Marian Krupa*

Efektywne zarządzanie ochroną zasobów informacyjnych firmy w globalnej cyberprzestrzeni w oparciu o metodę SMART ZBI

Wstęp

Rozwój cywilizacji informatycznej zmienia model biznesowy każdej firmy we wszystkich obszarach jej działalności. Na szczególną uwagę zasługuje kwestia tworzenia nowej wartości w zakresie wiedzy opartej na informacji biznesowej. Powyższa wiedza posiada swoje źródło w danych zapisanych w rozmaity sposób na różnych nośnikach elektronicznych. Tworzą one zasoby informacyjne powstałe w wyniku digitalizacji zdarzeń biznesowych realizowanych w ramach całego łańcucha logistycznego, funkcjonującego często w przestrzeni globalnej. Powyższe zasoby stanowią niezwykle cenne dobro dla różnych grup interesariuszy, co wymusza na właścicielach odpowiednie działania nie tylko w zakresie ich tworzenia, przetwarzania, komunikowania i archiwizowania, ale również, i być może przede wszystkich, ich chronienia.

Problematyka dotycząca wypracowania odpowiednich metod zarządzania ochroną zasobów informacyjnych jest również niezwykle aktualna z perspektywy wymagań zapisanych w rozporządzeniu ogólnym o ochronie danych osobowych (RODO) opublikowanym 4 maja 2016 r. w Dzienniku Urzędowym Unii Europejskiej (GDPR – *The General Data Protection Regulation*). Jak czytamy w założeniach powyższej reformy, ma ona „pozwolić obywatelom UE i przedsiębiorcom na czerpanie maksymalnych korzyści z tzw. Jednolitego Rynku Cyfrowego, przy jednoczesnym zachowaniu bezpieczeństwa danych osobowych i poszanowaniu prawa do prywatności" [Zawadzka, 2017, s. 1].

Celem głównym niniejszego opracowania jest opracowanie efektywnej i zarazem uniwersalnej metody zarządzania bezpieczeństwem zasobów informacyjnych firmy. Równocześnie, podejmowana jest próba odpowiedzi na następujące pytania szczegółowe: 1) Czym w istocie są zasoby informacyjne firmy i jaka jest ich wartość? 2) Jakie grupy interesariuszy są w sposób szczególny zainteresowane pozyskaniem aktywów w postaci danych biznesowych? 3) Jaka jest rzeczywista skala zagrożeń i poziom strat

* Dr, Instytut Zarządzania i Inżynierii Produkcji, Państwowa Wyższa Szkoła Zawodowa im. rtm. W. Pileckiego w Oświęcimiu, ul. Kolbego 8, 32-600 Oświęcim, marian.krupa@pwsz-oswiecim.edu.pl

ponoszonych w skali globalnej? 4) Jakie działania w zakresie zarządzania zasobami informacyjnymi należy podejmować w celu ich efektywnej ochrony? 5) Jakie strategie przedsiębiorca powinien wypracować w zakresie sprawnego zarządzania zasobami informacyjnymi firmy w perspektywie wymagań RODO?

Realizację celu głównego oparto o metodę modelowania symulacyjnego. W celu odpowiedzi na pytania szczegółowe zastosowano metodę analityczno-syntetyczną.

1. Wprowadzenie do problematyki zarządzania zasobami informacyjnymi firmy

Wartość każdej organizacji wyznaczają posiadane przez nią zasoby. Obok klasycznych zasobów, takich jak: ziemia, kapitał i praca, w cywilizacji informatycznej szczególną wartość dla przedsiębiorstwa tworzy wiedza biznesowa powstała w wyniku pozyskania, ustrukturyzowania i utrwalenia informacji [Czekaj, 2000, s. 13].

Pojęcie informacji jest wielowymiarowe. W literaturze przedmiotu informację możemy opisywać z perspektywy semiotycznej, społecznej, ekonomicznej czy też organizacyjno-technicznej [Oleński, 2001, s. 286–291]. Dla potrzeb niniejszego opracowania przyjmijmy, że informacja jest to zbiór danych (faktów biznesowych, ekonomicznych, prawnych itd.) ustrukturyzowanych z punktu widzenia potrzeb decyzyjnych, które wyznaczają główną funkcję zarządzania w każdej organizacji [Adair, 2001, s. 9; Drucker, 1994, s. 129–130]. Istotną kwestią jest również to, że informacja jest kategorią ekonomiczną [Zaskórski, Szwarc, 2013, s. 40; Oleński, 2001, s. 15–19], która podlega klasycznemu procesowi zarządzania [Martyniak, 2000, s. 11–22].

Z kolei przez zasoby informacyjne, zgodnie z normą PN-I-02000:2002, rozumiemy „wszelkie oprogramowanie, dane, sprzęt, zasoby administracyjne, fizyczne, komunikacyjne lub ludzkie w systemie informatycznym lub w działalności informatycznej". W praktyce będą to: dokumenty, bazy danych, zasoby fizyczne (np. sprzęt komputerowy, budynki – serwerownie, infrastruktura teleinformatyczna, oprogramowanie, posiadana przez pracowników wiedza i doświadczenie branżowe, technologiczne know-how jako zdolność świadczenia usług lub produkowania oraz dobra niematerialne, czego najlepszym przykładem będzie pozytywny wizerunek firmy lub też wysoka wartość znaku towarowego – marki [Molski, Łacheta, 2007, s. 78].

