PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU
Nr 49 2009
Zmiana warunkiem sukcesu
Rozwój i zmiany w małych i średnich przedsiębiorstwach

Zbigniew Malara, Artur Pajkert
Politechnika Wrocławska

BEZPIECZEŃSTWO I OCHRONA WIEDZY W PRAKTYCE ORGANIZACYJNEJ MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW W POLSCE. DOŚWIADCZENIA Z BADAŃ

1. Wstęp

We współczesnej gospodarce nadrzędny paradygmat o potrzebie posiadania aktywów fizycznych (materialnych), aby uzyskać wyższą efektywność, przyjmuje formę gasnącą, a znaczenia zaczynają nabierać byty niematerialne: wyniki badań, marka, lojalność pracowników i odbiorców, reputacja itp., oraz ludzie. W niektórych branżach, np. informatycznej, telekomunikacji, farmacji, konsultingu i edukacji, kapitał ten okazuje się na tyle ważny, że menedżerowie szukają sposobów na określenie jego wartości[1]. Przedsiębiorstwo wzbogacone o wiedzę rozwija bowiem swój kapitał intelektualny, a to oznacza nowe kompetencje i – w konsekwencji – poszerzenie przestrzeni działania oraz nowe szanse dla ekspansji i rozwoju przedsiębiorstwa. W związku z tym na rynku coraz liczniej pojawiają się przedsiębiorstwa, które nie mają zamiaru konkurować wyłącznie w oparciu o produkty, na dodatek o wysokim stopniu pracochłonności, lecz takie, które budują sukces, czerpiąc ze źródeł wiedzy pracowników i zasobów zgromadzonych „w przepastnych magazynach", zbudowanych z użyciem ultranowoczesnych technologii.

2. Wiedza w przedsiębiorstwie – atrybuty i charakter

Przedsiębiorstwo, zależnie od potencjału, jakim dysponuje, oraz jego bieżącej pozycji na rynku i zamiarów strategicznych, tworzy i uruchamia zasoby wiedzy o różnym stopniu istotności dla funkcjonowania przedsiębiorstwa. Czerpie przy tym z różnych kategorii wiedzy:

[1] Takie przedsiębiorstwa, jak: CIBA Speciality Chemicals, ICI, ICL, Monsanto, Nestle, Stat Oil Company oraz Unilever, tworzą konsorcja, dla których celem jest poszukiwanie sposobów na identyfikację i wykorzystywanie posiadanej wiedzy oraz tworzenie instrumentów wspomagających te procesy [Obłój 2002, s. 126].

– wiedzę podstawową (o minimalnym zakresie), która umożliwia konkurowanie na rynku w ograniczonym stopniu,
– wiedzę zaawansowaną, pozwalającą na osiąganie przewagi konkurencyjnej,
– wiedzę innowacyjną, nasyconą rozwiązaniami, którymi nie dysponują inni uczestnicy rynku [Malara 2007, s. 142].

O tym, w jakim stopniu udaje się korzystać z posiadanej wiedzy, decydują – z jednej strony – umiejętności służące jej wzbogacaniu i pozyskiwaniu nowej wiedzy, a z drugiej strony – zdolność tworzenia warunków do odpowiedniego reglamentowania (podziału) oraz dalszego jej transferu. Wymaga to opanowania umiejętności i swoistej biegłości w tworzeniu i obsłudze systemów ochrony wiedzy przed zawłaszczaniem jej przez konkurencję oraz w zapewnieniu bezpieczeństwa gromadzonych danych i kluczowych (ważnych strategicznie) informacji.

