dr Grzegorz Strupczewski

Uniwersytet Ekonomiczny w Krakowie

Ryzyko cybernetyczne jako wyzwanie dla branży ubezpieczeń w Polsce i na świecie[1]

Wprowadzenie

Ryzyko cybernetyczne można określić jako najpoważniejsze wyzwanie, przed jakim stanęła branża ubezpieczeniowa w ostatnim półwieczu. Nosi ono znamiona ryzyka systemowego, którego źródłem są wykorzystywanie technologii informatycznych i elektroniczne przetwarzanie danych. Jako nowoczesne społeczeństwo informacyjne żyjące w erze globalnej gospodarki cyfrowej jesteśmy w niespotykany dotychczas sposób zależni od internetu i związanych z nim technologii cyfrowych, dzięki którym funkcjonują kluczowe usługi finansowe, zdrowotne, administracji państwowej i inne. Jednakże ta tak ważna dla społeczeństwa i gospodarki infrastruktura jest narażona na rosnące ryzyko ataków cybernetycznych zagrażających dobrobytowi i jakości życia. Problem cyberataków może wydawać się w Polsce odległy. Choć większość działających tutaj przedsiębiorców zdaje sobie sprawę z istnienia tego typu niebezpieczeństw, tylko nieliczni podejmują działania ukierunkowane na zarządzanie ryzykiem cybernetycznym, również przez zakup specjalistycznego ubezpieczenia.

Obecnie cyberataki stanowią realne i coraz większe zagrożenie dla podmiotów gospodarczych, niezależnie od skali i obszaru działalności, dla osób fizycznych oraz całej gospodarki. Roczny koszt cyberprzestępczości dla globalnej gospodarki w 2015 r. oszacowano na 400 mld USD (McAfee 2016). W 2014 r. na świecie ujawniono prawie 43 mln cyberataków, co oznacza, że dziennie dochodzi średnio do 117 339 incydentów (Allianz 2015). Aż 37% przedsiębiorstw doświadczyło przynajmniej jednego poważnego aktu naruszenia bezpieczeństwa cybernetycznego (w tym naruszenia bezpieczeństwa danych elektronicznych) w ciągu ostatnich 2 lat. Były to zdarzenia o bardzo zróżnicowanym charakterze. Przeważały cyberataki hakerskie utrudniające bieżącą pracę przedsiębiorstwa, na co wskazała

[1] Publikacja została sfinansowana ze środków przyznanych Wydziałowi Finansów Uniwersytetu Ekonomicznego w Krakowie w ramach dotacji na utrzymanie potencjału badawczego.

blisko połowa respondentów. Znaczną uciążliwością cechowały się również awarie systemów IT (35%). Poważny problem stanowiło ponadto zapewnienie bezpieczeństwa poufnych danych przechowywanych w postaci elektronicznej, zagrożonych nie tylko w wyniku ataków hakerskich pochodzących z zewnątrz organizacji, ale także niesolidności i nieuczciwości pracowników danego przedsiębiorstwa – 30% (Ponemon & AON 2015).

Szacuje się, że w 2014 r. globalna ekspozycja branży ubezpieczeniowej na ryzyko cybernetyczne wyniosła 100 mld GBP. Jeśli założyć, że – podobnie jak w ubezpieczeniach mienia – maksymalna prawdopodobna strata (PML) stanowi 20% sumy ubezpieczenia, PML dla cyberryzyka może osiągnąć pułap 20 mld GBP. Jeśli utrzyma się dotychczasowe tempo rozwoju cyberubezpieczeń, ryzyko cybernetyczne może przekroczyć globalną pojemność ubezpieczeniową i reasekuracyjną dla takich ryzyk katastroficznych, jak katastrofy naturalne – 65 mld GBP, czy katastrofa nuklearna – 3 mld GBP (Marsh 2015a, s. 23).

Ogromny potencjał i zasięg oddziaływania, połączony z niebezpieczeństwem czasowych zakłóceń w normalnym funkcjonowaniu gospodarki lub instytucji publicznych, każe traktować ryzyko cybernetyczne podobnie jak terroryzm. W związku z tym być może uprawniony jest postulat, by cyberryzyko zaliczać do ryzyk systemowych oraz oczekiwać od władz państwa stosownego reagowania (III 2015, s. 24).

Według raportu Allianz (2015) głównymi czynnikami wzrostu częstotliwości oraz intensywności incydentów cybernetycznych (polegających m.in. na naruszeniu bezpieczeństwa danych) są globalizacja, komercjalizacja i intensyfikacja wzajemnych połączeń między poszczególnymi elementami systemów komputerowych w skali globalnej.

W kontekście powyższych spostrzeżeń został określony problem badawczy, który można zawrzeć w następujących pytaniach:

- Czym jest ryzyko cybernetyczne i jaka jest jego systematyka?
- Jaki jest poziom zagrożenia cybernetycznego we współczesnym świecie?
- Czy ryzyko cybernetyczne może być ubezpieczane?
- Jak rozwija się rynek ubezpieczeń cybernetycznych na świecie i w Polsce?

Z tak wyznaczonego problemu badawczego wynika główny cel badań podjętych przez autora, którym jest analiza barier i możliwości rozwoju ubezpieczeń cybernetycznych – aby, go osiągnąć sformułowano cele szczegółowe (będące jego integralną częścią):

1. Zdefiniowanie i usystematyzowanie ryzyka cybernetycznego.
2. Scharakteryzowanie poziomu zagrożenia cybernetycznego.
3. Zidentyfikowanie barier i możliwości rozwoju rynku ubezpieczeń cybernetycznych.

Struktura niniejszego opracowania odpowiada wskazanym celom badawczym. Pracę otwiera przegląd definicji i klasyfikacji ryzyka cybernetycznego. Następnie, na bazie licznych raportów branżowych, dokonano próby oszacowania skali

zagrożenia cybernetycznego. W kolejnym punkcie, po zidentyfikowaniu kręgu nabywców ubezpieczeń cybernetycznych, przeprowadzono analizę najważniejszych stymulant i destymulant rozwoju rynku cyberubezpieczeń. Dopełnieniem prezentowanych rozważań jest przegląd aktualnej sytuacji na globalnym rynku cyberubezpieczeń. Najistotniejsze spostrzeżenia oraz wnioski wynikające z przeprowadzonych analiz zostały zawarte w podsumowaniu.

1. Definicja ryzyka cybernetycznego

Choć w ciągu ostatnich kilku lat powstało wiele raportów branżowych i opracowań odnoszących się do cyberprzestrzeni, w żadnym z nich nie podano pełnej i jednoznacznej definicji ryzyka cybernetycznego (cyberryzyka)[2]. Jest to po części skutkiem różnych perspektyw, z których analizuje się to ryzyko. Dla organizacji cyberryzyko to ryzyko operacyjne pochodzenia antropogenicznego (Podolak 2015), a dla towarzystwa ubezpieczeń zawierającego umowy cyberubezpieczeń – ryzyko ubezpieczeniowe, definiowane przez enumeratywne zestawienie różnych możliwych form realizacji, w stosunku do których buduje się odpowiednią ochronę ubezpieczeniową[3].