Kluczowym zatem zadaniem każdej organizacji w ramach procesu zarządzania jest zapewnienie skutecznych metod ochrony tych strategicznych zasobów, które charakteryzuje wartość niematerialna i podatność, rozumiana jako „wady lub luki w strukturze fizycznej organizacji,

w procedurach, w zarządzaniu w sprzęcie/oprogramowaniu jak też zamierzone lub niezamierzone działania personelu, które mogą być wykorzystane do spowodowania szkód w systemie informatycznym lub działalności użytkownika" [PN-I-02000:2002].

System zarządzanie bezpieczeństwem zasobów informacyjnych (ZBZI) obok kwestii identyfikacji zasobów, oceny podatności, parametryzacji ryzyk itd. oznacza konieczność również przeprowadzenia analizy otoczenia zewnętrznego, tzn. kluczowych grup interesariuszy będących źródłem potencjalnych zagrożeń. Bardzo dobrym przykładem takiej refleksji jest tzw. trójkąt zarządzania bezpieczeństwem informacji.

2. Trójkąt zarządzania bezpieczeństwem informacji (ZBI) – analiza otoczenia zewnętrznego firmy

Zasoby informacyjne tworzone w firmie stanowią często niezwykle cenną wiedzę dla całego szeregu zewnętrznych grup interesariuszy. Należą do nich nie tylko środowiska świata przestępczego, definiowane zwyczajowo jako „hakerzy", ale również przedstawiciele międzynarodowych korporacji oraz różnych agend i instytucji rządowych.

W pierwszym wypadku możemy rozróżnić takie grupy, jak: pospolici przestępcy, grupy polityczne, terrorystyczne, ideologiczne, które dla przesłanek ekonomicznych lub też ideowych są zainteresowane pozyskaniem danych lub też przejęciem kontroli nad zasobami informacyjnymi firmy. Różne mogą być motywacje działania tych środowisk, jednak wspólną cechą tych działań jest traktowanie wiedzy o naszej działalności gospodarczej jako swoistego oręża walki ideologicznej lub swoistej przedsiębiorczości ukierunkowanej na korzyści finansowe lub prestiżowe. Istnieje cały szereg przykładów potwierdzających realność i dotkliwość aktywności tego typu środowiska przestępczego. W samym 2015 r. przeprowadzono 295 wykrytych cyberataków na infrastrukturę krytyczną w USA [Józefiak, 2016].

Drugą grupą interesariuszy są międzynarodowe korporacje, które chroniąc z jednej strony własne zasoby informacyjne, działają czasami na pograniczu prawa, starając się pozyskać wiedzę biznesową od konkurencji. Często przy pomocy wyspecjalizowanych firm są zainteresowane pozyskaniem danych strategicznych, które mogą być potem wykorzystane komercyjnie w zakresie działań promocyjnych czy też sprzedażowych. Poprzez tzw. szpiegostwo przemysłowe, wywiad gospodarczy (*due dilligence*) realizowany w cyberprzestrzeni korporacje mogą pozyskać dostęp do takich informacji, jak: planowane inwestycje, struktura sprzedażowa, rynki zbytu, źródła zaopatrzenia, struktura zatrudnienia i wynagrodzeń itd. [Janiec, 2002, s. 245–247]. Pozwala to na wypracowanie właściwych

strategii działania dla danej korporacji w wymiarze strategicznym lub też operacyjnym.

Przykładem tego typu praktyk może być niezwykle dynamicznie rozwijająca się grupa firm funkcjonujących w Izraelu, założonych często przez byłych pracowników informatycznych służb specjalnych. Należą do nich takie organizacje biznesowe, jak Caspiego Fifth Dimension, Deep Instinct, Check Point, SafeBreach, Argus Cyber Security, Mer Group, które sprzedając usługi w wymiarze ochrony zasobów informacyjnych, mogą przekazywać również wiedzę w zakresie metod i technik w zakresie dostępu do wiedzy krytycznej przy użyciu nowoczesnych technologii [*Hakerzy ze służb państwowych*, 2017].

