Jacek Łuczak

System zarządzania bezpieczeństwem informacji

Wprowadzenie

Bez wątpienia każda organizacja zabiega o bezpieczeństwo swoich informacji. Działania podejmowane w tym zakresie coraz częściej przybierają postać rozwiązań systemowych opartych na międzynarodowych standardach.

Organizacje mają różne motywacje dla ochrony informacji, podejmują działania o różnym stopniu skuteczności. Na pewno jednak wzrasta świadomość dotycząca znaczenia i konieczności ochrony informacji. Pokazują to wyniki badań, tak światowych[1], jak i przeprowadzonych przez autora[2]. Posłużyły one weryfikacji tez postawionych w niniejszym artykule:

1. Coraz większą popularność zyskują międzynarodowe standardy (szczególnie ISO/IEC 27001) – jako podstawa zarządzania bezpieczeństwem informacji.
2. Kluczowe czynniki związane z podejmowaniem działań w zakresie zarządzania bezpieczeństwem informacji dotyczą obaw o skutki niezgodności z wymaganiami prawnymi oraz utratę dobrej marki i reputacji.
3. Zarządzanie bezpieczeństwem informacji często postrzegane jest jako autonomiczny moduł zarządzania, nie stanowi elementu strategii zarządzania organizacją.
4. Rosnące znaczenie ryzyka pochodzącego z zewnątrz nie znajduje należytego odzwierciedlenia w systemie bezpieczeństwa informacji.
5. Plany ciągłości działania najczęściej ograniczają się do sfery IT.
6. Priorytetowe dane, jakie podlegają ochronie, to dane personalne; przy tym jako dane wrażliwe nie są należycie chronione.

[1] Zob. m.in. *Moving Beyond compliance*, Ernst & Young's 2008 Global, Information Security Survey, 2008; *Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2008*, Cert Polska 2009.

[2] Badanie przeprowadzone w 2008 roku na próbie 120 przedsiębiorstw zlokalizowanych w Polsce. Wybrane wyniki zostały zaprezentowane na tle kluczowych elementów systemu bezpieczeństwa informacji.

Tylko w przypadku rozwiniętych organizacji świadomość w zakresie zarządzania bezpieczeństwem informacji jest na satysfakcjonującym poziomie. Badania wykazują niekiedy także absolutny jej brak, niedostateczne zrozumienie i niewiedzę w zakresie wielu aspektów bezpieczeństwa informacji. Niekiedy świadomość w tym zakresie jest determinowana przez ograniczenia, jakie niesie z sobą stosowanie określonych zabezpieczeń, a nie następstwa ewentualnych negatywnych incydentów[3].

Informacja i jej znaczenie

„Informacja" etymologicznie wywodzi się z łacińskiego słowa *informatio*, co oznacza – wyobrażenie, wizerunek, zarys, pojęcie[4]. Pojęcie to jest jednak wieloznaczne, bowiem funkcjonuje w języku potocznym i występuje w wielu dziedzinach nauk, co stwarza obecnie wiele problemów definicyjnych. W zależności od kontekstu i obszarów nauki można wyodrębnić różne jej znaczenie uwarunkowane określonym punktem postrzegania rzeczywistości. Trudno wskazać definicję, która byłaby adekwatna do różnych dziedzin życia społecznego.

Niektórzy badacze ekonomii twierdzą, że informacja to wiedza potrzebna do określenia i realizacji zadań służących do osiągnięcia celów organizacji. W tej definicji podkreślony jest czynnik wartości dla organizacji. Inne definicje głoszą, że informacja to właściwość wiadomości lub sygnału polegająca na zmniejszeniu nieokreśloności lub niepewności co do stanu albo dalszego rozwoju sytuacji, której wiadomość dotyczy[5]. Definicja ta odwołuje się natomiast do zmniejszenia stanu niewiedzy (niepewności). Są też ujęcia odróżniające termin „dane" od pojęcia „informacji" rozumianej jako „dane przetworzone", z nadanymi cechami charakterystycznymi, mające wartość dla jednostki (np. wartość w procesie decyzyjnym)[6].

Dawniej, w języku potocznym, pojęcie „informacja" definiowano jako „uwiadomienie, nauczanie, nauka"[7]. Współcześnie, *Komputerowy słownik języka pol-*

[3] Patrz wyniki badań przeprowadzonych przez SKN Qualitas w 2008 roku na grupie kilkuset studentów uczelni poznańskich.

[4] K. Kumaniecki, *Słownik łacińsko-polski*, PWN, Warszawa 1996.

[5] G. Gierszewska, M. Romanowska, *Analiza strategiczna przedsiębiorstwa*, PWN, Warszawa 1997, s. 21.

[6] K. Kolegowicz, *Nowe funkcje informacji we współczesnych koncepcjach zarządzania*, [w:] *Informacja w zarządzaniu przedsiębiorstwem*, (red.) R. Borowiecki, M. Kwieciński, Wolters Kluwer Polska, Kraków 2003, s. 54 i literatura tam cytowana; B. Nogalski, B. M. Surawski, *Pozyskiwanie oraz bezpieczeństwo informacji w przedsiębiorstwie i państwie*, [w:] *Informacja w zarządzaniu przedsiębiorstwem*, op.cit., s. 204.

[7] S. B. Linde, *Słownik języka polskiego*, Warszawa 1951.

skiego definiuje informację jako „powiadomienie o czymś, zakomunikowanie czegoś, wiadomość, wskazówka, pouczenie"[8].

Warto też zwrócić uwagę na inną uniwersalną definicję przyjętą w ramach OAIS (*Open Archival Information System*) i wykorzystywaną między innymi przez NASA. Według tej definicji informacja to „wiedza dowolnego rodzaju, którą można się dzielić, niezależnie od formy (fizykalnej, cyfrowej) użytej do jej wyrażenia (reprezentacji). Z kolei dane (data) stanowią zgodnie z tym ujęciem formy reprezentacji konkretnej informacji. Dostęp do informacji jest więc możliwy dla odbiorcy, który dysponując danymi, interpretuje je zgodnie z zasadami dotyczącymi konkretnej formy reprezentacji"[9].

Standard ISO/IEC 17779:2005, który jest zbiorem dobrych praktyk do zastosowania w systemie zarządzania bezpieczeństwem informacji, bardzo pobieżnie traktuje jej definicyjne ujęcie. Według normy informacja określona jest jako „aktyw, który ma dla instytucji wartość i dlatego należy go odpowiednio chronić"[10]. Dodatkowo opisywane są różne „formy występowania informacji, które może przybierać, takie jak:

- wydrukowana,
- pisemna,
- elektroniczna,
- wiadomość elektroniczna,
- pliki audio i wideo,
- ustna"[11].

Informacja jest kluczowym zasobem we współczesnej gospodarce. Wprowadzanie technologii informatycznych i komputerowych oraz coraz powszechniejsze ich wykorzystanie doprowadziło do sytuacji, w której ma miejsce niemal nieograniczona wymiana informacji pomiędzy organizacjami, i nie ma znaczenia ich lokalizacja i odległość, jaka je dzieli, godziny pracy itd. Technika umożliwia równocześnie szybkie i prawidłowe gromadzenie, przechowywanie, przetwarzanie i przekazywanie danych i informacji w wielu dotychczas nieosiągalnych aspektach[12]. Przepływ i wymiana informacji są nadrzędnym czynnikiem twórczości i władzy człowieka. Burzliwy i bardzo dynamiczny rozwój technik informatycznych, jak również rosnąca ilość przetwarzanych informacji wymusiły poszukiwa-

[8] *Komputerowy słownik języka polskiego*, WP PWN, Warszawa 1998.

[9] L. Reich, D. Sawyer, *Archiving Referencing Model*, White Book, Issue 5, CCSDS 1999.

[10] ISO/IEC 17799:2005 *Information technology — Security techniques — Code of practice for information security management*, ISO, 2005, s. 9.

[11] Ibidem, s. 9.