Poszukując definicji ryzyka cybernetycznego na gruncie ryzyka operacyjnego, można przytoczyć kilka prób jej sformułowania. W najwęższym ujęciu ryzyko cybernetyczne to ryzyko wystąpienia szkodliwych zdarzeń elektronicznych, które powodują zakłócenia w działalności przedsiębiorstwa lub straty finansowe (Mukhopadhyay *et al.* 2013). Cyberryzyko można też ująć jako ryzyko gospodarcze związane z posiadaniem, działaniem, wykorzystaniem i oddziaływaniem urządzeń i technologii IT w przedsiębiorstwie (Marsh 2015b). Ryzyko bezpieczeństwa informacji (Ögűt *et al.* 2011) lub niebezpieczeństwo zakłócenia systemów informacyjnych (Böhme, Kataria 2006) to przykłady najogólniejszego i bardziej wszechstronnego spojrzenia na ryzyko cybernetyczne. W opinii autora najbardziej precyzyjnie, a jednocześnie w zgodzie z takim standardami zarządzania ryzykiem jak Bazylea II i Solvency II wyjaśnili znaczenie cyberryzyka Cebula i Young (2010). Zdaniem tych autorów jest to ryzyko operacyjne w sferze zasobów informacyjnych i technologicznych organizacji, którego negatywne skutki mogą oddziaływać na poufność, dostępność i integralność informacji lub systemów informatycznych.

---

[2] Przedrostek „cyber" powstał jako skrót od przymiotnika „cybernetyczny", który odnosi się do tego, co jest przekazywane drogą elektroniczną, przez internet lub inną sieć komputerową.

[3] Amerykański organ nadzoru ubezpieczeniowego NAIC wymienia następujące rodzaje cyberryzyka: kradzież tożsamości, przerwa w działalności spowodowana awarią systemu komputerowego, utrata reputacji, koszty odtworzenia danych utraconych w wyniku cyberataku, kradzież poufnych informacji handlowych, zainfekowanie złośliwym oprogramowaniem, nieuprawnione ujawnienie poufnych danych w wyniku błędu ludzkiego, koszty związane z naruszeniem bezpieczeństwa danych osobowych, naruszenie praw autorskich (NAIC 2016).

2. Systematyka ryzyka cybernetycznego

Ryzyko cybernetyczne najczęściej klasyfikuje się ze względu na rodzaj szkodliwych działań prowadzących do materializacji strat, a więc przyczyn cyberszkód. Zgodnie z systematyką opracowaną przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT przyczyny realizacji cyberryzyka dzielimy na działania celowe i niecelowe – przypadkowe (CERT 2015). Wśród działań celowych wyróżnia się:

- iniekcję złośliwego oprogramowania (wirus, robak sieciowy, koń trojański, dialer, botnet),
- przełamanie zabezpieczeń (nieuprawnione logowanie, włamanie na konto/ataki sieciowe, włamanie do aplikacji),
- publikacje w sieci internet (treści obraźliwe, pomawianie/zniesławienie, naruszenie praw autorskich, dezinformacja),
- nielegalne gromadzenie informacji (skanowanie, podsłuch, inżynieria społeczna, szpiegostwo, spam),
- sabotaż komputerowy (nieuprawniona zmiana informacji, nieuprawniony dostęp, nieuprawnione wykorzystanie informacji, atak odmowy dostępu DDoS, skanowanie danych, wykorzystanie podatności w urządzeniach, wykorzystanie podatności aplikacji),
- czynnik ludzki (naruszenie procedur bezpieczeństwa, naruszenie obowiązujących przepisów prawa),
- cyberterroryzm (przestępstwa o charakterze terrorystycznym popełnione w cyberprzestrzeni).

Działania przypadkowe w przestrzeni cybernetycznej podzielono na dwie kategorie:

- wypadki i zdarzenia losowe (awarie sprzętowe, awarie łącza, błędy oprogramowania),
- czynnik ludzki (naruszenie procedur, zaniedbanie, błędna konfiguracja urządzenia, brak wiedzy, naruszenie praw autorskich).

Autorami kompleksowej taksonomii cyberryzyka, często przywoływanej w publikacjach międzynarodowych, są Cebula i Young (2010). Wychodząc od źródeł cyberryzyka, wyróżnili oni 4 klasy ryzyka, następnie 13 jego podklas i 56 ich elementów składowych. Głównymi źródłami ryzyka cybernetycznego są zatem:

1) działania ludzkie,
2) zakłócenia w pracy systemów i urządzeń IT,
3) niewydolność procesów wewnętrznych w organizacji,
4) wypadki zewnętrzne.

Do zdarzeń wynikających z działań ludzkich można zaliczyć zdarzenia nieumyślne (np. błędy, pomyłki, zaniedbania), umyślne (oszustwa, sabotaże, kradzieże, akty wandalizmu) oraz polegające na niepodjęciu odpowiednich czynności (wynikające np. z braku wiedzy czy umiejętności). W kategorii obejmującej awarie

technologiczno-systemowe umieszczono zdarzenia, które mają negatywny wpływ na sprzęt komputerowy (obniżające jego wydajność lub pojemność oraz powodujące trudności w zapewnieniu prawidłowego funkcjonowania), na oprogramowanie (problemy z kompatybilnością, konfiguracją, utrzymaniem odpowiedniego poziomu zabezpieczeń) i na system komputerowy (skutkujące jego nieprawidłowym działaniem polegającym na braku spójności i kompleksowości). Jako ryzyka prowadzące do niewydolności procesów wewnętrznych wskazano te mające wpływ na tworzenie i realizację procesów, wsparcie oraz kontrolę. Do zdarzeń zewnętrznych zaliczono katastrofy naturalne, konsekwencje regulacji prawnych, zmiany w otoczeniu biznesowym, uzależnienie od zewnętrznych dostawców (Cebula i Young 2010).

Z uwagi na swój niejednolity charakter ryzyko cybernetyczne może przyjmować w organizacji następujące formy: ryzyko operacyjne, ryzyko finansowe, ryzyko regulacyjne, utraty reputacji, ryzyko utraty własności intelektualnej (tabela 1).

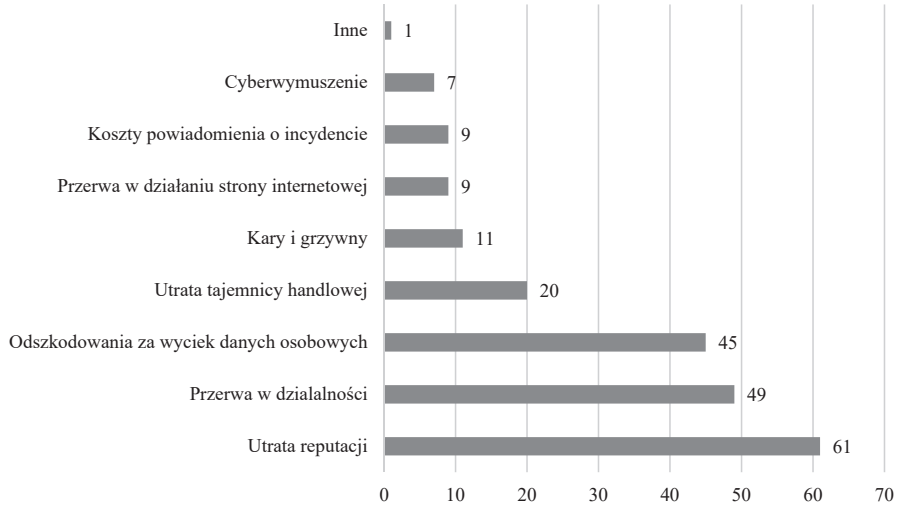
Tabela 1
Obszary występowania zagrożenia cybernetycznego wśród ryzyk organizacji

Nazwa ryzyka	Charakterystyka
Ryzyko operacyjne	Jego źródłem są niewłaściwe procedury wewnętrzne, błąd ludzki, wada systemu lub przyczyny zewnętrzne. W tej kategorii mieści się większość ryzyk cyfrowych. Ich skutki polegają np. na utracie klientów lub danych, zakłóceniach w łańcuchu dostaw, czasowym wyłączeniu wewnętrznej sieci komputerowej.
Ryzyko finansowe	Straty finansowe wynikają z niezdolności do prawidłowej realizacji procesów biznesowych w wyniku oszustwa lub kradzieży.
Ryzyko własności intelektualnej	Utrata dokumentacji produkcyjnej lub projektowej, planów marketingowych i dostanie się jej w ręce konkurencji może skutkować zmniejszeniem przewagi konkurencyjnej.
Ryzyko regulacyjne	Organizacja zostaje narażona na sankcje prawne w wyniku niespełnienia ustawowych wymagań w obszarze ochrony danych osobowych.
Ryzyko reputacji	Publikacja informacji o incydencie informatycznym może odbić się niekorzystnie na wizerunku, marce czy reputacji firmy.

