PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU nr 116
Zarządzanie strategiczne w praktyce i teorii 2010

Sławomir Wawak
Uniwersytet Ekonomiczny w Krakowie

ZARZĄDZANIE BEZPIECZEŃSTWEM WIEDZY W KONTEKŚCIE ROZWOJU ORGANIZACJI*

Streszczenie: Współcześnie zasoby wiedzy stają się głównym źródłem przewagi konkurencyjnej. Organizacje muszą podejmować działania na rzecz właściwego wykorzystania ich zasobów oraz zabezpieczenia ich przed ujawnieniem czy zmniejszeniem wartości. Systemy informatyczne pozwalają przedsiębiorstwom na ograniczenie liczby naruszeń bezpieczeństwa informacji. Jednak poza zasięgiem tych systemów pozostają zasoby wiedzy. W artykule omówiono ograniczenia systemów zarządzania bezpieczeństwem informacji oraz wskazano na możliwości ich rozwoju w kierunku systemu zarządzania bezpieczeństwem wiedzy.

Słowa kluczowe: bezpieczeństwo informacji, bezpieczeństwo wiedzy, zarządzanie wiedzą, systemy informacyjne, ISO 27001.

1. Uwagi wstępne

Rozważając, za A. Stabryłą, pojęcie zarządzania strategicznego, należy zauważyć, że jest ono „procesem informacyjno-decyzyjnym, którego celem jest rozstrzyganie o kluczowych problemach działalności przedsiębiorstwa" [Stabryła 2000, s. 11]. Ujęcie to wskazuje na rolę zarządzania informacjami, a w szerszym kontekście zarządzania wiedzą w organizacji[1]. Ważnymi aspektami są tu gromadzenie informacji, ich przetwarzanie, jakość i dostępność wiedzy niezbędnej do podjęcia decyzji strategicznych, wiedza o już podjętych decyzjach, jak i ich skutkach. Należy przy tym zwrócić uwagę na znaczenie zapewnienia dostępności i integralności informacji oraz poufności (wobec otoczenia lub pracowników). W tym kontekście pojawia się problem bezpieczeństwa wiedzy, które będzie rozumiane, za K.C. Desouza [2006, s. 1], jako część wspólna dwóch obszarów badawczych: bezpieczeństwa informacji oraz zarządzania wiedzą. Bezpieczeństwo informacji jest zarówno w literaturze, jak i w praktyce przedsiębiorstw traktowane głównie w kontekście zabezpieczeń informa-

* Artykuł jest efektem badań wstępnych projektu badawczego N N115 010638 realizowanego przez autora.

[1] Należy zwrócić uwagę na słabe zarysowanie w nauce zarządzania związków między informacją a wiedzą, wieloznaczność i wielopoziomowość tych pojęć. Z tego względu w niniejszych rozważaniach przyjęto jedną z koncepcji zaprezentowaną w [Stabryła 2009, s. 165 i n.].

tycznych oraz technicznych, ograniczeń fizycznego dostępu do wybranych pomieszczeń firmy, stosowania poziomów dostępu do dokumentów i baz elektronicznych czy zapewnienia ciągłości działania urządzeń. Z kolei badacze zarządzania wiedzą koncentrują się na identyfikacji, gromadzeniu, zachowywaniu, przekazywaniu i wykorzystaniu wiedzy w celu podniesienia efektywności funkcjonowania organizacji. Nierzadko w tych rozważaniach pomijane są kwestie bezpieczeństwa wiedzy. Problem ten ujawnia się szczególnie w obszarach, w których dostęp do wiedzy jest kluczowym czynnikiem decydującym o sukcesie lub porażce organizacji. Takim obszarem jest zarządzanie strategiczne.

