dr Jowita Sobczak
Akademia Finansów i Biznesu Vistula

Znaczenie informacji dla bezpieczeństwa przedsiębiorstwa

Wstęp

Aktualna i szybko dostępna informacja jest dzisiaj warunkiem skutecznego funkcjonowania każdej organizacji, decyduje często o powodzeniu lub porażce w dążeniu do wyznaczonego celu. Wartość rynkowa przedsiębiorstwa w znacznej mierze zależy od wartości przetwarzanej przez nie informacji, które wykorzystywane są w produkcji, usługach, działalności badawczo-rozwojowej itp. Dziś informacja determinuje pozycję ekonomiczną przedsiębiorstwa, a nie wielkość czy ilość posiadanych zasobów materialnych. Utrata lub niewłaściwe zarządzanie informacją mogą być przyczyną obniżenia pozycji rynkowej przedsiębiorstwa, a nawet doprowadzić do zakończenia prowadzonej działalności.

Rozwój gospodarki rynkowej w dobie konkurencji, rywalizacji w dziedzinie nauki i techniki wyznaczają ograniczenia w zakresie dostępu nieuprawnionych podmiotów i osób do określonych zasobów informacyjnych. Przedsiębiorstwa rozwijają się, stają się liderami w swojej działalności ponieważ posiadają określone informacje umożliwiające im szybki i dynamiczny rozwój. Nielegalne pozyskanie informacji o technologii pozwala zaoszczędzić ogromne środki finansowe przeznaczane na prace badawcze czy zdobywanie doświadczeń, dlatego tak duże znaczenie ma odpowiednia ochrona i zarządzanie bezpieczeństwem informacji w przedsiębiorstwach.

1. Informacja jako składnik wartości firmy

Informacja uważana jest za jeden z najważniejszych zasobów niematerialnych przedsiębiorstwa, jest podstawą jego funkcjonowania, zarówno w Polsce, jak i na świecie. Michael E. Porter (1985, s. 7), amerykański ekonomista, uważa, że informacja zmienia świat

DOI: 10.5604/18984509.1140880

ISSN: 1898-4509

i reguły gry rynkowej, a tym samym zasady konkurowania. Przedsiębiorstwa w celu osiągnięcia przewagi konkurencyjnej wykorzystują informacje i nowoczesną technologię informacyjną, jako narzędzie walki o klienta. Menadżerowie coraz częściej zwracają uwagę na wartość, jaką ma informacja dla przedsiębiorstwa. Wartość i znaczenie informacji wynikają często nie z faktu ich posiadania, lecz z możliwości ich wykorzystania do założonych celów. Zapewnienie bezpieczeństwa informacji jest niezbędne do prowadzenia działalności gospodarczej oraz osiągnięcia korzyści materialnych, dlatego tak istotne znaczenie ma ochrona informacji.

Warto przybliżyć etymologię słowa informacja. Wywodzi się ono z łacińskiego słowa *informatio*, które oznacza wyobrażenie, zarys, pojęcie (Kumaniecki, 1996). Słowo to jest jednak wieloznaczne, gdyż funkcjonuje w języku potocznym i w wielu dziedzinach nauk, co stwarza wiele problemów definicyjnych. W zależności od obszarów nauki można wyodrębnić różne znaczenie informacji. Trudno wskazać definicję, która odpowiadałaby potrzebom przynajmniej kilku obszarów życia społecznego (Gomółka, 2000, s. 9-14).

Niektórzy badacze ekonomii twierdzą, że informacja to wiedza potrzebna do określenia i realizacji zadań służących do osiągnięcia celów organizacji, podkreślając tym samym jej wartość dla przedsiębiorstwa. Inni zaś twierdzą, że jest to właściwość wiadomości lub sygnału, polegająca na redukcji niepewności, co do stanu albo dalszego rozwoju sytuacji, której wiadomość dotyczy (Gierszewska, 1997, s. 21). Według Krzysztofa Lidermana (2009, s. 10) informacja jest towarem o szczególnej właściwości, różniącym się od innych towarów tym, że nie trzeba jej odbierać jednym osobom, aby przekazać ją innym. James A.F. Stoner i Charles Wankel sądzą, że dane (surowe fakty) mogą stać się informacją (przeanalizowanymi danymi), która w konsekwencji doprowadza do działania (Shim, 1999, s. 21-31). Mariusz Maciejewski (2006, s. 31) uważa natomiast, że jest to komunikat o jakimś zdarzeniu, utrwalony w sposób materialny i możliwy do odczytania przez inne osoby. Donald L. Pipkin (2002, s. 15) określa, że informacja to jedyny i wyjątkowy aktyw posiadany przez instytucję, będący dźwignią prowadzonej przez nią działalności.

Natomiast standard ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management, który jest zbiorem praktyk do zastosowania w systemie zarządzania bezpieczeństwem informacji, określa ją jako aktyw mający dużą wartość dla organizacji, dlatego też należy ją odpowiednio chronić (ISO/IEC 27002:2005, s. 9).

Powyższe definicje to tylko część wybranych z literatury przedmiotu.