Źródło: opracowanie własne na podstawie Lloyds (2010, s. 5).

W badaniach *Allianz Risk Barometer 2015* jako główne przyczyny strat ekonomicznych w przedsiębiorstwach wskazano: utratę reputacji, przerwę w działalności oraz odszkodowania należne z tytułu wycieku danych osobowych – patrz rysunek 1 (Allianz 2015, s. 12).

Rysunek 1
Najważniejsze przyczyny strat ekonomicznych spowodowanych cyberryzykami (odsetek wskazań respondentów)



Źródło: Allianz (2015, s. 12).

3. Analiza potencjału ryzyka cybernetycznego

Kwantyfikacja ryzyka na potrzeby ubezpieczenia oznacza dokonanie pomiaru trzech kluczowych wielkości charakteryzujących skalę zagrożenia: prawdopodobieństwa wystąpienia, potencjalnych rozmiarów szkód oraz podatności podmiotu na działanie ryzyka.

Skalę zagrożenia cybernetycznego w danym kraju dobrze ilustruje stosunek strat powstałych w wyniku cyberprzestępczości do PKB. Z danych zebranych w tabeli 2 wynika, że wśród 10 najsilniejszych gospodarek świata największe straty w wartościach bezwzględnych ponoszą Stany Zjednoczone (108 mld USD), Chiny (60 mld USD) i Niemcy (59 mld USD). Jeśli jednak uwzględnić relację do PKB, okaże się, że jej skutki są najbardziej dotkliwe dla gospodarki niemieckiej (1,60%), podczas gdy w pozostałych państwach wskaźnik ten wynosi zdecydowanie poniżej 1%.

Interpretując powyższe informacje, należy wszakże pamiętać, iż oficjalne dane obejmują jedynie ujawnione przypadki naruszeń bezpieczeństwa danych, podczas gdy w rzeczywistości większość cyberataków pozostaje nieujawniona. Najwięcej ujawnionych incydentów naruszenia bezpieczeństwa danych notuje się w Stanach Zjednoczonych – w 2014 r. było ich 783, co jest rekordową liczbą w obecnej dekadzie (poprzedni rekord – z 2010 r. – wynosił 662 naruszenia). W 2015 r. miało miejsce 781 naruszeń (ITRC 2016).

Tabela 2
Wartość strat spowodowanych cyberprzestępstwami w relacji do PKB w 10 największych gospodarkach świata w 2013 r.

Lp.	Państwo	PKB (bln USD)	Straty spowodowane cyberprzestępczością (mld USD)	Straty wynikające z cyberprzestępczości w relacji do PKB (%)
1	USA	16,8	108,0	0,64
2	Chiny	9,5	60,0	0,63
3	Japonia	4,9	0,9	0,02
4	Niemcy	3,7	59,0	1,60
5	Francja	2,8	3,0	0,11
6	Wielka Brytania	2,7	4,3	0,16
7	Brazylia	2,4	7,7	0,32
8	Rosja	2,1	2,0	0,10
9	Włochy	2,1	0,9	0,04
10	Indie	1,9	4,0	0,21

Źródło: Allianz (2015, s. 7).

Eling i Wirfs (2016), analizując strukturę geograficzną cyberataków, ustalili, że do ponad ich połowy (52,6%) doszło w firmach zarejestrowanych w Ameryce Północnej, a co czwarty atak hakerski (24,9%) wydarzył się w Europie. Jeśli spojrzeć globalnie, trzy na cztery wypadki cybernetyczne dotknęły instytucje finansowe, a pozostałe 25% – podmioty z sektora niefinansowego. Ważnym czynnikiem różnicującym skalę zagrożenia cybernetycznego jest wielkość firmy. 87% wszystkich wypadków odnotowano w przedsiębiorstwach dużych, tj. zatrudniających ponad 250 osób. W firmach małych i średnich odsetek incydentów był podobny i wyniósł nieco ponad 4%.

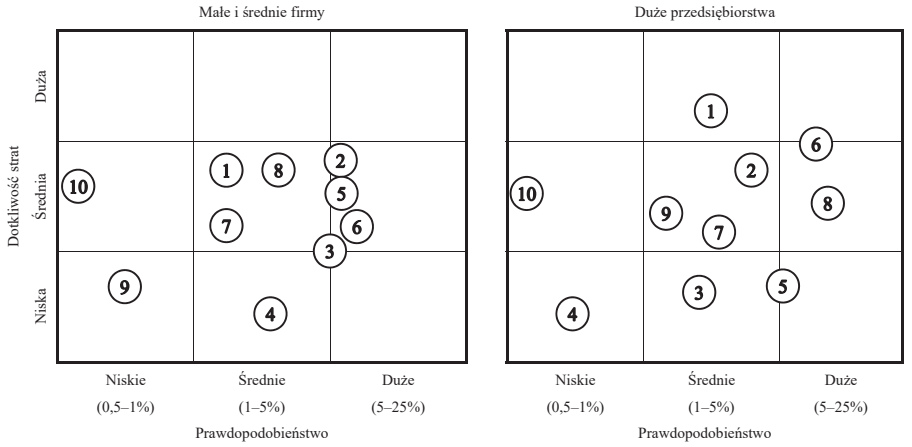
Podatność nowoczesnego społeczeństwa na zagrożenia informatyczne będzie wzrastać. Może to wynikać choćby z takich okoliczności, jak (Allianz 2015, s. 5; AON 2014):

- rozwój tzw. internetu rzeczy (ang. *Internet of Things*, IoT), którego fenomen polega na tym, że coraz więcej urządzeń codziennego użytku (AGD, RTV, instalacje domowe) może być sterowanych zdalnie, jak również za pośrednictwem internetu,
- rosnące uzależnienie bieżącego funkcjonowania podmiotów gospodarczych od informacji przekazywanych w czasie rzeczywistym, co powoduje, że w razie jakiegokolwiek zakłócenia w transferze danych konieczne jest wstrzymanie działalności,
- fakt, że część organizacji, zwłaszcza w sektorze MiŚ, nadal wykorzystuje przestarzałe sprzęt teleinformatyczny i oprogramowanie, przez co jest bardziej

narażona na cyberataki; należy także pamiętać o ryzyku zainfekowania ich kontrahentów, którzy mimo stosowania wyższych standardów bezpieczeństwa informatycznego mogą nie być odpowiednio przygotowani na pojawienie się ryzyka niejako od wewnątrz, tzn. ze strony zaufanego partnera biznesowego,
- outsourcing usług związanych z przechowywaniem i przetwarzaniem danych (61% przedsiębiorstw wykorzystuje w tym zakresie usługi firm zewnętrznych),
- fakt, iż coraz częściej zadania powierzane pracownikom firmy są realizowane za pośrednictwem prywatnego sprzętu IT (laptopy, tablety, smartfony), który może nie być odpowiednio zabezpieczony (politykę *Bring Your Own Device* stosuje 66% firm).

Graficzna prezentacja całego *spectrum* oszacowanych ryzyk dla danego podmiotu jest możliwa w formie mapy ryzyka. Profil ryzyka cybernetycznego dla segmentów małych i średnich przedsiębiorstw oraz dużych korporacji przedstawiono na rysunku 2.

