

Oryginalny artykuł naukowy
Original Article

Data wpływu/Received: 7.08.2017

Data recenzji/Accepted: 25.09.2017/25.09.2017

Data publikacji/Published: 28.12.2017.

Źródła finansowania publikacji: środki własne Autora

Authors' Contribution:

(A) Study Design (projekt badania)

(B) Data Collection (zbieranie danych)

(C) Statistical Analysis (analiza statystyczna)

(D) Data Interpretation (interpretacja danych)

(E) Manuscript Preparation (redagowanie opracowania)

(F) Literature Search (badania literaturowe)

DOI: 10.5604/01.3001.0010.8286

dr Ewa Wierzbicka ^{A B C D E F}

Szkoła Główna Handlowa w Warszawie

Instytut Zarządzania Wartością

ROLA UBEZPIECZEŃ W ZARZĄDZANIU RYZYKIEM PRZEDSIĘBIORSTWA

THE ROLE OF INSURANCE IN ENTERPRISE RISK MANAGEMENT

Streszczenie: W ostatnich kilkunastu latach zarówno w praktyce gospodarczej krajów OECD, jak i w towarzyszącej rozwojowi gospodarek myśli teoretycznej następuje istotny przełom w podejściu do ubezpieczeń przedsiębiorstw. Ubezpieczenia w zarządzaniu przedsiębiorstwem przestają być traktowane jedynie jako kategoria finansów i rachunkowości przedsiębiorstwa, co wynika z tradycyjnego rozumienia tego zagadnienia. Współcześnie tego typu podejście jest niewystarczające do określenia roli ubezpieczeń w zarządzaniu ry-

zykiem przedsiębiorstwa. W tradycyjnym podejściu do ubezpieczeń ocena ich znaczenia skupiona jest na ewidencji i analizie kosztów transferu ryzyka. W konsekwencji w praktyce wielu przedsiębiorstw i instytucji najważniejsze jest ujęcie krótkookresowe w zarządzaniu kosztem ubezpieczeń i analizie stopnia pokrycia ryzyka, przede wszystkim majątkowego, odpowiednimi ubezpieczeniami, w relacji do kosztu ochrony ubezpieczeniowej. Celem artykułu jest wyjaśnienie, jak asekuracja przyczynia się do zwiększenia bezpieczeństwa funkcjonowania przedsiębiorstwa i obrotu gospodarczego, zwłaszcza w sytuacji wzrostu cyber-ryzyka. W związku z tym stawiana jest teza, że w turbulentnym otoczeniu przedsiębiorstwa w globalnej gospodarce, przy rosnącej zmienności otoczenia i pod presją zmian wynikających z synergii zmian technologicznych, rośnie znaczenie ubezpieczeń w zarządzaniu ryzykiem, zwłaszcza ryzykiem regulacyjnym i ryzykiem technologicznym.

Słowa kluczowe: ubezpieczenie, zarządzanie ryzykiem, ryzyko regulacyjne, ryzyko technologiczne, zarządzanie wartością

Abstract: In the last several years, both in the economic practice of the OECD countries and in the development of theoretical thinking, there has been a significant breakthrough in the approach to corporate insurance. Insurance in business management is no longer considered only as a category of finance and accounting for an enterprises, which results from the traditional understanding of this issue. Today's approach is insufficient to define the role of business risk management. In the traditional approach to insurance, its importance is focused on the recording and analysis of the cost of risk transfer. As a consequence, in practise, many companies and institutions implement the short-term approach to managing the cost of insurance and analyzing the degree of risk coverage, primarily property, relative insurance, relative to the cost of insurance cover. The purpose of this article is to explain how insurance contributes to increasing business security and business turnover, especially in the context of cyberbullying. It is therefore hypothesized that in the turbulent environmental variability and under pressure of changes resulting from technological synergies, the importance of insurance in risk management, especially regulatory risk and technological risk, is growing.

Keywords: insurance, risk management, regulatory risk, technological risk, value management

Wstęp

Współcześnie ubezpieczenia są nie tylko tradycyjnie ważnym elementem analizy funkcjonowania przedsiębiorstwa i kosztów transferu ryzyka. W coraz większym zakresie są wykorzystywane jako rosnący w znaczenie komponent portfela niezbędnych instrumentów zarządzania ryzykiem przedsiębiorstwa, nie tylko w aspekcie mikroekonomicznym. Z punktu widzenia makroekonomicznego szersze korzystanie przez przedsiębiorstwa z ubezpieczeń w zarządzaniu różnego rodzaju ryzykiem poprawia bezpieczeństwo sfery realnej, a także bezpieczeństwo sektora finansowego. Wpływa więc na zwiększanie bezpieczeństwa obrotu gospodarczego, a zarazem jest czynnikiem sprzyjającym podnoszeniu nie tylko bezpieczeństwa, ale i efektywności działalności gospodarczej, a w konsekwencji sprzyja wzrostowi gospodarczemu.

Kolejnym elementem współczesnego podejścia do roli ubezpieczeń w zarządzaniu przedsiębiorstwem jest rosnące znaczenie ubezpieczeń nie tylko w zarządzaniu przedsiębiorstwem w zakresie ograniczania skutków materializacji ryzyka i podejmowania działań prewencyjnych, ale także w zarządzaniu wartością przedsiębiorstwa. Ubezpieczenia pomagają wieloaspektowo w tworzeniu i ochronie wartości, a także efektywnie użyte sprzyjają kształtowaniu jego przyszłej wartości w obliczu wyzwań wynikających z turbulencji otoczenia rynkowego i systemowego w kraju i za granicą, a także asekurują od strony finansowej skutki różnego rodzaju ryzyka w realizowanych kontraktach i podejmowanych działaniach rozwojowych.