Już w starożytności uważano, że informacje należy zabezpieczyć, stąd szyfry, kody, niewidzialne atramenty, tajni kurierzy itp. Sposoby zdobywania i ukrywania informacji są starsze niż sama instytucja państwa. W historii ludzkości znaleźć można wiele przykładów ochrony informacji strategicznych, np.: Chińczycy strzegli tajemnicy produkcji jedwabiu przez około 2000 lat, mając przez ten czas monopol na jego produkcję, i eksportowali go tzw. Jedwabnym Szlakiem. Każdego, kto zdradził tajemnicę jego wyrobu, czekała śmierć (Krysowaty, 2006, s. 115-116).

Mając na uwadze powyższe, można stwierdzić, że ochrona informacji posiada odrębne, autoteliczne znaczenie nie tylko dla bezpieczeństwa przedsiębiorstwa, ale również dla bezpieczeństwa gospodarczego państwa.

Określenie wartości informacji i jej znaczenia dla funkcjonowania przedsiębiorstwa należy rozpocząć od rozpatrywania jej w kategoriach zasobu organizacyjnego czy też aktywu niematerialnego. Jedna z wielu definicji stanowi, że zasób to pewna ilość czegoś, co zostało zebrane, nagromadzone w celu wykorzystania w przyszłości (Stefanowicz, 2004, s. 139). Zasoby mogą być materialne, np. pieniądze, oraz niematerialne, np.: wiedza, kwalifikacje, zdolności, motywacje, informacje, znaki i marki handlowe, reputacja przedsiębiorstwa i jego produktów (Penc, 1997, s. 591).

Rosnąca konkurencja spowodowała, że informacja stała się dla przedsiębiorstw czynnikiem istotniejszym niż zasoby materialne. Przykładem są przedsiębiorstwa przemysłowe, w których tajemnica technologii produkcji, patenty, prawa własności, znaki towarowe i tajemnice handlowe (know-how) mają podstawowe znaczenie dla ich funkcjonowania i utrzymania konkurencyjnej pozycji na rynku. Utrata istotnych informacji lub niewłaściwe nimi zarządzanie może być przyczyną problemów ekonomiczno-finansowych przedsiębiorstwa. Kradzież tajemnic handlowych, technologii czy produkcji może mieć nieodwracalne konsekwencje, a nawet doprowadzić do całkowitej degradacji firmy.

Powyższą opinię podziela również Marek Ciecierski, według niego przedsiębiorstwa XXI wieku wkraczają w erę „nowej ekonomii". Jej cechą jest dominująca rola zasobów niematerialnych nad zasobami środków materialnych. Oznacza to, iż przewagę uzyskują firmy, które najlepiej zarządzają swoimi zasobami niematerialnymi natomiast nie te, które mają największe fabryki lub zasoby finansowe (Ciecierski 2005, s. 169). W ocenie przywołanego autora, nowy informacyjny wzorzec działalności przedsiębiorstwa wymaga totalnego zaangażowania kadry w zdobywanie informacji, w „słuchanie otoczenia".

Podobną ocenę sformułował Jan Luberadzki stwierdzając, że wśród istotnych zagrożeń bezpieczeństwa obrotu gospodarczego coraz bardziej przybierają na znaczeniu – obok nieuczciwej konkurencji – wywiad i szpiegostwo gospodarcze. Przedsiębiorstwo, które – kierując się zasadami otwartości informacyjnej – zignoruje zasady bezpieczeństwa informacyjnego, może narazić się na poważne straty. Dotyczy to zarówno kwestii pozyskiwania informacji i wiedzy niezbędnej do zarządzania, jak też ochrony własnych ich zasobów, a w szczególności informacji prawnie chronionych. W ocenie autora, pozyskiwanie informacji i ich ochrona, to dwie strony tego samego medalu, którym jest bezpieczeństwo informacyjne i zdolność przetrwania organizacji na rynku. Osobliwość i wymóg współczesnych czasów to uczynienie z informacji towaru, będącego przedmiotem pożądania, zdobywania i obracania nim w coraz bardziej globalnym wymiarze (Luberadzki 2011, s. 103).

Syntetycznie rolę informacji w przedsiębiorstwie przedstawił także Dariusz Mikołajczyk, który odnotował, że zaczyna ona odgrywać coraz istotniejszą rolę w funkcjonowaniu firm w dwu ujęciach. W jednych z nich będzie esencją działalności firmy, jej najistotniejszym składnikiem twórczym i produkcyjnym (w myśl pojęcia tzw. „nowej ekonomii" określającej gospodarkę, jako napędzaną kapitałem i informacją, a nie zasobami materialnymi), a w innych będzie tylko zwykłym czynnikiem naturalnie występującym w ich funkcjonowaniu bez szczególnego dla nich znaczenia strategicznego (Mikołajczyk 2010, s. 170; cyt. za Borowiecki, Romanowska 2001, s. 23).

