Rozprawy Ubezpieczeniowe. Konsument na rynku usług finansowych nr 24 (2/2017): 65-83
Journal of Insurance, Financial Markets and Consumer Protection No. 24 (2/2017): 65-83

Zagrożenia cybernetyczne instytucji finansowych

Grzegorz STRUPCZEWSKI[1]
Uniwersytet Ekonomiczny w Krakowie,
Katedra Zarządzania Ryzykiem i Ubezpieczeń

Streszczenie. Celem artykułu jest analiza ryzyka cybernetycznego z perspektywy instytucji finansowych, a także wskazanie możliwości zastosowania ubezpieczeń cybernetycznych jako narzędzia minimalizującego finansowe skutki realizacji tego ryzyka. W pracy wykorzystano specjalistyczne raporty branżowe, w większości anglojęzyczne, publikowane zarówno przez instytucje rynku ubezpieczeń, jak i przez podmioty monitorujące bezpieczeństwo IT. Niniejszy tekst składa się z sześciu części. Na początek przedstawiono definicję oraz rodzaje ryzyka cybernetycznego. Następnie zobrazowano skalę zagrożenia cybernetycznego na świecie, posługując się danymi opracowanymi przez wyspecjalizowane ośrodki badawcze oraz instytucje otoczenia biznesu ubezpieczeniowego. Tematem rozważań w trzeciej części opracowania stała się specyfika ekspozycji na ryzyko cybernetyczne instytucji finansowych. W kolejnym punkcie dokonano syntetycznej analizy rynku ubezpieczeń cybernetycznych w USA i Europie, by w końcu przejść do charakterystyki ubezpieczeń cybernetycznych oferowanych w Polsce. W podsumowaniu sformułowano konkluzje wynikające z treści artykułu.

Słowa kluczowe: cyberryzyko, ryzyko cybernetyczne, cyberubezpieczenia, instytucje finansowe.
Kody JEL: G22, G200.

1. Wprowadzenie

Gospodarka internetowa odpowiada za ponad jedną piątą wzrostu PKB w UE, a każdego roku w sieci robi zakupy 200 mln Europejczyków. Jesteśmy 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.

[1] Kontakt z autorem: Grzegorz Strupczewski, Uniwersytet Ekonomiczny w Krakowie, Katedra Zarządzania Ryzykiem i Ubezpieczeń, ul. Rakowicka 27, 31-510 Kraków, Polska, e-mail: strupczg@uek.krakow.pl. Publikacja została sfinansowana ze środków przyznanych Wydziałowi Finansów i Prawa Uniwersytetu Ekonomicznego w Krakowie w ramach dotacji na utrzymanie potencjału badawczego.

Ataki cybernetyczne mają poważny wpływ zarówno na poszczególne przedsiębiorstwa, jak i szeroko rozumianą gospodarkę. Według raportu Europejskiego Komitetu Ekonomiczno-Społecznego każdego roku na całym świecie ofiary cyberataków tracą około 290 mld euro, co oznacza, że przestępczość ta jest bardziej dochodowa od światowego handlu marihuaną, kokainą i heroiną łącznie [EKES 2014]. Według innych szacunków roczny koszt cyberprzestępczości dla światowej gospodarki wynosi od 400 mld USD [McAfee 2016] do 445 mld USD [III 2015]. Zgodnie z zauważalną tendencją z każdym kolejnym rokiem globalna skala cyberprzestępczości jest coraz wyższa.

Raport Światowego Forum Gospodarczego na temat ryzyk globalnych [WEF 2014] umiejscowił cyberryzyko wśród pięciu najważniejszych rodzajów ryzyka pod względem prawdopodobieństwa wystąpienia. Według raportu *Allianz Risk Barometer Survey 2015* ryzyko cybernetyczne awansowało na piąte miejsce w zestawieniu dziesięciu największych globalnych ryzyk dla biznesu [III 2015]. W 2014 r. na świecie ujawniono prawie 43 mln cyberataków, co oznacza, że dziennie dochodzi średnio do 117 339 incydentów [Allianz 2015]. Oznacza to również, iż co trzecie przedsiębiorstwo na świecie doświadczyło incydentu naruszenia bezpieczeństwa danych lub poważnej awarii systemu komputerowego. Zdaniem menadżerów ryzyka najbardziej prawdopodobnym źródłem krytycznego zagrożenia dla ich organizacji będzie w przyszłości właśnie cyberryzyko. Wymaga to podjęcia skutecznych działań zapobiegawczych już teraz. Dlatego w opinii większości (77%) menadżerów ryzyka zarządzanie ryzykiem cybernetycznym będzie tym obszarem, na który w największym stopniu wzrosną nakłady w przedsiębiorstwach w perspektywie najbliższych dwóch lat [Marsh 2016].

Choć cyberryzyko stało się już powszechne, to jednak ekspozycja na ryzyko i przebieg incydentów naruszenia bezpieczeństwa informatycznego są różne w zależności od branży, w której działa dane przedsiębiorstwo. Sprawcy cyberataków zwykle kierują swoje działania przeciwko tym organizacjom, które dysponują bogatymi zbiorami informacji, takich jak dane klientów, kontrahentów lub pracowników. Instytucje finansowe, a zwłaszcza banki, są zatem doskonałym celem dla przestępców. Potwierdzają to zresztą liczne dane. Przykładowo, obserwuje się ponadprzeciętną częstość incydentów w usługach finansowych: 3,7 zdarzenia na 1000 podmiotów, podczas gdy średnia wynosi 2,4 zdarzenia. Wyższą częstość incydentów wykazuje tylko administracja publiczna (5,0). W bazie ponad 21 tys. incydentów cybernetycznych na całym świecie, tworzonej od 2004 r. (baza Advisen Cyber), zdarzenia w branży usług finansowych stanowią 18% wszystkich rekordów. Oznacza to, że jest to druga – po usługach (47%) – z najczęściej atakowanych branż gospodarki [Ayers 2015].

Zarządzenie bezpieczeństwem w cyberprzestrzeni to bez wątpienia temat istotny dla działów informatyki (IT), ale nie jest to zagadnienie tylko o charakterze technicznym. Mimo stale rosnących wydatków na bezpieczeństwo IT nie jest możliwe wyeliminowanie cyberryzyka w pełni. Dlatego można powiedzieć, że istnieje nisza rynkowa dla cyberubezpieczeń.

W Stanach Zjednoczonych wytyczne Komisji Papierów Wartościowych SEC zalecają, aby firmy z sektora usług finansowych zawierały umowy ubezpieczenia przed cyberryzykiem w ramach skutecznej strategii zarządzania nim. W Polsce takie rozwiązanie dopuszcza także KNF w *Rekomendacji D* dotyczącej zarządzania obszarem IT i bezpieczeństwem środowiska teleinformatycznego w bankach[2] [PWC 2014].

W Stanach Zjednoczonych i Wielkiej Brytanii ubezpieczenia cybernetyczne należą do najszybciej rosnących w segmencie ubezpieczeń specjalistycznych. W Polsce ubezpieczenia cybernetyczne są w początkowym stadium rozwoju, a prace naukowe dotyczące tej problematyki należą do rzadkości.

Celem artykułu jest analiza ryzyka cybernetycznego z perspektywy instytucji finansowych, a także wskazanie możliwości zastosowania ubezpieczeń cybernetycznych jako narzędzia minimalizującego finansowe skutki realizacji tego ryzyka.

W pracy wykorzystano specjalistyczne raporty branżowe, w większości anglojęzyczne, publikowane zarówno przez instytucje rynku ubezpieczeń, jak i przez podmioty monitorujące bezpieczeństwo IT. W rezultacie powstało opracowanie interdyscyplinarne, poruszające ważny i aktualny, a jednocześnie mało znany w Polsce problem, jakim jest zagrożenie cybernetyczne i możliwości jego ubezpieczenia.