Trzecią grupą zainteresowaną pozyskaniem wiedzy dotyczącej zasobów informacyjnych firmy jest państwo, reprezentowane przez różne agendy rządowe, takie jak: Urząd Skarbowy, Państwowa Inspekcja Pracy, Najwyższa Izba Kontroli, Agencja Bezpieczeństwa Narodowego, CBA, ZUS, KRUS itd. Ich głównym celem jest realizacja celów statutowych, takich jak: zapewnienie bezpieczeństwa, weryfikacja rzetelności rozliczeń, ochrona pracowników przez łamaniem prawa pracy ze strony pracodawców, weryfikacja źródeł pozyskania kapitału inwestycyjnego, powiązania biznesu ze światem przestępczym, w tym głównie z grupami terrorystycznymi itd. Istnieje jednak realne niebezpieczeństwo dla przedsiębiorcy, że zostaje on pozbawiony podstawowych praw w zakresie poufności danych, prywatności własnej i swoich pracowników, anonimowości partnerów biznesowych lub też w sytuacji prowadzonych śledztw oraz procesów sądowych, prawa do uczciwej obrony. Urzędnicy mogą również nadużywać swoich kompetencji, czy też wykonywać działania administracyjno-operacyjne na „granicy prawa" przy pomocy wyspecjalizowanych zewnętrznych „usług" w zakresie dostępu do zasobów informacyjnych, które mogą być potem wykorzystane dla celów np. politycznych. Dowodem tego typu zagrożeń jest zapis w raporcie opublikowanym przez firmę konsultingową PwC, w którym czytamy: „W wyniku przecieków Snowdena rośnie sceptycyzm przedsiębiorstw i całego społeczeństwa w związku z inwigilacją ze strony służb; rośnie też obawa o potencjalne skutki dla poufności zebranych danych i możliwości ich nieuprawnionego wykorzystania" [PricewaterhouseCoopers, 2014, s. 16].

3. Poziom i rodzaj zagrożeń oraz strat wynikających z cyberprzestępczości dokonywanej w skali globalnej – wyniki badań

Złożoność problematyki ZBI wynikająca z analizy otoczenia wpływa bezpośrednio na poziom świadomości menedżerów i skalę zagrożeń

zarówno w wymiarze wewnętrznym, jak i zewnętrznym firmy. Wydaje się, że coraz częściej polscy przedsiębiorcy dostrzegają realną wartość posiadanych zasobów informacyjnych, jak też podejmują działania w zakresie ich ochrony, chociaż nie zawsze w sposób skuteczny.

Bardzo dobrym instrumentem oceny poziomu dojrzałości polskich firm były badania przeprowadzone przez Kancelarię Ślązak, Zapiór i Wspólnicy w 2013 r. Autorzy raportu stwierdzają, że istotnie „77% organizacji zdaje sobie sprawę z dużej wartości informacji, a jej bezpieczeństwo uważa za jeden z priorytetów" [Góra, 2013, s. 4]. Z kolei, analizując dostrzegalny poziom ryzyka występującego w cyberprzestrzeni, zauważono, że „91% ankietowanych uważa wyciek danych za realne zagrożenie", co zapewne wynika z faktu, że aż „66% organizacji poniosło szkodę finansową z powodu takiego wycieku" [Góra, 2013, s. 9]. Nie budzi zatem zdziwienia deklaracja, że „96% ankietowanych uważa, że warto inwestować w zabezpieczenie informacji".

Niewątpliwie w tym punkcie analizy należy ocenić, na ile przedsiębiorcy są nie tyle świadomi ogólnych zagrożeń, ale przede wszystkim, jakie są ich rzeczywiste kompetencje w ZBI. Autorzy raportu stwierdzają niestety, że w tym zakresie zarówno samoocena[1], jak i obiektywna analiza wyników nie jest optymistyczna. Bardzo dobrym przykładem może być próba definiowania przez polskich przedsiębiorców źródeł zagrożeń, które przede wszystkim lokują w otoczeniu zewnętrznym – „52% badanych firm uważa, że niemożliwe lub mało prawdopodobne jest, aby do wycieku informacji doszło na skutek działania własnych pracowników" [Góra, 2013, s. 11]. Rzeczywistość jest jednak taka, że to właśnie pracownicy (źródła wewnętrzne), szczególnie kierownicy średniego szczebla, są najsłabszym ogniwem w zakresie zapewnienia ochrony zasobów informacyjnych – wyniki globalne badań firmy Pricewaterhouse Coopers wskazują, że ponad 70% przestępstw wykonanych w cyberprzestrzeni dotyczy obecnych i byłych pracowników [PricewaterhouseCoopers, 2014, s. 14].

Innym niezwykle interesującym spostrzeżeniem jest to, że nadal „43% informacji funkcjonuje w formie tradycyjnej – papierowej" [Góra, 2013, s. 8] co niewątpliwie wymusza swoisty dualizm w zarządzaniu bezpieczeństwem informacyjnym w firmie i co znacznie podnosi zarówno poziom ryzyka, jak i same koszty ZBI.