[12] I. Krysowaty, P. Niedziejko, *Bezpieczeństwo IT jako usługa kształtująca wartość i jakość informacji*, [w:] *Innowacyjność w kształtowaniu jakości wyrobów i usług*, (red.) J. Żuchowski, Wydawnictwo Instytutu Technologii Eksploatacyjnej, Radom 2006, s. 278.

nie rozwiązań pozwalających skutecznie zarządzać informacją z uwzględnieniem ryzyka, jakie jest z tym związane.

Logika gospodarki rynkowej sprawia, że przedsiębiorstwa oceniane są przez inwestorów głównie przez pryzmat ich zdolności do generowania dochodów, czemu oprócz właściwego wyposażenia majątkowego służy wiele innych elementów, między innymi właściwa organizacja produkcji i system zarządzania, konkurencyjność wyrobów, profesjonalizm zatrudnionych pracowników oraz elementy mające często charakter pozamaterialny, pozwalający jednak na tworzenie tak zwanej wartości reputacji (ang. goodwill)[13]. Zachowania inwestorów giełdowych pokazują, że rynek nie reaguje na konkretne zdarzenia, lecz na informację o zdarzeniach. Informacja kształtuje wartość akcji (a tym samym wartość rynkową danej spółki), powoduje ich wahania – niezależnie od czynników rzeczywistych. Informacje o: podziale akcji (*split*), zmianie polityki dywidend, dodatkowej emisji papierów wartościowych, wykupie akcji własnych, fuzji czy przejęciu dają impuls inwestorom do podjęcia decyzji portfelowych, zanim dane zdarzenie zostanie (i o ile zostanie) urzeczywistnione[14].

Informacja i umiejętność jej pozyskania stają się kluczowym elementem warunkującymi sukces w prowadzeniu biznesu i utrzymaniu konkurencyjności. Dlatego też informacja powinna być zaliczana do aktywów biznesowych i w skuteczny sposób chroniona przed zagrożeniami. Na przykład 70% firm mających siedzibę w budynku WTC zbankrutowało po zamachu w 2001 roku, wskutek utraty własnych danych tam zgromadzonych[15].

Powstanie informacji inicjuje jej swoisty cykl życia. W następstwie może zostać przekazana, przetworzona (zmodyfikowana), skopiowana. W toku procesów realizowanych w organizacji informacja może zostać wykorzystana, przechowywana, gromadzona, kojarzona z innymi zasobami informacyjnymi; może zostać utracona lub zniszczona. Nośnik na którym przechowywana jest informacja może zostać zniszczony, przez co informacja na nim zawarta także ulega zniszczeniu.

[13] R. Borowiecki, A. Jaki, J. Kaczmarek, *Metody i procedury wyceny przedsiębiorstw i ich majątku*, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 2002, s. 14.

[14] Henryk Gurgul w swojej pracy *Analiza zdarzeń na rynkach akcji*, Oficyna Ekonomiczna, Kraków 2006, poświęconej teorii analizy zdarzeń (ang. *event study analysis*) szczegółowo przedstawia wpływ zdarzeń (a tym samym wpływ informacji) na zmiany cen i wolumenu obrotów walorów na podstawie niemieckiego rynku akcji.

[15] B. Cienińska, J. Łunarski, R. Perłowski, D. Stadnicka, *Systemy zarządzania bezpieczeństwem w przedsiębiorstwie*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2006, s. 69.

Bezpieczeństwo informacji

Bezpieczeństwo informacji nie jest jednoznacznym pojęciem, na pewno musi być analizowane w sferze aspektów prawnych, organizacyjnych oraz technicznych[16].

Przewodnik dotyczący systemowego zarządzania bezpieczeństwem informacji ISO/IEC 17799:2005 definiuje je jako zachowanie trzech cech informacji: poufności[17] (*confidentiality*), spójności (integralności[18]) (*integrity*) oraz dostępności[19] (*availability*); i dodatkowo ostatnie wydanie standardu zwraca uwagę także na zachowanie takich cech jak: rozliczalność (*accountability*), autentyczność (*authenticity*), niezaprzeczalność (*non-repundation*) i niezawodność (*reliability*).

Znaczenie cech stanowiących o bezpieczeństwie informacji (poufność, integralność, dostępność) jest warunkowana specyfiką organizacji. Dla instytucji rządowych, konsultingowych, bankowych istotne znaczenia ma poufność, wyciek informacji do osób trzecich deklasuje istnienie takiej firmy na rynku. Na przykład, uzyskanie danych przez osoby nieupoważnione w istotny sposób podważa wiarygodność tych organizacji. Dla firmy przetwarzającej wyniki badań, przygotowującej raporty, najważniejsza będzie integralność w procesie przetwarzania danych. Dostępność jest najistotniejszym warunkiem funkcjonowania dla wszystkich organizacji z sektora usług, gdzie krótka przerwa w działaniu biznesu generuje straty finansowe, np. usługi bankowe, usługi telekomunikacyjne, biura maklerskie, sklepy internetowe, i w oczywisty sposób podważa wiarygodność w oczach klientów.

Elementy bezpieczeństwa informacji w ramach działań systemowych

Kreując politykę bezpieczeństwa informacji, konieczne jest zwrócenie uwagi na wszystkie elementy systemowego bezpieczeństwa informacji. Nadrzędnym

[16] Zob. zabezpieczenia w ISO/IEC 27001, załącznik A.

[17] Najczęściej kiedy mówimy o bezpieczeństwie informacji w potocznym tego słowa znaczeniu, mamy na myśli przede wszystkim zachowanie poufności. Wg normy ISO/IEC 27001 „poufność oznacza zapewnienie, iż informacja jest dostępna wyłącznie dla osób uprawnionych, posiadających odpowiednie prawa dostępu", ISO/IEC 17799:2005, op.cit., s. 9.

[18] Integralność to śledzenie procesu przetwarzania informacji we wszystkich formach występowania, po to aby uniemożliwić nieautoryzowaną modyfikację czy też wyeliminować niepoprawną metodę przetwarzania (ISO/IEC 17799:2005, op.cit., s. 9).

[19] Dostępność to zapewnienie, iż informacja jest dostępna dla osoby uprawnionej zawsze gdy tego potrzebuje (ISO/IEC 17799:2005, op.cit., s. 9).

celem działań w tym zakresie jest zarządzanie ryzykiem w taki sposób, aby minimalizować jego wpływ na poziom bezpieczeństwa, w szczególności poprzez opracowanie i implementację planów minimalizacji ryzyka.

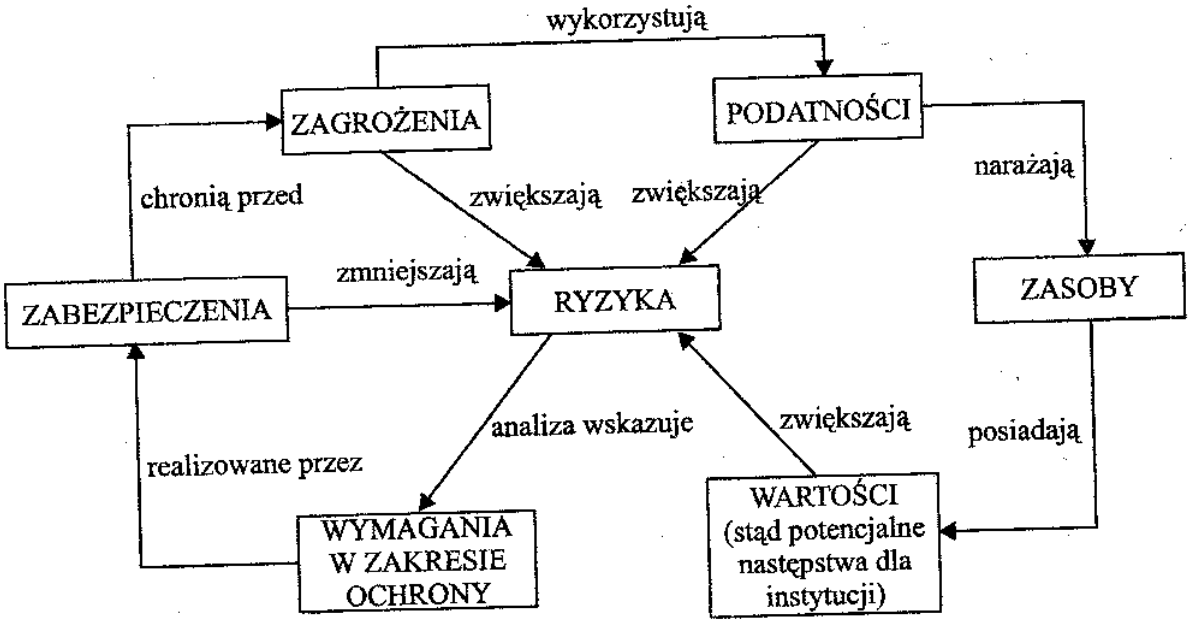
Kluczowe dla systemu zarządzania bezpieczeństwem informacji (ISMS) są także pojęcia:

- zagrożenie – potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub instytucji[20];
- zasoby – to wszystko, co ma wartość dla instytucji[21];
- zabezpieczenie – praktyka, procedura lub mechanizm redukujący ryzyko[22];
- podatność – słabość zasobu, lub grupy zasobów, która może być wykorzystana przez zagrożenie[23].

Związki pomiędzy tymi elementami zostały opisane i przedstawione poprzez model ujęty w normie ISO/IEC TR 13335 poświęconej technice informatycznej (rys. 1).

Analizując zasoby, należy mieć na uwadze ich sześć postaci, w jakich występują w organizacjach:

1. zasoby fizyczne (wszelkiego rodzaju sprzęt informatyczny, urządzenia komunikacyjne, budynki, infrastruktura techniczna i informatyczna),
2. informacje (dokumenty, bazy danych),



Rysunek 1. Wzajemne relacje w zarządzaniu ryzykiem
Źródło: ISO/IEC TR 13335-1

[20] PN-I-13335-1 – *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych*, PKN, 1999 s. 9.

[21] Ibidem, s. 8.

[22] Ibidem, s. 8.

[23] Ibidem, s. 9.

3. oprogramowanie (wszelkie systemy operacyjne, aplikacje),
4. zdolność produkowania lub świadczenia usług,
5. personel,
6. dobra niematerialne (reputacja, wizerunek)[24].

Każdy z wymienionych powyżej zasobów posiada określoną wartość dla organizacji, co jest jednym z ważniejszych parametrów dla zapewnienia ich ochrony. W systemie zarządzania bezpieczeństwem informacji należy wszystkie zasoby zidentyfikować, co jest związane z pełną inwentaryzacją wyposażenia. Przy identyfikowaniu zasobów konieczne jest zwrócenie uwagi na ich atrybuty, tj. ich wartość, wrażliwość oraz związane z nimi zabezpieczenia. Na wymagania w zakresie ochrony zasobów wpływa także ich podatność na konkretne zagrożenia.

Na zasoby oddziałuje wiele rodzajów zagrożeń. Zagrożenie może być potencjalną przyczyną niepożądanego incydentu, który może spowodować szkodę dla systemu lub instytucji i jej zasobów. Szkoda ta może powstać jako skutek bezpośredniego lub pośredniego ataku na informację, na przykład uszkodzenie, ujawnienie, modyfikacja, utrata informacji lub jej dostępności. Zagrożenie, które wykorzysta podatność zasobów, może wyrządzić określoną szkodę. Zagrożenia mogą mieć pochodzenie naturalne, mogą być przypadkowe lub rozmyślne. Należy zidentyfikować zarówno zagrożenia przypadkowe, jak i rozmyślne oraz określić ich poziom i prawdopodobieństwo[25].

Próbując usystematyzować identyfikację zagrożeń, można je opisać i rozróżnić w nich cechy, takie jak:

- źródło występowania (zewnętrzne, wewnętrzne);
- motywacja (zyski finansowe, wyprzedzenie konkurencji);
- częstotliwość pojawiania się;
- dotkliwość określona poprzez zakres szkodliwości lub określona poprzez różnego rodzaju skale, np. skala Richtera, Beauforta;
- rodzaj szkody (czasowa (np. przerwa w dostępie), stała (zniszczenie zasobu)).

Niekiedy, ze względu na specyficzne uwarunkowania kulturowe, pewne zagrożenia mogą w ogóle nie być uznane za szkodliwe. Analizując zagrożenia, należy mieć na względzie uwarunkowania kulturowe i środowiskowe[26].

Kolejnym elementem ważnym dla budowy systemu bezpieczeństwa są podatności. Są to pewne słabości fizyczne, organizacyjne, systemowe, proceduralne, osobowe, infrastrukturalne, oprogramowania czy informacji. Zasoby nierozerwalnie związane są z podatnością, która może być wykorzystane przez zagrożenia. To z kolei prowadzić może do wystąpienia pewnej szkody lub straty.

[24] Ibidem, s. 13.

[25] Ibidem.

[26] Ibidem, s. 14.

Podatność sama w sobie nie generuje szkody, lecz jest warunkiem lub zbiorem warunków, które mogą umożliwić zagrożeniu wpłynąć na zasoby. Obejmuje słabości w systemie bezpieczeństwa, które mogą być wykorzystane i w konsekwencji doprowadzać do niepożądanych efektów. Na przykład brak mechanizmu kontroli dostępu jest podatnością, która może pozwolić zaistnieć zagrożeniu, np. włamania i utraty zasobów.

Przeprowadzając analizę podatności, należy określić wszelkie słabości, które mogą być wykorzystywane przez zidentyfikowane wcześniej zagrożenia. Należy rozważyć podatności pochodzące z różnych źródeł, na przykład wewnętrzne względem zasobu. Podatność może istnieć dopóty, dopóki same zasoby nie zmienią się tak, że podatność nie będzie się do nich odnosić. Dodatkowo należy przy tym wziąć pod uwagę środowisko i istniejące zabezpieczenia. W pewnym uproszczeniu podatność konkretnego systemu lub zasobu jest określeniem łatwości, z jaką systemowi lub zasobowi może być wyrządzona szkoda. Możliwe jest, że w danym systemie lub instytucji nie wszystkie podatności będą, podlegały zagrożeniom. Natomiast konieczne jest natychmiastowe zainteresowanie się podatnością, z którą związane jest zagrożenie. Otoczenie zewnętrzne i wewnętrzne może zmieniać się dynamicznie, dlatego zachodzi potrzeba monitorowania podatności, aby zidentyfikować te, które zostały narażone na wcześniej występujące lub nowe zagrożenia.

W przypadku zaistnienia niepożądanego incydentu spowodowanego rozmyślnie bądź zaistniałego przypadkowo, konieczna jest analiza konsekwencji (następstw). Może to być zniszczenie zasobów, awaria sprzętu, strata finansowa, utrata jednej z cech bezpieczeństwa informacji. Niezbędne jest każdorazowe szacowanie następstw dla utrzymania równowagi pomiędzy konsekwencjami incydentu, a kosztami wprowadzonych zabezpieczeń. Zestawienie następstw i kosztów jest elementem określenia ryzyka i wyboru zabezpieczeń. Można je określić ilościowo czy jakościowo, uwzględniając m.in.:

- koszt finansowy,
- skale szkodliwości,
- częstotliwość (szkoda spowodowana przez incydent może nie być kosztowna, lecz łączny efekt wystąpienia wielu generuje znaczne straty dla organizacji).

Ryzyko jest prawdopodobieństwem określającym możliwość wykorzystania określonej podatności przez dane zagrożenie w celu spowodowania straty lub zniszczenia zasobu lub grupy zasobów, a przez to negatywnego bezpośredniego lub pośredniego wpłynięcia na instytucję. Jedno lub wiele zagrożeń może wykorzystać jedną lub wiele podatności.