Każde przedsiębiorstwo, bez względu na jego wielkość, formę organizacyjno-prawną oraz branżę, w której działa, narażone jest na różnego rodzaju ryzyko. Najmniejszą tolerancję na ryzyko zwykle wykazują – co potwierdzają badania sytuacji firm w Polsce – przedsiębiorstwa rozpoczynające działalność, a największą w większości przypadków przedsiębiorstwa najdłużej funkcjonujące na rynku. W działalności gospodarczej przyjmuje się, że ryzyko oznacza możliwość wystąpienia sytuacji niepożądaney, a jego materializacja powoduje, że cele przedsiębiorstwa nie zostają zrealizowane lub też uzyskane wyniki są odmienne od oczekiwanych.

Ryzyko dotyczy różnych sfer przedsiębiorstwa, w tym: mienia, finansów, zasobów ludzkich, a także wartości niematerialnych i prawnych. Stąd też ważne jest wielopłaszczyznowe postrzeganie roli ubezpieczeń w zarządzaniu przedsiębiorstwem. Ryzyko przedsiębiorstwa związane jest zarówno z otoczeniem rynkowym (krajowym i zagranicznym) przedsiębiorstwa, z jego relacjami z innymi podmiotami gospodarczymi, konkurentami, dostawcami i odbiorcami, jak również z otoczeniem instytucjonalnym, które tworzy warunki systemowe dla funkcjonowania podmiotów gospodarczych. Ryzyko wynika też z bieżących i przyszłych decyzji właścicieli i zarządzających przedsiębiorstwem, a także z błędów lub sprzeniewierzenia ze strony pracowników. Współcześnie rośnie też zagrożenie zewnętrzne związane z aktywnością firmy w Internecie, jak też ryzyko ataków hakerskich (cybersecurity).

Umiejętność zarządzania ryzykiem wpływa na pozycję konkurencyjną przedsiębiorstwa i zwiększa jego elastyczność w biznesie. Ubezpieczenie jako forma transferu ryzyka na wyspecjalizowaną instytucję finansową, jaką jest ubezpieczyciel, staje się trwałym elementem procesu zarządzania ryzykiem. Wybór ochrony ubezpieczeniowej powinien być adekwatny do zagrożeń zidentyfikowanych w danym przedsiębiorstwie.

1. Ryzyko przedsiębiorstwa

Ryzyko jest obiektywną prawidłowością i dotyczy realnych zjawisk gospodarczych, jak też w sferze finansowej. Towarzyszy każdej działalności gospodarczej, bo wynika z niepewności przyszłych skutków decyzji zarówno finansowych, operacyj-

nych, jak i inwestycyjnych oraz z braku możliwości przewidzenia wszystkich warunków gospodarowania czy też kierunku rozwoju określonych zjawisk i procesów¹. Ryzyko w działalności gospodarczej jest „silnie zdeterminowane rodzajem prowadzonej działalności, celami przedsiębiorstwa, hierarchią wartości w firmie i stopniem uzależnienia zewnętrznego”². Ryzyko oznacza możliwość wystąpienia zdarzeń niezależnych od działającego podmiotu, których nie może on dokładnie przewidzieć i którym nie może w pełni zapobiec³. Każda decyzja gospodarcza obciążona jest większym lub mniejszym ryzykiem. Ryzyko istnieje z powodu prawdopodobieństwa zajścia zdarzenia w przyszłości, które ma swoje finansowe skutki. Zachodzące procesy czy pojedyncze czynniki w bliższym i dalszym otoczeniu przedsiębiorstwa lub wewnątrz organizacji mogą mieć bezpośredni lub pośredni wpływ na wyniki przedsiębiorstwa.

Ryzyko przedsiębiorstw dotyczy zdarzeń i skutków przyszłych. W zależności od specyfiki firmy obszarem największych zagrożeń może być: struktura własnościowa przedsiębiorstwa, struktura organizacyjna, majątek, zasoby ludzkie, produkcja, magazynowanie, finanse, transport, dystrybucja, wykorzystywane systemy informatyczne itd. Każde przedsiębiorstwo, działając w zmiennym i niepewnym, czyli turbulentnym otoczeniu, jest narażone na wystąpienie różnego rodzaju ryzyka. Konieczność przystosowania się do zmian w otoczeniu stwarza potrzebę wykorzystywania skutecznych metod zarządzania, w tym także zarządzania ryzykiem⁴.

Wystąpienie ryzyka może być wywołane czynnikami zewnętrznymi lub wewnętrznymi przedsiębiorstwa. Ryzyko zewnętrzne to: zmiany koniunktury gospodarczej, zmiany w polityce gospodarczej państwa, polityka banku centralnego, zmiany w prawie, zmiany w otoczeniu bliższym przedsiębiorstwa, w preferencjach konsumentów i popycie na produkowane towary lub oferowane usługi, działania ze strony konkurentów. W zasadzie wymienione czynniki ryzyka nie podlegają kontroli ze strony przedsiębiorstwa. Natomiast ryzyko wewnętrzne może być przez przedsiębiorstwo w znacznym stopniu kontrolowane. Do wewnętrznych czynników ryzyka można zaliczyć: błędy i brak kompetencji osób zarządzających, awarie maszyn i urządzeń, utrata utalentowanych pracowników, błędy pracowników, nieuczciwość czy sprzeniewierzenie lub kradzież ze strony pracowników. Celem zarządzania ryzykiem jest kreowanie wartości dodanej przedsiębiorstwa, realizacja celów przedsiębiorstwa i podejmowanie działań zmierzających do akceptowanego poziomu ryzyka⁵.

¹ R. Waściński, P. Krasieński, *Ryzyko w działalności przedsiębiorstwa – elementy systematyki i identyfikacji*, [w:] J. Monkiewicz, L. Gąsioriewicz (red.), *Zarządzanie ryzykiem działalności gospodarczej*, C.H. Beck, Warszawa 2010 s. 34.