Rysunek 2
Mapy ryzyka cybernetycznego



Legenda:

1. Kradzież własności intelektualnej
2. Przerwa w działalności firmy
3. Utrata danych lub oprogramowania
4. Cyberwymuszenie
5. Kradzież środków finansowych
6. Naruszenie prywatności
7. Odpowiedzialność za niewłaściwe działanie sieci komputerowej
8. Utrata reputacji
9. Utrata lub uszkodzenie mienia rzeczowego
10. Szkoda osobowa

Źródło: opracowanie własne na podstawie Marsh (2015a, s. 12–13).

Największe zagrożenie dla dużych przedsiębiorstw stanowi utrata własności intelektualnej, zwłaszcza w takich branżach, jak: przemysł chemiczny, farmaceutyczny, lotniczy, zbrojeniowy oraz nowoczesne media (Marsh 2015a, s. 12). Poważne zagrożenie wiąże się również z nieautoryzowanym wyciekiem danych

osobowych oraz zakłóceniami w dostępie do sieci komputerowych. Choć prawdopodobieństwo ryzyka utraty reputacji jest stosunkowo wysokie, trudno oszacować potencjalny rozmiar szkód. Może on zależeć od szybkości i trafności reakcji organizacji na zaistniały problem. Występowanie ryzyka szkód rzeczowych w wyniku cyberataku wynika z wzajemnych połączeń, które powstają między rzeczywistością wirtualną a majątkiem rzeczowym. W obecnych czasach bez problemu można sobie bowiem wyobrazić zdalne sterowanie pracą urządzeń przemysłowych lub infrastrukturą techniczną. Mimo postępującej cyfryzacji trudno jednak oszacować ryzyko szkód osobowych inaczej niż jako niskie.

Choć małe i średnie przedsiębiorstwa postrzegane są jako mniej narażone na ryzyko cybernetyczne, to jednak ich mapa ryzyk w dużej mierze przypomina mapę dla dużych korporacji. Pewne różnice dotyczą częstości zdarzeń oraz potencjału prawdopodobnych szkód, który niekiedy może być wyższy w segmencie MiŚ. Dotyczy to choćby ryzyka utraty lub uszkodzenia danych i oprogramowania albo ryzyka przestępstwa cybernetycznego. Finansowe skutki tych ryzyk mogą być dużo dotkliwsze dla podmiotów dysponujących mniejszymi zasobami.

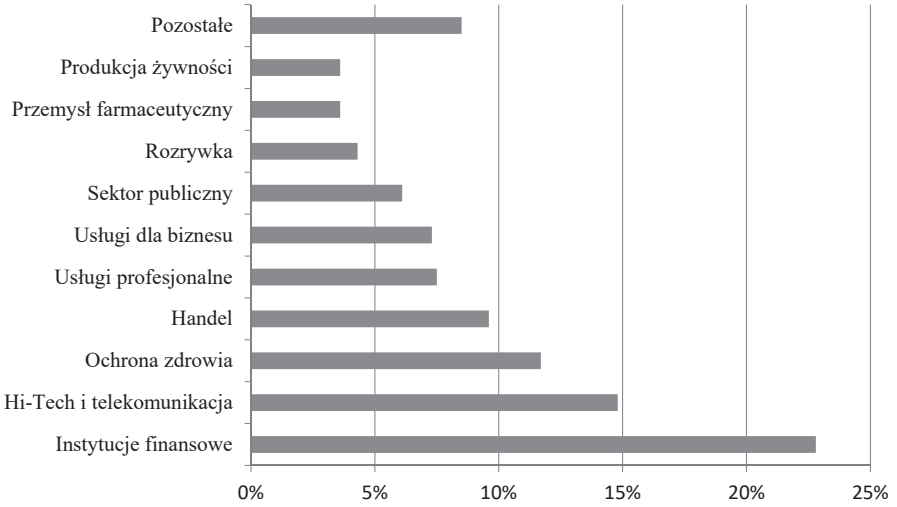
Asymetria informacji, która jest problemem nie tylko w przypadku cyberubezpieczeń, prowadzi do selekcji negatywnej, a więc braku możliwości doboru odpowiedniej stawki ubezpieczeniowej do danego segmentu klientów i w efekcie nadreprezentacji ubezpieczonych o substandardowym poziomie ryzyka.

4. Nabywcy ubezpieczeń cybernetycznych

Ubezpieczeniem cybernetycznym najbardziej zainteresowane są przedsiębiorstwa z sektora usług finansowych, telekomunikacyjnych, handlu hurtowego i detalicznego, ochrony zdrowia (patrz rysunek 3). Jednak kompozycja rodzajów cyberryzyka występującego w poszczególnych sektorach gospodarki może być bardzo różna. Na przykład instytucje finansowe są narażone przede wszystkim na wyciek poufnych danych osobowych i finansowych lub nieuprawniony dostęp do systemu informatycznego (co może skutkować utratą reputacji i przerwą w działalności), a firmy z sektora zaawansowanych technologii, takie jak koncerny farmaceutyczne – na kradzież własności intelektualnej. Z kolei zakłady przemysłowe, wytwórcy i dostawcy mediów powinni zwracać szczególną uwagę na ochronę elektronicznych (a zwłaszcza zdalnych) systemów kontroli maszyn i urządzeń.

Drugą, oprócz rodzaju działalności gospodarczej, determinantą znacząco wpływającą na prawdopodobieństwo zakupu cyberubezpieczenia jest wielkość firmy mierzona roczną sumą przychodów. W segmencie przedsiębiorstw z przychodami rocznymi w granicach 100 mln USD odsetek firm mających cyberubezpieczenie nie przekracza 10%, jednak w grupie firm o obrotach do 5 mld USD cyberpolisą dysponuje 20% podmiotów. Cyberubezpieczenia są najbardziej rozpowszechnione wśród największych korporacji, o obrotach przekraczających 5 mld USD rocznie – tam odsetek ubezpieczonych sięga 25% (AON 2014, s. 14).

Rysunek 3
Struktura alokacji składki za cyberubezpieczenia w 2013 r. wg branż gospodarki



Źródło: AON (2014, s. 12).

5. Stymulanty rozwoju rynku cyberubezpieczeń

Wśród czynników stymulujących rozwój rynku cyberubezpieczeń wskazuje się potrzebę ochrony prywatności (podsycaną doniesieniami medialnymi o incydentach naruszenia bezpieczeństwa danych), minimalizację finansowych konsekwencji wystąpienia cyberataku oraz ryzyko reputacji (ENISA 2012, s. 12).

W ostatnich 10 latach stymulantami rozwoju cyberubezpieczeń w Stanach Zjednoczonych były zmiany norm prawnych dotyczących sposobu postępowania w razie incydentu cybernetycznego prowadzącego do wycieku danych osobowych. Podobnego efektu można oczekiwać również w Europie.

Jak dotąd większość incydentów cybernetycznych nie jest ujawniana opinii publicznej ze względu na obawy dotkniętych nimi organizacji, że odbije się to negatywnie na ich reputacji i wiarygodności.

Obowiązek ujawniania przez przedsiębiorstwa telekomunikacyjne informacji o przypadkach naruszenia bezpieczeństwa sieci wprowadzono dyrektywą Parlamentu Europejskiego i Rady z 25 listopada 2009 r. (Dyrektywa 2009). Artykuł 13a wspomnianego aktu stanowi, że państwa członkowskie UE zapewniają, aby przedsiębiorstwa udostępniające publiczne sieci łączności lub świadczące publicznie dostępne usługi łączności elektronicznej podejmowały właściwe środki techniczne i organizacyjne w razie wystąpienia zagrożenia dla bezpieczeństwa sieci lub usług. W szczególności chodzi tu o powiadamianie właściwego krajowego organu regulacyjnego o każdym naruszeniu bezpieczeństwa lub utracie integralności. Organ

ten może w uzasadnionych przypadkach zobowiązać przedsiębiorcę do upublicznienia takiej informacji.