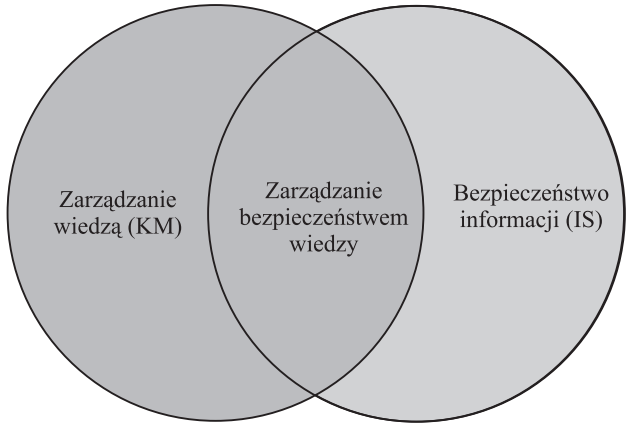
2. Istota zarządzania bezpieczeństwem wiedzy

Współcześnie w coraz większym stopniu zasoby wiedzy stają się źródłem przewagi konkurencyjnej przedsiębiorstwa. Organizacja musi podejmować wysiłki na rzecz właściwego wykorzystania posiadanych aktywów, a także zabezpieczenia ich przed nieprawidłowym użyciem, ujawnieniem czy zmniejszeniem ich wartości dla utrzymania przewagi konkurencyjnej (np. poprzez wprowadzenie imitacji, zamienników). Nie bez znaczenia jest przy tym fakt, że zasoby wiedzy stanowią czynnik napędowy dla wykorzystania innych zasobów materialnych czy finansowych. Zatem nie wystarczy zatrudnienie pracowników posiadających odpowiednią wiedzę. Nie mniej ważny jest dobór takich pracowników, którzy będą umieli ją przetworzyć i wygenerować nowe rozwiązania – produkty, usługi czy technologie. Dopiero wtedy maszyny, infrastruktura czy zasoby finansowe będą mogły zostać efektywnie spożytkowane.

Patrząc na zasoby wiedzy od strony ekonomicznej, należy zauważyć, że korzyści z ich wykorzystania są trudne do oceny *ex ante*. Może się bowiem zdarzyć, że wielomiesięczne badania, na które wydano dużą kwotę pieniędzy, zakończą się niepowodzeniem. Z kolei inny projekt może doprowadzić do przełomu bardzo szybko i przy niewielkich nakładach. Organizacje, które dążą do efektywnego wykorzystania zasobów wiedzy muszą być świadome tego, że tylko jeden na wiele projektów zakończy się sukcesem. Sukces ten być może pokryje koszty pozostałych badań. Jeżeli jednak dane takiego projektu zostaną wykradzione, ujawnione, skopiowane lub konkurencja samodzielnie znajdzie podobne rozwiązanie przed ukończeniem procesu patentowego, to przedsiębiorstwo poniesie straty. Zasoby wiedzy nie mogą zostać zastąpione innego rodzaju zasobami. Ich ujawnienie lub utracenie powoduje, że tracą swoją wartość dla organizacji. Inaczej niż w przypadku dóbr materialnych, ich odzyskanie po utracie może nie wiązać się z odzyskaniem pełnej wartości.

Zapobieżeniu tej sytuacji służyć ma system zarządzania bezpieczeństwem wiedzy. Zależność między zarządzaniem wiedzą, bezpieczeństwem informacji a zarządzaniem bezpieczeństwem wiedzy pokazano na rys. 1.

Zabezpieczenie zasobów wiedzy z wykorzystaniem metod proponowanych w systemach zarządzania bezpieczeństwem informacji (SZBI), np. ISO 27001:2005, jest niewystarczające. Należy od razu zauważyć, że odnośnie do informacji przecho-



Rys. 1. Relacja między zarządzaniem wiedzą, bezpieczeństwem informacji a zarządzaniem bezpieczeństwem wiedzy

Źródło: [Desouza 2006, s. 2].