Złożoność problemu w zakresie ZBI pogłębia nie tylko skala zjawiska kryminalnych działań w cyberprzestrzeni, ale również lista potencjalnych ryzyk. Obejmuje ona takie praktyki, jak: APT (*Advanced Persistent Threats*) – ataki ukierunkowane na organizacje, połączone ze „spear phishingiem",

[1] Zgodnie z przeprowadzonymi badaniami zaledwie 32% respondentów uważa swoją wiedzę z zakresu ZBI za bardzo dużą [Góra, 2013, s. 12].

ataki DDoS na podmioty komercyjne, ataki typu „Drive-by Download/ Watering Hole", ataki na „Cloud Computing", ataki na platformy hostingowe, ataki na system DNS, ataki na systemy sterowania przemysłowego ICS/SCADA, ataki na urządzenia medyczne, haktywizm, kradzież wirtualnych walut, „phishing email and www", powstawanie „botnetów" opartych o platformy mobilne, wycieki baz danych zawierających dane osobowe, hasła, nr kart kredytowych, itd., wykorzystanie gier sieciowych w atakach, zagrożenia dla platformy Android, zagrożenia dla platformy Ios, zagrożenia dla platformy Windows Phone/Mobile, zagrożenia typu „ransomware/scareware", zagrożenia w serwisach społecznościowych, zagrożenia zawiązane z BYOD, zagrożenia związane z „Internet of Things" [FBC, 2015, s. 4].

Opinie ekspertów w zakresie ZBI wskazują na trzy najbardziej krytyczne ryzyka, które obecnie (lata 2016–2017) wymagają szczególnej uwagi przez administratorów i użytkowników cyberprzestrzeni, są nimi [FBC, 2015, s. 13]:

- phishing e-mail and WWW,
- wycieki baz danych zawierających dane osobowe, hasła, numery kart kredytowych itd.,
- zagrożenia dla platformy Android.

Kolejnym elementem uniwersalnego modelu ZBI jest kwestia obliczania poziomu strat wynikających z działań przestępczych. Należy zwrócić uwagę, że sam proces szacowania szkód nie jest przedsięwzięciem łatwym, dlatego też wszelkie podawane w różnych opracowaniach wartości stanowią jedynie szacunki, obarczone dużym ryzykiem błędu. Według raportu firmy konsultingowej EY szacuje się zgodnie z badaniami przeprowadzonymi w 2014 r. przez Center for Strategic and International Studies and McAfee, że kradzież danych oraz praw autorskich to koszt pomiędzy 375 a 575 mld USD rocznie [EY, 2015, s. 14]. Zaś w raporcie opracowanym przez Uniwersytet w Cambridge kradzież danych osobowych kosztuje jej ofiarę średnio 572 USD rocznie [komputerswiat.pl, 2014].

Należy jednak pamiętać, że bezpośredni koszt utraty danych wynikający z działań kryminalnych realizowanych w cyberprzestrzeni nie oznacza strat całkowitych, jakie ponoszą firmy jak i ich klienci. Na podstawie studium firmy Deloitte realny koszt cyberataku może być do 40% wyższy od ogólnych szacunków firm i może być rozłożony w perspektywie 3–5 lat [Misztal, 2016].

Niezwykle interesującym, kolejnym wnioskiem zapisanym w cytowanym raporcie jest sposób kategoryzacji kosztów z podziałem na „nad powierzchnią" oraz „pod powierzchnią". W pierwszym przypadku należy wziąć pod uwagę takie aspekty, jak: śledztwo techniczne, powiadomienia klienta o naruszeniu, ochrona klienta po ataku, zgodność z przepisami, koszty

związane z PR, opłaty związane z procesami sądowymi i pomocą prawnika, poprawa cyberbezpieczeństwa itd. Z kolei koszty „pod powierzchnią" obejmują: wzrost sumy ubezpieczeniowej, zwiększony koszt pozyskania kapitału dłużnego, rozregulowanie działalności lub jej zniszczenie, niska wartość relacji z klientem, wartość utraconego zysku z umów, dewaluacja reputacji czy też strata własności intelektualnej [Misztal, 2016].

Wraz ze wzrostem znaczenia oraz kosztu pozyskania i zabezpieczenia informacji, przy równoczesnym dynamicznym rozwoju technologii tworzenia i przetwarzania tych zasobów (Internet, hurtownie danych, ERP, BI, Cloud Computing, IoT), istotnym zagadnieniem dla zarządzających staje się zapewnienie im bezpieczeństwa. Biorąc pod uwagę złożoność problematyki oraz nieuchronność zagrożeń, konieczne staje się wypracowanie skutecznej metody, systemu zarządzania tym strategicznym zasobem, jakim jest informacja.

4. Zarządzanie bezpieczeństwem zasobów informacyjnych – perspektywa metodologiczna w oparciu o rozwiązanie SMART ZBI

W praktyce zarządzania ochroną zasobów informacyjnych możemy zidentyfikować wiele metod, zarówno o charakterze diagnostycznym (audyt bezpieczeństwa), jak też implementacyjno-rozwojowych. Do najbardziej znanych zaliczyć możemy takie systemy korporacyjne, jak: CRAMM (CCTA *Risk Analysis and Management Method*) – analiza luk i opracowanie projektu poprawy bezpieczeństwa; COBRA (*Control Objectives for Risk Analysis*) – analiza holistyczna organizacji – 33 podkategorie + 429 pytań kontrolnych; MARION (*Mision Analysis and Risk Impact on Operational network-tool*) – definiowanie polityki bezpieczeństwa, w tym wynikające z uregulowań prawnych (np. Związek Banków Polskich); MEHARI (*Methode Harmonisee d'Analyse de RIsques*) – normy BS 7799 i ISO/IEC 13335 czy też ISACA (*Information Systems Audit and Control Association*) [Molski, Łacheta, 2007, s. 213–274].