Niniejszy artykuł składa się z pięciu części. Na początek przedstawiono definicję oraz rodzaje ryzyka cybernetycznego. Następnie zobrazowano skalę zagrożenia cybernetycznego na świecie na podstawie danych opracowanych przez wyspecjalizowane ośrodki badawcze oraz instytucje otoczenia biznesu ubezpieczeniowego. Tematem rozważań w trzeciej części opracowania stała się specyfika ekspozycji na ryzyko cybernetyczne instytucji finansowych. W kolejnym punkcie dokonano syntetycznej analizy rynku ubezpieczeń cybernetycznych w Stanach Zjednoczonych i Europie, by w końcu przejść do podsumowania, w którym sformułowano konkluzje wynikające z treści artykułu. Szczególną uwagę poświęcono identyfikacji szans i barier rozwoju rynku ubezpieczeń cybernetycznych w Polsce.

2. Pojęcie i systematyka ryzyka cybernetycznego

Cyberryzyko jest zwykle mylnie utożsamiane wyłącznie z zainfekowaniem komputera przez hakerów złośliwym oprogramowaniem (ang. *malware*). Choć jest to często spotykanym przejawem ryzyka cybernetycznego, nie można zapominać o innych, równie groźnych incydentach.

Jak dotąd nie powstała jedna spójna, powszechnie uznawana definicja ryzyka cybernetycznego. Problem z ujęciem tego zjawiska w sformalizowane ramy definicyjne może wynikać z jego interdyscyplinarnego charakteru, a także z ciągłego procesu ewolucyjnego związanego z postępem technicznym.

[2] „Bank powinien podejmować stosowne decyzje dotyczące podejścia do poszczególnych zagrożeń, polegające na […] transferze ryzyka, tj. przeniesieniu części lub całości ryzyka związanego z danym zagrożeniem na podmiot zewnętrzny, w szczególności poprzez […] stosowanie ubezpieczeń" – rekomendacja 18 *System zarządzania bezpieczeństwem środowiska teleinformatycznego*, *Rekomendacja D*, KNF, styczeń 2013.

Ryzyko cybernetyczne (cyberryzyko) można ująć jako ryzyko gospodarcze związane z posiadaniem, działaniem, wykorzystaniem i oddziaływaniem urządzeń i technologii IT w przedsiębiorstwie [Marsh 2015b]. Zdaniem Podolak [2015] ryzyko cybernetyczne obejmuje wszelkie sytuacje narażenia na potencjalne straty w wyniku używania sprzętu elektronicznego, komputerów oraz przetwarzania informacji w wirtualnej rzeczywistości. Zatem cyberryzyko może być zaliczone do grupy ryzyk operacyjnych o charakterze antropogenicznym.

Z kolei Europejska Agencja ds. Bezpieczeństwa Informatycznego (ENISA) podaje, że cyberprzestępstwo obejmuje rozmaite działania, które bezpośrednio wpływają zarówno na pojedyncze osoby (np. kradzież tożsamości), jak i na przedsiębiorstwa (np. kradzież własności intelektualnej) [ENISA 2012].

Jedną z form cyberprzestępstwa może być atak cybernetyczny. Jest on rozumiany jako wszelkiego rodzaju szkodliwe działanie, którego celem są komputerowe systemy informatyczne, infrastruktura, sieci komputerowe i osobiste urządzenia cyfrowe, prowadzone za pomocą różnego rodzaju czynów dokonywanych w zamiarze kradzieży, zmiany lub zniszczenia określonego celu. Celem mogą być pieniądze, dane lub technologie informacyjne.

Jeżeli celem ataku cybernetycznego są dane osobowe lub poufne dane handlowe, mówimy o tzw. incydencie naruszenia ochrony danych (ang. *data breach*). Zgodnie z art. 4 ogólnego rozporządzenia o ochronie danych[3] oznacza on naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób.

Najczęściej spotykaną klasyfikacją ryzyka cybernetycznego jest jego podział ze względu na kryterium rodzaju 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 działania niecelowe (przypadkowe) [CERT 2015]. Wśród działań celowych wyróżnia się:

– iniekcja 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),

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119/1 z dnia 4 maja 2016 r.).

– 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).

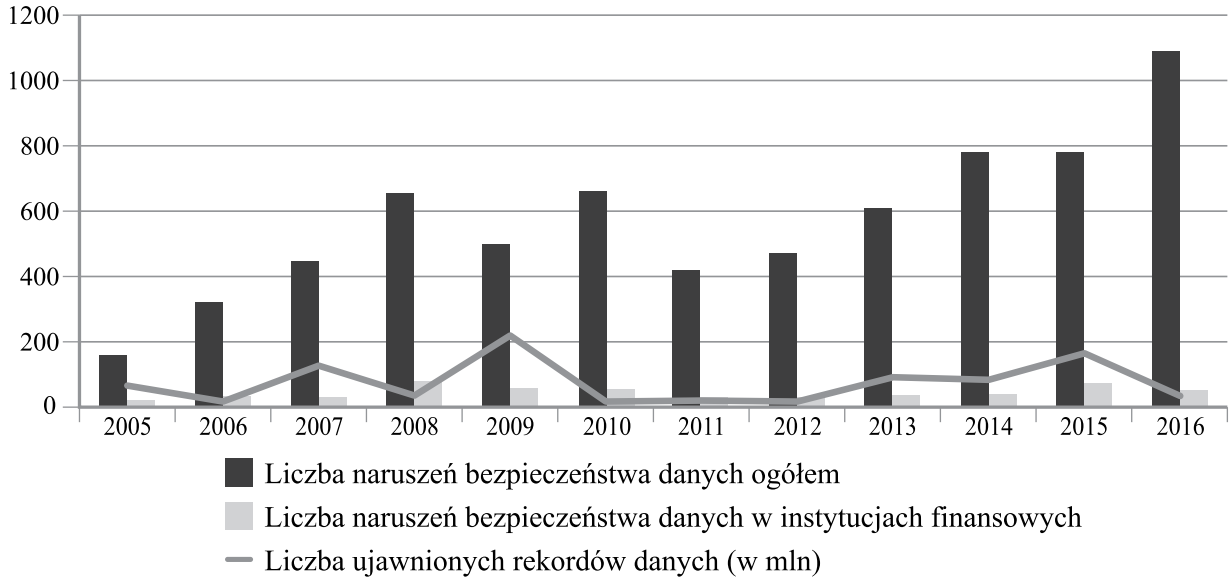
Autorami wrogich ataków cybernetycznych mogą być różne podmioty, między innymi: cyberprzestępcy, aktywiści (tzw. haktywiści), konkurencyjne przedsiębiorstwa, wrogie państwa, terroryści, byli lub obecni pracownicy. Każdym atakującym mogą kierować inne motywy, niekiedy bardzo indywidualne, jednak próbując dokonać choćby wstępnej klasyfikacji, wskazuje się następujące typowe przesłanki cyberataków: wojna, terroryzm, wroga propaganda, zdobycie przewagi konkurencyjnej, bezpośrednia korzyść finansowa, demonstracja siły, zemsta lub akt protestu [Marsh 2015b].