wywanych na nośnikach papierowych lub elektronicznych proponowane metody można uznać za dobre lub bardzo dobre. SZBI ogranicza się bowiem do tego, co łatwe do uchwycenia i zmierzenia, jak np. nadawanie uprawnień do aktywów, procedury zwrotu aktywów, postępowanie sprawdzające przy zatrudnieniu pracownika. Pomija natomiast to, czego nie da się łatwo sprawdzić podczas certyfikacji systemu – audyt wiedzy, narzędzia wspomagające kreowanie czy przekazywanie wiedzy, zabezpieczenie przed utratą wiedzy. Lista zabezpieczeń w grupie A.8 – dotyczących personelu – wskazuje wyraźnie na narzędziowe i proceduralne traktowanie pracowników, jako „czynnika ludzkiego" mającego swoje miejsce w określonych procesach. Sytuację pogarsza fakt dążenia do formalizacji wszystkich działań w systemie, co jest podyktowane realizacją zadania postawionego zespołowi wdrożeniowemu – uzyskać zgodność certyfikacyjną, czyli udokumentować system tak, aby audytor nie miał wątpliwości.

Tymczasem system ten należy projektować, opierając się na zasadzie zachowania konsensu między kierownictwem a pracownikami, w atmosferze dyskusji na temat sposobów zastosowania pewnych zabezpieczeń (szczególnie tych, które mogą być negatywnie odebrane przez zatrudnionych). Zwiększy to zainteresowanie i zaangażowanie w budowę systemu. Pozwoli także zwiększyć świadomość pracowników dotyczącą problemów bezpieczeństwa i oddziaływać dzięki temu nie tylko na informację, ale również na wiedzę.

W organizacji uczącej się kultura organizacyjna jest zorientowana na pozyskiwanie wiedzy. Wszelkie doświadczenia są wykorzystywane do kreowania nowej wiedzy. Panuje w niej otwartość, możliwość dyskusji, prezentacji odmiennych zdań. Wymaga to stosowania otwartego systemu komunikacji, do którego dostęp mają

wszyscy pracownicy. Warunkami koniecznymi są: osobiste doskonalenie, autonomia jednostek, niestabilność, nadmiarowość i różnorodność wiedzy oraz wzajemne zaufanie. Takie założenia znacznie utrudniają wdrożenie systemu zarządzania bezpieczeństwem informacji, który zmusza do stosowania ograniczeń przepływu informacji, zachęca do ograniczania nadmiarowości. Szeroki dostęp pracowników do wiedzy może stanowić zagrożenie, natomiast panowanie twórczego chaosu − prowadzić do ignorowania niektórych zabezpieczeń. Głównym problemem może jednak okazać się stabilność SZBI wobec częstej zmiany metod działania wynikającej z dynamicznego wprowadzania nowych rozwiązań organizacyjnych. Konieczne zatem staje się projektowanie takiego systemu, który nie ograniczy tej dynamiki.

Relację między SZBI a systemem zarządzania bezpieczeństwem wiedzy można przyrównać do relacji między ISO 9001 a TQM. Wdrożenie systemów opartych na normach ISO jest oczywiście ważnym i potrzebnym (w warunkach europejskich) krokiem na rzecz uporządkowania zarządzania organizacją, nie może być jednak postrzegane jako cel sam w sobie. Organizacje, które wdrażają SZBI bez świadomości długookresowych celów mogą wpaść w pułapkę biurokracji, podobnie jak to się dzieje w przypadku systemów zarządzania jakością. Może to doprowadzić do ucieczki pracowników wiedzy.

Procedura wdrożenia systemu zarządzania bezpieczeństwem wiedzy, budowanego jako rozszerzona wersja SZBI, powinna uwzględniać następujące kroki[2]:

1. Przeprowadzenie serii szkoleń pracowników w celu zwiększenia świadomości znaczenia bezpieczeństwa informacji i wiedzy dla organizacji.
2. Określenie zakresu i granic systemu.
3. Opracowanie polityki bezpieczeństwa wspólnie przez kierownictwo i pracowników. Opracowanie lokalnych polityk dla poszczególnych pionów lub działów.
4. Określenie metod audytu wiedzy, wyceny wiedzy oraz szacowania ryzyka.
5. Przeprowadzenie audytu wiedzy oraz jej wyceny.
6. Analiza i ocena czynników ryzyka.
7. Identyfikacja i ocena wariantów postępowania z czynnikami ryzyka.
8. Analiza możliwości zastosowania zabezpieczeń oraz ich wybór.
9. Akceptacja ryzyka szczątkowego przez kierownictwo. Autoryzacja dla wdrożenia systemu.
10. Powołanie i przeszkolenie zespołów wdrożeniowych.
11. Opracowanie przez zespoły szczegółowej dokumentacji systemu zarządzania bezpieczeństwem wiedzy, w tym: opisów zabezpieczeń, procedur, instrukcji, systemu pomiarowego, planów postępowania w przypadku wystąpienia zagrożeń, planów zachowania ciągłości działania.
12. Przegląd i analiza dokumentacji, uzupełnianie ewentualnych braków.
13. Akceptacja dokumentacji i wdrożenie.
14. Sprawdzenie skuteczności wdrożenia (audyty wewnętrzne).

