ZASTOSOWANIE STRATEGICZNEJ KARTY WYNIKÓW UWZGLĘDNIAJĄCEJ ELEMENTY SYSTEMU BEZPIECZEŃSTWA INFORMACJI W ORGANIZACJI

Piotr WOŹNIAK, Jarosław WĄSIŃSKI

Streszczenie: W pracy autorzy przedstawili ideę nowoczesnej metody wspomagającej zarządzanie w organizacjach jaką jest Strategiczna Karta Wyników (SKW). W publikacji zwrócono szczególną uwagę na istotę bezpieczeństwa informacji. W niniejszej pracy ukazano praktyczne elementy zastosowania europejskiego podejścia do SKW jako narzędzia wspomagającego skuteczność procesów wewnętrznych opartych na wymaganiach dedykowanego systemu bezpieczeństwa informacji.

Słowa kluczowe: Strategiczna Karta Wyników, system zarządzania, bezpieczeństwo informacji, skuteczność.

1. Strategiczna Karta Wyników

Strategiczna Karta Wyników (SKW) w ostatnim czasie stała się jedną z najbardziej popularnych metod wspomagania zarządzania wewnątrz firmy. Historia Strategicznej Karty Wyników autorstwa Roberta Kaplana i Davida Nortona sięga roku 1992, kiedy to twórcy metody uczestniczyli w projekcie badawczym Instytutu Nolan Norton pt. „Mierzenie skuteczności w organizacjach przyszłości" w 12 wybranych przedsiębiorstwach. Po przeprowadzeniu procesu badawczego na łamach „Harward Business Reviev" autorzy wskazywali wielokrotnie, że SKW to najbardziej skuteczne narzędzie służące poprawie zarządzania procesów wewnętrznych. Amerykanie zaproponowali narzędzie identyfikujące („mapujące procesy") kondycję organizacji w czterech głównych perspektywach:

- finansowej,
- klienta,
- operacyjnej,
- rozwoju.

Kolejne lata to swoista ewolucja metody na świecie, w wyniku której można obecnie wyróżnić dwa główne podejścia:

- podejście amerykańskie (ukierunkowane na obszary finansowe),
- podejście europejskie (ukierunkowane na obszary pozafinansowe).

Strategiczna Karta Wyników w ujęciu amerykańskim w przekonaniu autorów nie odzwierciedla w pełni europejskich warunków, zwłaszcza uwarunkowań prawnych Unii Europejskiej dotyczących prowadzenia działalności gospodarczej.

Drugim podejściem wyodrębnionym de facto przez dynamicznie zmieniające się wymagania rynku jest europejskie podejście do Strategicznej Karty Wyników (SKW), autorstwa Herwiga R. Friedaga oraz Waltera Schmidta opierające się w głównej mierze na pozafinansowych aspektach zarządzania. Bez wątpienia to właśnie drugi model Strategicznej Karty Wyników w ostatnich latach jest częściej wybierany przez organizacje jako bazę do wdrożeń. Głównymi cechami charakterystycznymi dla tego podejścia są indywidualne aspiracje i pomysły pracowników przy jednoczesnej budowie przez kadrę

zarządzającą na tej podstawie misji, wizji przedsiębiorstwa, która wspomagana jest przez dynamicznie zmieniające się drogi strategiczne/cele/mierniki skuteczności procesów.
Bezsprzecznym faktem jest, że obecnie w dobie globalizacji i coraz większej konkurencji wzrasta rola skuteczności procesowej wewnątrz firmy. Zdaniem Friedaga i Schmidta w SKW należy umieszczać jedynie cele o fundamentalnym znaczeniu dla organizacji, w SKW powinny znaleźć się cele umożliwiające rozwój potencjału firm. Potencjały firmy w tym ujęciu dzielą się na:

- te, które należy wykorzystać – obszar operacyjny,
- oraz te, które należy rozwijać, aby zagwarantować organizacji rozwój – obszar strategiczny [1].