Co więcej, zgodnie z linią wskazaną w dyrektywie o ochronie danych (Dyrektywa 1995) Dyrekcja Generalna Komisji Europejskiej ds. Sprawiedliwości i Konsumentów zawiadomiła o swoich planach wprowadzenia obowiązku informowania regulatora o przypadkach cyberataków, który miałby dotyczyć firm internetowych gromadzących i przetwarzających dane osobowe.

Implementacja takiego reżimu informacyjnego może spowodować, że przedsiębiorstwa w większym stopniu zaczną dostrzegać ryzyko szkód pośrednich wynikających z utraty danych osobowych kontrahentów – takich jak np. odpowiedzialność cywilna, utrata reputacji (ENISA 2012, s. 13).

Z punktu widzenia ubezpieczycieli rozszerzenie obowiązku informowania o incydentach naruszenia bezpieczeństwa danych może zniwelować asymetrię informacji, która jest jednym z najpoważniejszych wyzwań dla branży ubezpieczeniowej.

W Stanach Zjednoczonych Komisja Papierów Wartościowych i Giełd (SEC, Securities and Exchange Commission) od 2011 r. wymaga, by spółki giełdowe publikowały informacje o ekspozycji na ryzyko cybernetyczne, w szczególności dane o cyberatakach, ich częstotliwości i skali oddziaływania. Efektem tej regulacji był wzrost popytu na cyberubezpieczenia, co wobec interesariuszy spółki miało stanowić manifestację właściwej strategii zarządzania tym ryzykiem (ENISA 2012, s. 13).

6. Bariery rozwoju rynku ubezpieczeń cybernetycznych

W celu przeanalizowania barier rozwoju ubezpieczeń cybernetycznych wprowadzono rozróżnienie na czynniki popytowe (rozumiane jako zachowania klientów oraz uwarunkowania płynące z makrootoczenia) i podażowe (zależne od towarzystw ubezpieczeń).

6.1. Czynniki popytowe

Najważniejszą barierą po stronie popytowej jest niewłaściwa postawa właścicieli i zarządzających przedsiębiorstwami wobec zagrożenia cybernetycznego, co skutkuje niewystarczającym popytem na cyberpolisy.

Według badań *Allianz Risk Barometer 2015* cyberryzyko należy do zagrożeń najbardziej niedocenianych przez menadżerów ryzyka w przedsiębiorstwach na całym świecie[4] – 29% wskazań respondentów (Allianz 2015, s. 11). Większość zarządzających przedsiębiorstwami postrzega ryzyko cybernetyczne jako nieubezpie-

[4] Na kolejnych miejscach znalazły się zakłócenia w łańcuchu dostaw, katastrofy naturalne, terroryzm, przewroty polityczne.

czalne, mimo istnienia na rynku ubezpieczeń specjalistycznych produktów ochronnych (Marsh 2015a, s. 17). W świetle innych raportów, choć znaczna część (52%) przedsiębiorstw spodziewa się wzrostu ekspozycji na ryzyko cybernetyczne, 54% respondentów nie ma i nie planuje zakupu cyberubezpieczenia (Ponemon & AON 2015). Jednocześnie obserwuje się, że menadżerowie firm ubezpieczonych od ryzyka cybernetycznego zbyt optymistycznie oceniają zakres wykupionego pokrycia ubezpieczeniowego i są przeświadczeni, iż odszkodowanie ubezpieczeniowe zostanie wypłacone w przypadku każdej szkody cybernetycznej (Marsh 2015a, s. 17).

Zestawienie technik zarządzania ryzykiem stosowanych przez przedsiębiorstwa w odniesieniu do aktywów trwałych i zasobów informacyjnych prowadzi do wniosku, że ubezpieczonych jest 51% potencjalnych szkód zagrażających aktywom trwałym, a jedynie 28% podlega samoubezpieczeniu. W przypadku zasobów informacyjnych proporcje są odwrotne. Zatrzymanie cyberryzyka jest najczęściej stosowaną techniką (58% potencjalnych strat), ubezpieczenie zaś pokrywa zaledwie 12% szkód w dziedzinie IT (Ponemon & AON 2015).

Z badań sondażowych przeprowadzanych wśród kadry zarządzającej przedsiębiorstw (głównie na rynku amerykańskim) wyłania się następujący katalog przyczyn rezygnacji z nabycia ubezpieczenia cybernetycznego (Glascott, Aisen 2013):

- preferowanie inwestycji w techniczne środki bezpieczeństwa IT zamiast zakupu ubezpieczenia,
- brak odpowiedniej, kompleksowej oferty produktowej na rynku ubezpieczeń,
- niewystarczające przygotowanie merytoryczne brokerów ubezpieczeniowych,
- niezrozumienie korzyści płynących z cyberubezpieczenia,
- opinia o wysokim koszcie cyberubezpieczenia,
- obawa przed nadmiernymi komplikacjami na etapie wdrażania cyberubezpieczenia,
- brak akceptacji zbyt wysokich franszyz i udziałów własnych.

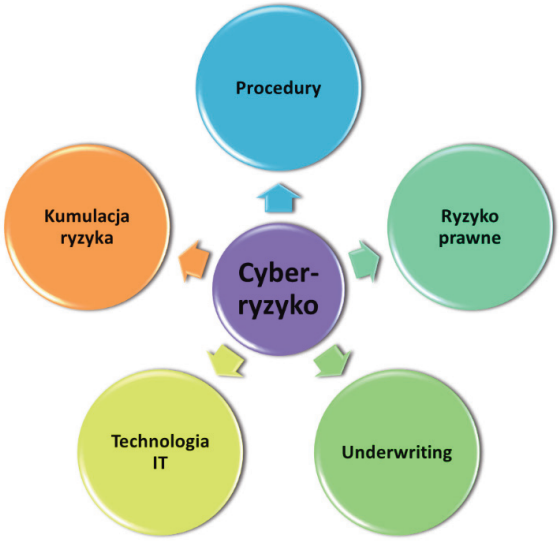
6.2. Czynniki podażowe

Towarzystwa ubezpieczeń są ostrożne przy wprowadzaniu do swojej oferty produktowej ubezpieczeń cybernetycznych, które nadal stanowią swego rodzaju nowość i słabo rozpoznane ryzyko. Z perspektywy techniczno-ubezpieczeniowej po stronie ubezpieczycieli można wskazać pięć obszarów problemowych, które wymagają rozwiązania, by umożliwić szybszy rozwój rynku cyberpolis (patrz rysunek 4):

- procedury (zakres informacji wymaganych przed zawarciem umowy ubezpieczenia, opracowanie uniwersalnych formularzy wniosków ubezpieczeniowych, organizacja procesu likwidacji szkód),
- ryzyko prawne (zgodność z przepisami prawa, orzecznictwo dotyczące naruszeń prywatności kształtujące wartość przyszłych roszczeń odszkodowawczych),

- underwriting (niedobór danych underwritingowych, wątpliwości wokół ubezpieczalności cyberryzyka, wysoki stopień asymetrii informacji),
- technologia IT (techniczny charakter ryzyka IT, dynamiczne zmiany profilu cyberryzyka i stale pojawiające się nowe aspekty tego ryzyka wymagające szybkiej reakcji towarzystw ubezpieczeń),
- ryzyko kumulacji szkód w wyniku wystąpienia jednego wypadku ubezpieczeniowego (prawdopodobny systemowy charakter cyberryzyka, co wymaga od ubezpieczycieli rygorystycznego stosowania ograniczonych limitów odpowiedzialności i wysokich udziałów własnych).

