Zeszyty Naukowe Politechniki Częstochowskiej
Zarządzanie Nr 23 t.1 (2016) s. 118–129
dostępne na: http://www.zim.pcz.pl/znwz

WYBRANE METODY POMIARU EFEKTYWNOŚCI EKONOMICZNEJ INWESTYCJI ZWIĄZANYCH Z ZARZĄDZANIEM RYZYKIEM IT W ORGANIZACJI

Artur Rot

Uniwersytet Ekonomiczny we Wrocławiu
Wydział Zarządzania, Informatyki i Finansów

Streszczenie: Zarządzanie ryzykiem IT jest prewencją wobec zagrożeń, gdyż polega na rozwiązaniach, których zasadniczym celem jest zapobieganie sytuacjom krytycznym przez dostrzeganie czynników zagrożeń, monitorowanie charakterystycznych i typowych symptomów ich aktywizowania się oraz zapobieganie ich interakcji z systemem działania organizacji lub jej otoczeniem. W tym celu konieczne jest wdrażanie odpowiednich narzędzi i rozwiązań, które łączą się z poniesieniem kosztów. Zarządzanie ryzykiem jest ciągłym procesem, wiążącym się z permanentnymi wydatkami, związanymi z planowaniem i projektowaniem zasad, procedur i adekwatnych zabezpieczeń, z zakupem sprzętu i programowych implementacji mechanizmów bezpieczeństwa, wdrażaniem odpowiednich zasad i procedur bezpieczeństwa, monitorowaniem, audytem i ewaluacją zabezpieczeń, dodatkową pracą specjalistów. Dlatego też dla praktyki biznesowej analiza efektywności inwestycji związanych z zarządzaniem ryzykiem staje się zagadnieniem niezwykłej wagi. Artykuł przedstawia wybrane modele i metody, które mogą znaleźć zastosowanie w ocenie efektywności inwestycji w obszarze zarządzania ryzykiem informatycznym.

Słowa kluczowe: bezpieczeństwo systemów informatycznych, zarządzanie ryzykiem informatycznym, efektywność inwestycji, ROI, NPV, IRR

DOI: 10.17512/znpcz.2016.3.1.12

Wprowadzenie

Technologie informatyczne (IT) rozwijają się niezwykle dynamicznie, powodując powstanie nowych produktów i usług. Coraz większe nasycenie środkami technicznymi informatyki różnorodnych obszarów działalności gospodarczej przedsiębiorstw sprawia, że nieustannie wzrasta ilość danych w formie elektronicznej, co powoduje jednak dynamiczną ekspansję nowych zagrożeń. Ryzyko związane z szerokim zastosowaniem technologii informatycznych w biznesie rośnie wraz ze zwiększaniem się współzależności organizacji od jej klientów, partnerów biznesowych i operacji zlecanych na zewnątrz. Obecny postęp technologiczny generuje zależności, które wywołują wzrost różnorodności, złożoności, nieokreśloności i ilości czynników ryzyka. W efekcie poważnym problemem staje się odpowiednie

zabezpieczenie gromadzonych, przetwarzanych i przesyłanych danych, stąd zagadnienie ich bezpieczeństwa nabiera niezwykłej wagi. Występuje tu swoisty paradoks ery informacji – z jednej strony organizacje dążą do otwartości i szerokiego dostępu do informacji, z drugiej chcą, aby ich systemy informatyczne zachowywały swoją wartość, integralność i ciągłą aktualność.

Zarządzanie ryzykiem IT to proces, który wiąże się z różnymi inwestycjami, a co za tym idzie – kosztami. Są to inwestycje zarówno w sprzęt, oprogramowanie, jak i koszty związane z pracą ekspertów. Przeprowadzenie analizy ryzyka powinno być podstawą do określenia optymalnych ekonomicznie inwestycji w tym obszarze. Efektywność ekonomiczną tych inwestycji można zatem zdefiniować jako dążenie do optymalizacji całkowitych kosztów tego procesu. Celem niniejszego artykułu jest analiza wybranych narzędzi ilościowych ukierunkowanych na ewaluację procesów inwestycyjnych w obszarze zarządzania ryzykiem IT.

Ryzyko w funkcjonowaniu systemów informatycznych

W związku z wszechobecnością występowania ryzyka w życiu społecznym i gospodarczym człowieka, pojęcie to stało się przedmiotem badań wielu dyscyplin naukowych związanych z teorią ekonomii, teorią ubezpieczeń, finansami, prawem, matematyką, statystyką, a samo ryzyko i niepewność nieodłącznie towarzyszą podejmowaniu decyzji gospodarczych.