² W. Ronka-Chmielowiec, *Wykorzystanie ubezpieczeń do zarządzania ryzykiem w przedsiębiorstwie*, [w:] J. Monkiewicz, L. Gąsioriewicz (red.), *Zarządzanie ryzykiem...*, s. 47.

³ T.T. Kaczmarek, M. Zarzycki, *Poradnik eksportera*, Wyd. Branta, Bydgoszcz – Warszawa 2005, s. 171.

⁴ E. Wierzbicka, *Wykorzystanie ubezpieczeń w zarządzaniu przedsiębiorstwem*, [w:] E. Wierzbicka (red.), *Ubezpieczenia w zarządzaniu ryzykiem przedsiębiorstwa*, Wyd. SGH, Warszawa 2016, s. 10.

⁵ K. Jajuga, *Teoretyczne podstawy zarządzania ryzykiem*, PWN, Warszawa 2005, s. 15.

Ryzyko przyjmowane do ubezpieczenia przez zakłady ubezpieczeń musi dotyczyć zdarzeń przyszłych, które mają charakter losowy i powinny być niezależne od woli ubezpieczającego. Ryzyko to musi się dać oszacować, a także łączyć się z innymi rodzajami ryzyka o podobnych cechach⁶.

Ubezpieczenie umożliwia transfer ryzyka na ubezpieczyciela i jego dyspersję, a więc rozproszenie ryzyka na wspólnotę ubezpieczonych, którym dane ryzyko zagraża. Przez ubezpieczenie następuje rozłożenie ciężaru pokrycia skutków zdarzeń losowych na wiele podmiotów gospodarczych, którym podobne zdarzenia zagrażają. Transfer ryzyka realizowany jest przez świadome porozumienie między ubezpieczycielem, który przejmuje na siebie odpowiedzialność w sytuacji materializacji ryzyka, a ubezpieczającym, który transferuje ryzyko w zamian za składkę, która jest ceną nabycia ochrony ubezpieczeniowej. W sytuacji wystąpienia zdarzenia objętego polisą przedsiębiorstwo ma możliwość uzyskania kompensaty szkód przez wypłatę przez ubezpieczyciela odszkodowania lub świadczenia⁷. Ustalona w polisie suma ubezpieczenia jest ważna z punktu widzenia realności ochrony ubezpieczeniowej, ponieważ jest górną granicą odpowiedzialności ubezpieczyciela. Wypłata odszkodowania lub świadczenia powinna umożliwić naprawienie szkody.

2. Kluczowe rodzaje ryzyka przedsiębiorstw w Polsce

Jednym z ważnych źródeł wiedzy na temat głównych rodzajów ryzyka, których doświadczają i których obawiają się zarządzający przedsiębiorstwami w Polsce, jest publikowany co dwa lata raport pt. *Zarządzanie ryzykiem i ubezpieczeniami w firmach w Polsce*, sporządzany na podstawie badań dokonywanych przez firmę brokerską Aon Polska. Raport bazuje na przeprowadzonym co dwa lata globalnym badaniu „Aon Global Risk Management Survey”⁸. W tabeli 1 przedstawiono najważniejsze rodzaje ryzyka wskazane w badaniu przedsiębiorstw w Polsce.

⁶ M. Fedor, *Bezwzględne kryterium ubezpieczalności*, „Gazeta Ubezpieczeniowa” z 3 sierpnia 2004 r.

⁷ B. Hadyniak *Ryzyko w przedsiębiorstwie*, [w:] B. Hadyniak, J. Monkiewicz (red.), *Ubezpieczenia w zarządzaniu ryzykiem przedsiębiorstwa*, tom 1: Podstawy, Poltext, Warszawa 2010, s. 47.

⁸ R. Ziomko, *Raport Aon Polska IV edycja. Zarządzanie ryzykiem i ubezpieczeniami w firmach w Polsce*, Warszawa 2016. W badaniu przeprowadzonym przez Aon Polska wzięło udział 168 respondentów zajmujących się w swojej praktyce zawodowej zarządzaniem ryzykiem i ubezpieczeniami w edycji globalnej 1418 z ponad 30 branż, przedstawicieli firm i instytucji z 60 krajów świata.

Tabela 1. Ranking ryzyka, kluczowe 10 rodzajów ryzyka w polskiej edycji badania Aon z lat 2009–2015

Table 1. Risk ranking, key 10 risks in the Polish edition of the Aon survey from 2009 to 2015

nr	2015	2013	2011	2009
1.	Wzrost konkurencji	Spowolnienie gospodarcze	Wahania kursów walut	Spowolnienie gospodarcze
2.	Spowolnienie gospodarcze	Wzrost konkurencji	Wzrost konkurencji	Wahania kursów walut
3.	Zmiany regulacji prawnych	Przepływy pieniężne/ ryzyko płynności	Spowolnienie gospodarcze	Wahania cen surowców
4.	Utrata reputacji	Kontrahenci/ należności handlowe	Wahania cen surowców	Zmiany regulacji prawnych
5.	Zmiany cen towarów	Zmiany regulacji prawnych	Kontrahenci/ należności handlowe	Wzrost konkurencji
6.	Przerwa w prowadzonej działalności	Wahania kursów walut	Zmiany regulacji prawnych	Kontrahenci/ należności handlowe
7.	Należności handlowe/ płatności kontrahentów	Wahania cen surowców	Przerwa w prowadzonej działalności / w łańcuchu dostaw	Przepływy pieniężne/ ryzyko płynności
8.	Zmienność kursów walut	Awaria technologiczna	Awaria technologiczna	Utrata danych
9.	Zniszczenie, uszkodzenie mienia	Nieuczciwość pracownicza	Utrata reputacji	Przerwa w prowadzonej działalności / w łańcuchu dostaw
10.	Awaria systemów informatycznych	Odpowiedzialność cywilna / roszczenia	Odpowiedzialność cywilna / roszczenia	Utrata reputacji

Źródło: Zarządzanie ryzykiem i ubezpieczeniami w firmach w Polsce, Raport Aon Polska 2013-2014, Warszawa 2013, Aon Risk Solutions; R. Ziomko, *Raport Aon Polska IV edycja. Zarządzanie ryzykiem i ubezpieczeniami w firmach w Polsce*, Warszawa 2016.

