dostaw, gdyż przez jego integrację posiadanie wiedzy i jej legalne wykorzystywanie w działaniach kooperacyjnych powoduje szybki rozwój innowacji, ale i szybką ich dyfuzję, kluczowym czynnikiem jest kwestia sprawiedliwego podziału korzyści. Tego typu ryzyko stało się ważne również ze względu na outsourcing działalności nie będącej kluczową kompetencją firmy. Zaopatrywanie się czy też lokowanie produkcji w krajach o niskich kosztach (LCCS – low cost country sourcing), takich jak Chiny, Indie powoduje obniżenie kosztów, ale nie wszystkich. Kosztami, które wzrastają są te wynikające z niskiego poziomu ochrony prawnej własności intelektualnych, powszechnym zjawiskiem jest produkowanie podróbek znanych marek, a wygranie sprawy w takiej sytuacji nie jest oczywiste. Poza tym dostawcy z krajów „o niskich kosztach" dostarczają również komponenty dla konkurentów, co zwiększa ryzyko utraty bądź przecieku ważnych informacji. Zarządzanie tego typu ryzykiem jest istotne dla łańcucha dostaw, gdyż unikalność produktu, usługi często decyduje o pozycji łańcucha dostaw na rynku, a działania związane z tworzeniem własności intelektualnej wymagają dużych nakładów finansowych i wkładu pracy a mogą być szybko naśladowane.

Przykładem strat powstałych w wyniku uzyskania dostępu do wartości intelektualnych, w tym przypadku *know-how* innej firmy może być podpisanie umowy między firmami General Electric (GE) i Samsung. Przy dużych inwestycjach w zdolności produkcyjne w Kolumbii, GE zdecydował się zlecić produkcję niektórych ze swoich modeli Samsungowi – wówczas skromnemu, mało znanemu poza Koreą przedsiębiorstwu. Pierwszy kontrakt opiewał zaledwie na 15 000 tysięcy sztuk. Jednak GE w ciągu dwóch lat doprowadził do cedowania większości inicjatyw związanych z rozwojem produkcji mikrofalówek swojemu dostawcy. Firmie Samsung powyższa umowa pozwoliła zdobyć niezbędne *know-how* i zwiększyć skalę swojej produkcji do poziomu, który bez dostępu do rynku amerykańskich konsumentów, nigdy nie byłby możliwy. W efekcie Samsung zaistniał na rynku światowym jako jeden z głównych producentów kuchenek mikrofalowych, kosztem swojego partnera[7].

Ryzyko outsourcingu dotyczy nie tylko outsourcingu działalności produkcyjnej, ale bardzo często systemów informacyjnych i technologii informatycznych. Wszechstronne wykorzystywanie narzędzi IT powoduje, że powstała

[7] Lei, Slocum, 1992.

nowa branża. Firmy najczęściej wykorzystują outsourcing, czyli podejmują decyzje o przekazaniu zewnętrznym usługodawcom działań dotyczących zarządzania działalnością IT, gdyż zmniejsza to koszty, podnosi poziom obsługi klientów i zwiększa możliwości skupienia się na kluczowych kompetencjach. Natomiast ryzyko mogą nieść: oportunizm sprzedawców, niska świadomość bezpieczeństwa informacji, ukryte koszty, utrata kontroli, deprecjacja usług, sprawy sądowe i spory. Przykładowo w 2001 roku firma Nike zakupiła nowy system planowania, który wywołał problemy z zapasami i zamówieniami przez co ceny akcji spadły o 20%, a firma odnotowała spadek przychodu w kwartale o 100 mln dolarów, za zaistniałą sytuację Nike obwiniał dostawcę systemu informatycznego, ten z kolei tłumaczył, że odbiorca nie przestrzegał zaleceń, o nieco późniejszym rozpoczęciu użytkowania – sprawa znalazła swój finał w sądzie, co pociągnęło za sobą dalsze koszty[8].