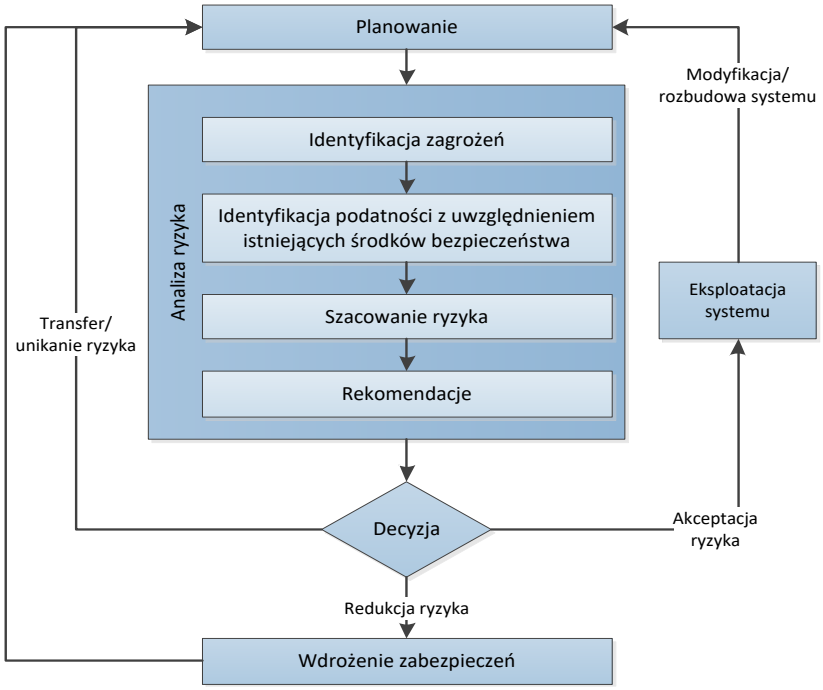
Szczególnym rodzajem ryzyka, którego dotyczą rozważania podejmowane w niniejszym artykule, jest ryzyko informatyczne, określane często w literaturze przedmiotu jako ryzyko IT. Podobnie jak przy definicji samego ryzyka, termin ten nie jest definiowany w sposób jednoznaczny.

Dla potrzeb bezpieczeństwa systemów informatycznych można przytoczyć następującą definicję podaną w normie IEC 61508: „Ryzyko oznacza miarę stopnia zagrożenia dla tajności, integralności i dostępności informacji wyrażoną jako iloczyn prawdopodobieństwa (lub możliwości) wystąpienia sytuacji stwarzającej takie zagrożenie i stopnia szkodliwości jej skutków (strat)" (*IEC 61508,* Part 1-7).

Zarządzanie ryzykiem IT – wybrane zagadnienia

Aktualnie zagadnienia zarządzania ryzykiem nabierają coraz większego znaczenia w działalności organizacji na całym świecie. Dowodem na to są licznie pojawiające się standardy, zalecenia dotyczące tej problematyki, a także stowarzyszenia zajmujące się zarządzaniem ryzykiem w różnych dziedzinach funkcjonowania organizacji, jak również pojawienie się nowej specjalności zawodowej: „menedżera ryzyka" (Chief Risk Officer). Widoczna jest także tendencja objawiająca się tym, iż wiele aspektów działalności współczesnych organizacji postrzeganych jest coraz częściej z perspektywy ryzyka. Ta aktualna „moda" na zarządzanie ryzykiem została poprzedzona podejściem z przełomu XX i XXI wieku, polegającym na patrzeniu na działalność organizacji z punktu widzenia procesów biznesowych (Liderman 2008). To podejście polegające na patrzeniu przez pryzmat ryzyka powoduje także, iż kwestie związane z bezpieczeństwem IT, które

jeszcze niedawno były traktowane niezależnie, rozpatrywane są coraz częściej w kontekście kompleksowego procesu zarządzania ryzykiem. Jest to szczególnie istotne w organizacjach, które w coraz większym stopniu zależne są od nowoczesnych technologii informacyjnych. Zgodnie z normą ISO/IEC TR 13335 zarządzanie ryzykiem jest rozumiane jako proces identyfikacji, kontrolowania i eliminacji lub minimalizowania prawdopodobieństwa zaistnienia niepewnych zdarzeń, które mogą mieć wpływ na zasoby IT (*ISO/IEC TR 13335-1*).



Rysunek 1. Model zarządzania ryzykiem według standardu ISO/IEC TR 13335

Źródło: (ISO/IEC TR 13335-1)

Jak wynika z powyższego modelu, kluczowy element tego procesu stanowi analiza ryzyka, która pozwala na identyfikację zasobów systemu, zlokalizowanie odpowiadających im podatności i zagrożeń oraz oszacowanie prawdopodobieństwa ich wystąpienia i wielkości potencjalnych strat. W ramach różnych koncepcji i standardów stosowane są różne metody postępowania z ryzykiem. W literaturze przedmiotu wymieniane są takie działania, jak unikanie i kontrolowanie ryzyka, redukcja ryzyka, transfer ryzyka oraz akceptacja ryzyka.