Kluczowe różnice pomiędzy podejściem europejskim, a amerykańskim zestawiono w tabeli nr 1.

Tab. 1. Różnice pomiędzy podejściem europejskim, a amerykańskim do Strategicznej Karty Wyników

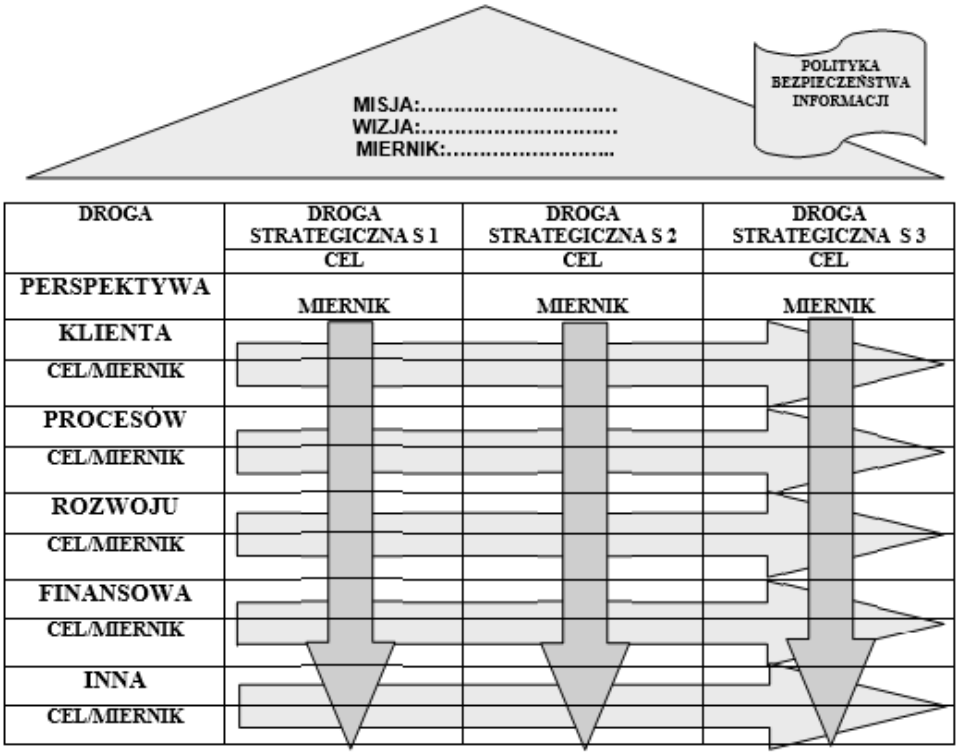
EUROPEJSKIE PODEJŚCIE DO SKW	AMERYKAŃSKIE PODEJŚCIE DO SKW
kapitał intelektualny równie istotny jak kapitał finansowy w strategii przedsiębiorstwa	strategia przedsiębiorstwa podporządkowana kapitałowi finansowemu
macierz domu SKW	mapa strategii SKW
indywidualne dążenia i aspiracje personelu	zespołowe dążenie do realizacji strategii podporządkowanej kapitałowi finansowemu
rozróżnienia dwóch typów celów: długookresowych i krótkookresowych	umieszczanie w mapie strategii zarówno celów długookresowych jak i operacyjnych (krótkookresowych)
zarządcza (ludzie i działania) i sprawozdawcza (mierniki) SKW	jednolita SKW
ponadwydziałowe „kooperacje" SKW	przyporządkowanie wyznaczonych elementów SKW ściśle do wyznaczonych komórek
realizacja „strategii wyłaniających się"	realizacja strategii zaplanowanej

Źródło: opracowanie własne.