3. Skala globalnego zagrożenia cybernetycznego

Ośrodek badawczy Identity Theft Resource Center (ITRC) gromadzi dane dotyczące wypadków naruszenia bezpieczeństwa prywatnych danych na rynku amerykańskim. Według najnowszych danych rok 2016 był rekordowy pod względem liczby incydentów informatycznych, która ukształtowała się na poziomie 1093 (patrz wykres 1). Jeśli chodzi o liczbę wykradzionych danych, rok 2015 był drugi w ciągu ostatnich dziesięciu lat – z liczbą 169,1 mln ukradzionych rekordów z danymi osobowymi ustąpił jedynie miejsca 2009 r., kiedy to ujawniono bezprawnie 222,5 mln rekordów [ITRC 2017]. Od 2011 r. zaobserwować można wyraźny trend wzrostowy ogólnej liczby naruszeń bezpieczeństwa danych raportowanych w Stanach Zjednoczonych. Można to tłumaczyć zmianami prawodawstwa federalnego i stanowego w zakresie obowiązku notyfikacji przypadków naruszeń poufności danych przez administratorów danych, a ponadto wzrostem zainteresowania problematyką cyberbezpieczeństwa. Z kolei niski udział instytucji finansowych w ogólnej liczbie naruszeń poufności danych można tłumaczyć wysokim stopniem zaawansowania stosowanych narzędzi bezpieczeństwa IT w tych podmiotach.

W niektórych przypadkach jeden udany atak hakerski na przedsiębiorstwo może skutkować uzyskaniem nielegalnego dostępu nawet do kilku milionów rekordów danych, czego doświadczyły w szczególności duże sieci handlowe lub instytucje finansowe (banki, systemy płatności elektronicznych, towarzystwa ubezpieczeń).

Wykres 1. Liczba wypadków naruszenia ochrony danych w USA



Źródło: opracowanie własne na podstawie danych [ITRC 2017].

W tabeli 1 zebrano największe w historii incydenty naruszenia bezpieczeństwa danych, uszeregowane według kryterium liczby danych osobowych.

Tabela 1. Największe incydenty naruszenia bezpieczeństwa danych

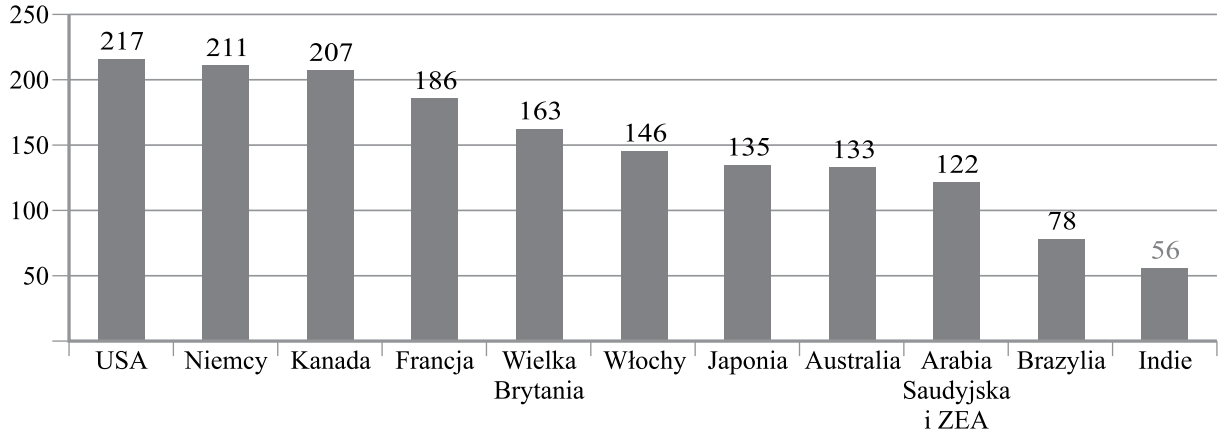
Nazwa firmy	Rok ataku	Liczba wykradzionych rekordów danych
Heartland Payment Systems	2009	130 000 000
TJ Max Stores	2007	100 000 000
Anthem	2015	80 000 000
U.S. Military Veterans	2009	76 000 000
Home Depot	2014	56 000 000
Target Corp.	2013	40 000 000
U.S. Department of Veterans Affairs	2006	26 500 000
Office of Personnel Management	2015	21 500 000
Bank of New York Mellon	2008	12 500 000
Sony, Playstation Network	2011	12 000 000
Fidelity National Information Service	2007	8 500 000
Global Payments Inc.	2012	7 000 000

Źródło: opracowanie własne.

Na świecie, w tym także w Polsce, dostrzega się wyraźny wzrost dynamiki ataków. Atakującymi są nie tylko pojedyncze osoby, ale też wysoko wyspecjalizowane grupy, które wykorzystują zaawansowane technologie i wektory ataku. Cyberprzestępcy wciąż mogą pochwalić się wysoką skutecznością w Polsce, m.in. ze względu na nieodpowiednie podejście instytucji do kwestii bezpieczeństwa systemów, a także redukcję wydatków na IT kosztem bezpieczeństwa [CERT 2015].

Eling i Wirfs [2016] analizowali statystyczne własności cyberryzyka, czerpiąc dane z globalnej bazy ryzyk operacyjnych (SAS OpRisk Global Data) zawierającej ponad 26 tys. zarejestrowanych przypadków szkód zaistniałych w latach 1995–2014. Na początek ustalili, że zdarzenia spełniające przesłanki zakwalifikowania ich jako cyberryzyko stanowiły 5,9% wszystkich incydentów w bazie. Następnie przebadali strukturę geograficzną cyberataków. Okazało się, że ponad połowa cyberataków (52,6%) miała miejsce w firmach zarejestrowanych w Ameryce Północnej, a co czwarty atak hakerski (24,9%) wydarzył się w Europie. Patrząc globalnie, trzy na cztery wypadki cybernetyczne dotknęły instytucje finansowe, a pozostałe 25% – podmioty z sektora niefinansowego. Ważnym czynnikiem różnicującym skalę zagrożenia cybernetycznego okazała się wielkość firmy. W przedsiębiorstwach dużych, tj. zatrudniających ponad 250 osób, wystąpiło 87% wszystkich wypadków, a w firmach małych i średnich odsetek incydentów był podobny i wyniósł nieco ponad 4%.

Wykres 2. Przeciętny koszt naruszenia ochrony danych osobowych per capita w przekroju terytorialnym (w USD)



Źródło: [Ponemon Institute 2015].

Jak podaje Ponemon Institute [2015], istnieją znaczne różnice w przeciętnym koszcie naruszenia bezpieczeństwa danych (ang. *data breach*) *per capita* w różnych branżach gospodarki. Jeżeli średni koszt *per capita* wynosi 154 USD, to w sektorach ochrony zdrowia i edukacji wskaźnik ten jest w przybliżeniu dwukrotnie wyższy (odpowiednio 363 USD i 300 USD). Instytucje finansowe (215 USD) również zaliczają się do sektorów gospodarki o ponadprzeciętnym koszcie naruszenia ochrony danych. Najniższy koszt jednostkowy ujawnienia danych odnotowano w instytu-

cjach publicznych (68 USD). Warto jeszcze dodać, iż o ile w większości przypadków przeciętne koszty jednostkowe nie ulegają zmianom na przestrzeni lat, o tyle w sektorze handlu detalicznego zaobserwowano drastyczny wzrost kosztów z 105 USD w 2014 r. do 165 USD w 2015 r. Jest to wynikiem zainteresowania mediów przypadkami ataków hakerskich na sieci sklepów detalicznych, co przekłada się na potrzebę ponoszenia wyższych nakładów na zarządzanie takimi sytuacjami kryzysowymi. Koszty związane w wyciekiem poufnych danych cechują się nadto zróżnicowaniem terytorialnym, co pokazuje wykres 2. Nie jest zaskakujące, że z najpoważniejszymi konsekwencjami wycieku danych muszą się liczyć organizacje prowadzące działalność w Stanach Zjednoczonych, Niemczech czy Kanadzie.

