Dariusz Wawrzyniak

Ekonomiczne aspekty zarządzania ryzykiem informatycznym w bankowości : wybrane zagadnienia

Ekonomiczne Problemy Usług nr 38, 374-381

2009

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 548 EKONOMICZNE PROBLEMY USŁUG NR 38 2009

DARIUSZ WAWRZYNIAK
Uniwersytet Ekonomiczny we Wrocławiu

EKONOMICZNE ASPEKTY ZARZĄDZANIA RYZYKIEM INFORMATYCZNYM W BANKOWOŚCI – WYBRANE ZAGADNIENIA

Wprowadzenie

Ryzyko informatyczne towarzyszy dzisiaj niemal każdemu przejawowi działalności gospodarczej. Zarządzanie ryzykiem informatycznym odgrywa szczególną rolę w instytucjach, w których bezpieczeństwo informatyczne nie tylko umożliwia poprawne funkcjonowanie, lecz wręcz warunkuje istnienie i możliwości rozwoju. Przykładem tego typu instytucji są banki, w których ryzyko informatyczne stało się w ostatnich latach problemem o charakterze strategicznym. Zarządzanie ryzykiem informatycznym jest interdyscyplinarnym, cyklicznym procesem, w którym znaczącą rolę ogrywają także aspekty ekonomiczne. Artykuł niniejszy jest próbą zasygnalizowania związków pomiędzy ryzykiem informatycznym postrzeganym z punktu widzenia informatyki a widzianymi w nieco szerszym kontekście finansowymi aspektami zarządzania tym rodzajem ryzyka.

Ryzyko informatyczne

Genezy pojęcia ryzyka informatycznego doszukiwać się można na długo przed upowszechnieniem się sieci Internet, aczkolwiek na przestrzeni ostatnich dwudziestu kilku lat zmienił się w istotny sposób charakter postrzegania problemu, który ewoluował od prostych koncepcji analizy ryzyka informatycznego do złożonych procesów zarządzania tym ryzykiem. Aby rozpocząć dyskusję nad pojęciem ryzyka informatycznego, przedstawić należy cztery kluczowe dla omawianego zagadnienia terminy, jakimi są: zasoby (aktywa), wrażliwość, zagrożenie i podatność[1]. Zasoby to wszystko, co dla instytucji ma wartość i co dla jej dobra należy chronić, aby mogła ona funkcjonować w sposób niezakłócony. Wrażliwość jest miarą ważności przypisaną do informacji przez jej autora lub dysponenta w celu wskazania konieczności oraz zasad jej ochrony. Zagrożeniami nazywamy potencjalne przyczyny niepożądanych zdarzeń, których skutkiem mogą być straty powstałe w systemie informatycz-

[1] Definicje przytoczone na podstawie: A. Białas: *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*. Wydawnictwa Naukowo-Techniczne, Warszawa 2006, s. 36 i n.

nym, a w dalszej konsekwencji w instytucji. Podatność natomiast to słabość lub luka w systemie informatycznym, która może być wykorzystana przez zagrożenia powodując straty. Sam fakt istnienia zagrożeń jest immanentną cechą każdego systemu oraz jego otoczenia i nie jest jeszcze bezpośrednią przyczyną incydentów – niekorzystnych zdarzeń negatywnie wpływających na bezpieczeństwo systemu. Do incydentu oraz wynikających z niego strat może bowiem dojść dopiero wtedy, gdy zagrożenie wykorzysta jakąś podatność systemu. Innymi słowy, strata jest efektem realizacji zagrożenia, a nie efektem jego istnienia.

Niewątpliwie najistotniejszy głos we współczesnej dyskusji terminologicznej nad pojęciem ryzyka informatycznego zabiera organizacja ISO, której efektem prac jest norma ISO/IEC 27001:2005 będąca podstawą nowego standardu zarządzania bezpieczeństwem i ryzykiem informatycznym[2]. Zgodnie z polską wersją normy (PN-ISO/IEC 27001:2007[3]) ryzyko to funkcja prawdopodobieństwa zdarzenia i jego konsekwencji[4]. Definicja wskazuje więc jednoznacznie na następujące atrybuty ryzyka informatycznego:

- jest określane za pomocą prawdopodobieństwa,
- nie wyraża wartościowo straty, lecz wiąże funkcjonalnie wartość tej straty z prawdopodobieństwem oraz konsekwencjami zdarzenia, które może ją spowodować.

