ZARZĄDZANIE RYZYKIEM TECHNOLOGICZNYM W PROCESIE WDRAŻANIA INNOWACJI

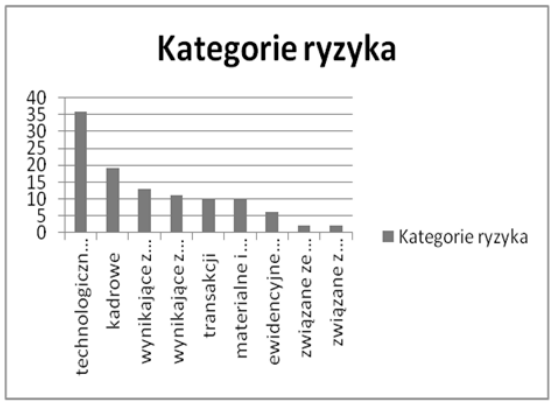
Jacek NAMYSŁO

Streszczenie: Niniejszy artykuł prezentuje wybrane rodzaje ryzyk występujących w procesach wdrażania innowacji, a także definiuje element wspólny dla poszczególnych faz rozwoju organizacji. W artykule wskazano rolę ryzyka związanego z tzw. czynnikiem ludzkim, jako szczególnie istotnego w przypadku prowadzenia działalności innowacyjnej. Analiza ta została dokonana w oparciu o dane ściśle związane z rzeczywistością gospodarczą, a dotyczące bankowości oraz innowacyjnych podmiotów informatycznych. W ostatniej części artykułu zaproponowano kilka prostych, niekosztownych i łatwych we wdrożeniu podstawowych zasad zarządzania ryzykiem technologicznym poprzez kontrolę ryzyka ludzkiego.

Słowa kluczowe: zarządzanie, ryzyko, technologie, innowacje, czynnik ludzki.

1. Postrzeganie ryzyka technologicznego

Większość doświadczonych i efektywnych menadżerów zdaje sobie sprawę z faktu, że zarządzanie każdym przedsięwzięciem, to nic innego, jak zarządzanie ryzykami z nim związanymi. Bazylejski Komitet Nadzoru Bankowego zdefiniował ryzyko operacyjne jako ryzyko straty wynikającej z niedostosowania lub zawodności wewnętrznych procesów, ludzi i systemów lub ze zdarzeń zewnętrznych. Definicja ta nie uwzględnia wszystkich zagrożeń (na przykład pomija ryzyko reputacji, czy też ryzyko strategiczne), jednak pokazuje w jakim kierunku zaczęły zmierzać działania instytucji bankowych, a więc jednego z istotniejszych elementów życia gospodarczego. Często spotykany w publikacjach pogląd identyfikuje ryzyko technologiczne jako składnik ryzyka operacyjnego. Podobnie zaczęła problem postrzegać bankowość, kiedy to w ślad za ankietą zleconą przez Generalny Inspektorat Nadzoru Bankowego, zdefiniowano profil ryzyka. Większość badanych instytucji za najważniejszą kategorię ryzyka operacyjnego uznało ryzyko technologiczne i techniczne (związane ze sprawnością systemów informatycznych i komunikacyjnych, błędami oprogramowania, utratą danych, adekwatnością wyposażenia, dostawą kluczowych usług, etc.). Drugą w kolejności najczęściej wymieniano kategorię ryzyka kadrowego

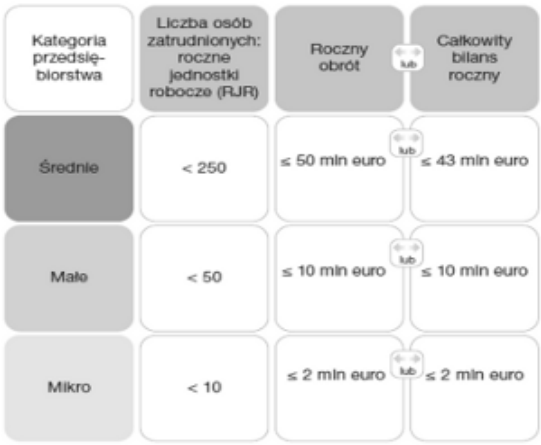


Rys. 1. Wyniki ankiety

(związane z dostępnością i kwalifikacjami pracowników, ich fluktuacją, zdolnościami do adaptacji, kulturą pracy, etc.). Jako istotne wskazano również zagrożenia związane z oszustwami, błędami oraz losowe.