3. Ochrona wiedzy w praktyce organizacyjnej przedsiębiorstwa

Zasoby wiedzy gromadzonej w przedsiębiorstwie poddawane są z założenia zarówno eksploatacji, jak i eksploracji. Ten pierwszy rodzaj działania jest oparty na bieżącej działalności (operacyjnej), której celem jest dostosowywanie się przedsiębiorstwa do konkurencyjnego otoczenia, w oparciu o działania reaktywne (*up to date*) przy wykorzystaniu mechanizmu sprzężenia zwrotnego (*feed back*). Eksploracja zaś umożliwia antycypację zmian w otoczeniu i formowanie wobec nich działań z właściwym wyprzedzeniem (*feed forward*), a w konsekwencji prowadzenie działań, których celem jest osiąganie i utrzymywanie przewagi konkurencyjnej w wymiarze strategicznym. Obydwa procesy tworzą platformę do identyfikacji pożądanych kierunków zmian, implementowania rozwiązań służących realizowaniu obranych strategii (głównej oraz cząstkowych) wraz z równoległym dostosowywaniem przedsiębiorstwa do wymagań burzliwego otoczenia.

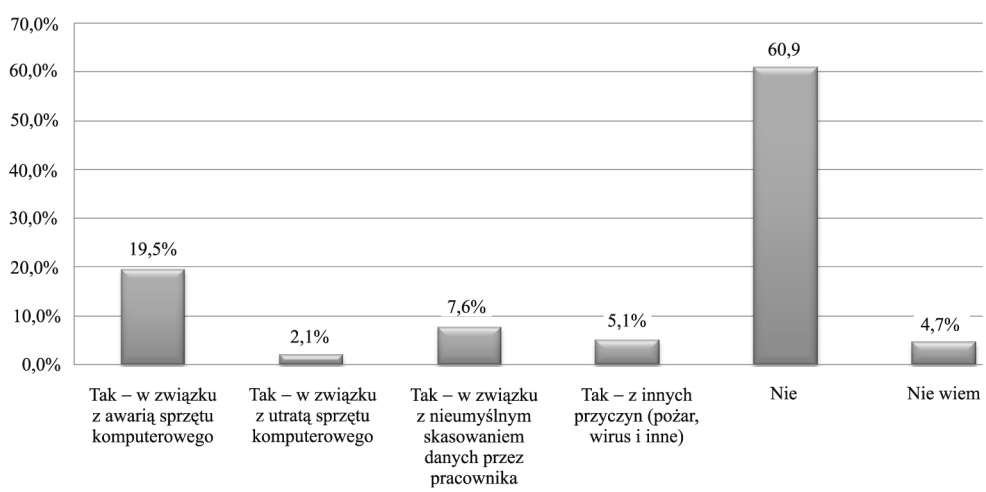
Wiedza w przedsiębiorstwie bywa w wysokim stopniu zdekomponowana do poziomu danych, przechowywanych i przetwarzanych w systemach komputerowych. Tak zgromadzone dane są narażone na liczne niebezpieczeństwa, jak choćby: atak wirusa, ludzkie błędy (przypadkowe skasowanie pliku, opróżnienie kosza), rozlanie płynu (kawy, herbaty) na komputer przenośny, awarie sieci elektrycznej i tzw. przepięcia, kradzież komputera czy włamanie do firmy), niestosowanie macierzy dyskowych w stacjach roboczych (praca na pojedynczych dyskach), zgubienie laptopa (np. pozostawienie w autobusie), uszkodzenie mechaniczne komputera (*vide*: przypadek ministra Ziobry, szarpnięcie laptopem podczas pracy dysku, upuszczenie komputera, strącenie go z biurka itp.), sabotaż, wydarzenia katastroficzne, takie jak: pożar, powódź czy katastrofa budowlana. Jak wynika z podanych przykładów, narażone są przede wszystkim, choć nie tylko, dane zgromadzone w komputerach przenośnych. W roku 2005 24% małych i aż 35% średnich przedsiębiorstw borykało się z problemami bezpieczeństwa sieci lub danych [*Społeczeństwo informacyjne...* 2008].

Zagadnienie wydaje się ważne, ponieważ utrata danych może powodować przedsiębiorstwie znaczne negatywne skutki. Można do nich zaliczyć: całkowity paraliż firmy, jeśli utracono kluczowe dane; konieczność odzyskiwania danych z uszkodzonego nośnika (z zasady bardzo kosztownego, sięgającego nawet kilku tysięcy złotych za odzyskanie danych z fizycznie uszkodzonego dysku); konieczność odbudowania danych finansowych w oparciu o dokumenty fizycznie istniejące (ogromny nakład pracy); bezpowrotną utratę korespondencji biznesowej; trudności w kontakcie z partnerami biznesowymi, w przypadku utraty danych adresowych; utratę kosztownego oprogramowania, zwłaszcza w modelu licencjonowania OEM; utratę zapisanych w komputerze haseł dostępowych do usług internetowych; konieczność zapłaty kar umownych za nieterminowe oddanie projektów itp.