Współczesne społeczeństwo, nowoczesna gospodarka oraz globalny system finansowy, mimo świadomości zagrożeń płynących z cyberprzestrzeni oraz coraz większych nakładów na bezpieczeństwo IT, stają się coraz bardziej podatne na cyberryzyko, co ma swoje źródła – zdaniem autora – w zjawiskach i procesach, które można ująć w dwie grupy:

– przesłanki techniczno-technologiczne – realizacja płatności elektronicznych, praca w chmurze (ang. cloud computing), dominacja oprogramowania Microsoft, wzrost złożoności programów komputerowych, stosowanie elektronicznych systemów sterowania infrastrukturą, maszynami i urządzeniami (tzw. systemy SCADA), rozwój bankowości elektronicznej oraz tzw. internetu rzeczy (ang. Internet of Things);
– przesłanki społeczno-behawioralne – popularność mediów społecznościowych, posługiwanie się urządzeniami mobilnymi, korzystanie ze słabo zabezpieczonego przed „podsłuchiwaniem" dostępu do internetu przez routery Wi-Fi (tzw. sniffing), nieklasyczne metody organizacji pracy (praca na odległość, wykorzystywanie w miejscu pracy prywatnego sprzętu komputerowego), powszechne wykorzystanie korespondencji e-mailowej w kontaktach biznesowych.

Reasumując, wyzwaniem dla zapewnienia cyberbezpieczeństwa – zwłaszcza w kontekście zapewnienia ciągłości funkcjonowania organizacji po wystąpieniu incydentu cybernetycznego – jest zrozumienie specyfiki i podatności na cyberzagrożenia nie tylko własnych systemów IT, ale także rozpoznanie wektorów oddziaływania ze strony systemów zewnętrznych, od których dany podmiot jest uzależniony.

4. Specyfika ekspozycji na ryzyko cybernetyczne instytucji finansowych

Od chwili, gdy banki i inne instytucje finansowe zaczęły świadczyć usługi z wykorzystaniem internetu, stały się podatne na wszelkiego typu cyberzagrożenia, co wynika z transgranicznego i anonimowego charakteru sieci.

Jednym z najpoważniejszych zagrożeń cybernetycznych dla banków i innych instytucji finansowych jest *phishing*[4]. Jest to metoda oszustwa, w której przestępca

[4] Warto dodać, że zagrożenia cybernetyczne stanowią istotny obszar ryzyka operacyjnego, które jest drugim pod względem ważności – po ryzyku kredytowym – rodzajem ryzyka w bankach [Thlon 2016].

podszywa się pod inną osobę lub organizację w celu wyłudzenia określonych informacji (np. danych logowania do bankowości internetowej) lub nakłonienia ofiary do realizacji określonych działań [Górnisiewicz, Obczyński, Pstruś 2014]. Ataki phishingowe przeciwko instytucjom finansowym i płatniczym stanowiły 28,7% wszystkich ataków tego typu w 2014 r., w tym ataki na banki stanowiły 16,3% całości, a na systemy kart płatniczych 5,1% (ok. 85% ataków phishingowych na systemy płatnicze dotyczyło trzech instytucji: Visa, PayPal, American Express). Jeśli chodzi o tego typu ataki na banki, połowa z nich dotyczyła zaledwie 13 największych banków na świecie [Kaspersky 2015b].

W 2014 r. zidentyfikowano na świecie 22,9 mln ataków o motywach finansowych z wykorzystaniem złośliwego oprogramowania typu *malware*, co stanowiło prawie 5% wszystkich incydentów tego typu. Atak *malware* polega na rozprzestrzenianiu poprzez wiadomości e-mail niebezpiecznych załączników, które uaktywniają się po otwarciu ich przez nieświadomych zagrożenia użytkowników poczty. W tym momencie zostaje zainfekowany komputer, na którym otwarto załącznik, i instaluje się na nim niewidoczne oprogramowanie, powodujące na przykład podmianę danych w dyspozycji przelewu składanej drogą elektroniczną. Klient banku nieświadomie przelewa pieniądze na konto przestępców. Celem tych ataków stało się 2,7 mln osób, z czego ok. 75% ataków dotyczyło bankowości internetowej. Na czele rankingu krajów najczęściej dotykanych atakami *malware* o podłożu finansowym od kilku lat znajduje się Rosja, która wyraźnie wyprzedza takie kraje, jak Brazylia, Turcja, Niemcy, Indie, USA, Wietnam, i Wielka Brytania [Kaspersky 2015b].

Stosunkowo często wykorzystywaną przez hakerów formą ataku na instytucje finansowe jest tzw. odmowa dostępu DoS (ang. *Denial of Service*) oraz jej odmiana tzw. rozproszona odmowa dostępu DDoS (ang. *Distributed Denial of Service*)[5] [CERT 2015]. Ich celem jest uniemożliwienie działania systemu komputerowego lub usługi sieciowej poprzez ciągłe wysyłanie na określony adres IP dużego strumienia danych, co prowadzi do przeciążenia i zablokowania łącza internetowego lub serwerów ofiary[6]. Atak DoS tym różni się od DDoS, że ten pierwszy wykonywany jest z jednej lokalizacji, natomiast ten drugi wykorzystuje do generowania nadmiarowego ruchu w sieci grupę komputerów innych użytkowników (tzw. botnet), które wcześniej zostały zainfekowane w celu przejęcia nad nimi kontroli. Co wydaje się szczególnie niepokojące, przeprowadzenie ataku typu DDoS stało się ostatnio niezwykle proste (nawet dla amatorów) ze względu na powszechnie dostępne w sieci specjalistyczne oprogramowanie służące do tego celu. Ponadto w internecie jest sporo serwisów, które oferują za niewielką opłatą realizację ataku DDoS na wskazany adres IP czy domenę [Dataspace 2017].

[5] Spektakularnym przykładem poważnego w skutkach ataku DDoS było włamanie do systemu komputerowego Giełdy Papierów Wartościowych w Warszawie, gdzie hakerom udało się przedostać przez systemy ochronne i uzyskać dostęp do poufnych informacji.

[6] Efektem skutecznego ataku DDoS jest przesłanie tak dużej ilości danych, które nie mogą zostać odebrane przez atakowane łącze internetowe. Przeciętne łącze internetowe w Polsce ma przepływność na poziomie 50–100Mb/s. Najmniejsze ataki DDoS zaczynają się od 6–10Mb/s, przez 200–500Mb/s, zaś największy wykryty i odparty atak na świecie miał przepływność ponad 400Gb/s [Dataspace 2017].

Niedocenianym jak dotąd zagrożeniem jest realizacja funkcji bankowości elektronicznej przy pomocy smartfonów i tabletów. Analitycy Kaspersky Lab zwrócili uwagę, że po raz pierwszy w historii w 2015 r. dwa bankowe trojany przeznaczone wyłącznie do ataków poprzez urządzenia mobilne znalazły się w pierwszej dziesiątce najczęściej spotykanych programów używanych do kradzieży pieniędzy. O niedostatecznej świadomości użytkowników urządzeń mobilnych mogą świadczyć dane dotyczące stosowania programów antywirusowych. Korzysta z nich zaledwie 26% użytkowników iPhone'ów, 44% posiadaczy Windows Phone, 60% użytkowników smartfonów z Androidem, podczas gdy instalowanie antywirusów na komputerach stacjonarnych jest obecnie regułą (93%) [Ramotowski 2016].