Ujęcie europejskie Strategicznej Karty Wyników pozwala kadrze zarządzającej zwrócenie uwagi w większym stopniu na indywidualny aspekt intelektualny pracowników. W toku takiego podejścia do SKW możemy wyróżnić następujące etapy wdrożenia według koncepcji Friedaga i Schmidta:

1. Zdefiniowanie celów, misja wizja.
2. Zdefiniowanie dróg strategicznych i perspektyw.
3. Zebranie pomysłów, wypełnianie ram strategicznych.
4. Powiązanie działań w projekty strategiczne i zabudżetowanie ich.
5. Zdefiniowanie zakresów odpowiedzialności i powiązanie z systemem motywacyjnym.
6. Kontrola wyników w ramach SKW (Zarządcza i Sprawozdawcza Karta Wyników).
7. Zorganizowanie procesu uczenia się [1].

Przykład macierzy europejskiej SKW (stanowiącej wzorzec do modyfikacji i wprowadzenia elementów związanych z bezpieczeństwem informacji) odzwierciedlającej jednocześnie specyfikę działalności firmy wraz z jej misją, wizją miernikami, drogami strategicznymi, mierzalnymi celami oraz perspektywami przedstawia rysunek 1.



Rys.1. Model domu macierzy europejskiej SKW

Źródło: Opracowanie własne na podstawie książki pt. Pod presją czasu. Strategiczna Karta Wyników w praktyce, autorstwa Adrianny Lewandowskiej oraz Marcina Linierskiego, Wydawnictwo C.H Beck Sp. z o.o., Warszawa 2005, s. 43.

Według autorów jednym z głównych elementów, które wpływają na elementarną wiarygodność europejskiego podejścia do SKW jest konieczność filtrowania w podejściu europejskim informacji jakie wypływają na zewnątrz organizacji. Wydaje się, że w odróżnieniu do innych metod oraz do podejścia amerykańskiego do SKW wdrożenie, a następnie utrzymanie takiej SKW pozwala na bardziej precyzyjne określenie mierzalnych i weryfikowalnych celów. W ocenie autorów sytuacja taka przyczynia się do motywacji i współdziałania personelu różnego szczebla w różnych perspektywach. Takie postępowanie związane z wdrożeniem i utrzymaniem SKW w organizacji powinno być jednak w obliczu wszechobecnych zagrożeń zewnętrznych (zwłaszcza o charakterze elektronicznym) wspomagane dedykowanymi rozwiązaniami systemowymi z zakresu bezpieczeństwa informacji.

2. Bezpieczeństwo informacji

Mnogość incydentów w ostatnich latach w różnych branżach przemysłu, czy też życia społeczno – gospodarczego związanych z bezpieczeństwem informacji wskazuje na konieczność zwiększania działań prewencyjnych w tym zakresie. Oczywistym faktem zatem staje się coraz większe zainteresowanie tematyką bezpieczeństwa informacji. Co ciekawe proces ten w ocenie autorów nie jest tylko domeną jak bywało kilka czy kilkanaście lat temu firm z przemysłu farmaceutycznego czy zbrojeniowego. Coraz większego znaczenia nabiera odpowiedzialność za własność klienta niezależnie od branży. Warto podkreślić w tej części niniejszego opracowania, że zdecydowane ożywienie na rynku wdrożeń dedykowanych systemów bezpieczeństwa zwiększa także zainteresowanie implementacją nowatorskich metod zarządzania takich jak np. SKW. Zwiększające się zainteresowanie normami w zakresie bezpieczeństwa informacji pozwala na bardziej światłe podejmowanie bieżących decyzji czy też dotyczących inwestycji infrastrukturalnych. Kluczowym i jednocześnie uznawany standardem światowym w tym zakresie jest norma PN-ISO/IEC 27001:2007 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania ISO 27 001 [2].

Kluczowe wymagania dla niniejszej normy zawarto w punktach od 4. do 8. Dotyczą one Systemu Zarządzania Bezpieczeństwem Informacji (SZBI):

- w zakresie odpowiedzialności kierownictwa, w tym jego zaangażowania, zarządzania i zapewnienia zasobów, potrzeby uświadamiania pracowników,
- w zakresie planowania, przeprowadzania, dokumentowania działań związanych z audytami wewnętrznymi,
- w obszarze przeglądu systemu zarządzania bezpieczeństwem informacji wykonywanych przez kierownictwo,
- w dziedzinie doskonalenia systemu zarządzania bezpieczeństwem informacji (SZBI), w tym ciągłego doskonalenia, działań korygujących i zapobiegawczych.