4. Ochrona i bezpieczeństwo danych w przedsiębiorstwie w świetle badań

Badanie przeprowadzono w sierpniu i wrześniu 2008 r. na próbie 470 małych i średnich przedsiębiorstw z terenu całego kraju. Badanie polegało na wyświetleniu w panelach użytkowników serwerów wirtualnych jednej z wiodących firm hostingowych, OGICOM Sp. z o.o., ankiet z pytaniami dotyczącymi zagadnień bezpieczeństwa danych i epizodów utraty danych. Przebieg i wyniki badań przedstawiono poniżej.

- Czy w ciągu ostatniego roku Pana/Pani firma utraciła istotne dane?

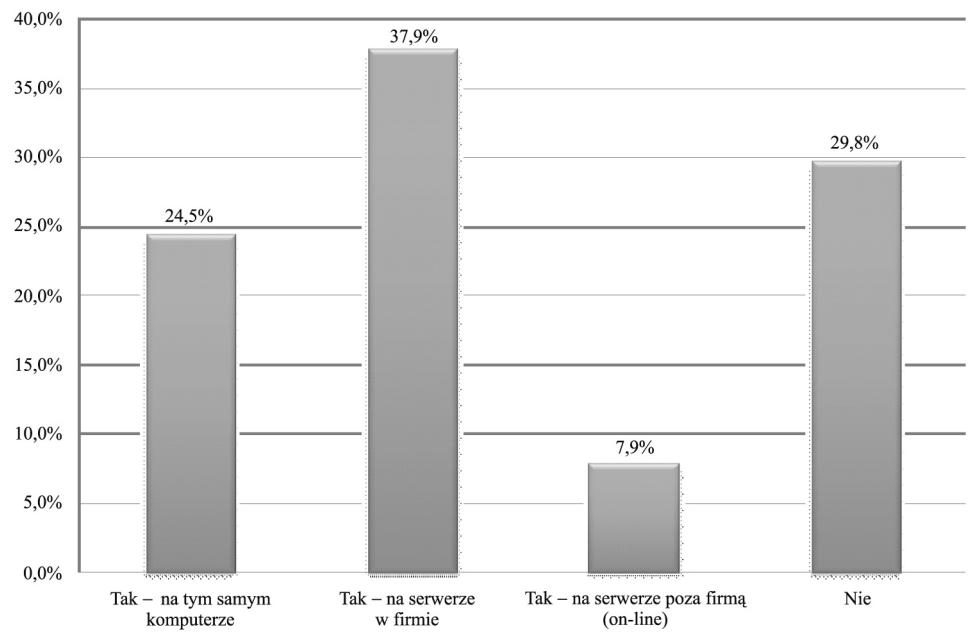


Rys. 1. Przypadki utraty danych

Źródło: opracowanie własne przy współpracy z OGICOM Sp. z o.o.

Z rysunku 1 wynika, że jedynie 5% respondentów nie potrafiło ocenić, czy w ciągu ostatniego roku doszło do utraty danych, czy też nie. Oznacza to, iż dla pozostałych przedsiębiorców dane jako zasób są na tyle istotne, iż mają oni świadomość, czy doszło do ich uszkodzenia. Blisko 35% respondentów przyznaje, że w ciągu ostatniego roku doszło w ich przedsiębiorstwie do incydentu utraty danych. Główną przyczyną była awaria sprzętu komputerowego (19,5%), co oznacza ochronę danych poprzez przymus zrzucania danych (*back up*). Winno się to wykonać za pomocą urządzenia zewnętrznego, jak bowiem pokazuje doświadczenie, aż w co piątym przedsiębiorstwie to urządzenie wewnętrzne komputera (dysk, kontroler, stacje dysków) uległo awarii.