Inny przykład postrzegania miejsca i znaczenia zarządzania ryzykiem technologicznym w procesie wdrażania innowacji pokazują wyniki kolejnej ankiety.
Została ona przeprowadzona na próbie 11 menadżerów, reprezentujących przedsięwzięcia innowacyjne, spełniające jednocześnie trzy
następujące założenia:

1. Działające w branży innowacyjnych technologii informatycznych;
2. Prowadzące działalność operacyjną na rynku polskim nie krócej, niż 3 lata;
3. Sklasyfikowane jako MSP, wg wytycznych UE;



Rys. 2. Klasyfikacja MSP wg UE

Celem badania była identyfikacja elementów ryzyka technologicznego w rzeczywistości gospodarczej polskich przedsięwzięć innowacyjnych. Jego wyniki posłużą do dalszych badań, zmierzających do opracowania nowych narzędzi, za pomocą których każdy przedsiębiorca będzie mógł łatwo, niedrogo i skutecznie wspomagać zarządzanie ryzykiem, w szczególności technologicznym. Przedsiębiorcy zostali poproszeni o przypisanie poszczególnym zagadnieniom wagi od „1" do „5" zgodnie ze znaczeniem, przedstawionym w tab.1.

Tab. 1. Znaczenie wag ankiety.

Wagi:	1	2	3	4	5
Znaczenie:	nie istotne	mało istotne	średnio istotne	ważne	bardzo ważne

Przedsiębiorcom zadano kilkanaście pytań w trzech kategoriach:

1. Postrzeganie ryzyka technologicznego:
   a) zarządzanie ryzykiem, a w szczególności ryzykiem technologicznym jest jednym z najważniejszych zadań organizacji i wszystkich jej członków;
   b) w każdej organizacji powinien zostać wdrożony w pełni funkcjonalny i efektywny system wspomagający zarządzanie ryzykiem, w tym technologicznym;
   c) zarządzanie ryzykiem technologicznym jest bardzo istotnym elementem ogólnej polityki zarządzania ryzykiem;
   d) ryzyko technologiczne w szczególności dotyczy przedsięwzięć innowacyjnych;
   e) efektywne zarządzanie ryzykiem technologicznym może ustrzec każdą organizację przed większością zagrożeń.
2. Stan bieżący, plany i bariery:

a) koszt wdrożenia i utrzymywania systemu wspomagającego zarządzanie ryzykiem technologicznym jest istotną barierą dla większości MSP innowacyjnych;
b) trudność obsługi jest istotną barierą dla wdrożenia systemu wspomagającego zarządzanie ryzykiem;
c) technologicznym;
d) brak dostępu do odpowiedniej wiedzy jest istotną barierą dla wdrożenia systemu wspomagającego zarządzanie ryzykiem technologicznym;
e) brak dostępu do uniwersalnych narzędzi jest istotną barierą dla wdrożenia systemu wspomagającego zarządzanie ryzykiem technologicznym;
f) jednym z najpilniejszych zadań w mojej organizacji, w perspektywie maks. 12 miesięcy, jest opracowanie odpowiedniej polityki oraz rozpoczęcie procedury wdrażania systemu zarządzania ryzykiem technologicznym.