Należy również zwrócić uwagę na metodykę zarządzania ryzykiem w cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów sektora publicznego. Powstała ona na podstawie Polskiej Normy PN-ISO/IEC 27005:2014 („Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji"). Zawiera ona pełną procedurę zarządzania ryzykiem w zakresie zapewnienia bezpieczeństwa danych, tj. identyfikację, analizę, ocenę, postępowanie z ryzykiem, strategię akceptacji czy też procedury w zakresie informowania, jak również zapisy dotyczące definicji, procedur, standardów w zakresie przygotowania dokumentacji, raportowania czy też przegląd typowych kategorii zagrożeń.

Oceniając użyteczność powyższych systemów, tj. korporacyjnych lub też tych opracowanych na potrzeby sektora publicznego, należy zauważyć, że dla przeciętnego przedsiębiorcy, w tym przede wszystkim sektora MŚP, są one z jednej strony zbyt wymagające w zakresie zaangażowanie zbyt dużych zasobów firmy – bariery biurokratyczne, z drugiej – stanowią poważny wysiłek finansowy, często przekraczający realne możliwości firmy.

Należy się zastanowić zatem nad takim uniwersalnym i elastycznym systemem czy też metodą zarządzania bezpieczeństwem ZI, która mogłaby stanowić konstruktywną i alternatywną propozycję dla przedsiębiorcy, bazując na właściwej relacji użyteczność–koszty. Wydaje się, że takim rozwiązaniem jest autorska metoda o nazwie SMART ZBI (*SMART ISM*).

Metoda SMART ZBI jest oparta na następujących założeniach:

1. Nie ma systemów i zabezpieczeń, które dają 100% pewności, poczucia bezpieczeństwa w zakresie ochrony zasobów informacyjnych.
2. Jakość zarządzania bezpieczeństwem informacji w firmie jest relacją realnego poczucia bezpieczeństwa do ponoszonych kosztów, tzn. że bezpieczeństwo informacyjne jest kategorią ekonomiczną (koszt wdrożenia i utrzymania), dlatego też wymaga ona racjonalnych merytorycznie i finansowo decyzji.
3. Zarządzanie ryzykiem w zakresie zagrożeń musi uwzględniać tzw. poziom akceptowalnego ryzyka przez danego przedsiębiorcę. Należy jednak pamiętać, że im wyższy poziom akceptowalnego ryzyka, tym wyższy koszt utrzymania takiego systemu.
4. Rozwiązanie docelowe wypracowane w wyniku przeprowadzonej analizy i diagnozy w zakresie bezpieczeństwa musi prowadzić do rekomendacji w formie strategii/decyzji/zadań, jakie przedsiębiorca powinien wdrożyć na poziomie strategicznym i operacyjnym. Powyższy proces zgodnie z przyjętą metodyką podlega monitorowaniu.
5. Zarządzanie bezpieczeństwem informacyjnym jest procesem ciągłym, które należy realizować z uwzględnieniem ograniczeń zasobowych danej firmy oraz zmian w otoczeniu biznesowym, technologicznym (trójkąt ZBI).

Kluczowa wartość SZBI (wskaźnik W_{SZBI}), w ramach SMART ZBI jest definiowana jako relacja oceny jakościowej ochrony ZI (wskaźnik ZBI_q) do kosztów całkowitych ponoszonych w wyniku jego opracowania (miernik K_c)[2], wdrożenia, utrzymania i rozwoju. Dlatego też, w oparciu o zasadę prakseologiczną sprawnego działania, realizacja wartości zapisanej

[2] W niniejszym opracowaniu „miernik" (*measure*) definiujemy jako pojedynczą kategorię ekonomiczną/biznesową, odzwierciedlającą zdarzenia i fakty gospodarcze, wyrażone w jednostkach miary, np. wielkość produkcji [szt.], koszty pracy [EUR], udział w rynku [%]. Wskaźnik (*indicator*) jest wartością wyjaśniającą wzajemny stosunek dwóch kategorii ekonomicznych, tj. mierników.

w przyjętej formule oznacza konieczność stałego poszukiwania równowagi pomiędzy poziomem realnego bezpieczeństwa ZI do kosztów całkowitych ponoszonych w wyniku ich ochrony.

Z kolei ocena jakościowa (wskaźnik ZBI_q) jest to suma iloczynów poziomów istotności zasobów informacyjnych (miernik I_n) i ocen poziomu rzeczywistej ochrony zasobów informacyjnych (miernik O_n).