Szczegółowe wymagania dotyczące bezpieczeństwa informacji w organizacji zawarto w załączniku A (normatywnym) do normy ISO 27 001. Zamieszczono w nim przede wszystkim wymagane cele stosowania zabezpieczeń i proponowane zabezpieczenia umożliwiające osiągnięcie celów zarządzania bezpieczeństwem informacji.

Wartym zanotowania jest fakt, że w ramach funkcjonowania SZBI w organizacji należy dokładnie zidentyfikować ryzyko, następnie sformułować plan postępowania z ryzykiem.

Plan powinien zawierać określone działania kierownictwa, zakresy odpowiedzialności, priorytety dla zarządzania ryzykiem bezpieczeństwa informacji. Po etapie opracowania planu następuje etap wdrożenia z wykorzystaniem personelu na poszczególnych stanowiskach, w których precyzyjnie określono role oraz zakresy obowiązków. Szczegółowa analiza zasobów infrastrukturalnych określanych w normie mianem aktywów musi doprowadzić do gwarancji osiągnięcia celów. Podobnie jak ma to miejsce w przypadku innych standardów opartych na normach z serii ISO kluczowym zagadnieniem okazuje się podejście procesowe, które oparte powinno być na ustanowieniu dedykowanych systemów mierniczych ukierunkowanych jednak w tym przypadku na zachowanie bezpieczeństwa informacji. Ważne jest zdefiniowanie sposobu pomiaru i oceny efektywności zabezpieczeń i grup zabezpieczeń przy zastosowaniu właściwych mierników (umożliwiającego porównywanie wyników). Pomiar efektywności jest ważny dla oceny skuteczności ochrony (zabezpieczeń).

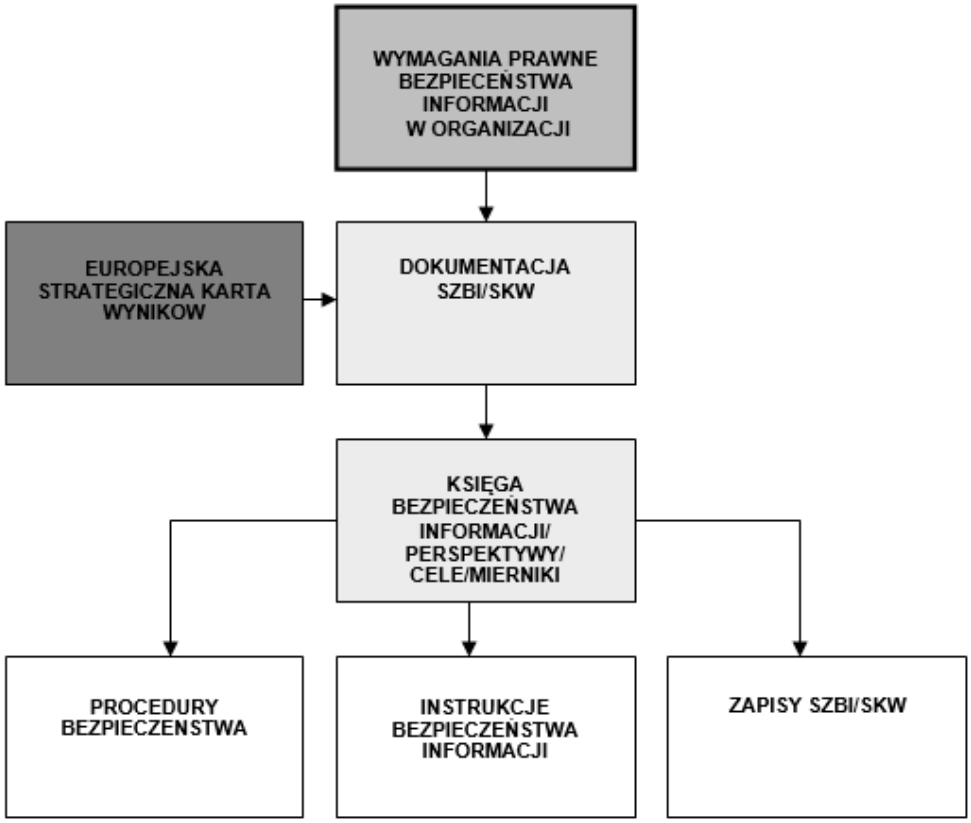
W opinii autorów posiadających kilkunastoletnie doświadczenie we wdrożeniach