Rys. 3. Wyniki ankiety, cz.1

3. Działania prewencyjne, które mogą uchronić:
a) Transfer ryzyka poprzez częściowe cedowanie odpowiedzialności na wyspecjalizowane firmy zewnętrzne;
b) Transfer ryzyka poprzez ochronę ubezpieczeniową;
c) Wdrożony plan utrzymania ciągłości biznesowej w sytuacji awaryjnej;
d) Wdrożona polityka bezpieczeństwa informacji;
e) Opracowane odpowiednie procedury kadrowe na etapie zatrudniania nowych pracowników;
f) Opracowane odpowiednie procedury ocen pracowniczych;
g) Dodatkowe regulacje cywilno-prawne zawarte pomiędzy pracodawcą, a wszystkimi pracownikami;
h) Wdrożona na stałe polityka;
i) cyklicznych szkoleń w zakresie zarządzania ryzykiem.

Rys. 4. Wyniki ankiety, cz.2

W kategorii pierwszej najwięcej punktów przyznano stwierdzeniu, że ryzyko technologiczne w szczególności dotyczy przedsięwzięć innowacyjnych, natomiast najmniejszą wagę przywiązywano do założenia, iż efektywne zarządzanie ryzykiem technologicznym może ustrzec każdą organizację przed większością zagrożeń.

W drugiej kategorii wskazano, że koszt wdrożenia i utrzymywania systemu wspomagającego zarządzanie ryzykiem technologicznym jest istotną barierą dla większości przedsięwzięć, z kolei najmniejszą wagę przywiązano do konieczności opracowania odpowiedniej polityki i rozpoczęcia procedury wdrażania.

Rys. 5. Wyniki ankiety, cz.3

Trzecia kategoria wskazuje, że jako podstawowy sposób ochrony przed zagrożeniami postrzegana jest możliwość transferu ryzyka poprzez ubezpieczenia, z kolei najmniejszą punktację przyznano zagadnieniom związanym z możliwością przeniesienia części odpowiedzialności na pracowników oraz dostawców zewnętrznych.

Wyniki dwóch, wcześniej przywołanych ankiet, a także wieloletnie doświadczenie biznesowe autora niniejszej publikacji, skłaniają do próby zdefiniowania następującej tezy:

Niezależnie od sposobu postrzegania ryzyka technologicznego, zdecydowana większość zagrożeń z niego wynikających, w przypadku przedsięwzięć innowacyjnych, związana jest bezpośrednio lub pośrednio z tzw. czynnikiem ludzkim. Jednocześnie znaczenie tegoż elementu, jak również wynikające z niego możliwości zarządzania ryzykiem, wciąż nie są dostrzegane przez przedsiębiorców w odpowiedni sposób, a często są wręcz niedoceniane.

W dalszej części opracowania przeprowadzona zostanie krótka analiza dwóch wybranych ryzyk, a mianowicie:

a) kradzieży i utraty informacji – jako przykładu na silne uzależnienie sukcesu od ludzkich błędów i nieświadomości, a także dla kontrastu:
b) zdarzeń losowych.

Następnie zostanie wskazanych kilka prostych metod o charakterze prewencyjnym, z których powinni korzystać wszyscy odpowiedzialni menadżerowie, jako wstęp do budowania przemyślanej polityki zarządzania ryzykiem technologicznym.

2. Ryzyka kradzieży i utraty informacji

Warto zwrócić uwagę na fakt, iż przedsiębiorca nie zawsze będzie zdawał sobie sprawę z utraty informacji, albowiem forma jej przechowywania w postaci elektronicznej powoduje, iż informację można powielać w łatwy i niedostrzegalny sposób. Kradzież informacji, to często wejście w posiadanie jej kopii, z jednoczesnym pozostawieniem oryginału u pierwotnego właściciela.