- Czy Pani/Pana firma regularnie wykonuje kopie zapasowe istotnych danych?



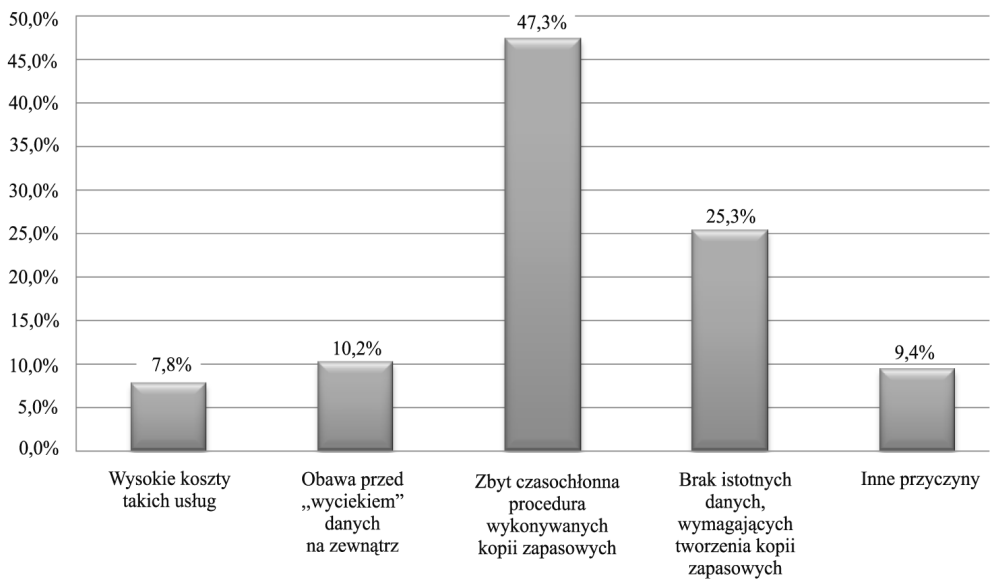
Rys. 2. Sposoby wykonywania backupu

Źródło: opracowanie własne przy współpracy z OGICOM Sp. z o.o.

Wyniki badań wskazują na niewielką świadomość tych przedsiębiorców, którzy wykonują kopie zapasowe (rys. 2). Ponad 40% z nich archiwizuje dane na tym samym komputerze, na którym zapisane są istotne informacje. Biorąc pod uwagę, że w prawie co piątym przypadku utrata danych jest wynikiem awarii sprzętu komputerowego, takiego rozwiązania nie można zaliczyć do skutecznych. Zaledwie 7,9% przedsiębiorców „backupuje" dane na zewnętrznych serwerach, a to oznacza, że ok. 92% przedsiębiorców nie chroni swoich danych przed wszystkimi możliwymi zagrożeniami. Istnieje wiele wymienionych wcześniej czynników ryzyka, które mogą

spowodować, że nie będzie można odzyskać danych, nawet jeśli były backupowane klasycznie. Zważywszy, że do częstej praktyki należy pozostawianie laptopa w aucie w czasie zakupów, zjawisko i ryzyko utraty danych wzrasta. Według statystyk policji w centrach handlowych w Polsce w 2007 r. dokonano blisko 11 483 kradzieży. Jeśli dodatkowo uwzględnimy także możliwość włamania, pożaru, powodzi lub uszkodzenia sprzętu – łatwo dostrzec, że backup na nośniki przechowywane w tym samym miejscu jest obciążony wyższym ryzykiem.

- Jeśli nie wykonuje się kopii – dlaczego (główna przyczyna)?