Unikanie ryzyka oznacza kierowanie samą działalnością w taki sposób, aby ryzyko związane z tą działalnością było możliwie najmniejsze, lub też możliwe jest wręcz niepodejmowanie określonej działalności (Wołowski 2006).

Kolejną formą reagowania na ryzyko jest jego redukcja, czyli ograniczanie. Ryzyko może być zredukowane poprzez wdrożenie architektury bezpieczeństwa, składającej się z zabezpieczeń, procedur, regulaminów itp. (Szczepankiewicz,

Szczepankiewicz 2006). Redukcja to wprowadzanie zabezpieczeń, mających na celu zwiększenie bezpieczeństwa. Podjęte działania mogą prowadzić do likwidacji ryzyka lub jego ograniczenia do akceptowalnego poziomu.

Transfer ryzyka polega na przeniesieniu konsekwencji wystąpienia szkody lub jej skutków finansowych na inny podmiot (najczęściej ubezpieczenia). Podstawową zasadą transferu jest dokonywanie go na podmiot, który potrafi ryzykiem zarządzać lepiej niż podmiot, który chce się ryzyka pozbyć lub je ograniczyć. Istnieje kilka form transferu ryzyka w organizacjach:

– outsourcing funkcji, które są obarczone szczególnie wysokim ryzykiem,
– ubezpieczenie ryzyka,
– korzystanie z wyspecjalizowanych usług zewnętrznych.

Ostatnia z wymienionych form transferu ryzyka to korzystanie z wyspecjalizowanych usług zewnętrznych. Jest to rozwiązanie uzasadnione w przypadku, gdy usługi zewnętrzne są tańsze, mają wyższą jakość i są lepiej zarządzane, niż miałoby to miejsce, gdyby były wykonywane przez wewnętrzny personel. Usługi takie w przypadku ryzyka IT mogą dotyczyć serwisu sprzętu komputerowego i oprogramowania, dostarczenia i uruchomienia sprzętu zastępczego na wypadek awarii, przechowywania rezerwowych kopii danych, usuwania szkodliwego oprogramowania (Szczepankiewicz, Szczepankiewicz 2006).

Powyższe działania związane z redukcją i transferem ryzyka wiążą się z koniecznymi inwestycjami finansowymi. Przed podjęciem określonych decyzji szczególnie istotna jest analiza efektywności ekonomicznej inwestycji związanych ze zwiększeniem poziomu bezpieczeństwa IT w organizacji.

Metody pomiaru efektywności ekonomicznej inwestycji

Zarządzanie ryzykiem związane jest z szeregiem czynników, wśród których jednym z istotniejszych jest aspekt finansowy. Jest ono ciągłym procesem, który wiąże się z permanentnymi wydatkami, związanymi z działaniami takimi jak:

– planowanie i projektowanie zasad, procedur i adekwatnych zabezpieczeń;
– zakup technicznych, fizycznych oraz programowych mechanizmów zabezpieczających;
– wdrażanie zasad i procedur bezpieczeństwa;
– praca specjalistów;
– opracowanie i wdrożenie programu szkoleniowo-uświadamiającego;
– koszty organizacyjne wydatkowane na nowe struktury i zarządzanie.

Efektywność ekonomiczną inwestycji można określić jako dążenie do optymalizacji całkowitych kosztów związanych z inwestycjami w obszarze zarządzania ryzykiem. Należy pamiętać, iż nie można zredukować ryzyka do zera, ponieważ nie ma niezawodnych rozwiązań. Mamy wtedy do czynienia z tzw. r**yzykiem szczątkowym** (residual risk), które pozostaje po wprowadzeniu mechanizmów zabezpieczających.

Wśród najważniejszych koncepcji oceny efektywności inwestycji w obszarze zarządzania ryzykiem można wymienić m.in. następujące podejścia (Wawrzyniak 2012, s. 254):

– metody statyczne (tradycyjne) oceny efektywności,
– metody dynamiczne analizy przepływów pieniężnych oraz wewnętrznej stopy zwrotu,
– mechanizmy ilościowe bazujące na koncepcji ROI (Return on Investment),
– rozwiązania wyznaczające optymalny (przy danych założeniach) poziom nakładów inwestycyjnych.

Metody statyczne

Metody statyczne nie uwzględniają zmiennej w czasie wartości pieniądza, a rachunek wyznaczany jest w oparciu o dane z pewnego przedziału czasowego. Jedną z podstawowych metod tego typu jest okres zwrotu nakładów inwestycyjnych, określający czas, w ciągu którego wpływy z inwestycji zrównoważą się z nakładami inwestycyjnymi (Wawrzyniak 2012, s. 257):

$$PB = \frac{N}{Z_n + A},$$

gdzie:

N – nakłady inwestycyjne,

Z_n – zysk netto,

A – amortyzacja.