Jak wynika z rezultatów badań zawartych w tabeli 1, w 2015 r. wzrost konkurencji, osłabienie tempa wzrostu gospodarczego oraz zmiany regulacji prawnych stanowiły główne zagrożenia dla działalności polskich przedsiębiorstw.

Według badań Aon dokonanych w Polsce do kolejnych rodzajów ryzyka drugiej dziesiątki zaliczono⁹:

- przepływy pieniężne / ryzyko płynności,
- odpowiedzialność cywilną,

⁹ R. Ziomko, *Raport Aon Polska IV edycja. Zarządzanie ryzykiem i ubezpieczeniami w firmach w Polsce...*

- zakłócenia w procesie dystrybucji / łańcuchu dostaw,
- odpowiedzialność władz spółki
- dostępność kapitału, ryzyko kredytowe,
- brak odpowiedniej kadry na rynku,
- kradzież i przestępczość pracownicza,
- kradzież i katastrofy naturalne,
- niezdolność do przyciągania i zatrzymania talentów,
- odpowiedzialność społeczna.

Wymieniona lista rodzajów ryzyka wskazanych przez respondentów w badaniu Aon Polska nie pokrywa się z rodzajami ryzyka wskazanymi w globalnym badaniu na poszczególnych kontynentach, według rankingu największego ryzyka. W globalnym badaniu w 2015 r. dla przedsiębiorstw w Europie najgroźniejsze były następujące ryzyka, w kolejności ich znaczenia dla respondentów:

- 1) spowolnienie gospodarcze,
- 2) wzrost konkurencji,
- 3) utrata reputacji,
- 4) zmiany regulacji prawnych,
- 5) przerwa w prowadzeniu działalności,
- 6) niezdolność do opracowania i wdrażania innowacji,
- 7) odpowiedzialność cywilna,
- 8) zmiany cen towarów,
- 9) niezdolność do przyciągnięcia i zatrzymania talentów,
- 10) przepływy pieniężne / ryzyko płynności.

Nie wszystkie z wymienionych rodzajów ryzyka można ubezpieczyć. Jest wiele rodzajów ryzyka, które zostały wymienione w rankingu ryzyka, ale nie dają się ubezpieczyć lub są tylko częściowo ubezpieczalne. Ubezpieczać można m.in. ryzyko majątkowe i finansowe przedsiębiorstwa, ryzyko odpowiedzialności cywilnej, w tym OC władz spółki, a także ryzyko osobowe i zdrowotne jego pracowników. Wysokość składki jest uzależniona od rodzaju ryzyka, a tzw. wielkość ryzyka od prawdopodobieństwa zajścia zdarzenia oraz wartości potencjalnej straty¹⁰.

Nie można także ubezpieczyć się przed bankructwem. Do grupy ryzyka bezwzględnie nieubezpieczanego należą takie, których nie można ubezpieczyć z tytułu prawa. Ponadto nie można ubezpieczyć zdarzeń, które już nastąpiły lub zostały umyślnie spowodowane przez ubezpieczającego lub wystąpiły z powodu rażącego niedbalstwa ubezpieczonego. W ubezpieczeniach majątkowych zazwyczaj wyłączone są działania i szkody wywołane wojną, zamieszkami, trzęsieniem ziemi, a także atakiem terrorystycznym. Wyłączenia odpowiedzialności ubezpieczyciela dotyczą szkód spowodowanych konfiskatą, zawłaszczeniem, nacjonalizacją, które wystąpiły

¹⁰ E Wierzbicka, *Ubezpieczenia w zarządzaniu ryzykiem przedsiębiorstwa...*, s. 29.

na mocy aktu prawnego wydanego przez władze państwowe, lokalne lub celne. Nieubezpieczalnych jest wiele rodzajów ryzyka wymienionych w rankingu Aon, w tym zagrożenia takie, jak: wzrost konkurencji, wahania koniunktury gospodarczej, dostępność kapitału, a także brak odpowiednich kadr na rynku.

Niektóre rodzaje ryzyka są częściowo ubezpieczalne, w tym: zakłócenia w procesie dystrybucji lub łańcuchu dostaw, utrata własności intelektualnej lub utrata wrażliwych danych, a także utrata reputacji.

Do rodzajów ryzyka, które można i należy ubezpieczyć, a które znalazły się na liście 10 największych zagrożeń, należą: przerwa w działalności gospodarczej (ubezpieczenie utraty zysku BI *business interraption*, które zazwyczaj nie jest samodzielnym ubezpieczeniem, ale najczęściej jest powiązane z ubezpieczeniem mienia od ognia i innych zdarzeń losowych), ryzyko nieotrzymania należności handlowych i płatności od kontrahentów (ubezpieczenie należności handlowych, w tym ubezpieczenie kredytu kupieckiego, a także ubezpieczenie factoringu), kradzież, zniszczenie, uszkodzenie mienia, sprzeniewierzenie ze strony pracowników (ubezpieczenie mienia od ryzyka kradzieży z włamaniem, rabunku, celowego uszkodzenia lub zniszczenia przez osoby trzecie¹¹), odpowiedzialność cywilna prowadzonej działalności, w tym OC władz spółki (chodzi o odpowiedzialność cywilną deliktową i kontraktową, ubezpieczenie D&O – Directors & Officers).