Scenariusz ryzyka opisuje, w jaki sposób dane zagrożenie lub grupa zagrożeń może wykorzystać konkretną podatność lub grupę podatności, narażając zasoby na szkodę. Ryzyko jest opisywane poprzez kombinację dwu czynników: prawdopodobieństwa wystąpienia niechcianego incydentu oraz związanych z nim następstw.

Dowolna zmiana w zasobach, zagrożeniach, podatnościach i zabezpieczeniach może mieć znaczący wpływ na ryzyko. Wczesne wykrywanie i świadomość zmian w środowisku i systemie, zwiększa możliwości podjęcia odpowiednich działań w celu redukcji ryzyka[27].

Zabezpieczenia to praktyki, procedury lub mechanizmy, które mogą chronić przed zagrożeniem, redukować podatność, ograniczać następstwa, wykrywać niepożądane incydenty i ułatwiać odtwarzanie. Efektywna ochrona wymaga zwykle kombinacji różnych zabezpieczeń w celu utworzenia warstw ochronnych dla zasobów. Na przykład mechanizmy kontroli dostępu stosowane dla komputerów powinny być wspomagane przez narzędzia audytu, procedury postępowania dla personelu, szkolenia i zabezpieczenia fizyczne. Pewne zabezpieczenia mogą już istnieć jako element środowiska lub jako cecha własna zasobów; mogą też być już zaimplementowane w systemie lub instytucji. Zabezpieczenia realizują jedną lub więcej następujących funkcji:

- wykrywanie,
- odstraszanie,
- zapobieganie,
- ograniczanie,
- poprawianie,
- odtwarzanie,
- monitorowanie,
- uświadamianie.

Odpowiedni dobór zabezpieczeń jest kluczowy dla prawidłowego wdrożenia polityki bezpieczeństwa. Wiele zabezpieczeń może służyć różnym funkcjom. Korzystny może być wybór zabezpieczeń, które będą jednocześnie spełniały wiele funkcji. Niektóre zabezpieczenia wyraźnie i jasno informują użytkowników o nastawieniu instytucji do bezpieczeństwa. W związku z tym ważne jest, aby wybrane zabezpieczenie było adekwatne do potrzeb i kultury organizacyjnej przedsiębiorstwa. Przy tym nie może być to mylone z niechcianymi przez pracowników ograniczeniami, jakie są związane zawsze ze stosowaniem zabezpieczeń.

Stosowanie zabezpieczeń ma oczywisty cel – redukcja ryzyka, choć nigdy go nie wyeliminuje, a tylko ograniczy. Skuteczność procesu ograniczania ryzyka jest wprost proporcjonalna do kosztów związanych z implementacją zabezpieczeń. Konieczne jest zatem monitorowanie ich skuteczności i efektywności.

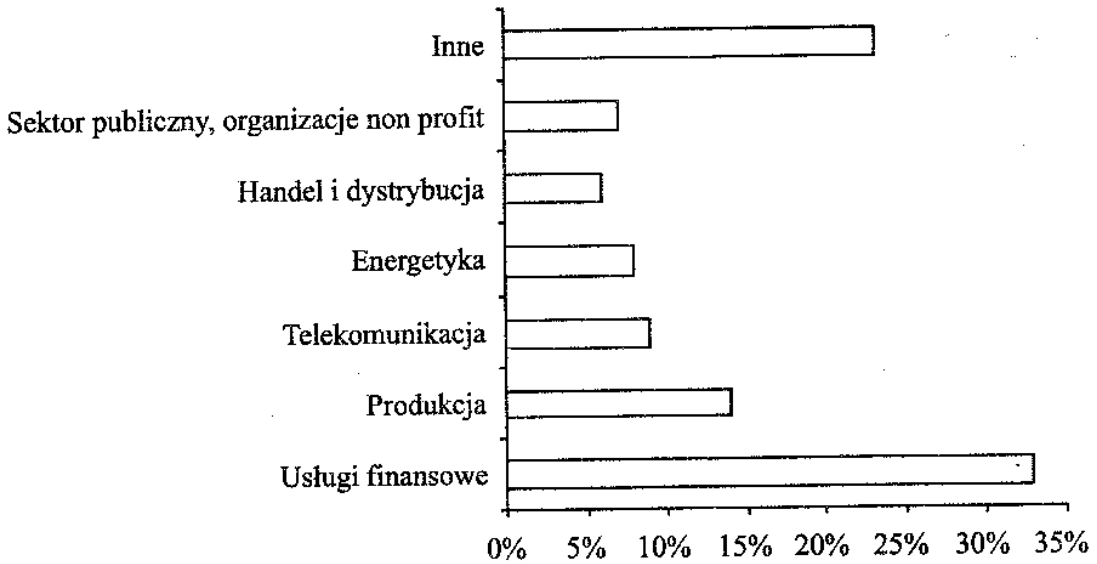
Elementem podejmowania decyzji o adekwatności zabezpieczeń ze względu na potrzeby instytucji jest akceptacja ryzyka szczątkowego. Proces ten znany jest jako akceptacja ryzyka. Kierownictwo organizacji powinno być świadome istnienia ryzyka szczątkowego w kontekście następstw oraz prawdopodobieństwa zajścia określonego zdarzenia. Decyzja o zaakceptowaniu ryzyka powinna być podejmo-

[27] Ibidem, s. 15.

wana przez te osoby, które są uprawnione do akceptacji konsekwencji ewentualnych skutków incydentu oraz autoryzacji wdrożenia dodatkowych zabezpieczeń, jeśli poziom pozostałego ryzyka szczątkowego jest nie do przyjęcia[28].

Zarządzanie bezpieczeństwem informacji w praktyce

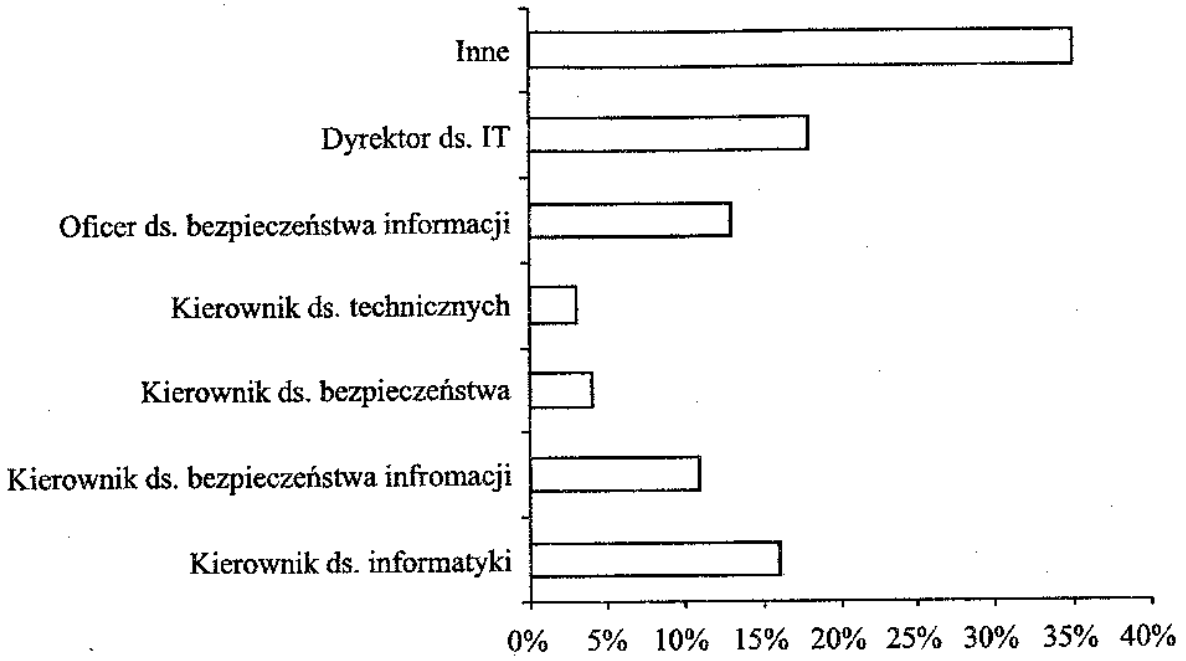
W niniejszym artykule zaprezentowane zostały wyniki badania, które miało udzielić odpowiedzi na wybrane pytania dotyczące koncepcji i realizacji w zakresie zarządzania bezpieczeństwem informacji. Badanie miało charakter ankietowy, przeprowadzone zostało metodą internetową na próbie 120 przedsiębiorstw. Dobór zbiorowości generalnej został dokonany w sposób celowy – były to przedsiębiorstwa posiadające certyfikowane systemy zarządzania bezpieczeństwem informacji ISMS (55) oraz inne eksponujące swoje zaangażowanie w zarządzanie bezpieczeństwem informacji.