2.1. Podsłuch w interesie publicznym

Wiele rządów wdraża swoje rozwiązania podsłuchowe, bądź korzysta z systemów międzynarodowych. Przykładem niech będzie Echelon, czyli największa na świecie sieć Wywiadu Elektronicznego. System ten powstał przy udziale państw: USA, Wielkiej Brytanii, Kanady, Australii i Nowej Zelandii i jest zarządzany przez amerykańską służbę wywiadu NSA. Na całym globie rozlokował urządzenia techniczne do przechwytywania wiadomości w kanałach telekomunikacji. Oczywiście działania te usankcjonowane są zazwyczaj koniecznością walki z terroryzmem, niemniej jednak systemy takie przechwytują, niejako przy tej okazji, różnego rodzaju informacje.

2.2. Podsłuch gospodarczy

W dzisiejszej rzeczywistości urządzenia podsłuchowe - zarówno te proste, tzw. amatorskie, jak też dla profesjonalistów – można kupić łatwo, szybko i niedrogo. Nie dziwi więc fakt, że z łatwego dostępu do nich korzysta również część podmiotów gospodarczych. Oczywiście można dywagować nad etyczną stroną takich działań, czy wręcz starać się je piętnować. Nie wolno jednak zapominać, że są coraz szerzej wykorzystywane w konkurencyjnej, często bezkompromisowej walce.

2.3. Włamania do wewnętrznych systemów

W 1989 r. liczba komputerów w Internecie przekroczyła 100 tys., a 3 lata później milion. Polska sieć powstawała w ramach programu NASK, w 1990 r. Polska otrzymała zgodę na podłączenie się do Internetu. Obecnie, jako jedno z największych osiągnięć ludzkości końca XX wieku, postrzegany jest jako ogromne wsparcie w wielu dziedzinach ludzkiej działalności. Coraz obszerniej i na coraz wyższym poziomie służy również szybkiemu postępowi nauki i rewolucji oświatowej. Wpływa na zwiększanie poczucia wspólnoty i wspólnej odpowiedzialności na poziomie globalnym. Sprzyja znoszeniu barier w wymianie handlowej, a więc poprzez wzrost poziomu gospodarek narodowych, pomaga wyrównywać różnice między poszczególnymi krajami i regionami. Jest szansą dla przedsiębiorców na poszukiwanie kapitału, umożliwia dostęp do nowoczesnych technologii i wspomaga wszelkiego rodzaju promocję.

Życie współczesnego człowieka jest ściśle związane z coraz szerszym korzystaniem z rozmaitych osiągnięć techniki i technologii, szczególnie zaś komputerów, Internetu, telefonów komórkowych oraz innych narzędzi technologii informacyjnych. Narzędzia technologii informacyjnych wraz z całą zawartością treściową i medialną są również źródłem rozrywki, narzędziami pracy, dostępu do informacji itp. Tak zwane „nowe media" to – tak naprawdę – te same, stare media, takie jak druk, fotografia i telewizja, które zostały przekształcone na postać cyfrową, zapisane według kodu dwójkowego, umożliwiając tym samym swobodny dostęp do danych oraz ich interakcję. „Niewątpliwie umieszczenie nowych mediów w szerokiej perspektywie kulturowej pozwala na zrozumienie ich specyficznej roli. A rola ta jest duża, bowiem obszar objęty działaniem jest już w tej chwili ogromny: witryny WWW, wirtualna rzeczywistość, wirtualne światy, multimedia, gry komputerowe, interaktywne instalacje, animacje komputerowe, cyfrowe wideo, kino, interfejs człowiek-komputer".

Oczywiście nowe technologie to również zagrożenia, włącznie z problemem włamań sieciowych, złośliwego oprogramowania, ułatwień dla różnego rodzaju przestępców.