podobnych standardów zarządzania; w przypadku stosowania systemów bezpieczeństwa informacji opartych na ISO z serii 27001 największymi problemami w organizacjach przy ich wdrożeniu i utrzymaniu wymagań okazują się być:

- brak ustalonych zasad posługiwania się nośnikami elektronicznymi,
- powszechne użycie niekreślonej precyzyjnie liczby kopii elektronicznych i nienadzorowanych egzemplarzy umieszczonych na dyskach, poczcie elektronicznej i pozostałych nośnikach,
- stosowanie nieaktualnych treści, lub formułowanie dyspozycji w niezrozumiały sposób dla użytkowników wewnątrz organizacji,
- indywidualne (niezatwierdzone systemowo) zasady nadzoru nad dokumentami,
- brak polityki zastępstw w zakresie stosowania wymagań polityki bezpieczeństwa w organizacji,
- brak zasad wykorzystywania poczty elektronicznej do przesyłania informacji ważnych dla organizacji,
- brak ustalonego priorytetu dla informacji (ważności, pilności danej sprawy, tym samym priorytetu bezpieczeństwa przekazywanej informacji przez poszczególne komórki organizacyjne),
- trudności z ustaleniem w krótkim okresie czasu, kompletu nadzorowanych dokumentów, szczególnie występujących na różnych nośnikach i w wielu wersjach,
- brak odpowiednich zabezpieczeń antyspamowych i innych,
- nieodpowiednia infrastruktura w organizacji,
- brak odpowiednich zasobów do stosowania wymagań,
- wykonywanie w nieodpowiednich sposób auditów wewnętrznych oraz symulacji postępowania w sytuacjach kryzysowych,
- niewystarczające dyspozycje dotyczące sposobu przeprowadzania zmian w dokumentach,
- brak nadzorowania nieaktualnych dokumentów.

W celu zmniejszenia prawdopodobieństwa wystąpienia w/w zagrożeń dla funkcjonującego systemu bezpieczeństwa w organizacji stosuje się odpowiednie zapisy systemowe, które powinny być konsekwencją przeanalizowanej i ustanowionej struktury dokumentacji opartej jednocześnie na aktualnych wymaganiach prawnych oraz specyfice metody podwyższenia skuteczności procesów wewnętrznych jaką jest Strategiczna Karta Wyników. Rysunek 2 przedstawia podział dokumentacji systemu bezpieczeństwa informacji w organizacji z uwzględnieniem europejskiego podejścia do Strategicznej Karty Wyników

Pozytywnym aspektem realizowanych czynności związanych z bezpieczeństwem informacji w organizacjach jest wdrażanie zabezpieczeń związanych z funkcjonowaniem wewnętrznej sieci intranetowej lub innych pozostałych. W ostatnich latach można odnieść wrażenie, że działania w zakresie bezpieczeństwa informacji w wielu przedsiębiorstwach, instytucjach są prowadzone bez precyzyjnego określenia harmonogramu, podziału zadań przy wdrożeniu i eksploatacji. Trudno nie zgodzić się z faktem, że wiele inicjatyw związanych z bezpieczeństwem informacji w firmach, instytucjach pojawia się wówczas, kiedy dochodzi do utraty danych lub innych incydentów w świetle wymagań normy ISO 27001. W opinii autorów wiele organizacji niestety nie przeprowadza w ogóle (lub robi to w sposób nieprofesjonalny) identyfikacji i szacowania ryzyka. Organizacje nie identyfikują zagrożeń w drodze kompleksowej analizy we wszystkich obszarach swojej działalności. Niestety organizacje nie badają również skuteczności stosowanych zabezpieczeń na podstawie sukcesywnie zaplanowanych symulacji w sytuacjach kryzysowych.