[2] Procedura została rozwinięta na bazie wymagań punktów 4.2 i 4.3 normy ISO 27001:2005 opisujących proces wdrażania SZBI [*Norma ISO*… 2007, s. 9].

W procedurze wdrożeniowej należy na każdym etapie, gdzie to tylko możliwe, uwzględniać działania na rzecz zwiększenia zaangażowania pracowników. Należy, poprzez szkolenia, zapewnić wysoki poziom przekonania pracowników o potrzebie stosowania systemu oraz celowości wprowadzania i przestrzegania ograniczeń. Jednocześnie należy wyczulić zespoły wdrożeniowe na poszukiwanie rozwiązań, które zapewnią wysoki poziom bezpieczeństwa, a przy tym będą w najmniejszym stopniu ograniczać efektywność procesów zarządzania wiedzą.

3. Trudności zabezpieczenia wiedzy

Wiedza jest trudna do zabezpieczenia ze względu na swój charakter. Inaczej niż w przypadku informacji, które są pewnym produktem, wiedzę można postrzegać jako strumień podlegający stałym przekształceniom. Jest ona przez to trudna do uchwycenia, wizualizacji czy zindeksowania. Nieograniczone dzielenie się wiedzą, które jest tak ważne dla kreowania nowych rozwiązań, stanowi jednocześnie (w ujęciu tradycyjnym) zagrożenie dla bezpieczeństwa organizacji. W małych firmach pracownicy dzielą się wiedzą bez istotnych ograniczeń organizacyjnych. Nie występują bariery pomiędzy komórkami organizacyjnymi, rozwój firmy oparty jest m.in. na wzajemnym zaufaniu, pracownicy znają cele i plany właściciela. W miarę wzrostu przedsiębiorstwa przekazywanie informacji pomiędzy niektórymi jego obszarami, jak badania i rozwój, marketing, planowanie strategiczne, jest ograniczane ze względów bezpieczeństwa przez procedury i formalne zasady. Rozdzielanie tych obszarów ogranicza przepływy wiedzy, co może doprowadzić do ich niewłaściwego działania. Optymalną z punktu widzenia rozwoju organizacji i dyfuzji wiedzy konfiguracją systemu bezpieczeństwa wiedzy jest sytuacja, gdy blokowane są tylko drogi przekazywania wiedzy na zewnątrz, bez ingerencji w powiązania wewnątrzorganizacyjne. Niestety, jak pokazują badania, znaczna część przypadków naruszenia bezpieczeństwa jest powodowana świadomie przez pracowników. Aż 2/3 pracowników rozstających się z różnych przyczyn z firmą zabiera ze sobą poufne informacje, które „mogą się przydać" [Lynch 2006, s. 40]. Każdy pracownik zabiera ze sobą wiedzę. Dlatego w praktyce taka konfiguracja nie jest możliwa.

Niewłaściwe zabezpieczanie wiedzy może polegać na próbie ograniczania jej integralności na poziomie pracownika poprzez udostępnianie tylko wybranych informacji lub formalne zakazy dyskusji o pewnych kwestiach. Takie działania powodują frustrację u pracowników, którzy chcą po prostu pracować i dobrze wykonywać swoje zadania. Zatrzymuje lub znacznie zwalnia to proces dyfuzji wiedzy, ogranicza zaangażowanie, a także może zwiększyć fluktuację. Te metody zabezpieczeń prowadzą do zorganizowania firmy na wzór służb wywiadowczych, co może zapewnić bezpieczeństwo, jednak nie zagwarantuje postępu i sukcesu na rynku.