Jak słusznie wskazała Maria Parlińska (2008, s. 5) informacja jest obecnie najbardziej poszukiwanym zasobem ekonomicznym, niezbędnym do funkcjonowania każdej organizacji, a w szerszym znaczeniu także państwa i gospodarki narodowej. Możliwości określenia oraz pomiaru zasobów informacyjnych instytucji, społeczeństwa lub gospodarki narodowej są ważnym problemem praktycznym i badawczym. Informacja zmienia reguły konkurowania przedsiębiorstw. Ponadto stwarza przewagę konkurencyjną, umożliwiając im osiągnięcie lepszych wyników niż konkurencja. Powoduje powstanie nowych dziedzin działalności, często bazując na obecnych operacjach firmy.

Informacje, od których zależy wartość rynkowa przedsiębiorstwa, mogą być różnego pochodzenia, np. mogą być to informacje wytworzone w komórkach organizacyjnych przedsiębiorstwa lub udostępnione przez partnerów biznesowych, albo przekazane przez organy administracji państwowej. Informacje wytworzone i udostępnione należy chronić ze względu na interes własny przedsiębiorcy i interesy partnerów biznesowych. Informacje przekazane, zwłaszcza informacje niejawne, chronione są z mocy prawa, a szczegółowe warunki ich ochrony ustala zleceniodawca w tzw. instrukcji bezpieczeństwa

przemysłowego. Zapewnienie w przedsiębiorstwie należytego bezpieczeństwa zasobom informacyjnym jest przedsięwzięciem skomplikowanym i dość kosztownym. Wizerunek (dobre imię) przedsiębiorstwa jest jednak nie do utrzymania bez zapewnienia bezpieczeństwa informacjom własnym, udostępnionym i przekazanym. Zatem w dobrze pojętym interesie przedsiębiorstwa nie powinno się oszczędzać na ochronie zasobów informacyjnych (Ryszkowski 2005, s. 203).

Istotne znaczenie informacji dla funkcjonowania współczesnych przedsiębiorstw wskazuje na potrzebę wprowadzenia zarządzania informacją, które obecnie traktowane jest, jako jeden z podstawowych elementów tworzenia i realizacji strategii przedsiębiorstwa.

2. Zarządzanie bezpieczeństwem informacji

Informacje posiadają określoną wartość dla przedsiębiorstw dlatego powinny być chronione. Ale co tak naprawdę oznacza pojęcie „bezpieczeństwo informacji"? Bezpieczeństwo informacji oznacza, że ważne z punktu widzenia prawnego i biznesowego informacje są chronione przed nieuprawnionym dostępem, zniszczeniem, modyfikacją oraz że są zawsze dostępne dla upoważnionej osoby. Z kolei zarządzanie informacją to określony zestaw sposobów postępowania, które wskazują, jak przedsiębiorstwa pozyskują, dystrybuują i używają informacji oraz wiedzy (Prusak, 1997, s. 134). Natomiast zarządzanie bezpieczeństwem informacji powinno uwzględniać przede wszystkim kontrolę jej pozyskiwania, wytwarzania i przetwarzania, dystrybucję, monitorowanie „ścieżki" informacji w strukturze danego przedsiębiorstwa oraz podnoszenie świadomości pracowników poprzez szkolenie w zakresie ochrony informacji.

Nowe technologie sprawiły, że wymiana danych pomiędzy oddalonymi od siebie podmiotami jest możliwa bez względu na uwarunkowania logistyczne (Krysowaty, 2006, s. 278). Czy w dobie nowych technologii i zaawansowanych technik przedsiębiorca może trwać w przekonaniu, że jego zasoby informacyjne są odpowiednio chronione? Tak postawione pytanie ma więcej niż jedną odpowiedź.

Po pierwsze, czy przekonanie osoby kierującej jednostką organizacyjną o tym, że tajemnice określone w przepisach prawa i własność intelektualna są należycie chronione przez zatrudnionych pracowników jest zgodne z prawdą? Jest to pytanie o istnienie w organizacji działającego systemu zarządzania bezpieczeństwem informacji, czyli procesów, procedur, wykorzystywanych do zapewnienia, że organizacja jest w stanie zrealizować wszystkie zadania niezbędne dla osiągnięcia swoich celów, bez względu na ich charakter. W systemie zarządzania bezpieczeństwem informacji bardzo ważne jest, aby

stanowił on część procesów przebiegających w przedsiębiorstwie i całkowitej struktury zarządzania oraz był z nimi zintegrowany. Powinien on również uwzględniać bezpieczeństwo informacji podczas tworzenia procesów, systemów informatycznych i systemów zabezpieczeń. Jednak najważniejsze jest, aby wprowadzony system był dostosowany do potrzeb biznesowych danej firmy. Wytyczne dotyczące ustanowienia w jednostkach organizacyjnych systemów zarządzania bezpieczeństwem informacji zostały określone m.in. w ISO/IEC 27001.

Po drugie, wycena tajemnicy przedsiębiorstwa: czy posiadane przez firmę informacje są na tyle cenne, że konkurencja zechce je pozyskać, a jeżeli tak, to, jakim nakładem kosztów należy je chronić? Zagadnienia te związane są z analizą ryzyka opisującą zagrożenia utraty poufności, dostępności lub integralności informacji. W dobie globalizacji, nasilającej się konkurencji informacja ma potężną wartość przeliczalną na gotówkę, incydentów należy oczekiwać zarówno z zewnątrz organizacji, jak i ze strony niezadowolonych i niedocenionych pracowników (Sobczak, 2014, s. 23).