Ryzyka te należy jednak postrzegać w odpowiednim kontekście, bowiem większość ingerencji do systemów informacyjnych, to nic innego, jak wykorzystanie ludzkiego błędu, zaniedbania lub nieświadomości. Za przykład niech posłuży historia bodaj najbardziej znanego włamywacza komputerowego - Kevina Mitnicka. Za pośrednictwem mediów społeczeństwo zapamiętało jego działalność, jako przykład osoby, która w niecnych celach wykorzystuje nieprzeciętne zdolności informatyczne, jako tzw. hakera. Jednak prawda jest zgoła inna. To po prostu znawca ludzkiej natury, potrafiący wykorzystywać jej słabości, o czym świadczy nie tylko opis jego działalności, ale nawet sam podtytuł jednej z książek: „Łamałem ludzi, nie hasła".

Twórcy wielu narzędzi powinni oczywiście dostrzegać zagrożenia płynące z nieodpowiedzialnego ich używania i dlatego już na etapie tworzenia tych rozwiązań, szczególny nacisk kłaść na kwestie związane z zapewnieniem wysokiego poziomu bezpieczeństwa, czy też poufności przesyłanych informacji. Nie wspominając o elementarnych kwestiach, narzuconych przez Ustawodawcę, jak np. zabezpieczenie danych osobowych, na przestrzeganie których powinien zwrócić uwagę każdy administrator danych osobowych oraz administrator bezpieczeństwa informacji, jak też działalność zgodna z zaleceniami dotyczącymi świadczenia usług elektronicznych. Warto jednak pamiętać, że to tylko środki do celu, jakim jest odpowiedzialność użytkownika. Nawet najlepsze drzwi, z najlepszymi zamkami, nie zapewnią bezpieczeństwa, jeśli człowiek nie użyje klucza.

3. Ryzyka związane ze zdarzeniami losowymi

Ryzyka losowe charakteryzują się przede wszystkim brakiem możliwości istotnego wpływu na ich wystąpienie. Niemniej jednak można próbować ograniczać efekty ich zaistnienia, a także można zarządzać ryzykiem poprzez transfer odpowiedzialności.

3.1. Siła natury

Wszelkiego rodzaju plany mogą zostać zniwelowane również przez nieprzewidywalne zjawiska przyrodnicze. Przykładem niech będzie pył wulkaniczny, który w kwietniu 2010 roku spowodował konieczność zamknięcia nieba nad Europą. Ta decyzja kosztowała wiele pieniędzy, jak i nerwów. Branża lotnicza traciła dziennie ok. 200 mln dolarów, tylko z tytułu utraconych przychodów, jak wskazywały szacunki Zrzeszenia Międzynarodowych Przewoźników Lotniczych. Do tego doszły koszty związane z utrzymaniem stojących maszyn w portach lotniczych. Dokładnie oszacowane straty, być może nie będą jeszcze długo znane, niemniej jednak z pewnością były wielomiliardowe, a to z kolei nie ułatwiło życia menadżerom związanym na przykład z branżą lotniczą, czy turystyczną, a więc było przykładem wystąpienia ryzyka losowego. W piątym dniu po ogłoszeniu wystąpienia zanieczyszczeń Międzynarodowe Zrzeszenie Przewoźników Powietrznych (IATA) oszacowało, że w wyniku zamknięcia przestrzeni powietrznej straty sektora lotniczego wyniosły co najmniej 1,7 mld USD. „Skala problemów jest większa niż po 11 września 2001 r. kiedy terroryści zaatakowali USA. Według Giovanii Bisignani, szefa IATA zakłócenia dotyczyły 29 proc. światowego transportu i dotykały dziennie około 1,2 mln pasażerów." Koncerny samochodowe w Europie, ale także w Japonii zmuszone były wstrzymać produkcję z powodu braku dostaw części. Łańcuchy powiązań, dostaw i kooperacji są często bardzo rozległe, co tylko spotęgowało straty. Skutki takich zakłóceń

w sprawnym funkcjonowaniu odczuły tysiące firm, w różnych częściach świata, różnej wielkości.