W 2014 r. odnotowano znaczny wzrost zagrożenia użytkowników urządzeń mobilnych z systemem Android. Celem blisko połowy ataków (48%) na urządzenia z Androidem były dane finansowe. Liczba tych ataków wzrosła trzykrotnie w porównaniu z 2013 r. (z 712 tys. do 2 mln 317 tys. ataków w 2014 r.). W takim samym stopniu wzrosła liczba ofiar tych ataków: z 213 tys. w 2013 r. do 776 tys. w 2014 r. Najczęściej atakowanym krajem z urządzeniami mobilnymi z Androidem ponownie okazała się Rosja (63,9% ataków), na kolejnych miejscach – choć z dużo mniejszym udziałem – znalazły się Kazachstan, Ukraina, Niemcy, Malezja, Wietnam, Hiszpania i Wielka Brytania [Kaspersky 2015b].

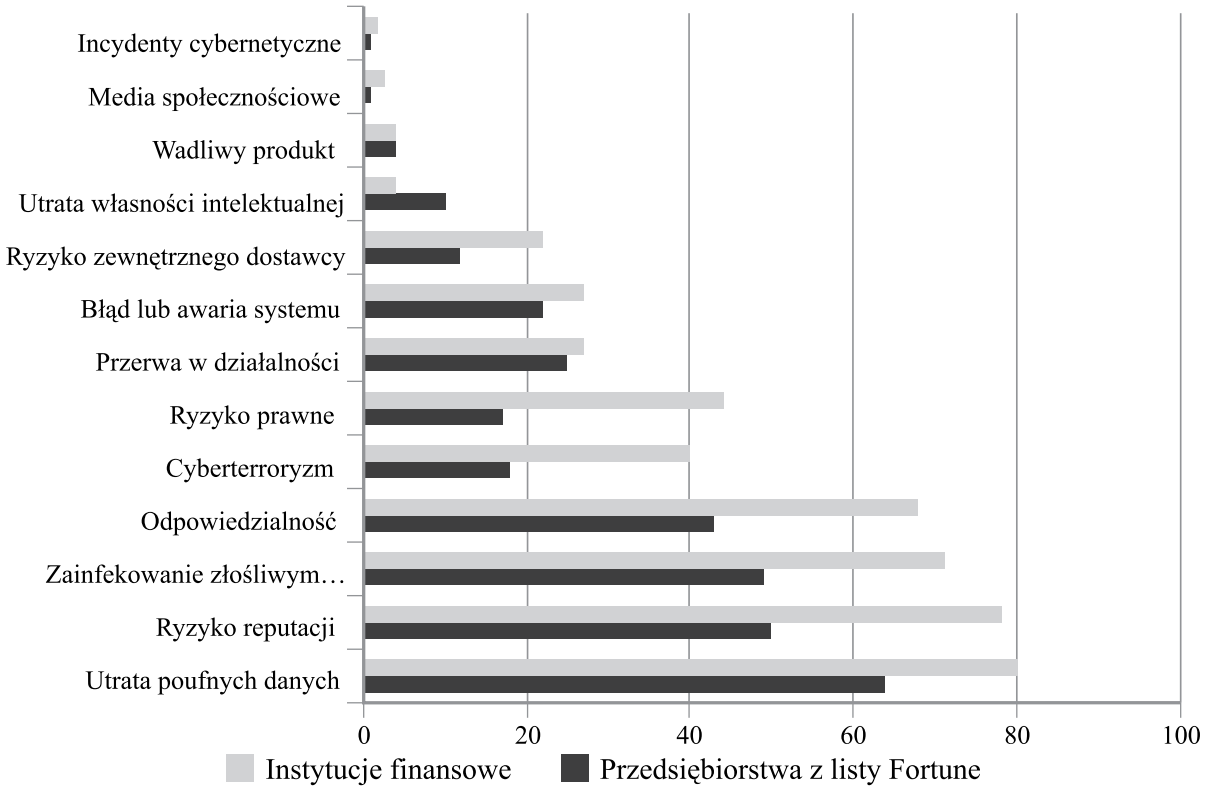
Celem różnego rodzaju cyberataków jest pozyskanie danych osobowych i innych wrażliwych informacji, które następnie stają się przedmiotem obrotu na czarnym rynku. I tak, pełne dane osobowe można kupić za 1 USD, numer CVV karty ze Stanów Zjednoczonych za 6 USD, numer CVV karty z Europy za 16 USD, pełny raport kredytowy za 25 USD, login do rachunku europejskiego banku za 200 USD, a login do rachunku brytyjskiego banku za 500 USD [Ramotowski 2016]. Oznacza to niestety, że informacje pozyskane w ten sposób stają się źródłem kolejnych przestępstw i wymuszeń.

Jeden z najbardziej spektakularnych cyberataków na sektor bankowy, pod nazwą Carbanak, miał miejsce pod koniec 2013 r. Prawie setka banków i instytucji finansowych została zaatakowana przez niezidentyfikowaną grupę przestępczą, która według organów ściągania mogła przechwycić nawet 1 mld USD. Początkowo rozesłano e-maile zawierające niebezpieczne załączniki. Po ich otwarciu dochodziło do zainfekowania komputerów użytkowników poczty programami szpiegowskimi, które umożliwiły hakerom wgląd do zawartości dysków i sieci poszkodowanych. Przestępcy koncentrowali się na uzyskaniu dostępu do sieci bankomatów, rachunków bankowych, kart kredytowych i przelewów bankowych. Według różnych szacunków udało im się uzyskać dostęp do około stu instytucji finansowych, zlokalizowanych głównie w Rosji, Stanach Zjednoczonych, Niemczech, Chinach i na Ukrainie. Skradzione pieniądze były przelewane na konta oszustów w Chinach oraz w Stanach Zjednoczonych [Kaspersky 2015a].

W ostatnim czasie obserwuje się zmianę celów cyberataków w obszarze usług finansowych. Zamiast atakować użytkowników końcowych (klientów banków), hakerzy zaczynają skupiać swoją uwagę na podmiotach, w których dochodzi do płat-

ności elektronicznych (zwłaszcza przy użyciu terminali na karty płatnicze POS). Chodzi tu m.in. o restauracje, hotele i sklepy. Hakerzy doprowadzają do zainfekowania terminala POS, z którego wykradają dane finansowe klientów. Drugim obiektem zainteresowania cyberprzestępców stają się same banki, choć w tym przypadku bardzo trudno uzyskać jakiekolwiek informacje o udanych cyberatakach. Trzecim trendem obserwowanym w ostatnim czasie jest odchodzenie od ataków masowych w kierunku działań skoncentrowanych na określonej grupie ofiar. Takie selektywne ataki mogą okazać się trudniejsze do wykrycia, pociągającego za sobą wydanie publicznego ostrzeżenia, i zapewne na to liczą cyberprzestępcy.

Wykres 3. Specyfika ekspozycji na ryzyko instytucji finansowych w porównaniu z przedsiębiorstwami amerykańskimi z listy Fortune 1000 (% odpowiedzi respondentów)



Źródło: [Willis 2013].

Ekspozycja na ryzyko instytucji finansowych istotnie różni się od przeciętnej struktury zagrożeń cybernetycznych spotykanej w przypadku przedsiębiorstw niefinansowych, co wyraźnie pokazują wyniki badań na próbie przedsiębiorstw amerykańskich z listy *Fortune 1000*. Po pierwsze, z wykresu 3 wynika, że wypadki cyberataków są częstsze w sektorze finansowym niż w populacji przedsiębiorstw. Po drugie, wyraźne dysproporcje w liczbie incydentów zaobserwowano w obszarze ryzyka regulacyjnego (17% wobec 44%) oraz ryzyka cyberterroryzmu (18% wobec 40%) [Willis 2013]. Można to wytłumaczyć rozległością regulacji występujących

w sektorze finansowym oraz tym, że banki stają się częstszym celem ataków haktywistów[7] [Deloitte 2016].