Zgodnie z SMART ZBI metodyka prac projektowych w zakresie wdrożenia systemu ZBI obejmuje:

1. Zdefiniowanie celu i zakresu prac projektowych ZBI, w tym krótką charakterystykę firmy, branży, założeń strategicznych w zakresie polityki bezpieczeństwa).
2. Zinwentaryzowanie zasobów informacyjnych dla wybranego podmiotu gospodarczego z perspektywy ich wartości i istotności.
3. Zdefiniowanie kluczowych zagrożeń (ryzyk) oraz ocenę ich prawdopodobieństwa wystąpienia z uwzględnieniem akceptowalnego poziomu analizowanego ryzyka.
4. Zdefiniowanie relacji pomiędzy posiadanymi zasobami informacyjnymi a realnym ryzykiem – pkt 3.
5. Dokonanie oceny poziomu jakości miernika (ZBI_{q1}) – stan obecny (AS-IS) w relacji do aktualnego wskaźnika wartości systemu ZBI – W_{SZBI1}.
6. Przeprowadzenie analizy luk i słabych punktów w systemie AS-IS i opracowanie rekomendacji zawierających strategię wzrostu wartości systemu ZBI, tj. realnej ochrony zasobów w relacji do zgłoszonych możliwości finansowych przedsiębiorstwa.
7. Opracowanie strategii zmian w zakresie ochrony zasobów informacyjnych uwzględnieniem ocenę docelowego poziomu bezpieczeństwa (ZBI_{q2}) w ramach dostępnych budżetów (*TO-BE*) z wykorzystaniem modelowania symulacyjnego typu „what-if". Efektem końcowym tych prac jest oszacowanie docelowego wskaźnika wartości systemu ZBI – W_{SZBI2}.
8. Opracowanie systemu monitorowania wdrażania zmian oraz systemu oceny skuteczności nowego rozwiązania zgodnie z zasadą ciągłego doskonalenia *PDCA*.

Podejście SMART ZBI wskazuje na całe spektrum strategii zarządzania ryzykiem ochrony zasobów informacyjnych firmy, takich jak: unikanie, ograniczenie, transfer czy też retencja [Zaskórski, Szwarc, 2013, s. 44]. Powinno być ono dostosowane do indywidualnych uwarunkowań firm oraz zdefiniowanych wymagań formalnych i istniejących zagrożeń.

Należy pamiętać, że coraz częściej o skuteczności działań lokalnych wypracowanych na poziomie przedsiębiorstwa, nawet w oparciu

o najlepsze praktyki projektowe, decyduje ostatecznie stan zabezpieczeń, wdrażanych procedur oraz intencji w otoczeniu zewnętrznym (patrz trójkąt ZBI), czy też w szerszym kontekście – jakość współpracy różnych agend rządowych i korporacyjnych na poziomie zarówno krajowym, jak i międzynarodowym [Fastyn, 2016].

5. Strategie zarządzania bezpieczeństwem informacji w ramach wytycznych RODO

Zarządzanie systemem bezpieczeństwa informacji obejmuje, w sposób oczywisty, z perspektywy uregulowań prawnych, kwestię danych osobowych. Każdy zatem przedsiębiorca równolegle do działań podejmowanych w zakresie ochrony tych zasobów, które dla niego stanowią dobro strategiczne, musi od 2018 r. spełniać również wymagania zapisane w ogólnym rozporządzeniu o ochronie danych osobowych (RODO).

Zawiera ono m.in. następujące wytyczne:

1) bezpośrednia odpowiedzialność przetwarzającego (przedsiębiorcy) za posiadane i przetwarzane dane;
2) obowiązkowe zgłaszanie wykrytych przypadków naruszeń do właściwego organu nadzoru – do 72 godzin;
3) zapewnienie prawa klientów (partnerów biznesowych) do „bycia zapomnianym";
4) obowiązek otrzymania zgody na profilowanie przed rozpoczęciem zbierania danych;
5) obowiązkiem wyznaczenie Inspektora Ochrony Danych Osobowych;
6) obowiązkowa inwentaryzacja danych i wymagania związane z dokumentacją;
7) konieczność uzyskiwania zgód na przetwarzanie danych osobowych od osób, których dane dotyczą;
8) obowiązek dotyczący komunikowania sposobu przetwarzania danych osobowych kierowanych do osób, których dane dotyczą;
9) obowiązek wykonania tzw. analizy oceny wpływu (istotności) ochrony danych oraz
10) zakaz transferu danych poza Unię Europejską [Pusz, 2017].

Uwzględniając założenia metody SMART ZBI, możemy wskazać na następujące strategie optymalizujące z jednej strony obowiązkową realizację wytycznych zapisanych w RODO, i z drugiej, minimalizację kosztów, które wynikają z ich wdrożenia:

1. Unikanie – strategia polega na wykluczeniu elementów systemu / zasobów, z którymi wiążą się wysokie koszty wdrożenia RODO, a ich usunięcie nie przeszkodzi w realizacji celów strategicznych lub operacyjnych.