3.2. Polityka

Skalę problemu powiększa złożona charakterystyka zjawisk ekonomicznych, w dużej mierze uzależnionych od wielu czynników decyzyjnych, w dodatku bardzo często nieprzewidywalnych. Historia światowego kapitalizmu, a w szczególności kilka ogólnie znanych i spektakularnych załamań gospodarki (tzw. kryzysów), dobitnie uzmysławia, że wszelkie próby analiz danych historycznych sprawdzają się doskonale do pewnego momentu, którym to jest dzień dzisiejszy. Natomiast, czym dalej w przyszłość próbuje sięgnąć prognoza, tym większym błędem potencjalnego ryzyka jest obciążona. Mimo, iż przyjęto, że cykl każdej zdrowej gospodarki jest formą stosunkowo przewidywalnej sinusoidy, nigdy nie można przewidzieć wszystkich elementów ryzyka i czyhających zagrożeń.

3.3. Gospodarka

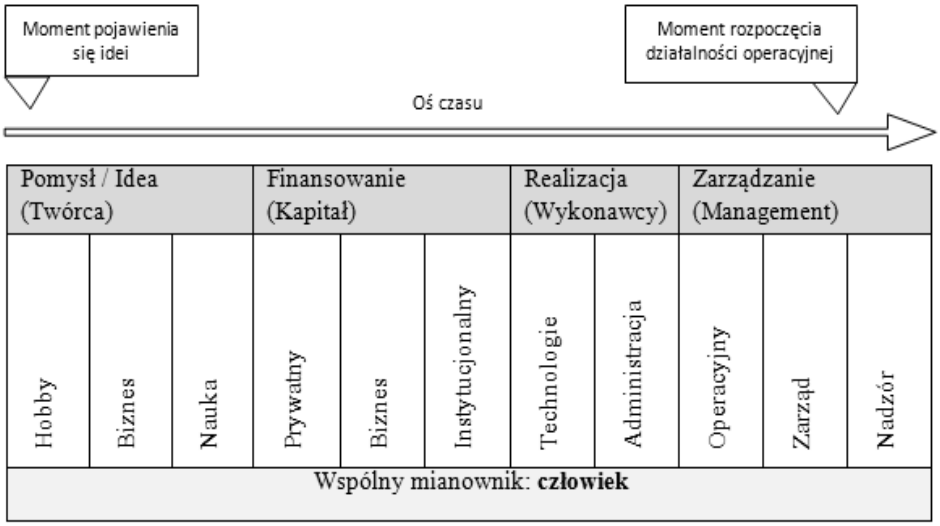
Duże znaczenie mają też informacje napływające ze światowych gospodarek, które często noszą wydźwięk sygnałów spowolnienia wzrostu gospodarczego, niezależnie od regionu. W kontekście ostatniego globalnego kryzysu, w szczególności dotyczyło to gospodarki USA. Boleśnie odczuwała ona skutki kryzysu na rynku kredytów hipotecznych, nazwanych z czasem kredytami NINJA („no income, no job, no assets" – „bez stałych dochodów, pracy i odpowiedniego majątku"). Ta stagnacja w USA zaczęła wpływać w sposób niekorzystny na inne gospodarki. Znalazło to odzwierciedlenie między innymi w spadku w I kwartale 2008 roku PKB w strefie euro (liczonym kwartał do kwartału), czy też w roku 2009. Tym samym została mocno podważona teza o odporności gospodarki europejskiej na szoki zewnętrzne.