Zarządzanie ryzykiem dotyczącym przepływu informacji posiada jeszcze jeden ciekawy aspekt. Jak już wspomniano na wstępie optymalne zarządzanie ryzykiem ogólnie jak i zarządzanie ryzykiem informacji, szczególnie na poziomie łańcucha dostaw nie byłoby możliwe bez wykorzystania narzędzi informatycznych. Pojawia się szereg propozycji przykładowo firma McAfee udostępniła rozwiązania ePolicy Orchestrator 4.0 (ePO), swojego oprogramowania do zarządzania bezpieczeństwem, zawierającego ulepszoną możliwość kontroli przez przeglądarki Web, możliwość dowolnej konfiguracji raportów i inne udogodnienia w kwestii raportowania. ePO pozwala łatwiej zarządzać personelowi IT wielowarstwową strukturą aplikacji bezpieczeństwo & zgodność, oferuje nowe możliwości zwiększenia ochrony przed zagrożeniami[9]. Zintegrowane produkty IRM (Information Risk Management) dostarcza firma Symantec Information Foundation 2007. Proponowane przez nią rozwiązanie służy do zabezpieczania przez utratą danych przedsiębiorstwa oraz zapewnia zunifikowaną ochronę poczty elektronicznej, komunikatorów i WWW pozwala na poddawanie informacji wchodzących i wychodzących z organizacji - archiwizacji, audytowi, oraz zapewnia wykrywanie czy jest ona właściwie chroniona.[10] Czy można więc posunąć się do stwierdzenia, że brakuje tylko narzędzi informatycz-

[8] The 11 Greatest Supply Chain Disasters, Supply Chain Digest, 2006

[9] Ł. Szewczyk, McAfee ulepsza zarządzanie ryzykiem, 12 czerwca 2007

[10] J. Muszyński Symantec zunifikował narzędzia do zarządzania ryzykiem, 18 czerwca 2007.

nych, które uchronią firmy przed ryzykiem związanym z właśnie z samymi systemami informatycznymi?

Współczesne przedsiębiorstwa dążą do jeszcze efektywniejszego przetwarzania informacji, zmierzającego do redukcji kosztów i przede wszystkim nadzoru nad zarządzanym ryzykiem. Współpraca pomiędzy systemami informatycznymi pozwala na integrację wielu obszarów działalności. Okazuje się że to już nie wystarcza. A korporacje transnarodowe funkcjonujące w globalnych łańcuchach dostaw mają coraz częściej problemy z tzw. zgodnością - *compliance*, również w odniesieniu do systemów informatycznych. Funkcja *compliance* jest jednym z najnowszych wzorców, pozwalających na znaczne ograniczenie ryzyka działalności, wzmocnienie konkurencyjności i pozycji rynkowej, jak również ułatwiających kontakty z innymi uczestnikami międzynarodowego rynku. AMR Research podaje, że w 2006 roku tylko na zapewnienie zgodności z uchwaloną w 2002 roku ustawą Sarbanes-Oxley (SOX) firmy wydadzą 6,1 mld USD[11]. Przykładowo *Nestle* przez ostatnich 15 lat pracowało na sześciu różnych lokalnych systemach informatycznych. Tego rodzaju praca, poprzez platformy umożliwiające przetwarzanie danych w różnych systemach, okazała się przestarzałą. Kierownictwo firmy doszło do wniosku, że liczba błędów wynikająca z dublowania informacji w systemach jest zbyt duża, a nadzór nad eliminowaniem błędów zbyt drogi. Dlatego podjęto działania zmierzające do znalezienia rozwiązania, które zredukowałoby koszty związane z utrzymaniem systemów i zapewniło sprawniejszy przepływ informacji. Z ofert przedstawionych przez producentów systemów informatycznych, *Nestle* wybrało firmę *Aon Corporation*, która zaproponowała wykorzystanie Internetu jako platformy łączącej poszczególne oddziały giganta spożywczego. Założeniem była redukcja kosztów. Aon zaproponowało rozwiązanie o nazwie *RiskConsole*, które spełniało wymagania *Nestle*. Jest to system wspomagający informację w zarządzaniu ryzykiem (*Risk Management Information System*). Specjaliści od zarządzania ryzykiem przewidują, że wdrożenie powyższego systemu, którego mocną stroną jest możliwość pracy w różnych językach i możliwość bieżącego przeliczania wielkości ryzyka w różnych walutach, co w przypadku międzynarodowej korporacji jest niewątpliwie wielką zaletą systemu, pozwoli zaoszczędzić ponad 100 000 €. Zaoszczędzone środki pochodzić będą z redukcji kosztów związa-