Ryzyko według normy postrzegane jest zatem jako:

$$R = f(P(Z), S(Z)) \tag{1}$$

gdzie:

R – ryzyko,
$P(Z)$ – prawdopodobieństwo wystąpienia zdarzenia Z,
$S(Z)$ – potencjalna strata wynikająca z wystąpienia zdarzenia Z.

Proces zarządzania ryzykiem informatycznym według normy ISO/IEC 27005 składa się z trzech podstawowych etapów: szacowania ryzyka, postępowania z ryzykiem, akceptacji ryzyka (rys. 1).

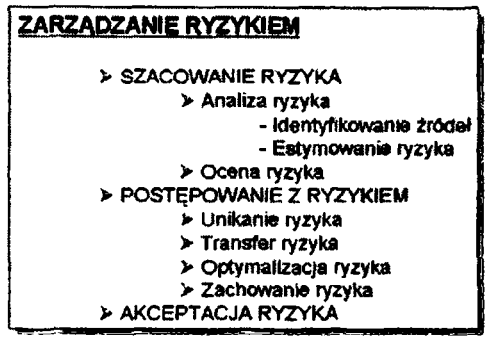
Problematyka zarządzania ryzykiem informatycznym nie może uniknąć naturalnej, wynikającej z powyżej przytoczonej definicji, konotacji ekonomicznej. Jest to związek szczególnie istotny w tych obszarach zastosowań informatyki, w których wymagania dotyczące poziomu bezpieczeństwa informatycznego są bardzo wysokie. Obszarem takim jest przede wszystkim bankowość.

---

[2] Information technology – Security techniques – Information security management systems – Requirements. Grupa norm ISO/IEC 27001, 27002, 27003, 27004, 27005 i następnych ma stanowić podstawę dla wszystkich norm ISO dotyczących omawianego zagadnienia.

[3] Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

[4] Na podstawie E. Andrukiewicz, ISO/IEC 27005 – Zarządzanie ryzykiem w procesie budowania systemu zarządzania bezpieczeństwem informacji. Prezentacja w ramach Forum Zarządzania Bezpieczeństwem Informacji, Warszawa 2006.



Rys. 1. Model zarządzania ryzykiem informatycznym według PN-ISO/IEC 27001

Źródło: na podstawie E. Andrukiewicz: *op.cit.*

Aspekt ekonomiczny omawianego zagadnienia przejawia się w co najmniej trzech obszarach:

- obszarze szacowania wartości zasobów systemowych,
- obszarze szacowania potencjalnych strat wynikających z realizacji zagrożeń bezpieczeństwa,
  obszarze analizy opłacalności (efektywności) działań związanych z zarządzaniem ryzykiem[5].

Szacowanie wartości zasobów systemowych

A. Białas identyfikuje następujące problemy wartościowania zasobów systemowych związane z[6]:

- opracowaniem dla instytucji jednolitej metody wyceny zasobów, które z natury są bardzo różnorodne i najczęściej niemożliwe do przedstawienia w postaci kwot pieniężnych,
  uwzględnieniem efektów propagacji i kumulacji wartości cząstkowych,
- uwzględnieniem efektu obniżania się wartości na skutek powielarności zasobu lub łatwości jego odtwarzania,
- wyrażeniem skomplikowanych, nie w pełni poznanych zależności między zasobami.

Autor zauważa także, że trudno jest wyrazić wartość zasobu w sposób czysto ilościowy, stąd nierzadko trzeba posługiwać się miarami umownymi – jakościowymi. W cyto-

[5] Problematyka pojęcia efektywności w informatyce oraz założeń metodycznych badania efektywności została wyczerpująco omówiona między innymi w: H. Dudycz, M. Dyczkowski: *Efektywność przedsięwzięć informatycznych. Podstawy metodyczne pomiaru i przykłady zastosowań.* Wydawnictwo Akademii Ekonomicznej im. Oskara Langego we Wrocławiu, Wrocław 2007.