3. Przestępczość elektroniczna i cyberryzyko

Nowe technologie i rozwój IT, a zwłaszcza rozwój nowych technologii w zakresie przetwarzania i przechowywania danych w chmurze (*cloud computing*), urządzeń mobilne, a także przetwarzanie i analiza wielkiej ilości danych (*big data*), zmieniają zasadniczo globalną gospodarkę i przedsiębiorstwa. Jednocześnie przestępczość elektroniczna staje się jednym z narastających zagrożeń przedsiębiorstw, a nie tylko instytucji finansowych. Różne rodzaje cyberryzyka, a więc i cybersecurity wraz ze wzrostem wykorzystania technologii informatycznych i upowszechnieniem Internetu stają się powszechnymi wyzwaniem XXI w.

Zgodnie z definicją Europejskiej Agencji ds. Bezpieczeństwa Informatycznego (ENISA) cyberprzestępstwo obejmuje różne działania, które bezpośrednio wpływają zarówno na pojedyncze osoby (np. kradzież tożsamości, kradzież danych osobowych), jak i na przedsiębiorstwa (na przykład kradzież własności intelektualnej)¹².

¹¹ Majątek rzeczowy przedsiębiorstwa jest narażony na zniszczenia lub utratę mienia w wyniku zjawisk o charakterze żywiołów takich jak ogień, powódź, huragan, deszcz nawalny itp., te rodzaje ryzyka pokrywa ubezpieczenie od ognia i innych żywiołów FLEXA, a także ubezpieczenie od wszystkich rodzajów ryzyk All risks.

¹² ENISA *Incentives and barriers of the cyber insurance market in Europe*, Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji, www.enisa.europa.eu, za: G. Strupczewski, *Zagrożenia cybernetycznej instytucji finansowych*, „Rozprawy Ubezpieczeniowe” 2017, nr 24(2).

Według badań Global Aon zagrożenie różnego rodzaju cyberatakami, związane z przestępczością elektroniczną, nasila się i znalazło się już w pierwszej dziesiątce globalnego rankingu ryzyka. W konsekwencji cybersecurity stało się jednym z kluczowych zagadnień biznesowych najwyższej rangi, którym zajmują się kadry zarządzające przedsiębiorstwami¹³.

Wyniki badania EY w 2016 r. pt. *Droga do cyberbezpieczeństwa*, w którym wzięło udział 1735 firm z całego świata, którego respondentami byli członkowie zarządów oraz kadra zarządzająca najwyższego szczebla, wskazują, że przedsiębiorstwa nieskutecznie przygotowują się do ataków hakerskich, bo cyberprzestępcy wciąż doskonałą i opracowują nowe sposoby ataków¹⁴.

Tabela 2. Kto/co jest najczęściej przyczyną incydentów cyberataków

Table 2. Who / What is most often the cause of cyber-attacks incident

Przyczyny incydentów	Procent wskazań respondentów
Pracownicy	64
Przestępcy komputerowi	57
Wadliwe, przestarzałe oprogramowanie	39
Wadliwe, przestarzałe procedury	32
Klienci	5
Kontrahenci *	4

*Do kontrahentów zaliczono podwykonawców i współpracujące firmy

Źródło: opracowanie własne na podstawie EY *Cyberbezpieczeństwo firm*, 2016.

Zdecydowana większość respondentów badania EY *Cyberbezpieczeństwo firm*¹⁵, które w Polsce realizowane było na próbie 500 pracowników, ocenia, że najsłabszym ogniwem w cyberbezpieczeństwie jest człowiek (por. tabela 2), czyli pracownicy organizacji. Przyczynia się do tego np. trywialność haseł i nieprzestrzeganie zasad ich tworzenia, lekceważenie zaleceń cyberbezpieczeństwa i procedur szyfrowania danych, otwieranie maili phishingowych, a przy tym wiele ataków hakerskich odbywa się przez konta administratorów sieci.

W Polsce – jak wskazują badania podane w polskiej edycji ostatniego raportu Aon – mimo że ważne jest zarówno zidentyfikowanie, monitorowanie, jak i za-

¹³ Raport Aon *Zarządzanie ryzykiem i ubezpieczeniami w firmach...*

¹⁴ *Cyberbezpieczeństwo firm – najbardziej szkodzą pracownicy*, Egospodarka.pl <http://www.egospodarka.pl/139426,Cyberbezpieczenstwo-firm-najbardziej-szkodza-pracownicy,1,12,1.html> [dostęp: 30.07.2017].

¹⁵ Autorami badania „Cyberbezpieczeństwo firm” są konsultanci CubeResearch, EY oraz Chubb. Badanie składało się z dwóch części – badania zasadniczego, gdzie na zadane pytania odpowiadały osoby na co dzień zajmujące się problematyką cyberbezpieczeństwa firm, oraz badania dodatkowego zrealizowanego na pracownikach firm. Badanie zasadnicze zrealizowano w listopadzie 2016 na próbie 350 firm. Badanie dodatkowe zrealizowano na próbie 500 pracowników zatrudnionych w polskich firmach.

rzządzanie oraz zabezpieczenie się przed konsekwencjami cyberryzyka – jest ono nadal niedoceniane. Ryzyko przestępczości elektronicznej znajduje się wśród 10 największych, lecz lokuje się w środku stawki priorytetów kadry menedżerskiej biorącej udział w badaniu Aon. Przedsiębiorcy w Polsce jeszcze nie doceniają znaczenia ubezpieczenia od ryzyka cybernetycznego. Jednakże z uwagi na to, że w maju 2018 roku wchodzi w życie unijne rozporządzenie o ochronie danych osobowych, przedsiębiorcy będą zmuszeni zainteresować się ubezpieczeniem cyberryzyka oraz polisami odpowiedzialności cywilnej dla zarządów spółek D&O¹⁶. Dane osobowe oraz wrażliwe informacje stanowią bowiem często kluczowe aktywa firmy, a więc podobnie jak przy innych aktywach, kadra zarządzająca zobowiązana jest do ich ochrony.