Oddziaływanie incydentu cybernetycznego na reputację organizacji jest bez wątpienia negatywne i obawia się tego połowa badanych przedsiębiorstw, aczkolwiek jego skutki mogą być szczególnie dotkliwe dla instytucji finansowych. Należą one bowiem do instytucji zaufania publicznego i ryzyko utraty klientów w wyniku ataku hakerskiego na system komputerowy banku jest ponadprzeciętnie wysokie. To tłumaczy wyraźnie wyższy odsetek wskazań (78%) ryzyka reputacyjnego przez przedstawicieli branży finansowej.

Na tle innych gałęzi gospodarki branża finansowa jest wyjątkowo powolna w wykrywaniu cyberataków. O ile 30% instytucji finansowych jest w stanie wykryć zagrożenie w ciągu kilku dni, to większość (38%) badanych banków i towarzystw ubezpieczeń dowiaduje się o tym, że stało się ofiarą hakerów, dopiero po upływie kilku miesięcy [Verizon 2015].

5. Rynek ubezpieczeń cybernetycznych w ujęciu globalnym

Niezwykle trudno jest podać wartość składki przypisanej z tytułu ubezpieczeń cybernetycznych, zarówno na całym świecie, jak i na poszczególnych kontynentach, gdyż brakuje jednolitego systemu gromadzenia danych o tej linii produktów. Z szacunków publikowanych przez różne instytucje branżowe, międzynarodowe firmy brokerskie lub największe grupy ubezpieczeniowe wynika, że łączny światowy przypis składki z cyberubezpieczeń sprzedawanych w formie produktów dedykowanych (tzw. *stand-alone policy*) wynosił w 2015 r. 2 mld USD, przy czym 90% tej kwoty przypada na Stany Zjednoczone [Allianz 2015].

Badanie Centre for the Study of Financial Innovation (CSFI) i firmy doradczej PriceWaterhouseCoopers, w którym wzięło udział ponad 800 przedstawicieli sektora ubezpieczeń oraz analityków branży z 54 krajów, wskazuje te obszary, które zdaniem respondentów będą stanowiły największe zagrożenie w ciągu następnych 2–3 lat. Cyberryzyko zostało wskazane jako największe zagrożenie przez respondentów reprezentujących ubezpieczycieli majątkowych. W pozostałych grupach respondentów (ubezpieczenia życiowe, reasekuracja, pośrednicy ubezpieczeniowi, obserwatorzy rynku) cyberryzyko za każdym razem znajdowało się w pierwszej dziesiątce. Skala tego ryzyka wynika z atrakcyjności danych wrażliwych, jakimi dysponują towarzystwa ubezpieczeń. Są to między innymi dane osobowe, dane medyczne i dane finansowe. Ryzyko cybernetyczne stanowi ponadto wyzwanie o charakterze underwritingowym, jako że ubezpieczyciele majątkowi stopniowo zaczynają wprowadzać do swojej oferty produktowej nowe ubezpieczenia cybernetyczne. W przekroju całego badania cyberryzyko zajęło wysokie, czwarte miejsce, tuż po takich zagrożeniach

[7] Słowo „haktywizm" pochodzi z połączenia dwóch wyrazów angielskich *hacking* i *activism.* Jak podaje Obserwatorium Językowe UW, haktywistą określa się hakera działającego z pobudek społecznych, politycznych, religijnych, a także dla pożytku publicznego. W praktyce bardzo trudno wytyczyć granicę pomiędzy haktywizmem a wymuszeniem okupu o podłożu kryminalnym.

dla branży ubezpieczeniowej, jak nowe regulacje, otoczenie makroekonomiczne, stopy procentowe. Warto podkreślić, że cyberryzyko stanowi zagrożenie globalne, o czym świadczy fakt, iż znalazło się wśród dziesięciu największych zagrożeń na każdym kontynencie, z wyjątkiem Ameryki Południowej. W branży ubezpieczeniowej panuje powszechne przekonanie, że cyberataki są czymś przesądzonym, pozostają pytania: kiedy one nastąpią i jakie przyniosą straty [PWC 2015b].

Wysoki poziom ekspozycji na ryzyko cybernetyczne został zasygnalizowany również przez banki w analogicznym do powyższego, cyklicznym badaniu sektora bankowego realizowanym przez firmę doradczą PWC. Wysokie, drugie miejsce zagrożenia przestępczością (awans z dziewiątego w poprzednim badaniu) oraz czwarta pozycja ryzyka technologicznego są wyraźnymi sygnałami wagi problemu cyberbezpieczeństwa w sektorze bankowym. Te dwa rodzaje ryzyka znalazły się na wysokich miejscach w rankingach zagrożeń stworzonych przez przedstawicieli banków (4. i 5.), menadżerów ryzyka (3. i 4.) i obserwatorów rynku (2. i 4.). Przestępczość cybernetyczna wzbudziła największe obawy wśród respondentów z Ameryki Północnej (1. miejsce), choć w Europie także jest zaliczana do kluczowych problemów branży (3. miejsce). Wśród ankietowanych można natrafić na obawy, iż zmasowany cyberatak może doprowadzić nawet do upadku banku i konieczności podjęcia interwencji państwa [PWC 2015a].

Na rynku europejskim instytucje finansowe są segmentem klientów generującym największy przypis składki z tytułu ubezpieczeń cybernetycznych (22,8% składki). Na kolejnych miejscach znalazły się firmy z branży technologicznej i komunikacyjnej (14,8%) oraz ochrony zdrowia (11,7%) [Marsh 2015a].

Badania przeprowadzone przez firmę Marsh wśród europejskich przedsiębiorstw pokazały, że skala wykorzystania cyberubezpieczeń na Starym Kontynencie jest dużo niższa w porównaniu ze Stanami Zjednoczonymi. Jedynie 12% respondentów posiada cyberubezpieczenie, 6% jest w trakcie zawierania umowy ubezpieczenia, a 27% planuje zakupić cyberpolisę w ciągu najbliższego roku. Jednak z drugiej strony 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 [Marsh 2015a]. Można to odczytać jako ogromne wyzwanie dla towarzystw ubezpieczeń i brokerów ubezpieczeniowych, polegające na potrzebie rzetelnego edukowania i informowania klientów.

Wbrew optymistycznym perspektywom rozwoju ubezpieczeń cybernetycznych w najbliższych latach agencja ratingowa Fitch przestrzega towarzystwa ubezpieczeń przed nadmiernym zaangażowaniem w ten typ 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].

6. Charakterystyka ubezpieczeń cybernetycznych dostępnych w Polsce

Specjalistyczne ubezpieczenie cyberryzyk może wypełnić wiele luk w tradycyjnych ubezpieczeniach[8], jak również zapewnić pokrycie strat bezpośrednich oraz ochronę przed ryzykiem odpowiedzialności związanej z używaniem technologii i danych w codziennej działalności [Marsh 2015c]. Zakres polisy jest elastyczny, dzięki czemu indywidualny program ubezpieczenia może zostać dostosowany do kluczowych ekspozycji na ryzyko przedsiębiorstwa, tak aby uwzględniał specyfikę funkcjonowania instytucji finansowych.

Obecnie (maj 2017 r.) na polskim rynku ubezpieczeń pokrycie ryzyk cybernetycznych dostępne jest w ofercie pięciu towarzystw ubezpieczeń:

– Chubb European Group Limited Oddział w Polsce – ubezpieczenie DataGuard Advantage,
– AIG Europe Limited Sp. z o.o. Oddział w Polsce – ubezpieczenie CyberEdge,
– TUiR Allianz Polska S.A. – ubezpieczenie Cyber Protect,
– STU Ergo Hestia S.A. – ubezpieczenie danych elektronicznych od ryzyk cybernetycznych,
– Leadenhall Polska S.A. – ubezpieczenie Leadenhall Cyber.