Kwestią o charakterze podstawowym, o której nie można zapomnieć, konstruując system zarządzania bezpieczeństwem wiedzy, jest znaczenie zaufania pomię-

dzy pracownikiem a organizacją w gospodarce opartej na wiedzy. Jak wskazał M. Morawski [Perechuda 2005, s. 193], „nie sposób kultywować wiedzy, dokonywać jej dyfuzji, tworzyć nowe jej pokłady bez poczucia emocjonalnej bliskości, więzi łączących ludzi i zespoły, gotowych do wzajemnej wymiany myśli i poglądów, otwartego dialogu i merytorycznych sporów". Na kwestię tę zwraca uwagę także P.M. Senge [2006, s. 325], pisząc o zmianie roli menedżerów i konieczności porzucenia dotychczasowych koncepcji władzy w organizacji na rzecz współpracy. Tymczasem w literaturze można spotkać propozycje wprowadzania kontroli czy zaawansowanego controllingu powiązanego z systemami motywacyjnymi, co stanowi jaskrawy przykład narzędziowego traktowania pracowników. M. Bugdol [2006, s. 22] wskazuje, że naruszenie zaufania przez pracodawcę lub pracownika, jak np. zmiana zasad *post factum*, kłamstwo, wyjawienie sekretów firmy, kradzież idei, mogą doprowadzić do bankructwa firmy. To, czy w organizacji będzie występował wysoki, czy niski poziom zaufania, zależy od szeregu czynników odnoszących się przede wszystkim do kierownictwa odpowiedzialnego za tworzenie klimatu zaufania, pracowników, ale także od czynników zewnętrznych, jak np. polityka społeczna państwa, oczekiwania obywateli wobec władz i przedsiębiorstw czy uwarunkowania strukturalne i kulturowe[3]. Jednocześnie M. Bugdol zauważa, że kontrola jako funkcja nie jest sprzeczna z ideą zarządzania wiedzą, jednak zbyt często zapomina się o jej skutkach ubocznych, w tym o zmniejszeniu poczucia odpowiedzialności pracowników za wykonywane zadania oraz ograniczeniu zaufania. Kontrola przygotowana w odpowiedni sposób może nawet zwiększyć zaufanie, o ile jest ustalona w szczegółach z pracownikiem na etapie planowania zadań. Zdaniem wspomnianego autora skuteczna kontrola (tzn. taka, która pozwala budować zaufanie) jest możliwa, jeżeli [Bugdol 2006, s. 39]:

- zagwarantowany jest udział wszystkich pracowników w uzgadnianiu procedur kontrolnych,
- wyniki kontroli służą tylko do doskonalenia pracy,
- sam system kontroli podlega doskonaleniu,
- kontrola jest oparta na zaufaniu.

4. Podsumowanie

Rozwój współczesnej organizacji zależy w dużej mierze od jej powodzenia w gromadzeniu, kreowaniu i wykorzystaniu zasobów wiedzy. E. Skrzypek [2009, s. 50] zwraca uwagę, że w dzisiejszej gospodarce źródłem uzyskania przewagi jest umiejętność dostarczania nowych idei, nie zaś dysponowanie dużym kapitałem. Przed-

[3] Nie bez znaczenia pozostaje fakt, że instytucje i otoczenie mają jednocześnie wpływ na poziom kreatywności pracowników poprzez zachęcanie do działań pożądanych, represjonowanie działań niestandardowych, utrwalanie sposobów myślenia, promowanie lub negowanie indywidualizmu członków społeczeństwa. Więcej miejsca temu problemowi poświęca T. Bal-Woźniak [2009, s. 357 i n.].

siębiorstwa wiodące w gospodarce opierają swój rozwój na [Romańczuk 2003, s. 141 i n.]:

- dzieleniu się wiedzą w rozwiązywaniu problemów biznesowych,
- wysokiej świadomości pracowników w zakresie zdobywania wiedzy i dzielenia się nią,
- powiązaniu głównych wartości firmy z samodoskonaleniem,
- stylu zarządzania wiedzą dopasowanym do środowiska organizacji,
- aktywnym promowaniu dzielenia się wiedzą przez menedżerów,
- nieformalnych grupach wymiany informacji działających w formie sieci,
- systemach motywacji zachęcających do dzielenia się wiedzą i współpracy.