Rysunek 4
Obszary problemowe w techniczno-organizacyjnej obsłudze ubezpieczeń cybernetycznych przez ubezpieczycieli



Źródło: opracowanie własne.

Niedostatek danych underwritingowych skutkuje brakiem możliwości zróżnicowania składek i dostosowania ich do profilu ryzyka poszczególnych ubezpieczających. Według danych dla rynku brytyjskiego koszt polisy dla cyberryzyka (wyrażony jako wskaźnik Rate-on-Line, czyli relacja składki ubezpieczeniowej do limitu odpowiedzialności) jest trzykrotnie wyższy od polisy OC ogólnej i sześciokrotnie wyższy od ubezpieczenia mienia. Jeżeli dodać do tego informację, że zróżnicowanie składek dla poszczególnych nabywców ubezpieczeń cybernetycznych jest o wiele mniejsze niż w tradycyjnych produktach ubezpieczeniowych, wyłania się obraz ubezpieczenia cybernetycznego jako nowatorskiego i słabo rozpoznanego instrumentu transferu ryzyka z konserwatywną polityką underwritingową (Marsh 2015a, s. 22). W tym kontekście dużą wagę należy przywiązywać do

współpracy między branżą ubezpieczeniową i agendami rządowymi powołanymi do gromadzenia i analizowania danych o zagrożeniu cybernetycznym. W Polsce funkcję tę częściowo pełni, powołany w 2008 r. przy Agencji Bezpieczeństwa Wewnętrznego, Rządowy Zespół Reagowania na Incydenty Komputerowe (CERT).

Fundamentalną kwestią zasygnalizowaną powyżej jest wątpliwość co do tego, czy cyberryzyko spełnia kryteria ubezpieczalności ryzyka, które sformułował B. Berliner (1982). Do tego problemu odnieśli się w swoich badaniach Eling i Wirfs (2016), formułując następujące wnioski:

- Pozytywny wpływ prawa wielkich liczb na rozłożenie ryzyka w portfelach cyberpolis budowanych przez towarzystwa ubezpieczeń jest ograniczony ze względu na małą liczbę ubezpieczonych.
- Niedostatek danych historycznych oraz niepewność dotycząca doboru właściwego modelu rozkładu zmiennej losowej sprawiają, że towarzystwa ubezpieczeń są zmuszone do naliczania w składce wyższych narzutów bezpieczeństwa, a to z kolei obniża atrakcyjność cyberubezpieczeń dla klientów i skutkuje tym, że ich koszt jest zbyt wysoki.
- Dynamiczny charakter cyberryzyka powoduje, że dane historyczne o szkodach mogą być nieadekwatne do budowania prognoz na przyszłość.
- Poziom ryzyka cybernetycznego danego podmiotu jest w znacznym stopniu uzależniony od standardów bezpieczeństwa IT przyjętych u kooperantów, których komputery mogą stać się źródłem zainfekowania złośliwym oprogramowaniem niejako tylnymi drzwiami. Skutkiem tych współzależności jest brak pełnej kontroli nad poziomem ryzyka objętego ochroną ubezpieczeniową. Bezpieczeństwo informatyczne organizacji zależy bowiem nie tylko od podejmowanych przez nią działań prewencyjnych, ale także od zaawansowania systemów ochrony w podmiotach z nią współpracujących. Globalna sieć komputerowa to system naczyń połączonych, przy czym na wypadkowy poziom bezpieczeństwa największy wpływ ma najsłabsze ogniwo. Brakuje zatem wystarczająco silnych bodźców ekonomicznych do inwestowania w kontrolę ryzyka cybernetycznego, co z kolei często jest warunkiem ochrony ubezpieczeniowej stawianym przez towarzystwa ubezpieczeń.
- Istnieje wysokie prawdopodobieństwo trudnych do oszacowania zdarzeń katastroficznych.
- Rozkład strat spowodowanych cyberryzykiem może mieć zarówno kształt typu *short-tail*, jak i *long-tail*. Ten pierwszy przypadek będzie miał miejsce np. w razie zdarzeń takich jak atak DDoS, który momentalnie paraliżuje system informatyczny organizacji, jednak skutki tego incydentu są możliwe do usunięcia w ciągu kilku godzin. Z kolei licznymi szkodami skutkują np. wyłudzenia wspierane programami szpiegującymi (*malware*), które mogą pozostać niewykryte przez wiele miesięcy i generować straty finansowe w długim okresie. Podobnym rozkładem czasowym charakteryzują się roszczenia osób trzecich wnoszone z tytułu odpowiedzialności administratora danych za niezapewnienie bezpieczeństwa danych osobowych.

- Realizacja cyberryzyka może nieść negatywne skutki zarówno dla samego ubezpieczonego (*first-party losses*), jak i dla osób trzecich (*third-party losses*), co wiąże się z pewnymi utrudnieniami na etapie definiowania zakresu ochrony ubezpieczeniowej i przedmiotu ubezpieczenia,
- Niezwykle istotny jest również problem korelacji między cyberszkodami, które mogą być rezultatem jednej przyczyny. Oznacza to, że z dużym prawdopodobieństwem cyberryzyko nie spełnia wymogu niezależności zdarzeń.

W innych publikacjach zwraca się także uwagę na problem asymetrii informacji, co dla towarzystw ubezpieczeń oznacza zagrożenie selekcją negatywną i hazardem moralnym oraz motywacyjnym (Gordon *et al.* 2003).

Towarzystwa ubezpieczeń dążą do ograniczenia hazardu moralnego i motywacyjnego, nakładając na ubezpieczonych różnego rodzaju wymogi pełniące funkcje prewencyjne, takie jak regularne wykonywanie kopii zapasowych danych czy stosowanie zabezpieczeń systemów IT. Ponadto wyłączają swoją odpowiedzialność w razie stwierdzenia nieuczciwych lub przestępczych działań ubezpieczonego, a w razie wypadku korzystają z pomocy rzeczoznawców z zakresu informatyki śledczej. Powszechną praktyką są także stosunkowo wysokie udziały własne w szkodzie.

7. Stan rynku ubezpieczeń cybernetycznych

Pierwsze polisy ubezpieczeniowe ukierunkowane na cyberryzyko pojawiły się pod koniec lat 90. XX w. w związku z tzw. pluskwą millenijną (tj. problemem, który mógł się pojawić w komputerach po wystąpieniu daty systemowej z rokiem 2000). Wtedy też po raz pierwszy uświadomiono sobie skalę utrudnień, które mogą wystąpić w gospodarce w razie awarii systemów komputerowych. Te pierwsze cyberpolisy ubezpieczenia mienia lub odpowiedzialności cywilnej miały bardzo ograniczony zakres pokrycia. Drugi etap rozwoju ubezpieczeń cybernetycznych rozpoczęło wprowadzenie prawnej ochrony poufności danych osobowych. Ich zakres obejmował koszty wynikające z niekontrolowanego wycieku zastrzeżonych informacji. Trzeci etap trwa obecnie i cechuje się wzrostem świadomości cyberzagrożeń, zwłaszcza poza Stanami Zjednoczonymi. Ubezpieczenia cybernetyczne zyskują coraz szerszy zakres, a także postępuje ich standaryzacja (Allianz 2015).

Zdaniem Kesana *et al.* (2005) do powstania cyberubezpieczeń przyczyniły się trzy czynniki:

1) proliferacja zagrożeń cybernetycznych,
2) nieadekwatność klasycznych ubezpieczeń majątkowych do nowych zagrożeń w cyberprzestrzeni,
3) unormowania prawne w zakresie odpowiedzialności za szkody związane z przetwarzaniem danych osobowych (zwłaszcza dopuszczenie do ich ujawnienia).