Rysunek 2. Uczestnicy ankiety wg rodzaju prowadzonej działalności
Źródło: badania własne

Badane przedsiębiorstwa w pierwszej kolejności zaliczały się do grupy organizacji reprezentujących usługi finansowe, produkcja oraz telekomunikacja (rys. 2). Odpowiedzi na pytania udzielały osoby bezpośrednio związane z bezpieczeństwem informacji, przede wszystkim kierownik ds. informatyki, kierownik ds. bezpieczeństwa informacji, oficer bezpieczeństwa informacji, dyrektor IT.

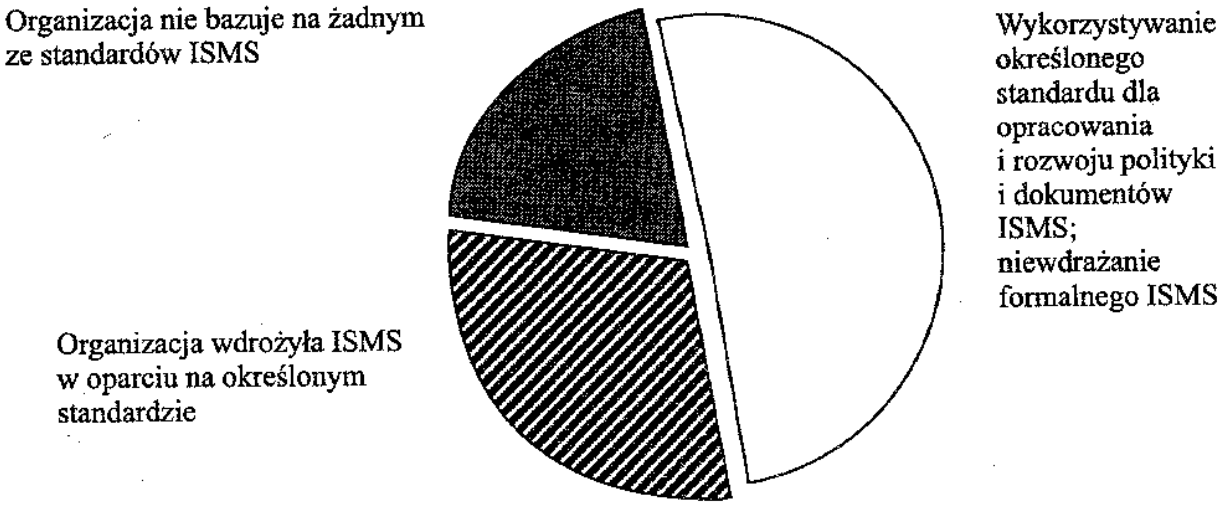
[28] Ibidem.



Rysunek 3. Uczestnicy ankiety wg zajmowanego stanowiska
Źródło: badania własne

Powszechność standardów w zakresie ISMS

Do końca 2007 roku zarejestrowanych zostało 7732 certyfikatów na zgodność z międzynarodowym standardem ISO/IEC 27001:2005, w 70 państwach[29]. Stanowi to wzrost o 25% w stosunku do liczby certyfikatów z roku poprzedniego. Przy tym fakt dbałości o bezpieczeństwo informacji nie jest jednoznaczny z ubieganiem się o certyfikat, choć wydaje się bardzo naturalne opieranie ISMS na dobrych praktykach w tym zakresie.



Rysunek 4. Wykorzystanie standardów międzynarodowych jako podstawy ISMS. Kształtowanie ISMS w organizacji
Źródło: badania własne

[29] *ISO Survey 2008*, ISO, Geneva 2008, s. 13.

Taki pogląd potwierdzają wyniki badań, bowiem połowa respondentów opiera swój system na określonym standardzie, choć nie ubiega się o certyfikat. 30% to organizacje posiadające certyfikaty, a 20% deklaruje indywidualną ścieżkę kształtowania polityki bezpieczeństwa informacji.

Przy tym należy zwrócić uwagę, że przedsiębiorstwa jako podstawę normatywną budowy ISMS podają nie tylko ISO/IEC 27001:2005[30], ale często także ISO/IEC 27002:2005[31] oraz *Information Security Forum's* (ISF)[32].

Ustanowienie, udokumentowanie i wdrożenie rozwiązań systemowych na podstawie rozpoznawalnych międzynarodowych standardów uznawane jest za poważne traktowanie zagadnień bezpieczeństwa informacji, bowiem nie pozostawia swobody w spełnieniu wymagań – uznanych za dobre i konieczne praktyki. Warto zauważyć, że często przy charakteryzowaniu zintegrowanych systemów zarządzania, coraz częściej pojawia się moduł bezpieczeństwa informacji, obok zarządzania jakością, środowiskiem i bhp. Dla wielu organizacji (ich klientów) poziom bezpieczeństwa informacji jest tożsamy z poziomem świadczonych usług.

Motywacja i korzyści związane z zarządzaniem bezpieczeństwem informacji

Uczestnicy badania, z uwagi na celowy dobór próby, wykazali świadomość w zakresie znaczenia informacji i konieczność ochrony jej bezpieczeństwa. Jak wynika z badań prowadzonych w zakresie czynników, jakie decydują o wdrażaniu ISMS, przede wszystkim wymienia się obawę o odpowiedzialność związaną z niezapewnieniem zgodności z wymaganiami prawnymi, dbałość o dobre imię firmy, zapewnienie zgodności z prawem i przez to ochrona organizacji przed negatywnymi skutkami incydentów.

Jednocześnie bezpieczeństwo informacji jednoznacznie kojarzone jest z efektami działalności gospodarczej, stąd obawa o utratę dochodów (72%) oraz klientów (71%). Niemal połowa ankietowanych wskazała także, że skutkiem łamania zasad bezpieczeństwa informacji będzie pogorszenie relacji międzypracowniczych.

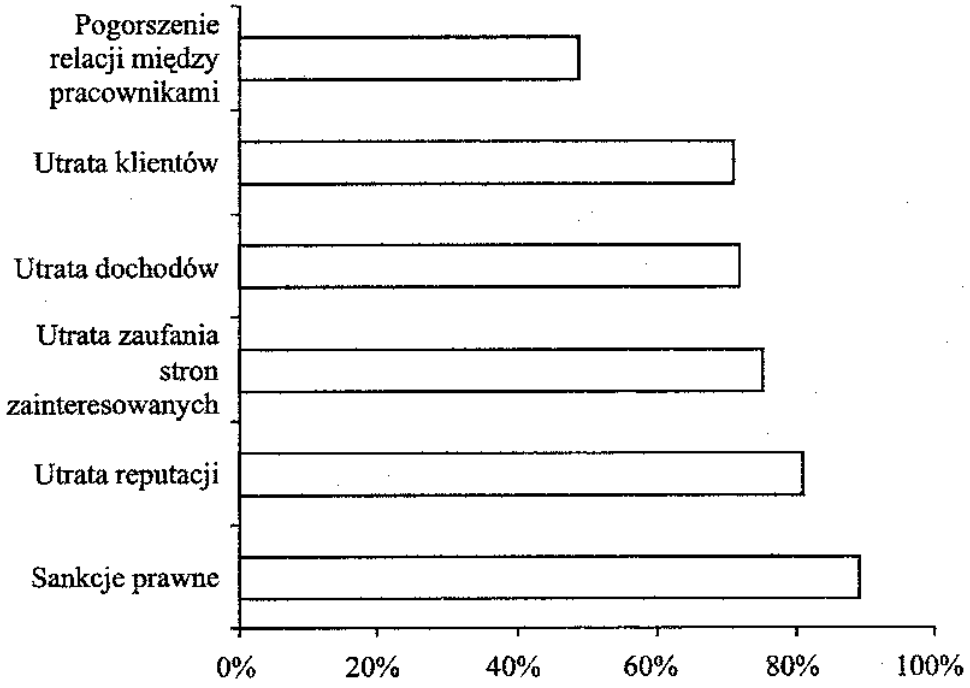
Czynnik – sankcje prawne, jest uznawany za najważniejszy, jednak kolejne istotne czynniki wskazują na wysoki poziom świadomości przedsiębiorców.