[6] A. Białas: *op.cit.*, s. 254 i n.

wanym opracowaniu nie odnajdujemy zatem konkretnych propozycji rozwiązań problemu wyceny, wart jednak podkreślenia jest fakt zaproponowania mechanizmu wspomagającego proces wyceny, związanego z ilościowym ujęciem czynników wpływających na wycenę. Znajdują się wśród nich[7]: zakłócenie ciągłości procesów biznesowych składających się na misję instytucji, zagrożenie dla zdrowia lub życia, zagrożenie dla środowiska naturalnego, zakłócenie porządku publicznego, możliwość naruszenia prawa lub zobowiązań, straty finansowe, utrata reputacji instytucji, możliwość zastąpienia, pozytywne cechy osobowe, poziom wiedzy, fachowości, poniesiony koszt wyszkolenia, autorytet, wartość księgowa, koszt odtworzenia.

O krok dalej w swoich rozważaniach idzie A. Jaquith, który generalnie odrzuca sensowność przypisywania zasobom jakichkolwiek wartości wyrażonych w pieniądzu, tłumacząc to brakiem możliwości realizacji takiego zadania w sposób konsekwentny i wiarygodny[8].

K. Liderman przedstawia omawiany problem raczej skrótowo, niemniej wskazuje na istotne jego atrybuty niewymienione powyżej. Pisze on, że oceniając wartość zasobów informacyjnych należy brać pod uwagę[9]:

- bezpieczeństwo osobiste i poufne informacje osobiste,
- zobowiązania prawne i regulaminowe firmy oraz personelu,
- obowiązujące przepisy prawa,
- interesy handlowe i ekonomiczne firmy,
- możliwe straty finansowe w przypadku utraty poufności, integralności lub dostępności informacji albo przerwania czy zniszczenia procesów biznesowych,
- porządek publiczny,
- politykę działania firmy,
- utratę reputacji firmy.

Analiza powyższych opinii nakazuje zadać dość istotne pytanie: czy wartościowanie zasobów oznaczać musi przypisanie do każdego zasobu odpowiadającej mu wartości wyrażonej w pieniądzu lub niemianowanej wartości liczbowej, czy raczej celem wartościowania jest przypisanie zasobów do określonych grup (kategorii) odpowiadających wymaganiom prawnym i biznesowym? Odpowiedź zdecydowanie bliższa jest drugiej opcji. Wartościo-

[7] A. Białas: *op.cit.*, s. 256. Cytowany autor dzieli zasoby na kilka kategorii poziomów, m.in.: funkcje wewnętrzne i zewnętrzne jej wizerunek i zaufanie klientów, infrastruktura techniczna, personel, dokumentacja, oprogramowanie.

[8] A. Jaquith: *Security Metrics*. Addison-Wesley, Pearson Education Inc., 2007, s. 95 i n. Autor podaje między innymi powszechnie wykorzystywany przykład wartościowania komputera przenośnego. Czy jest on wart tyle, ile jest wart sam komputer, czy jego wartość wzrasta wraz z pojawianiem się na jego dysku informacji. Jeśli tak, to wartość ta będzie zmieniać się cały czas i nigdy nie będzie możliwa do dokładnego określenia.

[9] K. Liderman: *Analiza ryzyka i ochrona informacji w systemach komputerowych*. Wydawnictwo Naukowe PWN, Warszawa 2008, s. 35 i n.

wanie w procesie analizy ryzyka powinno przypisać zasoby do określonych przez bank kategorii, niekoniecznie nadając tym zasobom stałe wartości wyrażane w pieniądzu.

Szacowanie strat wynikających z realizacji zagrożeń

Zagadnienia związane z szacowaniem potencjalnych strat wynikających z realizacji zagrożeń bezpieczeństwa mają charakter ocen eksperckich wspomaganych danymi historycznymi (wewnętrznymi i zewnętrznymi), niemniej możliwe jest także uzupełnienie tego typu ocen narzędziami ilościowymi. W szczególności straty wynikające z realizacji zagrożeń bezpieczeństwa przejawiać się mogą jako koszty: sprzętu, oprogramowania, usług informatycznych, utraty własności, utraty przychodów, grzywien i odszkodowań, przepływów pieniężnych, zasobów ludzkich.