Według szacunków Allianz (2015, s. 5) łączna wartość światowego rynku ubezpieczeń cybernetycznych wynosi 2 mld USD, z czego na USA przypada

90% tej kwoty. Prognozuje się jednak wysokie, dwucyfrowe tempo wzrostu, tak że w ciągu kolejnych 10 lat rynek ten będzie generował ponad 20 mld USD składek. Lwią część tego wzrostu mają wypracować małe i średnie przedsiębiorstwa.

Amerykański rynek cyberubezpieczeń charakteryzuje się następującymi trendami:

- wysokie jest tempo wzrostu przypisu ubezpieczeń w formie polisy *stand-alone* (25–30% rocznie),
- cyberpolisy są obecne w ofercie około 60 towarzystw ubezpieczeń,
- pojemność ubezpieczeniowa dostępna na rynku amerykańskim wydaje się przekraczać zapotrzebowanie generowane przez stronę popytową (pojemność ubezpieczeniowa waha się od 200 do 500 mln USD w zależności od towarzystwa),
- w ślad za zwiększeniem świadomości ubezpieczeniowej przedsiębiorstw w zakresie ochrony przed skutkami cyberryzyka rosną ich wymagania wobec nabywanych polis ubezpieczeniowych, zarówno w aspekcie warunków ochrony, jak i – przede wszystkim – wysokości limitów odpowiedzialności (wzrost przeciętnej sumy ubezpieczenia w 2015 r. o 15% porównaniu do 2014 r.),
- w 2015 r. zaobserwowano pierwsze symptomy „twardnienia rynku" (*hard market*), takie jak wzrost stawek średnio o 19% i zaostrzenie polityki underwritingowej (zwłaszcza wobec branż ochrony zdrowia i handlu), co nastąpiło w wyniku wzrostu wskaźnika szkodowości.

Poza Stanami Zjednoczonymi cyberubezpieczenia rozwijają się w Europie i w Japonii (rysunek 5), a także innych krajach wysoko uprzemysłowionych (Kanada, Australia).

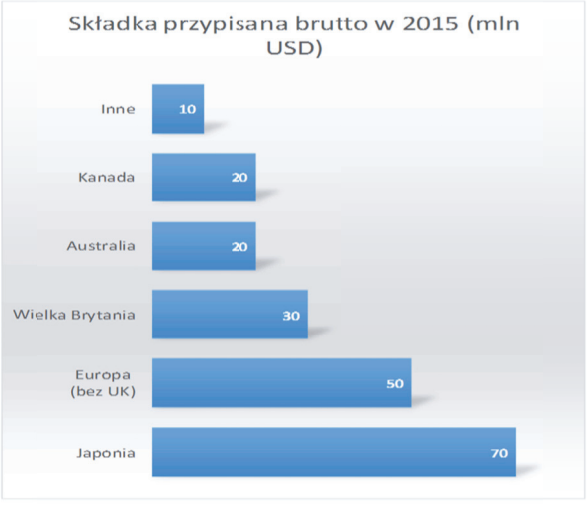
Badania przeprowadzone przez firmę Marsh wśród europejskich przedsiębiorstw pokazały, że skala wykorzystania cyberubezpieczeń na Starym Kontynencie jest dużo niższa w porównaniu z USA. Jedynie 12% respondentów ma cyberubezpieczenie, 6% jest w trakcie zawierania takie umowy, a 27% planuje zakupić cyberpolisę w ciągu najbliższego roku. Oznacza to, że aż 55% ankietowanych nie widzi potrzeby zakupu tego typu ochrony. To dość zastanawiające dane. Jednocześnie aż 57% spośród tych, którzy nie mają cyberubezpieczenia, przyznaje, że głównym powodem tego braku jest niedostateczna wiedza o produktach chroniących przed ryzykiem cybernetycznym. Można to odczytać jako ogromne wyzwanie dla towarzystw ubezpieczeń i brokerów ubezpieczeniowych, aby rzetelnie edukować oraz informować swoich klientów (Marsh 2015a).

W okresie 2009–2013 cyberubezpieczenia były najszybciej rozwijającą się linią produktów majątkowych w skali globalnej, osiągając średnioroczne tempo wzrostu składki przypisanej równe 38%. Znacząco wolniej rosły ubezpieczenia: ryzyk politycznych – 20%, finansowe – 16%), OC za produkt – 13%), lotnicze – 9% (AON 2014, s. 11).

Allianz wskazuje 5 głównych trendów ewolucji cyberubezpieczeń w perspektywie krótko- i średnioterminowej (Allianz 2015, s. 18):

1) dojdzie do stopniowego ograniczenia zakresu pokrycia cyberryzyka w klasycznych polisach ubezpieczeniowych przy równoczesnym wzroście dostępności specjalistycznych ubezpieczeń cybernetycznych, zwłaszcza w obszarze odpowiedzialności cywilnej,
2) zostanie zweryfikowana adekwatność pokrycia ubezpieczeniowego w zderzeniu z pojawiającymi się roszczeniami osób poszkodowanych i roszczeniami odszkodowawczymi,
3) wzrost penetracji ubezpieczeń cybernetycznych pozwoli ubezpieczycielom na segmentację klientów i zaoferowanie produktów lepiej dopasowanych do specyficznych potrzeb różnych podmiotów,
4) nastąpi pogłębienie świadomości ubezpieczeniowej wśród przedsiębiorców, a jednocześnie poprawi się znajomość cyberryzyka w towarzystwach ubezpieczeń,
5) będą doskonalone metody reagowania na kryzys spowodowany incydentem informatycznym, co powinno skutkować ograniczeniem rozmiarów szkód.

Rysunek 5
Przypis składki z tytułu ubezpieczeń cybernetycznych w 2015 r. (mln USD)



Źródło: opracowanie własne na podstawie Newman (2016).

Ze względu na brak danych nie sposób określić stopnia rozwoju polskiego rynku ubezpieczeń cybernetycznych. Bez wątpienia znajduje się on w stadium początkowym, które charakteryzuje się ograniczonym popytem oraz niewielką liczbą towarzystw oferujących cyberpolisy[5]. Nie wiadomo, jaką wartość składki

[5] Według wiedzy autora cyberpolisy w Polsce są dostępne u pięciu ubezpieczycieli (ACE, AIG, Allianz, Ergo Hestia, Leadenhall).

pozyskano ze sprzedaży tych ubezpieczeń. Z wywiadów przeprowadzonych z brokerami ubezpieczeniowymi przez autora niniejszego tekstu wynika, że ubezpieczenia cyberryzyka najczęściej są kupowane przez instytucje finansowe (głównie banki) oraz firmy prowadzące działalność w segmencie technologii IT.

Podsumowanie

Rozprzestrzenianie się ryzyka cybernetycznego skłania przedsiębiorców, rządy, wymiar sprawiedliwości, informatyków oraz konsumentów do dokładniejszego przyjrzenia się naturze tego ryzyka i jego możliwym konsekwencjom. Powoli rośnie świadomość potrzeby posiadania ubezpieczenia cybernetycznego, choć z punktu widzenia towarzystw ubezpieczeń underwriting i konstrukcja tego produktu nie należą do najprostszych. Główne problemy techniczne wynikają z braku danych historycznych, ryzyka kumulacji strat, trudności zdefiniowania przedmiotu ubezpieczenia i jego ekspozycji na ryzyko (możliwy krąg sprawców i celów cyberataków, ocena wartości przedmiotu ubezpieczenia).

Zdaniem ekspertów odpowiednie procedury zarządzania ryzykiem informatycznym, a zwłaszcza kontrola tego ryzyka mogą zredukować ryzyko cyberataków o 80% (Allianz 2015, s. 14). Oznacza to, że nadal istnieje pewne ryzyko rezydualne, którego sfinansowanie jest możliwe w drodze zakupu cyberubezpieczenia. Dostarczanie zaawansowanych rozwiązań w zakresie cyberryzyk stanie się bez wątpienia jednym z najważniejszych zadań branży ubezpieczeniowej nie tylko w Polsce, ale i na świecie.