Organizacje, które stawiają w swoim rozwoju na zasoby wiedzy, budują systemy ograniczające ryzyko wycieku informacji na zewnątrz. Aktualne rozwiązania informatyczne pozwalają na redukcję skuteczności ataków do minimum. Jednak poza zasięgiem tych zabezpieczeń są działania pracowników oraz wiedza będąca w ich posiadaniu. Dlatego do zapewnienia stabilnego rozwoju organizacji niezbędne jest rozszerzenie SZBI do systemu zarządzania bezpieczeństwem wiedzy.

Literatura

Awazu Y., Desouza K.C., *Open knowledge management: Lessons from the open source revolution*, „Journal of the American Society For Information Science and Technology" 2004, no. 55 (11).

Bal-Woźniak T., *Instytucjonalne stymulatory i ograniczenia kreatywności*, [w:] E. Skrzypek (red.), *Kreatywność i przedsiębiorczość w projakościowym myśleniu i działaniu*, UMCS, Lublin 2009.

Bugdol M., *Wartości organizacyjne. Szkice z teorii organizacji i zarządzania*, Wydawnictwo UJ, Kraków 2006.

Coley G., *Take advantage of open-source hardware*, „EDN", August 20, 2009.

Desouza K.C., *Knowledge security: An interesting research space*, „Journal of Information Science and Technology" 2006, vol. 3, iss. 1.

Desouza K.C., Awazu Y., *Securing knowledge assets*, „Jap@n Inc", August 2004.

Hoepman J.-H., Jacobs B., *Increased security through open source*, „Communications of The ACM" 2007, vol. 50, no. 1.

Liebowitz J., Rubenstein-Montano B., McCaw D., Buchwalter J., Browning C., *The knowledge audit*, „Knowledge and Process Management" 2000, vol. 7, no. 1.

Lynch D.M., *Securing against insider attacks*, „Information Security and Risk Management", November 2006.

Norma ISO 27001:2005 Technika informatyczna − Techniki bezpieczeństwa − Systemy zarządzania bezpieczeństwem informacji − Wymagania, PKN, Warszawa 2007.

Perechuda K. (red.), *Zarządzanie wiedzą w przedsiębiorstwie*, PWN, Warszawa 2005.

Richards G., *Time to hit the open source road*, „Engineering & Technology", September 12, 2009.

Romańczuk A., *Zarządzanie wiedzą w korporacjach*, [w:] B. Wawrzyniak (red.), *Zarządzanie wiedzą w przedsiębiorstwie*, WSPiZ, Warszawa 2003.

Senge P.M., *Piąta dyscyplina*, Oficyna Ekonomiczna, Warszawa 2006.

Skrzypek E., *Uwarunkowania projakościowego myślenia i działania – kreatywność, przedsiębiorczość i innowacyjność*, [w:] E. Skrzypek (red.), *Kreatywność i przedsiębiorczość w projakościowym myśleniu i działaniu*, UMCS, Lublin 2009.
Stabryła A. (red.), *Doskonalenie struktur organizacyjnych przedsiębiorstw w gospodarce opartej na wiedzy*, C.H. Beck, Warszawa 2009.
Stabryła A., *Zarządzanie strategiczne*, PWN, Warszawa 2000.

KNOWLEDGE SECURITY MANAGEMENT IN THE CONTEXT OF ORGANIZATION DEVELOPMENT

Summary: Nowadays, knowledge assets become the main source of competitive advantage. Organizations need to make efforts for the proper use of their assets and protect them from improper use, disclosure or decrease their importance. Current computer solutions allow companies to reduce security breaches with information assets. However, beyond the reach of these systems are knowledge assets. The article discusses some limitations ISMS and indicates the possibility of its development to the knowledge security management system.