Wiele przedsiębiorstw polskich i zagranicznych oczekuje od dostawców spełnienia określonych kryteriów w zakresie bezpieczeństwa informacji. Obok pytań związanych z zagwarantowaniem satysfakcji klientów, pojawiły się już także pytania o wiarygodność i bezpieczeństwo procedur zarządzania związanych

[30] ISO/IEC 27001:2005 *Information technology – Security techniques – Information security management systems – Requirements,* ISO, 2005.

[31] ISO/ IEC 27002:2005 *Information technology – Security techniques – Code of practice for information security management,* ISO, 2005.

[32] *Information Security Forum's (ISF) – The standard of Good Practice for Information Security.*



Rysunek 5. Negatywne konsekwencje incydentów związanych z bezpieczeństwem informacji. Motywatory zarządzania bezpieczeństwem informacji
Źródło: badania własne

z ochroną powierzanych informacji[33]. Organizacje sektora przemysłowego i usługowego (instytucje finansowe, jednostki opieki zdrowotnej, operatorzy usług telekomunikacyjnych) oraz jednostki administracji publicznej zwracają na to szczególną uwagę[34]. Z tego też względu wiele organizacji wdraża lub deklaruje konieczność wdrożenia systemu zarządzania bezpieczeństwem informacji[35].

Organizacje wskazują wiele korzyści, które niesie z sobą ISMS. Na potrzeby niniejszego opracowania zostały one podzielone na wewnętrzne, zewnętrzne, ale także biznesowe i marketingowe. W konfrontacji z nimi należy także podsumować kluczowe wyniki badań zaprezentowane w treści artykułu.

Do wewnętrznych korzyści związanych z ISMS należą przede wszystkim:
- uniknięcie kar za naruszenie bezpieczeństwa informacji;
- zapewnienie zgodności z wymogami prawa – systemowe podejście do spełniania wymagań prawnych, a nie akcje doraźne;
- ochronę informacji będących w organizacji;

[33] *Zarządzanie bezpieczeństwem informacji*, (red.) J. Łuczak, Oficyna Współczesna, Poznań 2004, s. 5.

[34] T. Hurmphreys, *Finding a language to address information security management*, ISO Bulletin 2000, s. 23.

[35] Odpowiednie dyrektywy wydała również w tym zakresie Unia Europejska (95/46/EC, 97/33/EC, 97/66/EC, 98/10/EC, 99/93/EC, 2002/58/EC oraz indywidualne państwa, w tym także Polska (DzU 29.08.97, DzU 03.06.98, DzU 08.02.99, DzU 05.03.99).

- zabezpieczenie informacji w razie wystąpienia katastrofy czy awarii;
- wzrost świadomości pracowników z zakresie ochrony informacji, zmiana mentalności pracowników;
- wiedza i możliwość wpływu na zdarzenia wewnątrz organizacji;
- określenie odpowiedzialności i uprawnień pracowników w obszarze bezpieczeństwa informacji;
- zapewnienie klientów, dostawców, organizacji i osób trzecich, że ich dane są właściwie chronione;
- oszacowanie ryzyka związanego z zarządzaniem informacją;
- organizacja bezpieczeństwa fizycznego i informatycznego informacji;
- zarządzanie systemami informatycznymi i sieciami komputerowymi pod kątem bezpieczeństwa informacji;
- wprowadzenie rozwiązań wspomagających wykrywanie potencjalnych oraz usuwanie obecnych incydentów dotyczących bezpieczeństwa (w ramach zakresu wdrożonego systemu zarządzania bezpieczeństwem informacji), a także przewidywanie zagrożeń;
- usystematyzowanie dokumentów i działań – pod kątem wymagań uznanego międzynarodowego standardu zarządzania z bezpieczeństwem informacji (ISO/IEC 27001:2005);
- zaufanie do własnej organizacji;
- wprowadzenie okresowych audytów bezpieczeństwa informacji[36] i innych mechanizmów kontroli, oceny i doskonalenia funkcjonowania:
  - ustalenie w formie procedur sposobu postępowania w trakcie standardowego funkcjonowania, jak i w sytuacjach kryzysowych;
  - ograniczenie ryzyka utraty, zniekształcenia, niepowołanego dostępu do wewnętrznych informacji;
  - możliwość bardziej precyzyjnego ustalania prawdziwych przyczyn powstania największych rodzajów ryzyka biznesowego, dzięki czemu możliwe będzie przeciwdziałanie ich powstaniu;
  - usprawnienie przepływu i dostępu do informacji przy jednoczesnym wzroście bezpieczeństwa procesów realizowanych w organizacji;
  - wzrost elastyczności działania organizacji poprzez lepsze dostosowanie struktury organizacyjnej do wewnętrznych i zewnętrznych wymogów funkcjonowania;
  - podejście do bezpieczeństwa informacji oparte na zarządzaniu ryzykiem;
  - wdrożenie i utrzymanie mechanizmów dla utrzymania ciągłości działania organizacji;

[36] Zob. m.in. J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Warszawa–Poznań, 2001, s. 32.

- wdrożenie mechanizmów regularnej weryfikacji skuteczności stosowanych zabezpieczeń.

Korzyści wewnętrzne korespondują bezpośrednio z zewnętrznymi, do których należy zaliczyć:

- spełnienie wymagań przetargowych w zakresie bezpieczeństwa informacji;
- uwiarygodnienie firmy dla klienta, który w dzisiejszych czasach jakość bardzo często utożsamia z bezpieczeństwem;
- umocnienie pozycji w walce konkurencyjnej;
- potwierdzenie wysokiego poziomu kultury organizacji;
- prestiż wynikający z posiadania certyfikatu systemu zarządzania bezpieczeństwem informacji;
- poprawa wizerunku firmy jako bezpiecznego, wiarygodnego i nowoczesnego partnera;
- spełnienie wymagań obowiązujących norm (standardów bezpieczeństwa);
- niezależny nadzór sprawowany przez jednostki zewnętrzne;
- ułatwienie zdobywania uznania zagranicznych kontrahentów i zwiększanie wiarygodności biznesowej;
- wzrost konkurencyjności na rynku;
- pozyskanie nowych rynków i klientów; podobnie jak certyfikat ISO 9001:2000, ISO/IEC 27001 otwiera drogę do klientów o nieprzeciętnych wymaganiach, dla których spełnienie określonych norm jest podstawowym warunkiem do rozpoczęcia współpracy;
- zarządzanie bezpieczeństwem informacji odbywa się w sposób sformalizowany, przewidywalny.