Aby wartość uzyskana w ten sposób mogła być wykorzystana przy podejmowaniu decyzji o inwestycjach w obszarze zarządzania ryzykiem IT, należy wyznaczyć przed tym wartość progową okresu spłaty (jeżeli *PB* jest mniejsze od niej, to projekt może zostać przyjęty do realizacji). Wadą tej metody jest również konieczność uszczegółowienia zysku netto i amortyzacji. Podobne utrudnienia związane są ze stosowaniem kolejnej metody – księgowej stopy zwrotu (Wawrzyniak 2012, s. 258):

$$ARR = \frac{Z_n + O}{N},$$

gdzie *O* to koszty odsetkowe oprocentowanych rozwiązań.

Metody dynamiczne

W analizie ryzyka wykorzystywać można również tradycyjne wskaźniki, stosowane w naukach o finansach, między innymi metody analizy przepływów pieniężnych oraz wewnętrznej stopy zwrotu. Zastosowanie znaleźć mogą dyskontowe metody rachunku ekonomicznego, z których najczęściej wykorzystywane w praktyce to metoda wartości zaktualizowanej netto (Net Present Value – NPV) oraz metoda wewnętrznej stopy zwrotu (Internal Rate of Return – IRR). Wskaźniki te stosowane w tradycyjny sposób nie uwzględniają specyfiki ryzyka IT. Mogą stanowić jednak uzupełnienie i wsparcie innych metodologii ukierunkowanych na problematykę ryzyka IT (Wawrzyniak 2009, s. 107).

Celem metody wartości zaktualizowanej netto jest wyznaczenie aktualnej wartości NPV wpływów i wydatków związanych z projektem (inwestycją związaną z redukcją ryzyka), przy założeniu stałej stopy dyskontowej (procentowej). Metoda ta pozwala określić aktualną wartość nakładów oraz efektów związanych z danym przedsięwzięciem (Dudycz, Dyczkowski 2007, s. 91). Wielkość NPV obliczamy następująco (Flasiński 2007, s. 146):

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

gdzie:
n – kolejny rok *n*-letniego okresu obliczeniowego,
$NCF_t -$ przepływy pieniężne netto w roku *t*, t = 0,…,
$DF_t -$ współczynnik dyskontowy w roku *t*, dla stopy procentowej *r*.
Projekt (inwestycja w mechanizmy redukujące ryzyko) jest opłacalny, jeśli $NPV \geq 0$.

Metoda wewnętrznej stopy zwrotu (Internal Rate of Return – IRR) jest drugą powszechnie stosowaną metodą oceny opłacalności przedsięwzięć, obrazującą, jaka jest stopa rentowności badanych przedsięwzięć. Analizowany projekt będzie opłacalny, jeżeli jego wewnętrzna stopa zwrotu będzie wyższa od najniższej akceptowalnej stopy granicznej. Wskaźnik IRR wyliczamy za pomocą następującego wzoru (Flasiński 2007, s. 149):

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

Zarówno w teorii, jak i w praktyce spotkać można inne dynamiczne modele i metody stosowane w ocenie efektywności inwestycji. Również one mogą stanowić uzupełnienie i wsparcie dla narzędzi typowych dla obszaru ryzyka IT. Są to m.in.: zdyskontowany okres zwrotu (Discounted Payback Period – DPB), wskaźnik zyskowności inwestycji – indeks rentowności PI (Profitability Index) oraz zmodyfikowana wewnętrzna stopa zwrotu MIRR (Modified Internal Rate of Return).

Mechanizmy ilościowe bazujące na koncepcji ROI

Wskaźnikiem, który zyskuje na popularności, jest wskaźnik umożliwiający określenie zwrotu z inwestycji w bezpieczeństwo – ROI (Return on Investment) (Gordon, Loeb 2002a, s. 438-457). Jest on syntetycznym wskaźnikiem efektywności wszelkich projektów, w tym również informatycznych. Można go stosować także w odniesieniu do inwestycji w bezpieczeństwo. W najprostszym ekonomicznym ujęciu zwrot z inwestycji jest różnicą pomiędzy korzyściami będącymi skutkiem inwestycji a poniesionymi nakładami. Podkreślić należy, że w projektach IT poszukiwanie księgowego ROI, wyrażonego w udokumentowanych wartościach, może być bardzo trudne.