Obecnie nawet najmniejsze firmy posiadają strony internetowe i komunikują się ze swoimi partnerami biznesowymi i klientami w formie elektronicznej. Coraz powszechniej wykorzystują też media społecznościowe do promowania produktów oraz działalności, a także pozyskiwania klientów. Natomiast crowdfunding, finansowanie społecznościowe rozwija się jako sposób finansowania przedsięwzięć biznesowych.

Ryzyko przestępczości elektronicznej może dotyczyć informacji kluczowych dla przedsiębiorstw, takich jak: dane klientów, wyniki sprzedaży, informacje o projektach i transakcjach, a zazwyczaj wrażliwe dane są przechowywane w formie elektronicznej. Częstotliwość i różnorodność ataków hakerskich rośnie, a przy tym wzrastają koszty przeciwdziałania kolejnym przejawom cyberryzyka, o czym przekonały się także rządy wielu krajów wysoko rozwiniętych. Różne są także motywy działania przestępców cybernetycznych, np. chęć kradzieży informacji lub własności intelektualnej, uzyskanie okupu lub zemsta zwolnionych pracowników.

Konsekwencje ataku hakerskiego, w tym utraty, nielegalnego ujawnienia lub sprzeniewierzenia poufnych danych oraz informacji, są szerokie i wykraczają poza bezpośrednią utratę przychodów, ponieważ dochodzi też ryzyko reputacji. Atak może być przeprowadzony przez pojedynczego hakera. Jednakże coraz częściej takim procederem zajmują się wyspecjalizowane grupy przestępcze. Ponadto rosną koszty związane z wykrywaniem i neutralizacją luk w systemach zabezpieczeń infrastruktury informatycznej przedsiębiorstw. Na negatywne wieloaspektowe skutki cyberataków narażeni są: pracownicy, kontrahenci, a także całe przedsiębiorstwo, które ponosi koszty materializacji ryzyka, w tym też konsekwencje ryzyka reputacji lub nawet zagrożenie bankructwem. W tabeli 3 zawarto dane dotyczące czynników i zagrożeń, na jakie narażone są organizacje, według badania ankietowego pt. *Cyberbezpieczeństwo firm* przeprowadzonego przez EY w Polsce (ostatnie w listopadzie 2016 r.).

¹⁶ R. Skibińska, *Cyberzagrożenia przekładają się na większe zainteresowanie specjalnymi polisami*, <http://obserwatorfinansowy.pl/> <https://www.obserwatorfinansowy.pl/tematyka/rynki-finansowe/cyberzagrozenia-przekladaja-sie-na-wieksze-zainteresowanie-specjalnymi-polisami/> [dostęp: 31.07.2017].

Tabela 3. Jakie zagrożenie i podatności istotnie zwiększyły w ostatnim czasie ryzyko, na jakie narażone są organizacje

Table 3. What threats and causes have significantly increased the risk that organizations are exposed to recently

Rok	2013	2014	2015	2016
Podatności				
Beztroski lub nieświadomy pracownik	53%	57%	44%	55%
Nieaktualne zabezpieczenie/architektura	51%	52%	34%	48%
Nieautoryzowany dostęp	34%	34%	32%	54%
Zagrożenia				
Złośliwe oprogramowanie	41%	34%	43%	52%
Phishing	39%	39%	44%	51%
Cyberatak w celu kradzieży danych finansowych	46%	51%	33%	45%
Cyberatak w celu kradzieży własności intelektualnej lub danych	41%	44%	30%	42%
Ataki wewnętrzne	28%	31%	27%	33%

Źródło: Według badania EY. pt. *Cyberbezpieczeństwo firm* 2016 r.

Jak wynika z danych zawartych w tabeli 3, najwięcej zagrożeń w 2016 wynikało z wprowadzenia złośliwego oprogramowania, jak również z phishingu. Phishing jest formą oszustwa internetowego, w ramach którego podstępem wyludza się od użytkownika jego osobiste dane. Phishing obejmuje kradzież haseł, numerów kart kredytowych, danych kont bankowych i innych poufnych informacji.

Mimo że dotychczas najwięcej cyberataków miało miejsce w Ameryce Północnej, stale rośnie liczba ataków również w Europie. Dlatego coraz więcej przedsiębiorstw w UE interesuje się ubezpieczeniem od tego typu zagrożeń. Głównie nabywają one pakiety ubezpieczeniowe, których celem jest rekompensata skutków finansowych w sytuacji materializacji cyberryzyka, w tym również rekompensata z tytułu poniesionych kosztów odpowiedzialności cywilnej władz spółki. W Polsce rynek polis dotyczących cyberryzyka i przestępczości elektronicznej dopiero się rozwija. W 2017 r. na polskim rynku ubezpieczeniowym pokrycie cyberryzyka (czyli w miarę szeroka ochrona ubezpieczeniowa) dostępne jest w zasadzie w ofercie pięciu towarzystw ubezpieczeń¹⁷ (oczywiście elementy tego typu ubezpieczeń występują jeszcze u kilku ubezpieczycieli, lecz jest to zazwyczaj komponent innych rodzajów ubezpieczeń):

1. Chubb European Group Limited Oddział w Polsce – ubezpieczenie DataGuard – Advantage,

¹⁷ G. Strubczewski, *Zagrożenia cybernetyczne instytucji finansowych*, „Rozprawy Ubezpieczeniowe” 2017, nr 24(2), s. 80.

2. AIG Europe Limited Sp. z o.o. Oddział w Polsce – ubezpieczenie CyberEdge,
3. TUiR Allianz Polska S.A. – ubezpieczenie Cyber Protect,
4. STU Ergo Hestia S.A. – ubezpieczenie danych elektronicznych od ryzyk cybernetycznych,
5. Leadenhall Polska S.A. – ubezpieczenie Leadenhall Cyber.