Większość z wyżej wymienionych ubezpieczeń (z wyjątkiem ubezpieczenia Leadenhall Cyber, o którym nieco później) ma konstrukcję pakietową, opartą na podziale na trzy sekcje obejmujące różne rodzaje ryzyka cybernetycznego. Sekcja I traktowana jest z reguły jako wariant bazowy (zakres podstawowy), zaś pozostałe dwie sekcje oraz opcjonalne klauzule dodatkowe stanowią możliwe rozszerzenia zakresu ochrony. Punktem wyjścia w ubezpieczeniach Chubb i Hestii jest zatem ochrona danych elektronicznych przed ryzykiem cybernetycznym. W ramach sekcji II Chubb daje możliwość dodania do zakresu ubezpieczenia innych ryzyk (w systemie *all risk*), na jakie narażone są dane komputerowe. Dodatkowo w sekcji III przewidziano ubezpieczenie ryzyka utraty przychodów przedsiębiorstwa i powstania kosztów dodatkowych wskutek realizacji jednego z rodzajów ryzyka cybernetycznego objętego ochroną w ramach sekcji I lub II.

Hestia, oprócz wymienionego wcześniej zakresu podstawowego, proponuje rozszerzenie ubezpieczenia o zwiększone koszty działalności firmy wynikające z utraty lub uszkodzenia danych elektronicznych (w szczególności: *public relations* w celu przywrócenia reputacji, przeniesienie nieutraconych danych na inne serwery, porady prawne, ograniczenie skutków utraty danych). W sekcji III oferowane jest ubezpieczenie odpowiedzialności cywilnej za szkody wyrządzone osobom trzecim w następstwie ataku komputerowego lub hakerskiego. Na zasadzie klauzuli dodatkowej

[8] Takich jak ubezpieczenia: mienia, sprzętu elektronicznego, odpowiedzialności cywilnej przedsiębiorstwa, odpowiedzialności cywilnej zawodowej i od ryzyka sprzeniewierzenia. Produkty te nie zapewniają pokrycia (lub zapewniają w sposób niepełny) w takich obszarach, jak: ochrona aktywów elektronicznych, utrata zysku przedsiębiorstwa wskutek zakłócenia działania systemu teleinformatycznego, odpowiedzialność za ujawnienie danych, cyberwymuszenia, odpowiedzialność za bezpieczeństwo sieci oraz odpowiedzialność związana z prowadzeniem działalności multimedialnej.

możliwe jest też ubezpieczenie danych przechowywanych w chmurze obliczeniowej.

Główną osią konstrukcji ubezpieczeń AIG i Allianz są zawarte w sekcji I ryzyka odpowiedzialności cywilnej ubezpieczonego za szkody wyrządzone różnymi aspektami działalności gospodarczej w sferze przechowywania i wykorzystania danych elektronicznych (w tym danych osobowych). Jako że pewne niewłaściwe zachowania w tym obszarze mogą być penalizowane przez GIODO, AIG oferuje możliwość ubezpieczenia na wypadek nałożenia kar administracyjnych przez uprawnione do tego instytucje i organy publiczne, a także kosztów reprezentowania ubezpieczonego w postępowaniu przed tymi organami (sekcja II). W sekcji III natomiast możliwe jest wykupienie ochrony na wypadek powstania różnych kosztów dodatkowych związanych z realizacją cyberzagrożenia (np. informatyka śledcza, ochrona reputacji, zawiadomienie poszkodowanych o naruszeniu bezpieczeństwa danych, odzyskanie utraconych danych, wynajęcie eksperta IT). Koszty te ubezpiecza również Allianz w sekcji III. AIG i Allianz dają także szansę ochrony firmy przed finansowymi skutkami cyberwymuszenia oraz utratą zysku spowodowaną zakłóceniem w działaniu systemu komputerowego przedsiębiorstwa (patrz tabela 2).

Tabela 2. Ogólne porównanie pakietowych ubezpieczeń ryzyk cybernetycznych

Ubezpieczyciel	Chubb	AIG	Allianz	Ergo Hestia
Sekcja I	Ubezp. danych (cyberryzyka)	OC	OC	Ubezp. danych
Sekcja II	Ubezp. danych (*all risk*)	Kary administracyjne	BI, cyberwymuszenie	Koszty dodatkowe (PR, porady prawne, usunięcie skutków utraty danych)
Sekcja III	*Business Interruption* (BI)	Koszty dodatkowe (reputacja, zawiadomienie)	Usługi: koszty PR, ekspert IT	OC
Rozszerzenia	brak	OC media, BI, wymuszenia	brak	dane w chmurze obliczeniowej

Źródło: opracowanie własne na podstawie badań autora.

Nieco inaczej skonstruowano zakres ochrony w ubezpieczeniu Leadenhall Cyber, wydzielając w nim siedem sekcji:

– Sekcje A, D i E obejmują odpowiedzialność cywilną i koszty obrony w postępowaniach cywilnych z tytułu naruszenia prywatności, naruszenia bezpieczeństwa danych klientów lub publikacji nieodpowiednich treści w ramach działalności multimedialnej.

– Sekcje B i C stanowią uzupełnienie ochrony opisanej we wcześniejszym punkcie o takie wydatki, jak kary administracyjne i koszty obrony w postępowaniach regulacyjnych z tytułu naruszenia prywatności prowadzonych przez GIODO, a także koszty reakcji i zarządzania kryzysowego w związku z naruszeniem bezpieczeństwa informacji.
– Sekcja F zapewnia pokrycie ryzyka cyberwymuszenia.
– Sekcja G stanowi ubezpieczenie utraty zysku przedsiębiorcy w związku z przestojem wywołanym zakłóceniem systemu IT oraz zapewnia pokrycie kosztów odtworzenia danych.

Ustalając wysokość składki ubezpieczeniowej, towarzystwa ubezpieczeń biorą pod uwagę takie czynniki, jak ilość przechowywanych danych wrażliwych (dane osobowe, numery kart kredytowych itp.) oraz wrażliwość na ryzyko utraty zysku w konsekwencji cyberataków lub awarii systemów IT.

7. Podsumowanie

Cyberprzestępczość stała się problemem globalnym. Złożoność złośliwego oprogramowania, szybkość działania hakerów, doskonała znajomość wewnętrznych systemów transakcyjnych banków dowodzą wagi problemu, wobec którego stoją instytucje finansowe. Rosnąca liczba doniesień medialnych o atakach cyfrowych powoduje, że powoli rośnie poziom świadomości zagrożeń zarówno wśród konsumentów, jak i zarządów instytucji finansowych.

W ostatnim czasie zwraca uwagę stopień zorganizowania cyberprzestępców. Nieskoordynowane działania pojedynczych hackerów zostały zastąpione przez wyspecjalizowane grupy przestępcze, zasługujące na miano mafii XXI w. Ich intensywne i wielotorowe działania wywodzą swoją skuteczność z efektu skali.

Jak pokazują regularne ćwiczenia zdolności reagowania banków i towarzystw ubezpieczeń na sytuacje kryzysowe związane z incydentem cybernetycznym Cyber-EXE Polska, polskie banki są coraz lepiej przygotowane na cyberzagrożenia i potrafią dobrze koordynować niezbędne działania podejmowane w chwili wystąpienia cyberataku. Nadal jednak istnieje dość duży problem, jeśli chodzi o współpracę pomiędzy bankami, które w ograniczonym stopniu informują się nawzajem o zaistniałych zagrożeniach [ISBNews 2016].