Wprowadzenie zarządzania bezpieczeństwem informacji w przedsiębiorstwie wymaga systemowego podejścia do analizy ryzyka. W oparciu o wyniki analizy ryzyka dostosowuje się zabezpieczenia. Zastosowane zabezpieczenia powinny być efektywne kosztowo i uwzględniać wymagania wynikające z przepisów prawa, wymagań biznesowych i wymagań z analizy ryzyka. Zagadnienie zarządzania ryzykiem, w tym ryzykiem bezpieczeństwa informacji, ma coraz większe znaczenie dla przedsiębiorstw w Polsce. Od kilku lat w firmach coraz częściej tworzy się etat menadżera ds. zarządzania ryzykiem. Zadaniem osoby zatrudnionej na takim stanowisku jest stworzenie systemu zarządzania ryzykiem w organizacji, nadzorowanie jego skutecznego funkcjonowania, a także koordynowanie działań menadżerów operacyjnych na arenie zarządzania ryzykiem. Wprowadzenie skutecznego systemu zarządzania bezpieczeństwem informacji i ryzykiem dla posiadanych zasobów informacyjnych, w dobie gospodarki opartej na wiedzy i w sytuacji uczestnictwa w globalnej rywalizacji, jest jednym z najważniejszych problemów współczesnych przedsiębiorstw. Na szczególną uwagę zasługuje międzynarodowy standard dotyczący zarządzania ryzykiem bezpieczeństwa informacji – ISO/IEC 27005: 2008. Pokazuje, on w jaki sposób zaimplementować ocenę ryzyka podczas projektowania i wprowadzania systemu zarządzania bezpieczeństwem informacji.

Szacowanie ryzyka jest niezbędne do wdrożenia systemu zarządzania bezpieczeństwem informacji. Istotne jest także, aby w ramach systemu zarządzania bezpieczeństwem informacji zapewnić powtarzalność przeprowadzania tego procesu, np. raz na rok. Proces taki kończy się sporządzeniem raportu dla kierownictwa przedsiębiorstwa.

Bez względu na to, czy zamierza ono wprowadzać kompleksowy system zarządzania bezpieczeństwem informacji, czy tylko realizować wymogi prawa związane z bezpieczeństwem informacji (np. ustawy o ochronie danych osobowych), ważne jest, aby cyklicznie dokonywać szacowania ryzyka dla posiadanych zasobów informacyjnych.

Wielu przedstawicieli firm błędnie uznaje inwestycje w system bezpieczeństwa za bardzo kosztowne i uważa, że nie posiada wystarczających środków na ich sfinansowanie. Małe firmy uważają także, że zagrożenie utraty informacji jest niewielkie, bo na ataki narażone są tylko duże przedsiębiorstwa, a system zarządzania bezpieczeństwem jest im zbyteczny. Drugą kategorię stanowią firmy rozwijające się - małe, które stały się średnimi i średnie, które stały się dużymi. Te przedsiębiorstwa przekształcały się tak szybko, że nie zdążyły przygotować się do nowej skali problemów. Często są to firmy rodzinne, których obszar działania tak się zwiększył i rozwinął, że firma nie była w stanie wdrażać odpowiednich procedur w obszarze zarządzania bezpieczeństwem informacji.

Należy zauważyć, że przedsiębiorstwa często skupiają swoje działania głównie na produkcji i zarabianiu środków finansowych, zapominając, że jedno zdarzenie związane z nieuprawnionym ujawnieniem np. informacji o technologiach, innowacjach może spowodować ogromne starty finansowe. Dla przykładu, według danych Ponemon Institute największe koszty związane z utratą informacji w 2013 roku poniosły Niemcy i Stany Zjednoczone (US). Wyniosło to ich odpowiednio 199 i 188 dolarów za jeden rekord z bazy danych. Łącznie państwa te poniosły straty: US 5,4 miliarda dolarów i Niemcy 4,8 miliarda dolarów (Ponemon Institute, 2013, s. 1).

Dlatego tak ważna w obszarze zarządzania bezpieczeństwem informacji jest świadomość i zobowiązanie najwyższego kierownictwa o ustanowieniu tego systemu. Wszystkie standardy, normy dotyczące bezpieczeństwa informacji stanowią o zaangażowaniu kierownictwa, które jest kluczem do osiągnięcia sukcesu w tym obszarze. Jednak, pomimo, iż standardy te wydają się być dobrze opisane i opracowane, często nie wskazują źródła problemu. Kluczem do zaangażowania najwyższego kierownictwa do wprowadzenia systemu zarządzania bezpieczeństwem informacji jest pokazanie, w jaki sposób narzędzia informatyczne i system oddziaływają na specyficzne środowisko przedsiębiorstwa nie wywierając negatywnego wpływu na procesy biznesowe (Dubey, 2013, s. 39).