Kolejnym ciekawym zjawiskiem, mającym swoje podłoże w niedalekiej przeszłości, a jednocześnie będącym wynikiem coraz większej standaryzacji zachowań rynków inwestycyjnych i związanego z nim nieporozumienia, jest reakcja kursu złotego po ogłoszeniu przez premiera Węgier kłopotów jego gospodarki. Standaryzacja produktów i usług to odpowiedź na globalizację i jednocześnie ułatwienie jej rozwoju, ułatwienie przewidywań, ujednolicenie reakcji na zagrożenia. Skrajnym przykładem standaryzacji jest tzw. „mc`donaldyzacja", czyli ujednolicenie wszystkich aspektów działalności, niezależnie od części świata, w której działa każda z jednostek przedsiębiorstwa. Okazało się jednak, iż standaryzowanie reakcji świata finansów na zagrożenia nie jest dobrym pomysłem. Na przykład w drugim kwartale 2010r. nastąpiło duże wahanie kursu złotego i nikt nie wiedział co mogło być tego powodem. Okazało się, że był to skutek wypowiedzi premiera Węgier, mówiącej o zagrożeniu bankructwem jego kraju. W świadomości międzynarodowych rynków finansowych Polska, Węgry, Słowacja i Czechy to jeden rynek, co w konsekwencji oznacza, że kłopoty jednego z tych krajów automatycznie powodują odpływ kapitału z pozostałych.

4. Działania prewencyjne

Część z ryzyk natury losowej trudno przewidywać, trudno też z nimi walczyć. W tym zakresie osoba zarządzająca powinna położyć główny nacisk na poszukiwanie i wdrażanie

narzędzi związanych z ubezpieczeniami. Na szczęście zdarzają się one stosunkowo rzadko (co nie oznacza, iż można je bagatelizować). Jednak o wiele częściej menadżer ma do czynienia z pozostałymi rodzajami zagrożeń. Bezpośrednio, bądź pośrednio wiele z nich związanych jest z ryzykiem wynikającym z działalności człowieka, tak zwanym ryzykiem czynnika ludzkiego. Zagrożenie to z łatwością można zidentyfikować na każdym z etapów tworzenia, rozwoju i funkcjonowania podmiotu gospodarczego.



Rys. 6. Etapy rozwoju przedsięwzięcia

Nowoczesna gospodarka oparta jest na wiedzy, a więc w dużej mierze związana z ludzkim umysłem. Ponadto zakres, sposoby i charakter informacji, jako nośnika tejże wiedzy, czynią ją bardzo podatną na zagrożenia. Dlatego właśnie to człowiek jest dla firmy innowacyjnej zarówno:

- jej największym dobrem i aktywem,
- jak również – największym ryzykiem i zagrożeniem.

4.1. Kilka prostych i niekosztownych zasad

Niezależnie od wielkości organizacji oraz budżetu, jaki jest w stanie wyasygnować na tego typu cele, w pierwszej kolejności można zadbać o kilka prostych, łatwych i niedrogich w implementacji elementów, jak na przykład:

1. Zapewnić osobom odpowiedzialnym za poszczególne zespoły ludzkie dostęp do wiedzy (np. poprzez publikacje i szkolenia) oraz rzetelnych i prawdziwych informacji na temat zagrożeń występujących w danej organizacji. Dzięki temu management będzie miał prawdziwy obraz ryzyk na wszystkich szczeblach działalności podmiotu.
2. Menadżerowie z kolei powinni ‘scedować’ tę wiedzę na wszystkich podległych pracowników (np. poprzez coaching i wewnętrzne szkolenia). Dzięki temu wszystkie zespoły będą zdawały sobie sprawę z zagrożeń

3. Uświadamiać wszystkim członkom zespołów, że wszyscy powinni wspólnie chronić dobro firmy, dzięki czemu możliwie największa część zespołu winna traktować ryzyko w firmie na poziomie zbliżonym do ryzyka osobistego. Człowiek najlepiej chroni to, co kocha, bądź za co czuje się odpowiedzialny.
4. W stosunkowo niewielkich odstępach czasu (min. 2 razy w roku) powinno się wszystkim przypominać (np. poprzez coaching i nadzór) o istniejących ryzykach i konieczności ich unikania.