Wiele firm podejmuje wyzwanie – wdrożenie i rozwój ISMS z uwagi na zamiar wzmocnienia marki i dbałość o dobre imię organizacji. Stąd warto przytoczyć korzyści, jakie niesie z sobą skuteczny system bezpieczeństwa informacji w wymiarze marketingu i promocji:

- poprawę wizerunku i prestiżu organizacji i jej produktów zarówno w oczach jej obecnych, jak i potencjalnych klientów;
- ochrona marki i dobrego imienia organizacji;
- budowanie profesjonalnego wizerunku organizacji godnej zaufania (dodatkowo poparte certyfikatem);
- zwiększenie poczucia pewności i zaufania, jakim klienci i partnerzy darzą organizację;
- podnosi wiarygodność organizacji i daje zapewnienie, że powierzone, przetwarzane informacje są w odpowiedni sposób chronione;
- uzyskanie dodatkowego elementu budowy wizerunku rzetelnej organizacji – dla klientów i stron trzecich;
- uzyskanie efektu postrzegania jako organizacji oferującej usługi na najwyższym poziomie w zakresie bezpieczeństwa;

- uzyskanie certyfikatu z zakresu zapewnienia bezpieczeństwa informacji dodatkowo służy jako narzędzie promocji i wyróżnienie w ramach danego zakresu na tle konkurencji.

Ostatecznie jednak ISMS należy postrzegać jako kategorię biznesową, stąd warto zwrócić uwagę, że zarządzanie bezpieczeństwem informacji zapobiega i ogranicza częstotliwość incydentów i ich negatywnych skutków:

- przecieki poufnych informacji do prasy, konkurencji, na rynek, itp.;
- zniszczenie informacji i nośników z powodu pożaru, zalania, sabotażu;
- łamanie prawa z powodu niedozwolonego wykorzystania informacji (np. wykorzystywanie poufnych danych lub publikacja danych osobowych bez uzyskania stosownej zgody);
- straty finansowe, prestiżowe, utrata wiarygodności spowodowana niedbałością o rzetelność przetwarzanych i posiadanych informacji;
- pewniejsze działanie w sytuacji zagrożeń powodowanych przez czynniki wewnętrzne i zewnętrzne – ciągłość biznesu;
- zabezpieczenie informacji na wypadek katastrof lub awarii – zarządzanie ciągłością działania;
- wzrost elastyczności działania organizacji poprzez lepsze dostosowanie struktury organizacyjnej do wewnętrznych i zewnętrznych wymogów funkcjonowania.

W tym miejscu należy zwrócić uwagę na korzyści dla klientów, partnerów i stron trzecich organizacji, która chroni informację w sposób systemowy. Do głównych korzyści można zaliczyć m.in.:

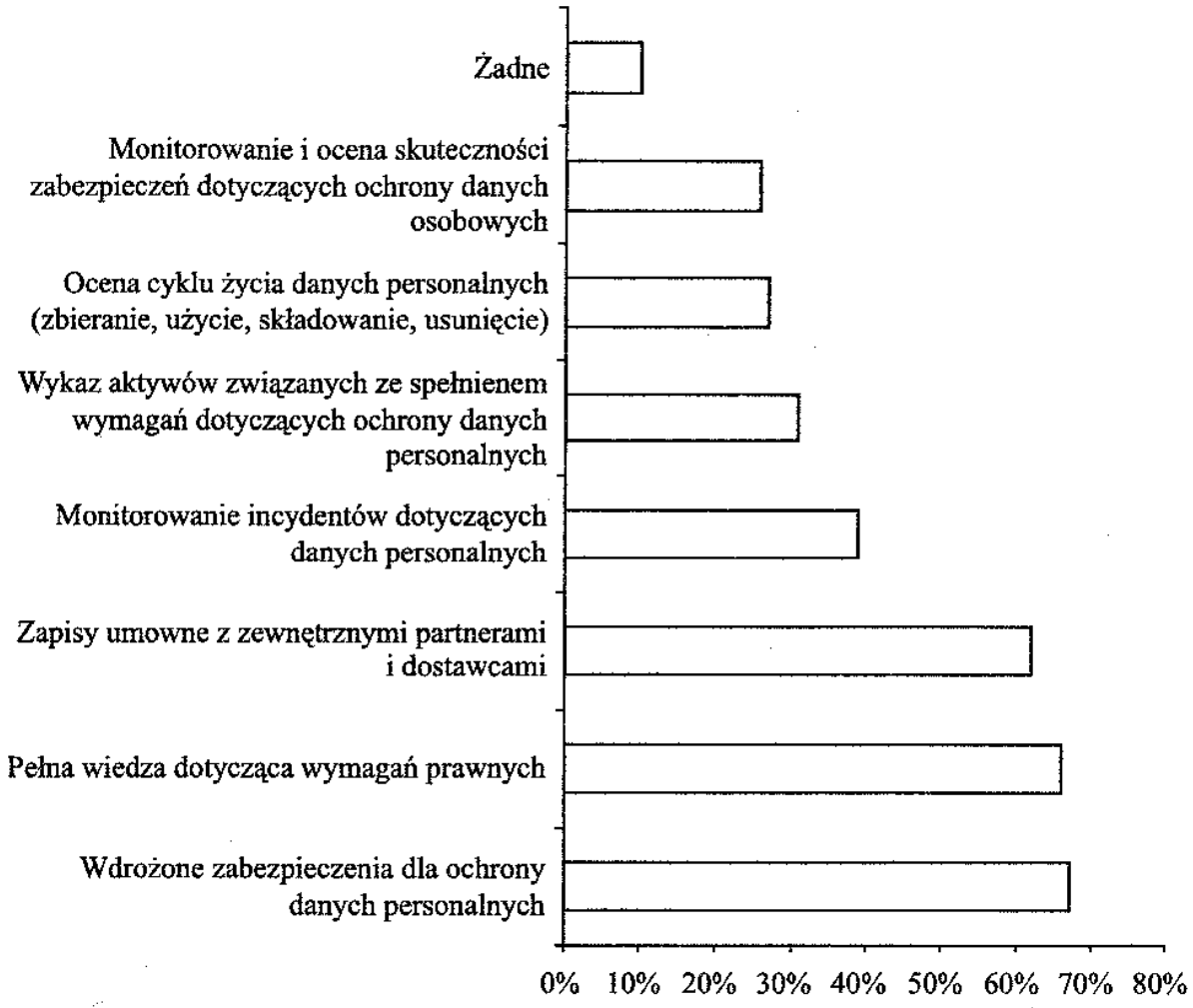
- klienci, partnerzy biznesowi i dostawcy wiedzą, kto za co odpowiada i jak mają postępować w zakresie ochrony informacji, z którą mają do czynienia; jasno określone są odpowiedzialność, procedury, podejmowane działania;
- zapewnienie klientów i zainteresowane instytucje, że ich dane są właściwie chronione;
- zwiększenie satysfakcji i zadowolenia klienta, spełniając jego wymagania poprzez stosowanie reguł systemu zarządzania bezpieczeństwem informacji.

Dane wrażliwe

Respondenci pytani o klasyfikację informacji oraz kategoryzację ich wrażliwości, jednoznacznie określili dane personalne jako kategorię najważniejszą.

Pytani o zabezpieczenia w niniejszym zakresie ponad 60% potwierdziło, że zna prawo dotyczące ich ochrony, dysponuje zabezpieczeniami na nie ukierunkowanymi, dostrzega ryzyko, jakie niosą w tym zakresie zewnętrzne, współpracujące organizacje.

Znacznie mniej wskazań jednak dotyczy zarządzania incydentami dotyczącymi danych personalnych czy ciągłego monitorowania procesu ich zabezpieczenia.