Podczas projektowania i ustanowienia systemu zarządzania bezpieczeństwem informacji, przedsiębiorstwa muszą uwzględnić przede wszystkim specyfikę swojej działalności i wszystkie akty prawa powszechnego, które są zobowiązane przestrzegać, a które w swojej treści zawierają zasady dotyczące ochrony informacji, np. ustawa Prawo pocztowe, ustawa Prawo energetyczne itp. W przypadku, gdy przedsiębiorstwo zamierza

ubiegać się o certyfikowany system zarządzania bezpieczeństwem informacji, musi skoncentrować się dodatkowo na tym, aby prowadzona w związku z wprowadzeniem tego systemu dokumentacja była zgodna z normą ISO/IEC 27001.

W Polsce działa 213[1] firm, które posiadają certyfikat potwierdzający zgodność wdrożonego systemu bezpieczeństwa informacji z ww. normą. Bardzo często osoby kierujące przedsiębiorstwami uważają, że stosowanie się do wymagań ww. normy wymusza niepotrzebną biurokratyzację. Tymczasem określa ona tylko minimum wymaganych dokumentów. Ponadto przewiduje, że dokumentacja ta może być zróżnicowana z uwagi na wielkość organizacji i rodzaj prowadzonej działalności (PN-ISO/IEC 27001:2007, 2007, s. 14). Dzisiaj coraz częściej firmy wybierając dostawcę wymagają różnych zapewnień, które stanowią warunek dalszych relacji handlowych. Dotychczas, wymagano od dostawców legitymowania się zgodnością z normą ISO 9001, jednak coraz częściej oczekuje się, że wykażą się także zgodnością z ISO/IEC 27001. Istotne jest, aby firma potwierdziła dbałość o informacje pozostającą pod jej nadzorem. W przypadku, gdy wymienia tę informacje z dostawcą – pojawia się ryzyko, braku należytej ochrony informacji. W ostateczności, mniejsze znaczenie ma to, czy firma podejmuje decyzję o ustanowieniu systemu zarządzania bezpieczeństwem informacji z powodu kwestii rynkowych czy wewnętrznych – najistotniejsze jest, że decyduje się zadbać o bezpieczeństwo informacji.

W ramach systemu zarządzania bezpieczeństwem informacji wymagane są monitorowanie i przegląd systemu. Bardzo ważnym elementem jest także powołanie w przedsiębiorstwie osoby odpowiedzialnej za nadzorowanie i doskonalenie systemu zarządzania bezpieczeństwem informacji, podległej bezpośrednio najwyższemu kierownictwu, np. pełnomocnika ds. systemu zarządzania bezpieczeństwem informacji. Osoba taka powinna sporządzać dla najwyższego kierownictwa raporty, analizy, sprawozdania miesięczne, kwartalne, roczne w celu przedstawienia bieżącej sytuacji związanej z realizacją przez całe przedsiębiorstwo wdrożonego systemu. Osoby odpowiedzialne w przedsiębiorstwie za monitorowanie i nadzorowanie systemu muszą realizować postanowienia procedur w tym zakresie (PN-ISO/IEC 27001:2007, 2007, a 1–5, s. 13).

Przedsiębiorstwa mogą wydawać każdego roku, ogromne środki finansowe na inicjatywy związane z bezpieczeństwem informacji, ale nadal nie osiągną odpowiedniego poziomu poufności, integralności i dostępności informacji, jeżeli nie będą wykonywać

[1] Dane z Rejestru certyfikatów ISO/IEC 27001 (dostęp:20.06.2014).

okresowych przeglądów i doskonalić wprowadzonego systemu zarządzania bezpieczeństwem. Dla przykładu nieuwzględnienie powiązań pomiędzy systemami kadrowymi, domeną użytkowników (Active Directory) i innymi aplikacjami biznesowymi może prowadzić do błędnej identyfikacji pracowników w tych systemach (Ravindran, 2013, s. 40), np., jeżeli pracownik nie jest już zatrudniony w danej organizacji i jest to odnotowane w systemie kadrowym, ale nie jest to uwzględnione w pozostałych aplikacjach, lub gdy pracownik awansował i zostały mu zmienione uprawnienia dostępu do zasobów, co również powinno mieć odwzorowanie zarówno w systemie kadrowym jak i w innych systemach.

Przedsiębiorstwa prowadząc działalność nieustanie narażone są na działania związane z nieuprawnionym pozyskiwaniem czy kradzieżą informacji. Należy pamiętać, że fakt, iż dane przedsiębiorstwo nie wykorzystuje narzędzi wywiadu gospodarczego nie jest przesłanką, by sądzić, że takie działania nie są prowadzone wobec niego przez konkurencję. Zagrożeń dla bezpieczeństwa informacji można oczekiwać zarówno z zewnątrz jak i wewnątrz organizacji jednak najsłabszą stroną w ochronie informacji jest jej dysponent – człowiek, narażony na zgubny wpływ prostych socjotechnik stosowanych dla zdobycia i wykorzystania informacji.