Rozwój ubezpieczeń cybernetycznych leży w interesie nie tylko poszczególnych przedsiębiorstw i instytucji, ale także całej gospodarki. Kesan *et al.* (2005) dowodzą, że stosowanie cyberubezpieczeń daje w skali makrospołecznej trzy istotne korzyści:

- wzrost inwestycji w bezpieczeństwo IT,
- stymulowanie tworzenia kodeksu dobrych praktyk w obszarze zarządzania ryzykiem cybernetycznym,
- podniesienie ogólnego poziomu zamożności społeczeństwa.

Z uwagi na skalę zagrożenia i jego powszechność zasadne wydaje się rozważenie wprowadzenia w przyszłości obowiązku ubezpieczenia ryzyk cybernetycznych, przynajmniej w zakresie odpowiedzialności cywilnej.

Perspektywy rozwoju cyberubezpieczeń, mimo istniejących barier, są optymistyczne. Swiss Re postawiło wręcz odważną hipotezę, iż do 2025 r. cyberryzyko znajdzie się w standardowym zakresie ochrony wszystkich ubezpieczeń dla przedsiębiorstw (III 2015, s. 21).

Wbrew optymistycznym perspektywom rozwoju ubezpieczeń cybernetycznych w najbliższych latach agencja ratingowa Fitch przestrzega towarzystwa ubezpieczeń przed nadmiernym zaangażowaniem w tę linię biznesu. Niewystarczająca ilość danych historycznych o cyberryzyku oznacza zwiększoną niepewność odnośnie do

underwritingu, kształtowania warunków ochrony, ekspozycji na ryzyko czy nawet polityki rezerw techniczno-ubezpieczeniowych. Te wszystkie bariery sprawiają, że nadmierna rozbudowa portfela ubezpieczeń cybernetycznych może skutkować obniżeniem ratingu ubezpieczyciela (Fitch 2016).

Bibliografia

Allianz, *A guide to cyber risk. Managing the impact of increasing interconnectivity*, 2015, www.agcs.allianz.com (data dostępu 12.11.2015).

AON, *Exploring the latest cyber risk trends in EMEA*, 2014, www.aon.com (data dostępu 14.11.2015).

Berliner, B., *Limits of insurability of risks*, Prentice-Hall, Englewood Cliffs 1982.

Böhme, R., Kataria, G., *Models and measures for correlation in cyber-insurance*, Working Paper, Workshop on the Economics of Information Security (WEIS), University of Cambridge, 2006, http://www.econinfosec.org/archive/weis2006/docs/16.pdf (data dostępu 12.04.2016).

Cebula, J.J., Young, L.R., *A taxonomy of operational cyber security risks*, Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University, 2010.

CERT, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014*, Rządowy Zespół Reagowania na Incydenty Komputerowe, marzec 2015, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html (data dostępu 11.01.2016).

Dyrektywa 95/49/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. UE L 281/31 z 23.11.1995).

Dyrektywa 2009/140/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r. (Dz.U. UE L 337/37 z 18.12.2009).

Eling, M., Wirfs, J.H., *Cyber risk: Too big to insure?*, University of St. Gallen, 2016, http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf (data dostępu 15.04.2016).

ENISA, *Incentives and barriers of the cyber insurance market in Europe*, Europejska Agencja ds. Bezpieczeństwa Sieci I Informacji, 2012, www.enisa.europa.eu (data dostępu 10.11.2015).

Fitch, *Fitch: Rapid Growth in Cyber Insurance Would Be Credit-Negative*, Fitch Ratings, 21.03.2016, https://www.fitchratings.com/site/fitch-home/pressrelease?id=1001233 (data dostępu 31.03.2016).

Glascott, M.T., Aisen, A.J., *The emperor's new clothes and cyber insurance*, Federation of Defense & Corporate Counsel Quarterly, wiosna 2013, http://www.thefederation.org/documents/22.The%20Emperors%20New%20Clothes.pdf (3.05.2016).

Gordon, L.A., Loeb, M.P., Sohail, T., *A framework for using insurance for cyber-risk management*, "Communications of the ACM" 2013, 44(9).

III, *Cyber risk: Threat and opportunity*, Insurance Information Institute, październik 2015, http://www.iii.org/sites/default/files/docs/pdf/cyber_risk_wp_final_102015.pdf (data dostępu 22.02.2016).

ITRC, *ITRC data breach reports December 31, 2015*, Identity Theft Resource Center, kwiecień 2016, http://techorchard.com/wp-content/uploads/2016/04/DataBreachReports_2015.pdf (data dostępu 2.05.2016).

Kesan, J.P., Majuca, R.P., Yurcik, W., *Cyber insurance as a market-based solution to the problem of cybersecurity – case study*, Proceedings of Workshop on the Economics of Information Security, Harvard, MA, czerwiec 2005.

Lloyd's, *Managing digital risk. Trends, issues and implications for business*, 2010, www.lloyds.com (data dostępu 8.11.2015).

Marsh, (2015a), *European 2015 cyber risk survey report*, październik 2015, http://uk.marsh.com/Portals/18/Documents/European%202015%20Cyber%20Risk%20Survey%20Report-10-2015.pdf (data dostępu 11.04.2016).

Marsh, (2015b), *UK cyber security. The role of insurance in managing and mitigating the risk*, 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf (data dostępu 12.01.2016).

McAfee, *McAfee Labs threats report*, marzec 2016, http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2016.pdf (data dostępu 24.04.2016).

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., Sadhukhan, S., *Cyber-risk decision models: To insure IT or not?*, Decision Support Systems, kwiecień 2013, http://dx.doi.org/10.1016/j.dss.2013.04.004.

NAIC, *Cybersecurity*, National Association of Insurance Commissioners, 25.01.2016, http://www.naic.org/cipr_topics/topic_cyber_risk.htm (data dostępu 22.05.2016).

Newman, G., *Cyber Market Overview: Product, Pricing & Positioning*, CFC Underwriting, 14.04.2016, London.

Ögűt, H., Raghunathan, S., Menon, N., *Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection*, Risk Analysis 2011, 31(3), doi: 10.1111/j.1539-6924.2010.01478.x.

Podolak, G.D., *Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow 's Challenges*, Quinnipiac Law Review 2015, t. 33.

Ponemon & AON, *2015 Global Cyber Impact Report*, kwiecień 2015, http://www.aon.com/attachments/risk-services/2015-Global-Cyber-Impact-Report-Final.pdf (data dostępu 12.12.2015).

Słowa kluczowe: ubezpieczenia cybernetyczne, cyberryzyko, zarządzanie ryzykiem, bezpieczeństwo cybernetyczne

Cyber risk as a challenge for the polish and global insurance market

Summary

The problem of cyberattacks may seem distant in Poland. Although most entrepreneurs operating in Poland are aware of the existence of such threats, few of them undertake actions aimed at managing cyber risk, also through the purchase of specialist cyber insurance. Cybercrime can be described as the most serious challenge the insurance industry has faced in the last half-century. It reminds systemic risk, the source of which is the use of information technology and electronic data processing. Among the factors driving the development of the cyber-insurance market are the growing need for privacy in global society, large-scale cyber-attacks, legal regulations that impose high financial fines for data breaches, strive to minimize financial consequences of cyber attacks, potential damage to reputation resulting from cyber incident. The purpose of this article is to identify cyber risk, assess the degree of cyber threat, and analyze the degree of development of the cyber insurance market. The most serious difficulties in operating cyber insurance from the point of view of insurance companies have been indicated.

Keywords: cyber insurance, cyber risk, risk management, cyber security