Ryzyko cybernetyczne można określić jako najpoważniejsze wyzwanie, przed jakim stanęła branża ubezpieczeniowa w ostatnim półwieczu. Nosi ono znamiona ryzyka systemowego, którego źródłem jest wykorzystywanie technologii informatycznych i elektroniczne przetwarzanie danych. Może skutkować szkodami we własnych dobrach majątkowych lub roszczeniami osób trzecich [IUA 2016].

Rozbudowa techniczno-organizacyjnych systemów bezpieczeństwa IT nie gwarantuje całkowitej eliminacji ryzyka cyberataków. W stosunku do tej rezydualnej, zatrzymanej części ryzyka właściwym rozwiązaniem może być jego transfer na zakład ubezpieczeń w formie cyberpolisy. Specjalistyczne ubezpieczenie cybernetyczne zapewnia szeroki zakres ochrony, zarówno w obszarze szkód własnych (ang.

first-party losses), jak i odpowiedzialności cywilnej wobec osób trzecich (ang. *third-party losses*). Dzięki budowie modułowej ubezpieczyciel może również zapewnić specjalistyczne usługi dodatkowe, takie jak świadczenie pomocy dla ubezpieczonego o charakterze *assistance*, informatyka śledcza, pomoc prawna, wsparcie eksperta *public relations*.

Na koniec trzeba jednak przyznać, iż w porównaniu z największą plagą polskich banków – standardowymi wyłudzeniami kredytów, których skala sięga miliarda złotych rocznie – na razie straty spowodowane atakami z sieci są niewielkie. Za to ich potencjał wzrostowy jest niepokojąco wysoki.

Bibliografia

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

Ayers E., 2015, *Advisen loss insight: Cyber by the sector*, Advisen, http://www.cyberrisknetwork.com/2015/10/01/advisen-loss-insight-cyber-by-the-sector/ (dostęp: 23.03.2015).

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

Dataspace, 2017, *Co to jest atak DDoS i jak się przed nim chronić?*, https://dataspace.pl/ddos_broszura_web.pdf (dostęp: 31.05.2017).

Deloitte, 2016, *Hactivism. A defender's playbook*, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-hacktivism.pdf (dostęp: 31.05.2017).

EKES, 2014, *Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie ataków cybernetycznych w UE*, Bruksela, http://www.eesc.europa.eu (dostęp: 12.03.2017).

Eling M., Wirfs J.H., 2016, *Cyber risk: Too big to insure? Risk transfer options for a mercurial risk class*, Uniwersytet St. Gallen (Szwajcaria), http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf (dostęp: 23.04.2016).

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

Fitch, 2016, *Fitch: Rapid Growth in Cyber Insurance Would Be Credit-Negative*, https://www.fitchratings.com/site/fitch-home/pressrelease?id=1001233 (dostęp: 31.03.2016).

Górnisiewicz M., Obczyński R., Pstruś M., 2014, *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną*, Komisja Nadzoru Finansowego, https://www.knf.gov.pl/Images/Bezp_finansowe_tcm75-39005.pdf (dostęp: 12.03.2017).

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

ISBNews, 2016, *Cyber-EXE Polska: Banki są coraz lepiej przygotowane na cyberzagrożenia*, „Puls Biznesu" z 19.01.2016, http://www.pb.pl/4418180,22148,cyber-exe-polska-banki-sa-coraz-lepiej-przygotowane-na-cyberzagrozenia (dostęp: 26.03.2016).

ITRC, 2017, *ITRC data breach reports December 13, 2016*, Identity Theft Resource Center, styczeń 2017, http://www.idtheftcenter.org/images/breach/DataBreachReport_2016.pdf (dostęp: 2.03.2017).

IUA, 2016, *Cyber risks and insurance. An introduction to cross class cyber liabilities*, International Underwriting Association of London, http://www.maritimelondon.com/wp-content/uploads/2016/01/005_Cyber_Risks_Combined_110116.pdf (dostęp: 12.03.2016).

Kaspersky, 2015a, *Carbanak APT. The great bank robbery*, Kaspersky Lab, https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf (dostęp: 12.03.2016).

Kaspersky, 2015b, *Financial cyberthreats in 2014*, Kaspersky Lab Report, https://securelist.com/files/2015/02/KSN_Financial_Threats_Report_2014_eng.pdf (dostęp: 22.03.2016).

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

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

Marsh, 2015c, *Zarządzanie ryzykiem cybernetycznym*, https://www.marsh.com/content/dam/marsh/Documents/PDF/pl/pl/Poland-Zarzadzenie-Ryzykiem-Cybernetycznym-Nasze-Rozwiazania.pdf (dostęp: 22.05.2017).

Marsh, 2016, *Emerging risks: Anticipating threats and opportunities around the corner*, https://www.marsh.com/us/insights/research/excellence-in-risk-management-xii1.html (dostęp: 3.05.2016).

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

Podolak G.D., 2015, *Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow 's Challenges*, „Quinipiac Law Review" Vol. 33, s. 369–409.

Ponemon Institute, 2015, *2015 Cost of Data Breach Study: Global Analysis*, Ponemon Institute, http://www-03.ibm.com/security/data-breach/index.html (dostęp: 26.12.2015).

PWC, 2014, *Zarządzanie ryzykiem w cyberprzestrzeni*, PricewaterhouseCoopers, https://www.pwc.pl/pl/publikacje/assets/gsiss_2015_polska.pdf (dostęp: 20.11.2015).

PWC, 2015a, *Banking banana skins 2015*, PricewaterhouseCoopers, https://www.pwc.com/gx/en/financial-services/pdf/Banking-banana-skins-2015-final.pdf (dostęp: 20.11.2015).

PWC, 2015b, *Insurance banana skins 2015*, Pricewaterhouse Coopers, https://www.pwc.com/gx/en/insurance/banana-skins/assets/pwc_insurance_banana_skins_2015.pdf (dostęp: 11.04.2016).

Ramotowski J., 2016, *Cybermafia groźniejsza od nieuczciwego pracownika*, „Obserwator Finansowy" z 6.02.2016, http://www.obserwatorfinansowy.pl/tematyka/bankowosc/cybermafia-grozniejsza-od-nieuczciwego-pracownika/ (dostęp: 25.03.2016).

Thlon M., 2016, *Podstawy zarządzania ryzykiem operacyjnym*, Wyd. UE w Krakowie, Kraków.

Verizon, 2015, *2015 Data breach investigations report. Financial services*, Industry Report, https://msisac.cisecurity.org/whitepaper/documents/1.pdf (dostęp: 12.03.2016).

WEF, 2014, *Global Risks 2014. Ninth Edition*, World Economic Forum, http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf (dostęp: 22.02.2016).

Willis, 2013, *Willis special report: Fortune 1000 cyber disclosure by financial institutions*, Special Report 10/13, http://www.willis.com/documents/publications/Services/Executive_Risks/2013/Willis_Fortune1000-Cyber-Disclosure_Financial-Institutions.pdf (dostęp: 12.03.2016).

Cyber-threats of financial institutions

Abstract. The aim of the article is to analyse cyber-risk from the perspective of financial institutions, and to indicate the possibility of use of cyber-insurance as a tool for minimising financial impact of such risk. The study is based on branch reports, mostly in English-language, published by institutions of insurance market as well as by entities monitoring IT security. The paper consists of six parts. At the beginning, the definition and types of cyber risks have been shown. Then the global scale of cyber-threat was presented using data gathered by specialized research centers and organizations active in insurance area. In the third part of the study, the specifics of the risk-exposure of financial institutions were analysed. The next part briefly describes the development of the North American and European cyber-insurance market. Section 5 characterizes cyber insurance products available on the Polish insurance market as stand-alone policies. The last paragraph summarizes the conclusions from the article.

Keywords: cyber-risk, cyber-insurance, insurance, financial institutions.
JEL Codes: G22, G200.