Jednym z najszybciej rozwijających się zagrożeń są zapewne popularne portale społecznościowe jak Facebook i Twitter. Facebook został założony przez Marka Zuckerberga i jego przyjaciół z Uniwersytetu Harvard w 2004 roku. Portal miał służyć do wymiany informacji pomiędzy studentami. Dzisiaj Facebook jest jednym z największych internetowych serwisów społecznościach licząc blisko 845 miliona członków. Jack Dorsey wraz z przyjaciółmi założył w 2006 r. serwis Twitter, który dzisiaj ma więcej, niż 600 miliona użytkowników (Srinivasan, 2012, s. 21). Wielu z nich przekazuje na tych portalach informacje, które są dostępne nie tylko dla przyjaciół czy znajomych. Niejednokrotnie w pracy, pracownicy korespondując ujawniają informacje branżowe właśnie poprzez te portale. Rodzi to nowe zagrożenie dla pracodawcy, który i z tym problemem musi sobie poradzić, jednak bez odpowiednich procedur, polityk, zabezpieczeń nie ma szans na zminimalizowanie tego zagrożenia. Według badania Deloitte i Gazeta.pl (Raport, 2008.) większość przedsiębiorców zauważa zagrożenie ze strony portali społecznościowych.

Jednocześnie najchętniej stosowanym rozwiązaniem, mającym zabezpieczyć organizacje przed ryzykiem ze strony tychże portali, jest blokowanie dostępu do nich. Można powiedzieć, że koncentracja pracodawców na blokowaniu korzystania z serwisów społecznościowych w czasie pracy nie sprzyja ochronie informacji. Słusznym kierunkiem

myślenia o serwisach społecznościowych w kontekście bezpieczeństwa informacji wydaje się być zwiększanie świadomości pracowników odnośnie informacji zawodowych ujawnianych przez nich on-line poza czasem pracy. Powszechność portali społecznościowych sprawia, że coraz więcej ludzi umieszcza tam dużą ilość informacji – zarówno o ich życiu prywatnym, jak też służbowym. Często są to informacje, które w sposób bezpośredni bądź pośredni ujawniają dane wrażliwe, które powinny podlegać ochronie.

Aż 40% respondentów uważa, że informacje o fizycznej lokalizacji, w tym o planowanych podróżach pracowników, nie powinny podlegać ochronie, a kolejne 20% z nich nie ma w tej kwestii zdania. Równocześnie 47% respondentów uważa, że informacje o kontaktach biznesowych (prezentowanych np. na portalach typu LinkedIn, GoldenLine) nie powinny podlegać ochronie, a kolejne 20% z nich nie ma w tej kwestii zdania. Powyższe dane świadczą o znikomej świadomości zagrożeń, jakie mogą płynąć z korzystania przez pracowników z portali społecznościowych. Funkcje takie jak np. TripIT (informacja na temat planowanych podróży służbowych) mogą stanowić realne zagrożenie dla bezpieczeństwa przedsiębiorstwa. Inteligentny przeciwnik może w prosty sposób powiązać informacje zawarte w ogólnodostępnych portalach oraz serwisach społecznościowych, wchodząc w posiadanie danych, które jeszcze niedawno dostępne były jedynie przy wykorzystaniu technik szpiegostwa przemysłowego. Tymczasem kierownictwo przedsiębiorstwa może nawet nie zdawać sobie sprawy z wszechstronności informacji, jakie jego pracownicy umieszczają w tego typu portalach.

Zapewnienie właściwego poziomu ochrony informacji ma istotne znaczenie nie tylko ze względów biznesowych przedsiębiorstwa, to także obowiązek wynikający z przepisów prawa. Nie przestrzeganie np. ustawy o ochronie danych osobowych, ustawy o ochronie informacji niejawnych itp., może skutkować nie tylko nakładaniem kar, ale także prowadzić do:

1) problemów z załogą i środowiskiem branżowym,
2) ograniczenia zdolności spełniania wymagań klientów,
3) utraty wizerunku i szans rozwojowych,
4) ścigania poszczególnych osób i odwoływania członków władz organizacji.

Przedsiębiorstwa tworząc procedury bezpieczeństwa, powinny traktować przepływ informacji, jako całościowy proces, którego elementy należy nadzorować od momentu stworzenia, aż do ich zniszczenia. Dopiero wówczas można uznać, że informacje są właściwie chronione. Wiele przedsiębiorstw uważa, że program antywirusowy zapewnia całkowite bezpieczeństwo. Owszem, jest on ważnym elementem systemu zabezpieczenia, jednak nie eliminuje całkowicie zagrożeń związanych z przetwarzaniem informacji.

Bardzo ważne jest, aby przedsiębiorstwa pamiętały o podstawowych zasadach ochrony informacji i dbały o kulturę ich ochrony na każdym szczeblu zarządzania.