Obok wspomnianego wskaźnika ROI w procesach analizy i szacowania ryzyka bardzo przydatny jest również model **ROSI** (Return on Security Investment), bazujący na wspomnianym już wskaźniku ROI, definiowany jako (Wei i in. 2001):

$$ROSI = \frac{ALE_0 - ALE_1}{k},$$

gdzie:

ALE_0 – ALE (opisany wcześniej wskaźnik, Annual Loss Expected) przed zastosowaniem zabezpieczeń,

ALE_1 – ALE po zastosowaniu mechanizmów bezpieczeństwa,

k – koszt wdrożonych mechanizmów bezpieczeństwa.

Wskaźnik ALE obliczany jest według następującego wzoru:

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

gdzie:

$\{O_1, O_2, \ldots, O_n\}$ – zbiór negatywnych skutków zdarzenia,

$I(O_i)$ – wartościowo wyrażona strata wynikająca ze zdarzenia,

F_i – częstotliwość i-tego zdarzenia.

Model ten w literaturze przedstawiany jest czasem także następująco (Sonnenreich 2002):

$$ROSI = \frac{(E \cdot S_m) - S_c}{S_c},$$

gdzie:

E – ryzyko przed wdrożeniem zabezpieczeń,

S_m – procent eliminacji ryzyka przez zabezpieczenie,

S_c – całkowity koszt inwestycji (zabezpieczeń).

Modele ROI i ROSI tylko częściowo charakteryzują inwestycje w bezpieczeństwo IT, z uwagi na to, iż nie biorą pod uwagę potencjalnych zysków intruzów, a zakładanie, iż straty organizacji są równe zyskowi atakującego, jest daleko idącym uproszczeniem. Ponadto koszt ataku nie może być powiązany z kosztem środka zabezpieczającego. W związku z tym, w celu lepszej oceny inwestycji w środki redukcji ryzyka, autorzy proponują stosowanie wskaźnika ROI lub jego pochodnych wraz z miarą, którą określają jako **ROA** (Return-on-Attack), który wyraża się następującym wzorem (Cremonini, Martini 2005):

$$ROA = \frac{GI}{CA_0 + CA_1},$$

gdzie:

GI – oczekiwany zysk intruza z udanego ataku,

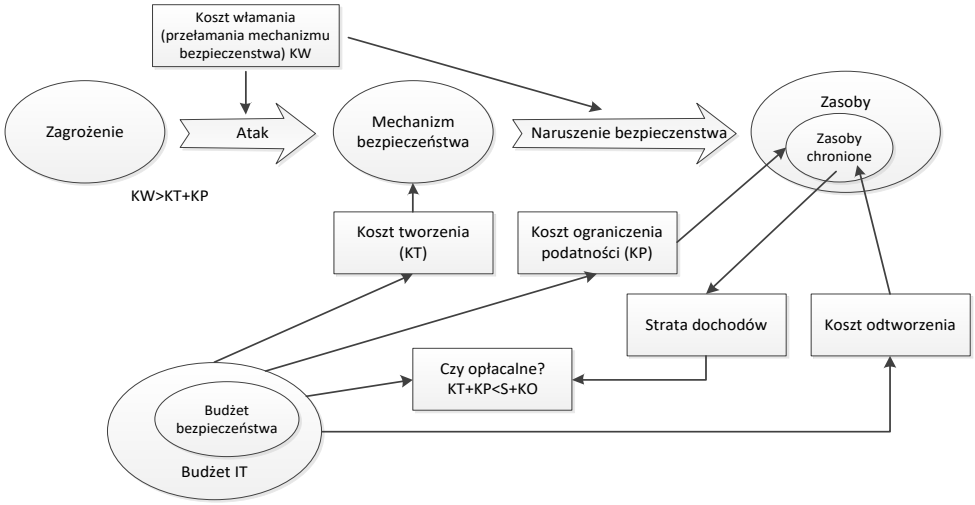
CA_0 – koszt intruza przed wdrożeniem zabezpieczeń,

CA_1 – dodatkowy koszt intruza wynikający z wdrożenia zabezpieczeń.

Kombinacja powyższych podejść może stanowić punkt wyjścia do tworzenia kolejnych metod, tak aby ich przydatność dla oceny efektywności inwestycji była jak największa.

Rozwiązania wyznaczające optymalny poziom nakładów inwestycyjnych

W literaturze przedmiotu pojawiają się modele efektywności inwestycji redukujących ryzyko w organizacji, które mogą zostać uwzględnione i zastosowane w procesie analizy ryzyka. Jednym z nich jest model rentowności wydatków związanych z bezpieczeństwem IT (Mizzi 2005) (*Rysunek 2*).