2. Retencja – zapewnienie odpowiednich środków w sytuacji materializacji ryzyka w zakresie nieprzestrzegania zapisów rozporządzenia. Należy jednak pamiętać, że zgodnie z RODO instytucje kontrolujące mogą nakładać bardzo wysokie i dotkliwe dla funkcjonowania firmy kary.
3. Ograniczanie – podejmowanie racjonalnych ekonomicznie działań o charakterze prewencyjnym oraz opracowanie scenariuszy kryzysowych zmierzających do minimalizacji wystąpienia dodatkowych kosztów, wynikających z dostosowania systemu do wysoce prawdopodobnie zmieniających się wymagań prawnych.
4. Transfer – przekazanie całości lub części ryzyka na wyspecjalizowane podmioty, które za określoną opłatą są gotowe realizować niezbędne dla nas usługi. Bardzo dobrym przykładem mogą być to usługi realizowane w tzw. chmurze, które przenoszą znaczną część obowiązków zapisanych w RODO na podmioty sprzedające swoje usługi w tej technologii.

Biorąc pod uwagę szanse i zagrożenia, jakie wynikają z dostępnych strategii, możemy wskazać, że najbardziej optymalnym rozwiązaniem będzie przeprowadzenie działań w następującej kolejności:

1. Wykonanie inwentaryzacji posiadanych zasobów informacyjnych oraz prowadzonych działań w powyższym zakresie i wyeliminowanie tych elementów, które są zbędne z punktu widzenia realizowanych celów biznesowych – strategia unikania.
2. Przeprowadzenie analizy kosztowej w zakresie dostępnych usług wdrożenia wytycznych RODO i ewentualne wdrożenie zaleceń przy pomocy firmy zewnętrznej – strategia ograniczania.
3. W sytuacji istnienia zbyt dużej bariery finansowej w zakresie realizacji strategii ograniczania przez firmę zewnętrzną zaleca się zmianę technologii przetwarzania danych z modelu stacjonarnego na rozwiązania „chmurowe" – strategia transferu.

Zakończenie

Głównym celem niniejszego projektu badawczego było opracowanie efektywnej metody zarządzania bezpieczeństwem zasobów informacyjnych firmy. Na podstawie przeprowadzonych symulacji opisana metoda SMART ZBI spełnia postawione przed nią wymagania w zakresie uniwersalności zastosowań, skalowalności oraz elastyczności w wymiarze doboru strategii.

Dodatkowo na podstawie przeprowadzonej analizy literatury przedmiotu możemy wskazać na następujące wnioski:

1. Prowadzenie działalności gospodarczej przy wykorzystaniu technologii informatycznych tworzy niezwykle wartościowe dla różnych grup interesariuszy zasoby wiedzy biznesowej i przez to stwarza wiele kosztownych zagrożeń.
2. Poziom realnych zagrożeń w cyberprzestrzeni jest bardzo wysoki, a wartość bezpośrednich strat wynikających z aktywności przestępczej w cyberprzestrzeni jest szacowana na poziomie 500 mld dolarów rocznie.
3. Dane zawarte w systemach informatycznych muszą być chronione na mocy ustaw i rozporządzeń – szczególnie są uregulowane branże i dane wrażliwe, które tworzą i przechowują cenne treści z punktu widzenia interesu państwa czy obywatela.
4. Wdrażanie systemów ZBI wymaga niezwykle kosztownych i skomplikowanych organizacyjnie i technicznie działań, które wymagają zaangażowania wyspecjalizowanych firm zewnętrznych.
5. Nawet najbardziej zaawansowany system ochrony zasobów informacyjnych nie gwarantuje w 100 procentach ich bezpieczeństwa.

W sposób szczególny należy zwrócić uwagę na następujące rekomendacje:

1. Na obecnym poziomie digitalizacji oraz wymiany danych poprzez Internet praktycznie każda firma musi opracować i wdrożyć skuteczny system zarządzania ochroną zasobów informacyjnych.
2. Zaleca się dokonać wyboru takiej metody wdrożenia SZBI, który uwzględnia postulaty sprawnego działania – np. metoda SMART ZBI.
3. SZBI wymaga stałego doskonalenia ze względu na zmiany w obszarze technologii i otoczeniu prawnym – zasada PDCA.
4. Wytyczne RODO wymuszają na przedsiębiorcach konieczność przeprowadzenia tzw. analizy wykonalności, która musi uwzględniać nie tylko realizację celu, jakim są wymagania, ale również koszt takiego projektu.
5. Wybór strategii wdrożenia RODO powinien uwzględniać najbardziej optymalne dla przedsiębiorcy rozwiązanie.

Reasumując, problematyka ZBI nie jest już tylko obszarem zainteresowań działów IT, ale również wyznacza nowe wyzwania w zakresie projektowania i doskonalenia nowoczesnych modeli biznesowych.

Literatura

Adair J. (2001), *Anatomia biznesu. Podejmowanie decyzji. Podstawowa umiejętność w procesie zarządzania*, EMKA, Warszawa.

Czekaj J. (2000), *Metody zarządzania informacją w przedsiębiorstwie*, Wydawnictwo Akademii Ekonomicznej w Krakowie, Kraków.

Drucker P. (1994), *Menedżer skuteczny*, Akademia Ekonomiczna w Krakowie/Czytelnik, Kraków.