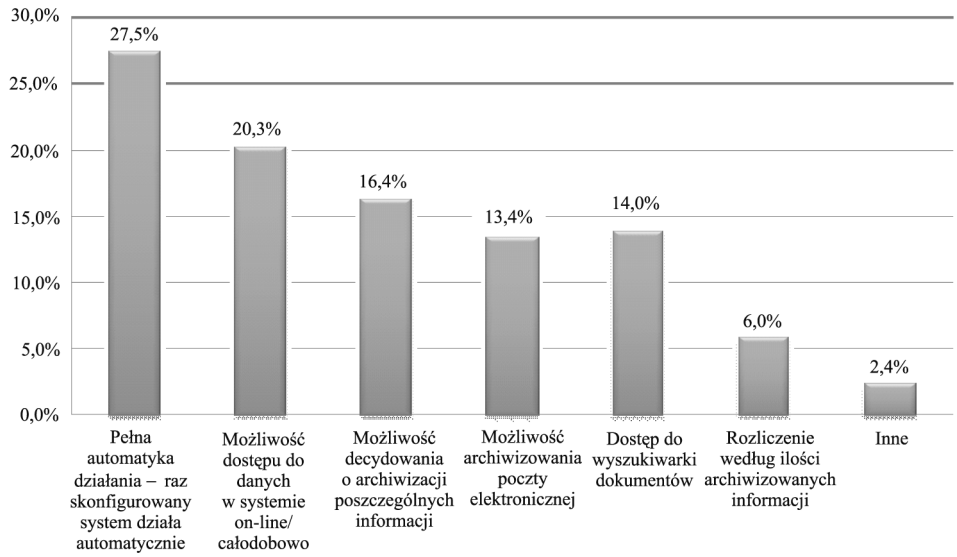


Rys. 3. Przeszkody w wykonywaniu backupu

Źródło: opracowanie własne przy współpracy z OGICOM Sp. z o.o.

Blisko połowa respondentów uznała czasochłonną procedurę za istotną przeszkodę w wykonywaniu kopii zapasowych (rys. 3). Dlatego, poza skutecznością, istotną cechą rozwiązań do backupu powinna być prostota i bezobsługowość. Duży wydaje się odsetek przedsiębiorstw nie dostrzegających konieczności tworzenia kopii zapasowych danych. Co czwarte przedsiębiorstwo nie uważa, aby zgromadzone w komputerach dane należało backupować. Jak widać więc, polskie przedsiębiorstwa wciąż nie wydają się przywiązywać wielkiej wagi do bezpieczeństwa zgromadzonej wiedzy.

- Jakie funkcje powinien posiadać system archiwizacji danych, aby Pana/Pani firma chciała skorzystać z takiej usługi?



Rys. 4. Pożądane funkcje backupu

Źródło: opracowanie własne przy współpracy z OGICOM Sp. z o.o.

W przypadku tego pytania (rys. 4) uzyskane odpowiedzi potwierdzają, że automatyzacja działania jest bardzo ważnym kryterium dla przedsiębiorcy, a raz skonfigurowany system powinien działać automatycznie – tę opinię potwierdza blisko 1/3 respondentów. Co piąty przedsiębiorca wskazuje natomiast, że istotny jest dostęp do danych w trybie *on-line*. Ta właściwość wydaje się bardzo pożądaną cechą, ponieważ zjawisko utraty danych ma z zasady charakter losowy i cechuje je duża niepewność. Dlatego przedsiębiorcy nie są w stanie przewidzieć, kiedy i w jaki sposób może dojść do utraty danych. W tym miejscu backup w trybie *disk-to-disk* ujawnia wyraźną przewagę nad innymi rozwiązaniami, ponieważ w przeciwieństwie do np. backupu taśmowego dane są archiwizowane na dyskach i są dostępne nieprzerwanie.

5. Podsumowanie

W świetle przeprowadzonych badań można stwierdzić, że przyjęta przez autorów hipoteza została zweryfikowana pozytywnie. Małe i średnie przedsiębiorstwa wydają się przykładać wciąż zbyt małą wagę do zagadnienia backupowania danych. Mimo powszechności oprogramowania antywirusowego, stosowanego przez 91% przedsiębiorstw [*Społeczeństwo informacyjne*... 2008], należy powiedzieć, iż mnogość rodzajów zagrożeń wymaga także stosowania wielorakich zabepieczeń. Wprawdzie backup nie chroni całkowicie przed utratą danych, jednakże pozwala uniknąć negatywnych skutków takiego zdarzenia lub przynajmniej je zminimalizować. Ponieważ backup danych stanowi swoistą „ostatnią linię obrony", powinno się stosować meto-

dy, które pozwalają na ochronę danych w najszerszym zakresie. Wydaje się, że najlepszym środkiem ochrony jest *back up on-line*, pozwalający na składowanie danych w odległej, profesjonalnej serwerowni. Metodę tę wykorzystuje jednak zaledwie 7,9% respondentów.