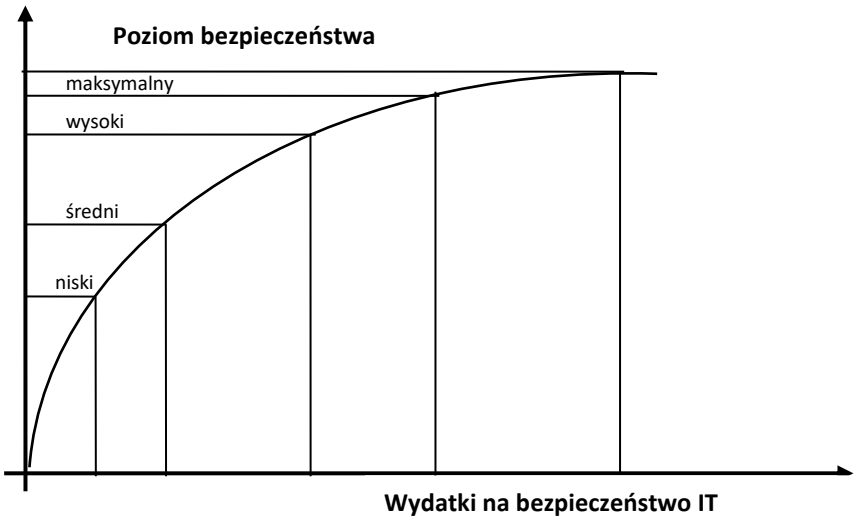
Rysunek 2. Model rentowności wydatków związanych z zarządzaniem ryzykiem

Źródło: (Mizzi 2005; Wawrzyniak 2012)

Zabezpieczenia muszą być adekwatne do wartości dóbr chronionych, zagrożeń oraz gotowości do podjęcia ryzyka. Finanse przeznaczone na zarządzanie ryzykiem muszą być zawsze porównywane z otrzymywanymi z tego tytułu korzyściami. Koszty redukcji i transferu ryzyka IT, w postaci zastosowania dodatkowych środków ochrony, ubezpieczenia od ryzyka, outsourcingu itp., są ekonomicznie uzasadnione tylko wtedy, gdy zmniejszenie strat operacyjnych będzie istotnie mniejsze w porównaniu z kosztem ich wdrożenia i utrzymania.

Zwiększanie środków zabezpieczeń wiąże się oczywiście ze zwiększonymi kosztami ich wprowadzenia, utrzymania i kontrolowania. Związek między osiąganym bezpieczeństwem a poniesionymi wydatkami obrazuje *Rysunek 3*. Zaprezentowana na nim krzywa redukcji ryzyka obrazuje umowny poziom bezpieczeństwa w zależności od poniesionych nakładów.

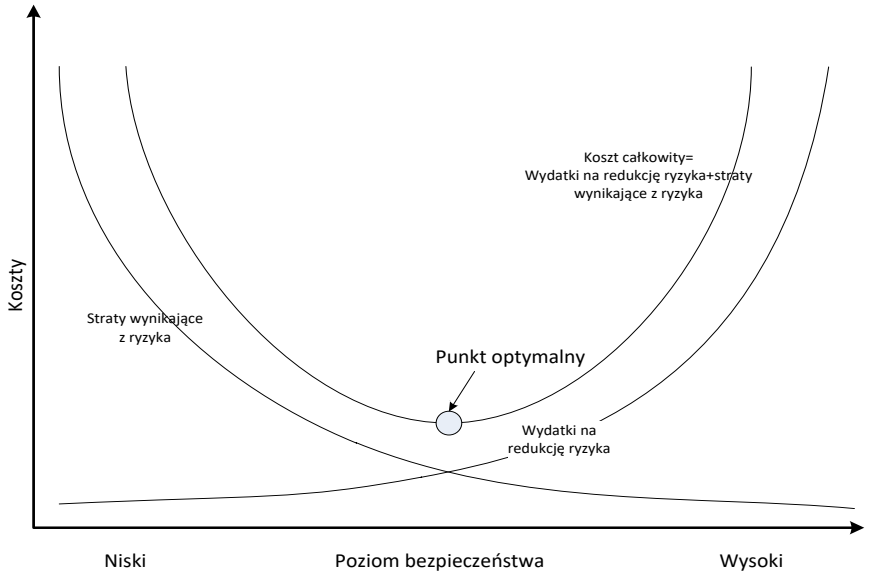
Efektywność ekonomiczną inwestycji w procesie zarządzania ryzykiem informatycznym można określić jako dążenie do minimalizacji sumy ryzyka wyrażonego w jednostce walutowej i kosztu zabezpieczenia (co zostało zobrazowane na *Rysunku 4*).



Rysunek 3. Krzywa redukcji ryzyka – związek między poziomem bezpieczestwa IT a poniesionymi wydatkami

Źródło: Opracowanie własne na podstawie (*IT Grundschutzhandbuch*)

Analizując poniższy wykres, łatwo zauważyć, iż na początku niewielki koszt zabezpieczeń daje znaczne zwiększenie poziomu bezpieczeństwa. Od pewnego momentu zwiększanie inwestycji na zarządzanie ryzykiem w niewielkim stopniu podnosi bezpieczeństwo.