Analiza opłacalności działań związanych z zarządzaniem ryzykiem

W obszarze analizy opłacalności działań związanych z zarządzaniem ryzykiem wykorzystuje się najczęściej rozwinięcia i modyfikacje klasycznych metod przepływów pieniężnych netto oraz wewnętrznej stopy zwrotu. Celem metody wartości zaktualizowanej netto jest wyznaczenie aktualnej wartości NPV wpływów i wydatków związanych z danym projektem, przy założeniu stałego poziomu stopy procentowej. Wielkość NPV oblicza się następująco[10]:

$$NPV = \sum_{t=0}^{n} NCF_t \cdot DF_t, \tag{2}$$

gdzie $t = 0, \ldots, n$ jest kolejnym rokiem n-letniego okresu obliczeniowego, NCF_t oznacza przepływy pieniężne netto w roku t, DF_t jest współczynnikiem dyskontowym w roku t, który dla stopy procentowej r wynosi:

$$DF_t = \frac{1}{(1+r)^t} \tag{3}$$

Drugą powszechnie stosowaną metodą oceny opłacalności przedsięwzięć informatycznych jest metoda wewnętrznej stopy zwrotu. W ogólnym przypadku wykonywana jest ona w trzech etapach[11]:

1. Ustalenie wartości przepływów pieniężnych netto NCF_t dla kolejnych lat okresu obliczeniowego.

[10] Zob. np. M. Flasiński: *Zarządzanie projektami informatycznymi*. Wydawnictwo Naukowe PWN, Warszawa 2007, s. 146 i n.

[11] Zob. np.: *ibidem*, s. 149 i n. Jak zauważa autor, analiza opłacalności projektów przy wykorzystaniu NPV i IRR może dać przeciwstawne rezultaty. W takich przypadkach zaleca się przyjęcie metody NPV jako bardziej wiarygodnej.

2. Oszacowanie (metodą kolejnych przybliżeń) dwóch wielkości stopy procentowej i_1 oraz i_2, takich że:
   - wartość NPV obliczona dla i_1 jest bliska zeru, ale dodatnia (PV),
   - wartość NPV obliczona dla i_2 jest bliska zeru, ale ujemna (NV).
3. Obliczenie IRR za pomocą poniższej zależności:

$$IRR = i_1 + \frac{PV(i_2 - i_1)}{PV + |NV|} \tag{4}$$

Wewnętrzna stopa zwrotu może być także pochodną metody straty oczekiwanej (*ALE – Annual Loss Expected*) – prostej metody szacowania ryzyka informatycznego. Metodę ALE można przedstawić za pomocą jednego z trzech poniższych modeli:

$$ALE = (\textit{prawdopodobieństwo zdarzenia}) \times (\textit{wartość straty}) \tag{5}$$

$$ALE = (\textit{skutek zdarzenia}) \times (\textit{częstość występowania zdarzenia}) \tag{6}$$

$$ALE = \sum_{i=1}^{n} I(O_i)F_i \tag{7}$$

gdzie $\{O_1, ..., O_n\}$ to zbiór negatywnych skutków zdarzenia; $I(O_i)$ to wartościowo wyrażona strata wynikająca z zaistnienia zdarzenia, a F_i to częstotliwość zdarzenia i.

Bez względu na to, który model uznamy za najwłaściwszy, praktyczne znaczenie metody straty oczekiwanej pozostaje bez zmian. ALE może służyć także jako podstawa tworzenia innych miar ryzyka oraz nieco odmiennego od przytoczonego powyżej podejścia do wewnętrznej stopy zwrotu (tab. 1).