Wielu ludzi zdaje sobie sprawę z tych kilku powyższych zasad, a wręcz może je postrzegać jako bardzo banalne. Często jednak rzeczywistość jest zgoła odmienna. Jako przykład niech posłuży tutaj problem haseł dostępowych do komputerów. Niby wszyscy wiedzą, że nie mogą być zbyt proste, że należy je często zmieniać oraz, że pod żadnym pozorem nie wolno ich zapisywać w miejscu dostępnym dla innych, a jednak przyzwyczajenia i naturalny pęd do uproszczeń robią swoje. To z kolei czyni okazję dla złodzieja.

5. Wnioski

Analiza przeprowadzona na podstawie badań oraz zachowań występujących w praktyce rynkowej, pozwala na wyciągnięcie dwóch głównych wniosków:

1. W przypadku przedsięwzięć innowacyjnych, w szczególności w zakresie działalności informatycznej, gdzie zdecydowana większość wartości inwestycji opiera się o informację i wiedzę, jednym z najważniejszych niebezpieczeństw wydają się być ryzyka związane z tak zwanym czynnikiem ludzkim.
2. Wśród przedsiębiorców dopiero zaczyna kształtować się świadomość istnienia i skali ‘ryzyka ludzkiego’, a więc warto zwracać ich uwagę na tego typu zagrożenia, a także uczyć w jaki sposób mogą sobie radzić z tymi problemami.

Z pewnością warto również uświadamiać menadżerów różnego szczebla, że ochrona informacji na podstawowym poziomie nie jest ani trudna, ani też kosztowna. W rzeczywistości wymaga przede wszystkim odpowiedniej wiedzy na temat zagrożeń, wdrożenia systemu przestrzegania kilku prostych procedur i wreszcie kontroli. W porównaniu do ogromu strat, jakie może wywołać naruszenie tychże zasad i utrata informacji, koszt wdrożenia jest wręcz znikomy.

Literatura

1. Bazylejski Komitet Nadzoru Bankowego: Sound practises for the management and supervision of operational risk, luty 2003.
2. Krajowa Izba Biegłych Rewidentów [online]: Pismo Generalnego Inspektora Nadzoru Bankowego do prezesów banków dotyczące zarządzania ryzykiem operacyjnym.
3. Zalecenie Komisji 2003/361/WE, opublikowane w Dzienniku Urzędowym Unii Europejskiej L 124 z 20 maja 2003 r.
4. Kosewski A.: Techniki komputerowe w przekazie edukacyjnym. X jubileuszowe ogólnopolskie sympozjum naukowe. [W:] Internet – historia i przyszłość. Wydawnictwo Naukowe Akademii Pedagogicznej w Krakowie, Kraków, 2000.
5. Morbitzer, J.: 17. Ogólnopolskie sympozjum naukowe nt "Komputer w Edukacji. [W:] Człowiek w świecie technologii informacyjnych. Wydawnictwo Naukowe Akademii Pedagogicznej w Krakowie, Kraków, 2007.

6. Wieczorek-Tomaszewska M.: 17. Ogólnopolskie sympozjum naukowe nt "Komputer w Edukacji". [W:] Nowe media. Komunikacyjna funkcja obrazu. Wydawnictwo Naukowe Akademii Pedagogicznej w Krakowie, Kraków, 2007.
7. Mitnick K., Simon W.: Sztuka podstępu. Łamałem ludzi, nie hasła. Helion, 2003.
8. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych - Dz. U. z 1997r. nr 133, poz. 883 z późn. zm.
9. Kral P.: Dane osobowe w firmie. Instrukcja przetwarzania. Ośrodek Doradztwa i Doskonalenia Kadr, Gdańsk, 2006.
10. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną - Dz. U. Z 2002r., nr 144, poz. 1204 z późn. zm.
11. P Puls Biznesu [online]: Sektor lotniczy stracił 1,7 mld USD.

Mgr Jacek NAMYSŁO
VidCom.pl Sp. z o. o.
40-156 Katowice, Al. Korfantego 125a
tel./fax.: (32) 450 20 85
e-mail: jacek.namyslo@vidcom.pl