Rysunek 4. Optymalizacja inwestycji na zarządzanie ryzykiem IT

Źródło: (Dynes, Brechbühl, Johnson 2005)

Optymalną ekonomicznie wartość ryzyka można wyznaczyć również, korzystając z krańcowego kosztu zabezpieczenia i krańcowego ryzyka (Kreft 2012). Krańcowy koszt zabezpieczenia MSC (Marginal Safeguard Cost) wyliczamy następująco (Kreft 2012):

$$MSC(i) = SC(i+1) - SC(i),$$

gdzie $SC(i)$ – koszt zabezpieczenia.

Krańcowe ryzyko wyrażone w jednostce walutowej (Marginal Risk Value-Currency) to:

$$MRVC(i) = RVC(i) - RVC(i+1),$$

gdzie $RVC(i)$ – ryzyko wyrażone w jednostce walutowej.

Natomiast optymalnie ekonomicznie inwestycja w obszarze zarządzania ryzykiem informatycznym wyrażona jest następująco:

$$MSC(i) = MRVC(i)$$

Warunek ten jest zgodny z założeniem minimalizacji sumy kosztu zabezpieczenia i ryzyka wyrażonego w jednostce walutowej.

Powyższe zależności ułatwiają podczas procesu analizy ryzyka określenie optymalnych środków finansowych przeznaczonych na dobór mechanizmów bezpieczeństwa w procesie zarządzania ryzykiem.

Podsumowanie

Podsumowując, należy podkreślić, iż przeprowadzenie analizy ryzyka jest podstawą do określenia efektywnego ekonomicznie poziomu inwestycji w obszarze zarządzania ryzykiem IT. Tę efektywność ekonomiczną można zdefiniować jako dążenie do optymalizacji całkowitych kosztów związanych z inwestycjami. W artykule dokonano próby przeglądu wybranych, ważniejszych metod analizy efektywności inwestycyjnej w tym obszarze.

Literatura prezentuje różne teoretyczne modele i współczynniki, których celem jest optymalizacja finansowania działań w obszarze zarządzania ryzykiem, niestety w praktyce korzysta się z nich w ograniczonym wymiarze. Głównym problemem jest identyfikacja rozkładów zmiennych losowych opisujących prawdopodobieństwo realizacji zagrożeń w obszarze bezpieczeństwa. Ponadto w praktyce organizacje niejednokrotnie nie radzą sobie z dokonaniem dokładnego pomiaru efektywności i kosztów ich działalności w zakresie bezpieczeństwa. Powodem tego jest to, że inwestycje w tym obszarze nie mają bezpośredniego wpływu na poziom przychodów, za to minimalizują poziom kosztów, które mogą powstać w wyniku incydentów. Dlatego też przedsiębiorcy często mają problem w podejmowaniu decyzji o wielkości inwestycji w obszarze bezpieczeństwa IT. Dodatkowym utrudnieniem w kalkulacji takich inwestycji może być także fakt, iż wiele organizacji nie analizuje kosztów incydentów, a co za tym idzie – nie jest w stanie stwierdzić, jak efektywne mogą być ich przyszłe inwestycje. Potwierdzają to przykładowo badania

przeprowadzone przez PwC – *Badanie przestępczości gospodarczej Polska 201*5 (PwC 2014), w których aż 43% firm zadeklarowało brak wiedzy w zakresie strat i kosztów związanych z incydentami, a według badania przeprowadzonego przez firmę EY *Światowe Badanie Bezpieczeństwa Informacji 2015* (EY Poland 2015) 37% organizacji uważa, że nie posiada aktualnych danych o zagrożeniach w cyber-przestrzeni (4itSecurity 2016).