Na przykład ubezpieczenie AIG Ubezpieczenie CyberEdge kierowane jest do każdej firmy, która zbiera, przetwarza lub przekazuje dane. Nowością jest modularna konstrukcja ubezpieczenia CyberEdge, która pozwala na dopasowanie oferty dla przedsiębiorstwa dowolnej wielkości, działającego w każdej branży. Ubezpieczenie Cyber Edge obejmuje¹⁸:

- ochronę ubezpieczeniową dla firmy na wypadek włamania do jej systemu komputerowego, ataku hakerskiego, wycieku danych, zainstalowania złośliwego oprogramowania w sytuacji niewystarczającego zabezpieczenia systemu komputerowego,
- ochronę ubezpieczeniową na wypadek działalności przestępczej lub zwykłego zaniedbania ze strony pracowników ubezpieczonego,
- wsparcie firm wyspecjalizowanych w informatyce śledczej, kancelarii prawnych oraz ekspertów ds. public relations w celu zminimalizowania negatywnego wpływu na reputację ubezpieczonego.

W wielu krajach UE oraz w USA oferowane są znacznie szersze pakiety ubezpieczeń od ryzyka komputerowego niż w Polsce. Między innymi z tego powodu poziom korzystania z cyberpolis jest wyższy. Szacuje się, że do 2020 roku wartość rynku w USA może wynosić nawet 10 miliardów dolarów¹⁹. Jest to jeden z najszybciej rozwijających się segmentów rynku ubezpieczeń zwłaszcza w krajach wysoko rozwiniętych. Zdaniem T. Grelli, szefowej American International Group Inc. w Nowym Jorku, rosnący rynek ubezpieczeń przed cyberprzestępczością stoi przed ogromnym wyzwaniem, co będzie wymagało od ubezpieczycieli zbierania i przetwarzania większej ilości danych, a działając w bardzo konkurencyjnym otoczeniu, mogą obniżyć standardy i gromadzić mniej danych. Główni gracze w branży ubezpieczeniowej powinni monitorować i zarządzać cyberryzykiem, w przeciwnym razie nie sprostają potrzebom klientów, a cyberprzestępczość ujawni się dopiero po wielkim katastroficznym wydarzeniu²⁰.

Podsumowanie

We współczesnej gospodarce zmienia się rola ubezpieczeń, które przestają być postrzegane wyłącznie jako koszt dla przedsiębiorstwa, ale stają się istotnym, nie-

¹⁸ Ubezpieczenie CyberEdge AIG, <https://www.aig.pl/business/produkty-i-uslugi/finansial.../cyber-edge> [dostęp: 30.07.2017].

¹⁹ M. Adamski, *Czy cyber-ubezpieczenia mają sens*, rp.pl [dostęp: 30.07.2017].

²⁰ M. Lerner, *Cyber insurers should beware of pitfalls in competitive environment*, 10.06.2017 Business Insurance, www.businessinsurance.com/.../Cyber-insurers-should-beware-agg. [dostęp: 2.10. 2017].

zbędnym instrumentem w zarządzaniu ryzykiem przedsiębiorstwa. Ubezpieczenie umożliwia transfer na ubezpieczyciela finansowych skutków materializacji ryzyka. Ubezpieczenia zwiększają poczucie bezpieczeństwa zarówno w wymiarze jednostkowej działalności gospodarczej, małej i średniej firmy, jak i dużego przedsiębiorstwa. Ubezpieczenia sprzyjają także podejmowaniu działań prewencyjnych służących ochronie majątku, pracowników i klientów, zapobiegających materializacji ryzyka i minimalizujących straty.

Współcześnie ubezpieczenie stało się wieloaspektowym komponentem systemu zarządzania różnego rodzaju ryzykiem przedsiębiorstwa, nie tylko ryzykiem szkód tzw. kradzieżowych, ogniowych i wynikających z działania sił natury. Dzisiaj rodzaje i poziom ubezpieczenia są ważnym elementem oceny ryzyka przedsiębiorstwa jako klienta banku lub firmy faktoringowej, a także jako partnera gospodarczego dla szerokiego spektrum innych podmiotów publicznych oraz gospodarczych, tj. np. dostawców i odbiorców. Stąd też rośnie znaczenie innych niż klasyczne majątkowe rodzajów ubezpieczeń, a zwłaszcza ubezpieczeń finansowych z grup 14, 15 i 16 działu II, oraz ubezpieczeń odpowiedzialności cywilnej. Nowym obszarem rynku ubezpieczeniowego jest ochrona przed szeroko rozumianym ryzykiem przestępstw komputerowych. Stopniowo kształtuje się także świadomość roli ubezpieczenia w zarządzaniu wartością przedsiębiorstwa, co jest perspektywicznym obszarem analizy i refleksji teoretycznej oraz zarządczej. Ponadto tempo zmian technologicznych w sferze IT spowodowało wzrost znaczenia ubezpieczeń w zarządzaniu związanym z wykorzystaniem systemów informatycznych. Równolegle rośnie też znaczenie ubezpieczeń w zarządzaniu ryzykiem regulacyjnym czego przykładem mogą być ubezpieczenia D&O MAR.

Niedostatecznie rozwinęła się jeszcze oferta produktowa w zakresie objęcia ochroną cyberryzyka, ale modyfikację pakietów ubezpieczeń utrudnia zmienność i różnorodność form przestępczości w tym obszarze.

Zainteresowanie ubezpieczeniem od cyberryzyka wzrosło w krajach UE, kiedy od 25 maja 2018 r. zacznie obowiązywać w krajach członkowskich UE rozporządzenie Parlamentu Europejskiego i Rady z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie przepływu takich danych (RODO, tj. Rozporządzenie o Ochronie Danych Osobowych, a wersji angielskiej GDPR General Data Protection Regulation). Rozporządzenie wprowadza nowe sankcje za niezgodne z prawem przetwarzanie danych osobowych, brak odpowiednich zabezpieczeń, a także rozszerzony został katalog danych wrażliwych.