Rys. 2. Podział dokumentacji systemu bezpieczeństwa informacji w organizacji z uwzględnieniem europejskiego podejścia do Strategicznej Karty Wyników
Źródło: Opracowanie własne

3. Wnioski

W niniejszej publikacji podjęto próbę ukazania głównych aspektów bezpieczeństwa informacji w organizacji w kontekście stosowania metod poprawy skuteczności procesów wewnętrznych. Omówienie idei podejścia europejskiego do Strategicznej Karty Wyników w organizacji (w kontekście bezpieczeństwa informacji) w przekonaniu autorów stanowi o nowatorskości niniejszego opracowania.
Europejskie podejście do Strategicznej Karty Wyników oraz bezpieczeństwo informacji w ramach prowadzonej działalności gospodarczej będą odrywały coraz większe znaczenie w najbliższych latach. Należy zwrócić uwagę, że nie chodzi tylko i wyłącznie o zmieniające się dynamicznie prawodawstwo w tym zakresie, a przede wszystkim wymagania kontrahentów, częstokroć wobec powierzonej do administrowania np. własności intelektualnej. Niewątpliwie jest to obszar, w działalności wielu organizacji, który będzie się dynamicznie rozwijał.

Z przeprowadzonych obserwacji oraz doświadczenia we wdrożeniach systemów zarządzania, skorelowanych z innymi elementami zarządczymi takimi jak np. systemy bezpieczeństwa informacji, można stwierdzić, że wprowadzenie metod opartych na

podejściu procesowym (wspartym innymi elementami poprawy skuteczności zarządzania) umożliwia poprawę stopnia realizacji mierzalnych celów, strategii czy też wizji organizacji. Sprofilowanie działalności organizacji na dynamiczne postępowanie zarządcze w/w obszarach powoduje, że poprawia także funkcjonowanie wewnętrznej komunikacji, co w konsekwencji prowadzi to poprawy osiąganych na bieżąco parametrów w ustanowionych miernikach skuteczności procesów.

Konkludując jednoznacznie należy stwierdzić, że dla każdej organizacji niezależnie od jej specyfiki działalności priorytetami powinny stać się: bezpieczeństwo informacji oraz poprawa skuteczności zarządzania. Dzięki odpowiedniemu nadzorowaniu informacji organizacji zwiększa prawdopodobieństwo uzyskania przewagi konkurencyjnej, która w konsekwencji przy zaplanowanej i realizowanej świadomie strategii organizacji może przyczynić się do poprawy skuteczności procesów wewnętrznych w organizacji.

Literatura

1. Lewandowska A., Likierski M.: Pod presją czasu. Strategiczna Karta Wyników w praktyce, Wydawnictwo C.H Beck Sp. z o.o., Warszawa 2005.
2. PN-ISO/IEC 27001:2007, Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania, PKN, Warszawa 2007.

Dr inż. Piotr WOŹNIAK
Instytut Zarządzania Państwowej Wyższej Szkoły Zawodowej w Nysie/ Regionalne Centrum Transferu Wiedzy i Technologii Innowacyjnych przy Państwowej Wyższej Szkole Zawodowej w Nysie
48-300 Nysa ul. Armii Krajowej 7
tel./fax: (77) 409 16 82
e-mail: rctwiti@pwsz.nysa.pl
wozniakpiotr@op.pl

Dr inż. Jarosław WĄSIŃSKI
Wyższa Szkoła Zarządzania „EDUKACJA" we Wrocławiu
ul. Krakowska 56-62, 50-425 Wrocław
tel. 71/ 37 72 100, 101, fax. 71/ 37 72 107
e-mail: edukacja@edukacja.wroc.pl