[11] W. Machowiak, S. Konecka, *Kryzysogenne kategorie ryzyka specyficzne dla struktur logistycznych*, 1st International Conference of Logistics INTLOG 2006.

nych z zarządzaniem informacją. Nestle jest w trakcie wdrażania projektu. Pierwszymi krajami biorącymi udział w tym przedsięwzięciu będą Francja, Szwajcaria, Wielka Brytania i USA. Już w trakcie wdrożenia *RiskConsole*, *Nestle* czerpie korzyści z centralizacji systemu wspomagającego informację w zarządzaniu ryzykiem. [12]

Generalnie większość organizacji dostrzega duże korzyści w rozwoju i stosowaniu narzędzi IT wspierających między innymi proces zarządzania ryzykiem[13]. Warto też pamiętać o ograniczeniach systemów informacyjnych, często podaje się, że są one: kosztowne oraz trudne w opracowywaniu i stosowaniu; nie nadają się do wykonywania wszelkich zadań i rozwiązywania wszystkich problemów; menedżerowie czasem w zbyt dużym stopniu na nich polegają i mają wobec nich nierealistyczne wymagania; a informacje w nich zawarte mogą nie być tak doskonałe, pełne, aktualne czy odpowiednie jakby się wydawało, w końcu system informacyjny jak wspomniano może być narażony na sabotaż, wirusy komputerowe bądź przestoje.

Poza tym wskazane przykłady dotyczyły dużych, światowych koncernów, a większość polskich firm to małe i średnie przedsiębiorstwa (MSP). Największe przedsiębiorstwa są wyposażone w odpowiednie systemy do wymiany danych ze swoimi partnerami. Posiadają dobrze rozwinięte, zaawansowane systemy zarządzania informacjami wraz ze wszystkimi możliwymi modułami komunikacyjnymi, wdrażają systemy zarządzania ryzykiem w łańcuchach dostaw**.** Z badań dotyczących systemów informacyjnych MSP w łańcuchach dostaw wynika, że MSP stosują tradycyjne środki komunikacji. Połowa wykorzystuje komputery, ale bardzo rzadko rozwiązania sieciowe, a tylko 10% aktywnie wykorzystuje sprzęt komputerowy. 79% małych firm i prawie wszystkie średnie zainstalowały Internet, ale używają go biernie: małe firmy do wyszukiwania informacji, 77% średnich firm - dla celów biurowych, 2-5% dokonuje zakupów przez Internet, a 7-27% korzysta z bankowości elektronicznej. 60% MSP nie ma witryny internetowej. Badania dowiodły, że MSP stosują bardzo podobne rodzaje systemów informacyjnych. Nie tworzy się profesjonalnych baz danych, a manualny charakter oraz powolna aktualizacja i wyszukiwanie uniemożliwiają ich wykorzystanie do codziennego zarządzania operacjami. Bazy służą celom

[12] T. Dowding, Risk Information Technology The Great Leap Forward, Business Insurance Europe, 29.01.2007, www.BIEurope.com.

[13] Rudnicki R., Oprogramowanie wspomagające niektóre funkcje zarządzania ryzykiem, www.rudnicki.com.pl

promocyjnym, a respondenci najczęściej nie mieli zapotrzebowania na szerszy zakres informacji zarządczej. Wiele wdrożyło systemy informatyczne dla lepszego zarządzania produkcją, bo wymusiły to duże firmy w funkcjonujących łańcuchach dostaw[14]. W przypadku MSP problemem jest brak podstawowych systemów informatycznych, a co się z tym ściśle wiąże – całkowity brak systemów komunikacji zewnętrznej[15]. Przyczynami, z powodu których przedsiębiorstwa najczęściej rezygnują z wdrażania narzędzi IT są przede wszystkim[16]: wysokie inwestycje, klienci, którzy sami nie posiadają takiej technologii i zbyt mała liczba transakcji.