3. Podejście przedsiębiorstw do zarządzania bezpieczeństwem informacji

Przedsiębiorstwa wykazują często bierne podejście do zapewnienia bezpieczeństwa informacji, oznacza to, że organizacja niejednokrotnie czeka, aż „coś" się wydarzy. Reaguje wyłącznie na działania organu nadzoru (np. Generalnego Inspektora Ochrony Danych Osobowych, Agencji Bezpieczeństwa Wewnętrznego itp.), pracowników lub opinii publicznej. Typowe dla takiego podejścia jest ograniczenie zasobów dedykowanych w kwestii bezpieczeństwa informacji oraz skoncentrowanie uwagi wyłącznie na sprawach bieżących. Takie działanie powoduje, że organizacja nie posiada informacji o rzeczywistym stanie bezpieczeństwa, a co za tym idzie - rośnie prawdopodobieństwo incydentów i ryzyko nieprzewidzianych działań ze strony organów nadzoru, a tym samym kar.

Część przedsiębiorstw podejmuje działania tylko wówczas, gdy problem braku właściwej ochrony informacji staje się oczywisty np. w sytuacji wystąpienia incydentu związanego z utratą danych. Często te przedsiębiorstwa uważają takie działania za wystarczające w obszarze bezpieczeństwa informacji. Nawet o ile przeprowadza się audyty wewnętrzne czy zewnętrzne bądź oceny – opierają się one wyłącznie na próbkowaniu. Gdy chodzi o dedykowane zasoby, sytuacja jest podobna, jak w przypadku podejścia biernego. Problem takiego działania przedsiębiorstw polega na tym, że nie daje ono wystarczająco pełnego obrazu sytuacji. Reakcja na problemy następuje zawsze po fakcie. Choć podejmuje się działania dla zapewnienia bezpieczeństwa informacji, mają one jedynie miejsce wtedy, gdy obszar niezgodności zostanie zidentyfikowany w związku z pojawieniem się jakiegoś incydentu. Firmy, przyjmując takie podejście muszą się liczyć z większymi kosztami i większym nakładem czasu, niż w przypadku systemowego zapobiegania wystąpieniu incydentu.

Przedsiębiorstwa powinny działać aktywnie w obszarze zarządzania bezpieczeństwem informacji, określać poziom swojego bezpieczeństwa informacji oraz ustanowić procesy pozwalające na utrzymanie tego stanu. Powinny dążyć do zintegrowania tego zagadnienia z procesami biznesowymi. Takie działania nie gwarantują uniknięcia incydentów, ale powinny zapewniać bezzwłoczne identyfikowanie zagrożeń.

Utrata informacji może spowodować przerwę ciągłości działania przedsiębiorstwa. Jeżeli firmy nie są przygotowane na takie zagrożenie, tj. nie posiadają stosownych planów ciągłości działania, to mogą być narażone na przestój. W praktyce niewiele przedsiębiorstw przeznacza środki finansowe na wprowadzenie systemu ciągłości działania. Niewątpliwie te z nich, które posiadają taki plan na wypadek nieprzewidzianych w czasie i w skutkach zdarzeń, są lepiej przygotowane na nadzwyczajne sytuacje związane np. z utratą dostępności do kluczowego systemu teleinformatycznego. Łatwiej też dostosują się do nowych warunków i lepiej przetrwają okres wystąpienia niekorzystnego zdarzenia (Kaczmarek, 2009, s. 67).

Utrata ważnych informacji może prowadzić do obniżenia pozycji ekonomicznej przedsiębiorstwa, a nawet do jego upadłości. Mimo tego firmy nadal przedkładają oszczędności nad bezpieczeństwo informacji. Bardzo często inwestują w bezpieczeństwo w sytuacji, gdy nastąpi już utrata informacji lub inny incydent szkodliwie wpływających na działalność przedsiębiorstwa. Powodem tego jest zapewne problem z oszacowaniem korzyści, jakie niosą ze sobą tego typu inwestycje. Ciężko jest także określić ewentualne straty, które zostaną poniesione w przypadku zmniejszenia budżetu przeznaczonego na ochronę informacji.

Zakończenie

Podsumowując, powyższe należy stwierdzić, że bezpieczeństwo informacji wymaga spełnienia, co najmniej trzech warunków, aby można było mówić o jego skuteczności:

1) wysokiej świadomości pracowników, poczynając od najwyższego kierownictwa,
2) efektywnego zarządzania informacjami w taki sposób, aby zapewnić ich bezpieczeństwo,
3) stworzenia odpowiednich rozwiązań technologicznych, które zapewniają realizację polityki bezpieczeństwa informacji (Brdulak, 2011, s. 21).

Informacja jest zasobem łatwym do wytworzenia i rozpowszechniania, lecz trudnym do ochrony. Wprowadzenie systemu zarządzania bezpieczeństwem w przedsiębiorstwie wiąże się z obwarowaniem poszczególnych działań procedurami i może wydłużać czas pracy, jednakże skutki jego braku, a także nieprzestrzegania wewnętrznych procedur ochrony informacji mogą być przyczyną obniżenia pozycji rynkowej firmy, a nawet upadłości przedsiębiorstwa.

Żyjemy w dobie szybkich środków przekazu informacji, takich jak telewizja lub portale internetowe, i to z tych właśnie mediów dowiadujemy się o incydentach mających

miejsce w wielu przedsiębiorstwach. Czasami niewielkie zdarzenie związane z utartą informacji w przedsiębiorstwie nagłośnione przez media może doprowadzić do utraty jej pozytywnego wizerunku, a tym samym do utraty korzyści finansowych związanych z odejściem kluczowych klientów.