6. Konkluzje

Instrumentem wspomagającym ochronę i bezpieczeństwo wiedzy w przedsiębiorstwie jest właściwie funkcjonujący system działania, bez którego nie będzie możliwe zapewnienie bezpieczeństwa danych i informacji przed utratą, nierzadko bezpowrotną. Wymaga to respektowania w przedsiębiorstwie swoistego dekalogu, w którym można zawrzeć następujące wskazania:

- Powinno się zapewniać stałość (powtarzalność i cykliczność) funkcjonowania systemów kopiowania danych i informacji.
- Należy tak organizować zrzucanie wszelkich zasobów, aby równocześnie przyporządkować je konkretnemu kontekstowi działania (celowi). Redukuje się wówczas nadmiary zasobów (często zbędnych) i ogranicza koszty związane z ich przechowywaniem.
- Konieczne jest tworzenie ścieżek dostępu (systemów bibliograficznych i katalogów), usprawniających dostęp do kopiowanych zasobów.
- Bezwzględnie należy systematyzować i porządkować bazy danych, tworząc równocześnie, pakiety określonych rodzajów wiedzy.
- Na potrzeby kopiowania danych i informacji trzeba sięgać po wyspecjalizowane narzędzia eksperckie, służące automatyzowaniu i niezawodności procesu kopiowania.
- Przetwarzanie i przechowywanie zasobów danych i informacji winno odbywać się w oparciu o jednolite zasady, wspólne dla całego przedsiębiorstwa.
- Należy tworzyć tzw. bramki dostępu, to jest organizować dostęp do zasobów w taki sposób, aby zapewnić możliwość odnajdowania potrzebnej wiedzy z wielu poziomów zarządzania.
- Koniecznie uwzględnić poufność i tajność w tworzeniu (i korzystaniu) z zasobów, a to oznacza wymóg korzystania z tzw. kluczy wiedzy (*applets*) i dostęp do niej tylko przez wybranych (upoważnionych) pracowników.
- Zapewnić ciągłość dopływu do zasobów nowych danych i informacji, kierując się przy tym kryterium maksymalizowania danych i informacji sprawdzonych i minimalizowania bezużytecznych.
- Przestrzegać zasad odpowiedzialności za różne zasoby, a to oznacza konieczność przypisywania odpowiedzialności konkretnym pracownikom za konkretne zasoby.

Przedstawione wyżej zapisy mogą się wydawać zbędne lub przekraczające możliwości pojedynczego przedsiębiorstwa, zwłaszcza w przypadku przedsiębiorstw o niskich aspiracjach w zakresie zarządzania wiedzą i niewielkim potencjale (tech-

nicznym, finansowym, organizacyjnym), lecz w przypadku przedsiębiorstw o zdywersyfikowanym zakresie działalności, zarówno gdy idzie o charakter, stopień i geografię jej zróżnicowania, problem ten nie wydaje się marginalny i mało znaczący.

Literatura

Malara Z., *Przedsiębiorstwo w globalnej gospodarce. Wyzwania współczesności*, Wydawnictwo Naukowe PWN, Warszawa 2007.
Obłój K., *Tworzywo skutecznych strategii*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2002.
Społeczeństwo informacyjne w Polsce, GUS, Warszawa 2008.
www.policja.pl, data dostępu 29.09.2008.

KNOWLEDGE AND DATA RESOURCES PROTECTION IN SMALL AND MEDIUM ENTERPRISES – RESEARCH EXPERIENCE

Summary

The paper's aim is to present the behaviour of Polish small and medium enterprises faced with the problem of knowledge and data resources protection.

The authors verify the assumption of inadequate data protection level and the risk of data loss and data take-over. They point out the low level of data-safety awareness among the entrepreneurs.