Podsumowując w łańcuchu dostaw należy zapewnić wymianę wysokiej jakości informacji między wszystkimi podmiotami. Firmy powinny mieć dostęp do danych, które wpływają na podniesienie efektywności zarządzania łańcuchem i są konieczne do ograniczania zjawiska wzmocnionych zmian popytu. Niezbędne jest wyposażenie przedsiębiorstw w dane o źródłowym popycie z punktów sprzedaży detalicznej na podstawie, których można opracowywać prognozy popytu i planować działania firmy. Informacje o planowanych akcjach promocyjnych, o ilości i dostępności zapasów na poszczególnych szczeblach łańcucha, a także dostęp do wewnętrznych danych dotyczących planów produkcyjnych czy możliwość śledzenia procesu realizacji zamówienia są ważne dla zarządzania przepływami materiałowymi w łańcuchu. Przejrzystość zapasów w całym łańcuchu pozwala minimalizować ich poziom i koszty, co zapobiega zamawianiu przez klientów na zapas w celu antycypowania braku towarów i racjonowaniu produktów przez dostawcę. Warunkiem efektywnej wymiany informacji jest wdrożenie technologii informatycznej we wszystkich firmach łańcucha, pożądany jest dostęp do danych w czasie rzeczywistym i wdrażanie zarządzania ryzykiem, między innymi informacji w całym łańcuchu dostaw.

---

[14] D. Kisperska-Moroń, Logistyka: łańcuch wymagań i korzyści, CEO Magazyn Top Menedżerów wrzesień 2004.

[15] M. Starostka-Patyk, Wymiana danych EDI i B2B jako kluczowy czynnik współpracy i koordynacji partnerów w łańcuchu dostaw.

[16] P. Bradley: It is time to get plugged In. [w] Logistics, wrzesień 2000.

Literatura

1. Bradley P.: It is time to get plugged In. [w] Logistics, wrzesień 2000.
2. Dowding T., *Risk Information Technology The Great Leap Forward*, *Business Insurance Europe*, 29.01.2007, www.BIEurope.com
3. Kisperska-Moroń D., Logistyka: łańcuch wymagań i korzyści, CEO Magazyn Top Menedżerów wrzesień 2004.
4. Lei, Slocum, 1992.
5. Machowiak W., Konecka S., Kryzysogenne kategorie ryzyka specyficzne dla struktur logistycznych, 1st International Conference of Logistics INTLOG 2006.
6. Muszyński J. , Symantec zunifikował narzędzia do zarządzania ryzykiem, 18 czerwca 2007.
7. Nishat Faisal M., Banwet D.K. and Shankar R., Information risks management in supply chains: an assessment and mitigation framework, Journal of Enterprise Information Management, Vol. 20 No. 6 2007.
8. Pluta-Zaremba A., Efekt byczego bicza w łańcuchu dostaw, Gospodarka Materiałowa i Logistyka, nr 5, 2002.
9. Rudnicki R., Oprogramowanie wspomagające niektóre funkcje zarządzania ryzykiem, www.rudnicki.com.pl
10. Starostka-Patyk M., Wymiana danych EDI i B2B jako kluczowy czynnik współpracy i koordynacji partnerów w łańcuchu dostaw.
11. Szewczyk Ł., McAfee ulepsza zarządzanie ryzykiem, 12 czerwca 2007.
12. Tajwan: Trzęsienie ziemi wywołało chaos komunikacyjny w Azji, 2006-12-27, PAP, zab/ kan/
13. The 11 Greatest Supply Chain Disasters, Supply Chain Digest, 2006.

RISK MANAGEMENT CONCERNING INFORMATION FLOW IN THE SUPPLY CHAINS

Summary

Functioning of integrated supply chain is dependent on high quality information exchange between all links. Subsequently, effective information exchange is possible through implementation of information technology. World concerns leading in supply chains management perceive the necessity and advantages of the implementation of IT

tools in supporting supply chain risk management. Therefore, it seems necessary to determine supply chain risk categories, including risk involving information flow, classified as information security/ breakdown risks, forecast risks, intellectual property risks and IT/IS outsourcing risks. Several short case studies were included here to support the listed groups of risk. The article is a contribution to further considerations and research.

Translated by Sylwia Konecka