EY (2015), *Megatrends 2015. Making sense of a world in motion*, www.ey.com, dostęp: 30.05.2017.

Fastyn T. (2016), *Ranking cyberzagrożeń według Deloitte*, 2016, www.cyberdefence24.pl, dostęp: 21.06.2017.

Fundacja Bezpieczna Cyberprzestrzeń (2015), *Największe zagrożenia dla bezpieczeństwa w internecie w 2016 roku*, FBC, Warszawa.

Góra J. (2013), *Efektywne zarządzanie bezpieczeństwem informacji*, Kancelaria Ślązak, Zapiór i Wspólnicy, Katowice.

Hakerzy ze służb państwowych, http://wiadomosci.onet.pl, dostęp: 30.01.2017.

Janiec M. (2002), *Zagrożenia dla bezpieczeństwa informacyjnego przedsiębiorstw*, w: A. Stabryła (red.), *Zarządzanie firmą w społeczeństwie informacyjnym*, Akademia Ekonomiczna w Krakowie/EJB, Kraków.

Józefiak B. (2016), *295 cyberataków na infrastrukturę krytyczną w USA w 2015 r.*, www.cyberdefence24.pl, dostęp: 21.06.2017.

Kreft P. (2014), *Jakie straty ponosi światowa gospodarka z powodu cyberprzestępczości?* www.komputerswiat.pl, dostęp: 21.06.2017.

Kreuziger J. (2000), *Solutions for the Knowledge Worker*, „The mySAP Business Intelligence Conference 2000", SAP Global, Hamburg.

Martyniak Z. (2000), *Zarządzanie informacją i komunikacją. Zagadnienia wybrane w świetle studiów i badań empirycznych*, Wydawnictwo Akademii Ekonomicznej w Krakowie, Kraków.

Misztal B. (2016), *Firmy nie wiedzą, jakie są koszty cyberataku*, www.cyberdefence24.pl, dostęp: 21.06.2017.

Molski M., Łacheta M. (2007), *Przewodnik audytora systemów informatycznych*, Helion, Gliwice.

Oleński J. (2001), *Ekonomika informacji*, PWE, Warszawa.

Polska Norma PN-I-02000:2002. Technika informatyczna – Zabezpieczenia w systemach informatycznych – Terminologia.

PricewaterhouseCoopers (2014), *Zarządzanie ryzykiem w cyberprzestrzeni. Kluczowe obserwacje z wyników ankiety. Globalny stan bezpieczeństwa informacji 2015*, PricewaterhouseCoopers, Warszawa.

Pusz S. (2017), *10 najważniejszych zmian, które wprowadzą RODO*, www.pwc.pl. dostęp: 20.06.2017.

Stech G. (2017), *NIK: Cena za cyberbezpieczeństwo będzie wysoka…*, „Computerworld", nr 6.

Zaskórski P., Szwarc K. (2013), *Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki", nr 9, Warszawa.

Zawadzka N. (2017), *Rozporządzenie ogólne o ochronie danych osobowych*, www.lubasziwspolnicy.pl, dostęp: 20.06.2017.

Użyte skróty
RODO – ogólne rozporządzenie o ochronie danych osobowych
ZBI – zarządzanie bezpieczeństwem informacji
SZBI – system zarządzania bezpieczeństwem informacji
GDPR – *The General Data Protection Regulation*
IoT – *Internet of Things*
ISM – *Information Security Management*

Streszczenie

Zarządzanie bezpieczeństwem zasobów informacyjnych nie jest już tylko dobrą praktyką menedżerską, ale również obowiązkiem każdej firmy wynikającym z wytycznych RODO. Podstawowym dylematem każdego przedsiębiorcy jest znalezienie właściwej równowagi pomiędzy koniecznymi działaniami a ograniczonymi zasobami. Artykuł przedstawia problematykę zarządzania zasobami informacyjnymi firmy, analizę otoczenia zewnętrznego w zakresie bezpieczeństwa informacyjnego, poziomy i rodzaje zagrożeń oraz strat wynikających z cyberprzestępczości dokonywanej w skali globalnej. W sposób szczególny została opisana metoda SMART ZBI oraz strategie zarządzania projektem wdrożenia systemu bezpieczeństwa informacji w ramach wytycznych RODO.

Słowa kluczowe
digitalizacja, wywiad gospodarczy, RODO, ZBI, SZBI, SMART ZBI

The effective Information Security Management System in the global cyber environment (Summary)

The information security management is not just a good business practice but also it is the legal obligation of all firms accordingly to The General Data Protection Regulation (GDPR). The basic dilemma of all business is to find an appropriate balance between the tasks that have to be performed and the limited recourses. The article presents information resources management issue, the analysis of the environment in area of information security, different levels and types of security risks and losses that are the effect of criminal activity in cyber environment in the global perspective. A special attention is focused on SMART ISM methodology and GDPR project management strategies.

Keywords
digitalization, due diligence, GDPR, ISM, ISMS, SMART ISM