Współcześnie, w XXI w., ubezpieczenie przyczynia się do zwiększenia bezpieczeństwa funkcjonowania nowoczesnego przedsiębiorstwa i obrotu gospodarczego. Przedsiębiorstwa w globalnej gospodarce, przy rosnącej zmienności, czyli turbulentności otoczenia rynkowego oraz systemowego (w tym zwłaszcza regulacyjnego) i pod presją zmian wynikających z synergii zmian technologicznych, szukają port-

felowych rozwiązań w zakresie zarządzania ryzykiem, zwłaszcza ryzykiem rynkowym, ryzykiem regulacyjnym i ryzykiem technologicznym. W związku z tym rośnie znaczenie ubezpieczeń w zarządzaniu wspomnianymi rodzajami ryzyka.

Bibliografia

- Adamski M., *Czy cyber-ubezpieczenia mają sens*, rp.pl.
- Badania EY. pt. *Cyberbezpieczeństwo firm* 2016 r.
- Cyberbezpieczeństwo firm – najbardziej szkodzą pracownicy*, Egospodarka.pl. <http://www.egospodarka.pl/139426,Cyberbezpieczenstwo-firm-najbardziej-szkodza-pracownicy,1,12,1.html>.
- Continental European Cyber Risk Survey: 2016, Marsh Report , Oktober 2016 , <https://www.marsh.com/.../continental-european-cyber-risk-survey-2016-report.html>.
- Fedor M., *Bezwzględne kryterium ubezoieczalności*, „Gazeta Ubezpieczeniowa” z 3 sierpnia 2004 r.
- Hadyniak B., *Ryzyko w przedsiębiorstwie*, [w:] B. Hadyniak, J. Monkiewicz (red.), *Ubezpieczenia w zarządzaniu ryzykiem przedsiębiorstwa*, tom 1: Podstawy, Poltext, Warszawa 2010.
- Jajuga K., *Teoretyczne podstawy zarządzania ryzykiem*, PWN, Warszawa 2005.
- Kaczmarek T.T., Zarzycki M., *Poradnik eksportera*, Wyd. Branta, Bydgoszcz – Warszawa 2005.
- Lerner M., *Cyber insurers should beware of pitfalls in competitive environment*, 10.06.2017 Business Insurance, www.businessinsurance.com/.../Cyber-insurers-should-beware-agg.
- Ronka-Chmielowiec W., *Wykorzystanie ubezpieczeń do zarządzania ryzykiem w przedsiębiorstwie*, [w:] J. Monkiewicz, L. Gąsorkiewicz (red.), *Zarządzanie ryzykiem działalności organizacji*, C.H.Beck, Warszawa 2010.
- Skibińska R., *Cyberzagrożenia przekładają się na większe zainteresowanie specjalnymi polisami*, <http://obserwatorfinansowy.pl/> <https://www.obserwatorfinansowy.pl/tematyka/rynki-finansowe/cyberzagrozenia-przekladaja-sie-na-wieksze-zainteresowanie-specjalnymi-polisami/>.
- Strubczewski G., *Zagrożenia cybernetyczne instytucji finansowych*, „Rozprawy Ubezpieczeniowe 2017, nr 24 (2).
- Ubezpieczenie CyberEdge AIG, <https://www.aig.pl/business/produkty-i-uslugi/financial.../cyberedge>,
- Waściński R., Kasiński P., *Ryzyko w działalności przedsiębiorstwa – elementy systematyki i identyfikacji*, [w:] J. Monkiewicz, L. Gąsorkiewicz (red.), *Zarządzanie ryzykiem działalności gospodarczej*, C.H.Beck, Warszawa 2010.
- Wierzbicka E., *Ubezpieczenia w zarządzaniu ryzykiem przedsiębiorstwa*, [w:] E. Wierzbicka (red.), *Wykorzystanie ubezpieczeń w zarządzaniu przedsiębiorstwem*, Wyd. SGH, Warszawa 2016.
- Ziomko R., *Raport Aon Polska IV edycja. Zarządzanie ryzykiem i ubezpieczeniami w firmach w Polsce*, Warszawa 2016.
- Zarządzanie ryzykiem i ubezpieczeniami w firmach w Polsce*, Raport Aon Polska 2013-2014, Warszawa 2013, Aon Risk Solutions.

Nota o Autorze:

Ewa Wierzbicka – doktor nauk ekonomicznych, adiunkt w Instytucie Zarządzania Wartością w Szkole Głównej Handlowej w Warszawie. Członek Towarzystwa Naukowego Prakseologii i Rady Programowej Insurance Forum. Wcześniej pracowała w Instytucie Finansów i Wyższej Szkole Ubezpieczeń i Bankowości (obecnie Akademia Finansów). Ma w swoim dorobku ponad 120 publikacji. Jest kierownikiem studiów podyplomowych Akademia Ubezpieczeń – ubezpieczenia gospodarcze dla przedsiębiorstw w SGH w Warszawie (obecnie IX edycja studiów).

Author's resume:

Ewa Wierzbicka – PhD in economics, Assistant Professor at the Institute of Value Management at the Warsaw School of Economics. She is a member of the Praxeology Science Society and a member of the Insurance Forum Program Board. Previously she worked at the Institute of Finance and the School of Insurance and Banking (now the Academy of Finance). He has over 120 publications. He is the head of postgraduate studies of the Insurance Academy - business insurance for companies at the Warsaw School of Economics (now the 9th edition of studies).

Kontakt/Contact:**Ewa Wierzbicka**

Instytut Zarządzania Wartością
Szkoła Główna Handlowa w Warszawie
Al. Niepodległości 162
02-554 Warszawa
e-mail: ewierz1@sgh.waw.pl