Współczesna nauka ekonomii, zarządzania i legislacja muszą radzić sobie z problemami wynikającymi z zastosowania technologii informacyjnych, a także z prawem do informacji i z ich ochroną. Informacja ma istotne znaczenie w działalności gospodarczej, jest zasobem strategicznym dla funkcjonowania przedsiębiorstwa, a właściwe zarządzanie bezpieczeństwem informacji jest jednym z podstawowych elementów osiągnięcia sukcesu na globalnym rynku.

Literatura

Brdulak H. (2011), *Rola polityki bezpieczeństwa informacji w ochronie danych konsumenta/przedsiębiorstwa*, w: *Modelowanie Procesów i Systemów Logistycznych*, (red.) Chaberska M., Reszka L., część X, „Zeszyty Naukowe Uniwersytetu Gdańskiego – Ekonomika Transportu Lądowego" Nr 40, Gdańsk, Wydawnictwo Uniwersytetu Gdańskiego

Ciecierski M. (2005), *Ochrona informacji w przedsiębiorstwach prywatnych – kontrwywiad gospodarczy*, w: *Ochrona informacji niejawnych i biznesowych. Materiały I Kongresu*, (red.) Gajos M., Zalewski S., Katowice, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych

Dubey N. (2013), *Corporate Responsibility, Retaining Top Management Commitment*, "ISACA Journal", Vol. 2

Gierszewska G., Romanowska M. (1997), *Analiza strategiczna przedsiębiorstwa*, Warszawa, PWE

Gomółka Z. (2000), *Cybernetyka w zarządzaniu*, Warszawa, PLACET

ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management

Kaczmarek T.T, Ćwiek G. (2009), *Ryzyko kryzysu a ciągłość działania*, Warszawa, Difin

Krysowaty I., Niedziejko P. (2006), *Informacja w systemach IT jako towar strategiczny*, w: *Innowacyjność w kształtowaniu jakości wyrobów i usług*, (red.) Żuchowski J., Radom, Wydawnictwo Instytutu Technologii Eksploatacyjnej

Kumaniecki K. (1996), *Słownik łacińsko-polski*, Warszawa, PWN

Liderman K. (2009), *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa, PWN

Luberadzki J. (2011), *Wywiad i szpiegostwo gospodarcze w konkurencji rynkowej*, w: *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały VII Kongresu*, (red.) Gajos M., Katowice

Maciejewski M. (2006), *Prawo informacji – zagadnienia podstawowe*, w: *Prawo informacji. Prawo do informacji*, (red.) Góralczyk jun. W., Warszawa, LKAEM Publishing House

Mikołajczyk D. (2010), *Bezpieczeństwo informacji w firmie – budowa systemu i zagrożenia*, w: *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały VII Kongresu*, (red.) Gajos M., Katowice

Niedzielska E. (1998), *Informatyka ekonomiczna*, Wrocław, Akademia Ekonomiczna.

Parlińska M. (2008), *Rola informacji w gospodarce rynkowej na podstawie wybranych rolnych rynków hurtowych*, Warszawa, SGGW

Penc J. (1997), *Leksykon biznesu*, Warszawa, Placet

Pipkin D.L. (2002), Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa, Warszawa, Wydawnictwo Naukowo-Techniczne.

Ponemon Institute (2013), *Cost of Data Breach Study: Global Analysis*, Symantec Corporation

Prusak L., Davenport T.H. (1997), *Information Ecology*, „Mastering the Information and Knowledge Environment", New York, Oxford University

Ravindran S.T. (2013), *Solving the identity and Access management conundrum*, "ISACA Journal", Vol. 5

Shim J.K., Siegel J.G., Chi R. (1999), *Technologia informacyjna*, Warszawa, Dom Wydawniczy ABC

Sobczak J. (2014), *Zagrożenia wynikające z utraty bezpieczeństwa informacji*, w: *Przeszłość, teraźniejszość i przyszłość ochrony informacji niejawnych w zapewnieniu bezpieczeństwa narodowego*, (red. nauk.) Sobczak J., Katowice, KSOIN i UŚ

Srinivasan S. (2012), *Lack of Privacy Awareness in Social Networks*, "ISACA Journal", Vol. 6

Stefanowicz B. (2004), *Informacja*, Warszawa, SGH

Jowita Sobczak

Importance of Information for Company Security

Abstract

The issue of the information safety management in enterprises was characterized. The research of literature was conducted with the aim to present different definitions of the concept of information. The importance and the role of information for enterprises was defined. The approach of organizational units to the process of establishment of the safety management information system was presented.

The role and importance of risk management and the estimation of risk in the information safety process was determined and the threats resulting from the use of social networking websites were discussed. It was attempted to find the reasons for the passive approach of enterprises to ensure the safety of information. It was shown that enterprises prefer savings over the safety of information and they often make investments in a situation when the information is already lost or another incident occurred that adversely affected their operation.

Key words: *information, safety management, risk, przedsiębiorstwo*

E-mail contact to the Author: jowita.sobczak@poczta.onet.pl