Literatura

1. 4itSecurity (2016), *Zwrot z inwestycji w bezpieczeństwo*, http://4itsecurity.pl/blog/1-Bezpiecze%C5%84stwo-informacji/26-zwrot-z-inwestycji-w-bezpieczenstwo.html (dostęp: 23.06.2016).
2. Cremonini M., Martini P. (2005), *Evaluating Information Security Investments from Attackers Perspective: The Return-On-Attack (ROA)*, Proceedings of Fourth Workshop on the Economics of Information Security, University of Cambridge, http://infosecon.net/workshop/pdf/23.pdf (dostęp: 23.06.2016).
3. Dudycz H., Dyczkowski M. (2007), *Efektywność przedsięwzięć informatycznych. Podstawy metodyczne pomiaru i przykłady zastosowań*, Wydawnictwo Akademii Ekonomicznej we Wrocławiu, Wrocław.
4. Dynes S., Brechbühl H., Johnson M.E. (2005), *Information Security in the Extended Enterprise: Some Initial Results From A Field Study of an Industrial Firm*, Glassmeyer/McNamee Center for Digital Strategies Tuck School of Business at Dartmout, 13.04.2005, http://www.tuck.dartmouth.edu/digital/assets/images/InfoSecurity%20(1).pdf (dostęp: 23.06.2016).
5. EY Poland (2015), *Światowe Badanie Bezpieczeństwa Informacji EY 2015*, http://www.ey.com/PL/pl/Services/Advisory/ey-swiatowe-badanie-bezpieczenstwa-informacji-2015 (dostęp: 23.06.2016).
6. Flasiński M. (2007), *Zarządzanie projektami informatycznymi*, Wydawnictwo Naukowe PWN, Warszawa.
7. Gordon L.A., Loeb M.P. (2002), *Return on Information Security Investments: Myths vs. Realities*, "Strategic Finance", Vol. 84(5).
8. Gordon L.A., Loeb M.P. (2002a), *The Economics of Information Security Investment*, ACM Transactions on Information and System Security, November 2002.
9. *IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*, The Institution of Electrical Engineers, Part 1 to 7.
10. *ISO/IEC TR 13335-1 Information Technology – Security Techniques – Guidelines for the management of IT Security − Part 1: Concepts and models of IT Security.*
11. *IT Grundschutzhandbuch (IT Baseline Protection Manual)*, Bundesamt für Sicherheit in der Informationstechnik, Bonn, DIN-Berlin, 2000-2003.
12. Kreft K. (2012), *Zarządzanie ryzykiem IT*, „Studia i Materiały Instytutu Transportu i Handlu Morskiego", nr 9.
13. Liderman K. (2008), *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Wydawnictwo Naukowe PWN, Warszawa.
14. Mizzi A. (2005), *Return on Information Security Investment. Are You Spending Enough? Are You Spending Too Much?*, http://www.infosecwriters.com/text.../pdf/ROISI.pdf (dostęp: 23.06.2016).
15. PwC (2014), *Zarządzanie ryzykiem w cyberprzestrzeni. Kluczowe obserwacje z wyników ankiety „Globalny stan bezpieczeństwa informacji 2015" (The Global State of Information Security Survey 2015)*, https://www.pwc.pl/pl/publikacje/assets/gsiss_2015_polska.pdf (dostęp: 23.06.2016).
16. Sonnenreich W. (2002), *Return on Security Investment (ROSI): A Practical Quantitative Model*, A Summary Of Research And Development Conducted at SageSecure.

17. Szczepankiewicz E.I., Szczepankiewicz P. (2006), *Analiza ryzyka w środowisku informatycznym do celów zarządzania ryzykiem operacyjnym. Część 3: Strategie postępowania z ryzykiem operacyjnym*, „Monitor Rachunkowości i Finansów", nr 8.
18. Wawrzyniak D. (2009), *Zarządzanie ryzykiem informatycznym – wybrane aspekty ekonomiczne*, [w:] Niedźwiedziński M., Lange-Sadzińska K. (red.), *Wybrane problemy budowy aplikacji dla gospodarki elektronicznej*, Wydawnictwo Marian Niedźwiedziński - Consulting, Łódź.
19. Wawrzyniak D. (2012), *Ryzyko informatyczne w działalności bankowej*, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław.
20. Wei H., Frinke D., Carter O., Ritter C. (2001), *Cost-Benefit Analysis for Network Intrusion Detection Systems*, Proceedings of the 28-th Annual Computer Security Conference, Cupertino.
21. Wołowski F. (2006), *Zarządzanie ryzykiem systemów informacyjnych*, [w:] Niemiec A., Nowak J.S., Grabara J.K. (red.), *Bezpieczeństwo systemów informatycznych*, PTI – Oddział Górnośląski, Katowice.

SELECTED METHODS OF MEASURING ECONOMIC EFFECTIVENESS OF IT RISK MANAGEMENT INVESTMENTS IN THE ORGANIZATION

Abstract: IT risk management is prevention against threats, its main goal is to prevent critical situations by seeing threat factors, monitoring the typical symptoms of these factors activation and to prevent their interaction with the system of the organization or its environment. It is necessary to implement appropriate tools and solutions which are associated with costs. Risk management is a continuous process that involves the permanent expenses associated with planning and designing of policies, procedures and adequate countermeasures, the purchase of hardware and software, implementation of adequate policies for security, monitoring, auditing and evaluation of security, additional work of experts etc. Therefore, analysis of the efficiency of IT risk management investments is becoming an issue of extraordinary importance for the practice of business. The article presents some models and methods that can be applied in assessing the efficiency of investments in the area of IT risk management.

Keywords: information system security, IT risk management, investment effectiveness, ROI, NPV, IRR