Tabela 1

Strata oczekiwana oraz wskaźniki pochodne

Wskaźnik	Symbol	Sposób wyznaczenia wartości
Oczekiwana strata	*OS*	Prawdopodobieństwo wystąpienia ryzyka × wartość potencjalnej straty
Zysk z tytułu zastosowanych zabezpieczeń	*Z*	*OS* *OS* z zabezpieczeniami
Wartość dodana	*WD*	*Z* + nowe możliwości
Zwrot z inwestycji	*ROI*	$\frac{WD}{\textit{koszty zabezpieczeń}}$
Wewnętrzna stopa zwrotu	*IRR*	$K_0 \quad \sum_{t=1}^{n} \frac{WD_t - K_t}{(1 + IRR)^t}$

Źródło: E. Schechter: *Computer Security Strength & Risk: A Quantitative Approach*. Thesis presented to The Division of Engineering and Applied Sciences. Harvard University, 2004.

Podsumowanie

Artykuł przedstawia jedynie sygnalne prezentacje wybranych zagadnień związanych z problemem ekonomicznej analizy procesu zarządzania ryzykiem informatycznym w bankowości. Podsumowując powyższe rozważania, należy oczywiście zadać kluczowe w przypadku problematyki bezpieczeństwa w bankowości pytanie: Czy wyniki implementacji jakichkolwiek metod oceny opłacalności (efektywności) rozwiązań wspomagających proces zarządzania ryzykiem informatycznym powinny warunkować – choćby w nieznacznym stopniu – zakres (merytoryczny, czasowy i finansowy) decyzji podejmowanych w ramach tego procesu? Można bowiem podać wiele przykładów rozwiązań z obszaru zarządzania ryzykiem informatycznym, których implementacja w naturalny sposób skutkuje negatywnymi ocenami opłacalności, jednak z punktu widzenia zarządzania ryzykiem jest konieczna. Wydaje się, że rozwiązaniem tego problemu mogłoby być wykorzystanie metod oceny efektywności rozwiązań informatycznych uwzględniających nie tylko przepływy pieniężne, ale także generowane przez te rozwiązania zmiany w poziomie ryzyka informatycznego. Przykładem takiej metody może być metoda ROSI (*Return on investment for a security investment*), która bazuje na poniższej formule:

$$ROSI = \frac{(Ryzyko \times \%\ Eliminacji\ \ ryzyka) - Koszt}{Koszt} \tag{8}$$

Oczywiście przy takim podejściu problemem samym w sobie staje się zagadnienie możliwości szacowania zmian poziomu ryzyka informatycznego[12]. Ryzyko to – szczególnie w działalności bankowej – jest bowiem problemem, którego ilościowe ujęcie nie poddaje się standardowym metodom wykorzystującym tylko dane historyczne. Niezbędne w procesach szacowania tego typu ryzyka są eksperckie oceny oraz odpowiednie mechanizmy ilościowe.

W artykule przedstawiono jedynie skromny wybór mechanizmów wspomagających zarządzanie ekonomicznymi aspektami ryzyka informatycznego. Wśród niewymienionych powyżej wskazać należy: ISRAM (*Information security risk analysis metod*), pochodne VaR adaptowane do problematyki zarządzania ryzykiem informatycznym, rozwiązania bazujące na podejściu bayesowskim, metodę całkowitego wpływu ekonomicznego (*Total Economic Impact*) i wiele innych.

[12] Zob. np. D. Wawrzyniak: *Wybrane problemy oceny ryzyka informatycznego w działalności bankowej*. „Rachunkowość Bankowa" 2006, 10(23), a także D. Wawrzyniak: *Information Security Risk Assessment Model for Risk Management*. W: *Trust, Privacy, and Security in Digital Business*. Third International Conference, TrustBus 2006 Proceedings. Red. S. Fisher-Hubner, S. Furnell, C. Lambrinoudakis. Wydawnictwo Springer, 2006.

ECONOMIC ASPECTS OF INFORMATION SECURITY RISK MANAGEMENT IN BANKING – CHOSEN PROBLEMS.

Summary

The article presents chosen problems dealing with the economic issues concerning information security risk management in banking. The information security risk definition has been given as well as its short description based on ISO/IEC 27005 standard. Three economic issues have been identified: system assets valuation, valuation of losses dealing with security threats and risk management effectivity. These issues were briefly presented. Some problems dealing with risk management effectivity analysis were emphasized.