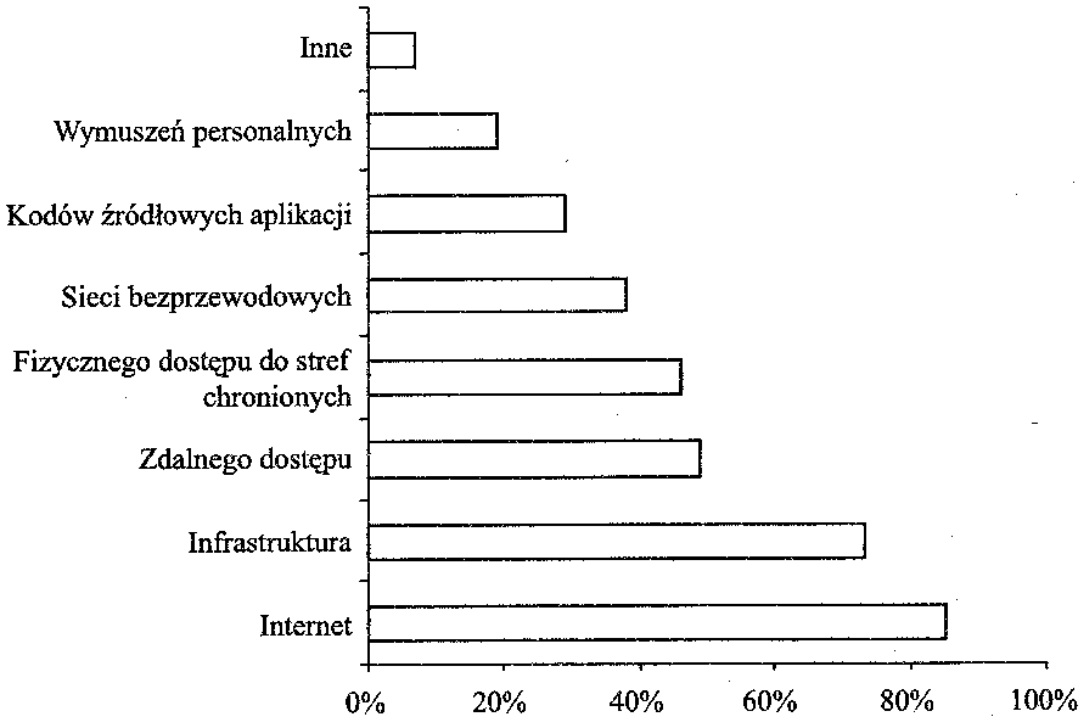


Rysunek 6. Zabezpieczenia związane z ochroną danych personalnych
Źródło: badania własne

Plany ciągłości działania (BCM) oraz ocena skuteczności zabezpieczeń

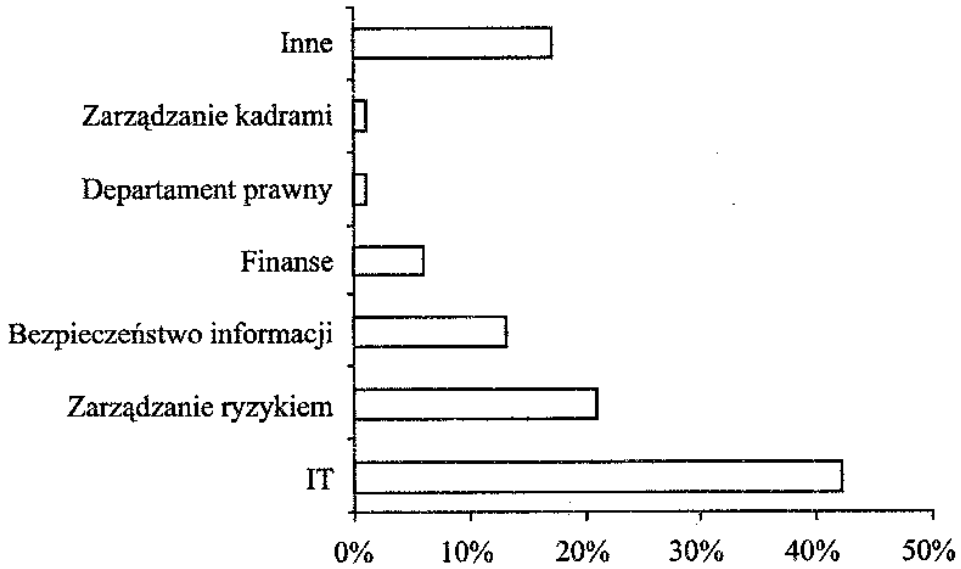
Zarządzanie ciągłością działania (ang. *Business Continuity Management* – BCM) to podejście do prowadzenia działalności organizacji w sposób pozwalający na utrzymanie określonego poziomu dostarczania produktów lub świadczenia usług w przypadku wystąpienia wszelkich zakłóceń w funkcjonowaniu procesów organizacji. Motywacją do zarządzania ciągłością działania stają się bardzo często wymogi branżowe wynikające z odpowiednich przepisów prawa. W polskim prawie wymóg ten znajduje się w rekomendacji „M" Głównego Inspektora Nadzoru Bankowego – dla banków; rozporządzeniu Ministerstwa Infrastruktury z lipca 2005 roku dla operatorów telekomunikacyjnych w sprawie obowiązku posiadania planów ciągłości działania oraz Ustawie z 27 kwietnia 2001 roku Prawo ochrony środowiska (Tytuł IV. Poważne awarie – Dział Instrumenty prawne służące przeciwdziałaniu poważnej awarii przemysłowej – od art. 251).

Zarządzanie ciągłością działania polega na identyfikacji zagrożeń dla funkcjonowania organizacji i opracowaniu sposobów postępowania w przypadku



Rysunek 7. Testy w zakresie ISMS regularnie prowadzone w organizacjach w ramach ISMS
Źródło: badania własne

wystąpienia zdarzeń, które mogą zakłócić to funkcjonowanie. Zdarzenia, które mogą spowodować zakłócenie działania organizacji, to nie tylko powodzie, pożary lub inne katastrofy, ale i chociażby opóźnienia. Rozważyć należy również wypadki nieoddziałujące bezpośrednio na organizację, które także mogą powodować znaczne zakłócenia w pracy.



Rysunek 8. Główna odpowiedzialność (struktury organizacyjne) za BCM
Źródło: badania własne

Należy zwrócić uwagę, że są sfery przedsiębiorstwa, które standardowo podlegają ocenie z punktu ciągłości działania, gdzie niekiedy bez zastosowania wystarczającej metodyki uznaje się je za uregulowania w tym względzie.

Najintensywniej testowane są Internet (85%), infrastruktura (73%), a ponadto – zdalny dostęp do systemów (49%), dostęp do stref chronionych (46%). Niniejsze wskazania pokazują także, w jakich obszarach koncentrują się formalnie opracowywane BCM.

Organizacje udowadniają także, że mają przygotowane struktury do oceny skuteczności zabezpieczeń, tworzenia i rozwoju planów kontynuacji biznesu. Wyniki badań w pewnym stopniu przełamują podporządkowanie bezpieczeństwa informacji informatyce, choć nadal jest ona kluczową strukturą w tym zakresie (rys. 8).

Respondenci poza IT (42%) wskazali na odpowiedzialność za BCM działów zarządzania ryzykiem (21%), bezpieczeństwa informacji (13%).

Uwagi końcowe

Wyniki badań przedstawione w niniejszym artykule mogą zostać wykorzystane przy projektowaniu ISMS oraz jego komponowaniu w ramach systemu zarządzania organizacją:

- włączenie zarządzania bezpieczeństwem informacji – jako elementu zarządzania strategicznego,
- większe wykorzystywanie międzynarodowych standardów w kształtowaniu ISMS,
- istotne zwiększenie skuteczności ochrony danych personalnych,
- przykładanie większej wagi do szkoleń dotyczących świadomości bezpieczeństwa informacji oraz stosowanych zabezpieczeń,
- skuteczniejsze monitorowanie ryzyka, jakie niesie z sobą współpraca ze stronami trzecimi.

Wyniki badań wykazały dużą świadomość przedstawicieli organizacji w zakresie bezpieczeństwa informacji. Stąd dojrzałe motywatory budowy ISMS. Wiodące wcześniej czynniki skłaniające firmy do tego typu inwestycji, takie jak dążenie do zgodności z obowiązującymi regulacjami, zostały niemal zastąpione przez chęć wzmacniania marki i ochronę dobrej reputacji firmy. Przy tym jednak w niewystarczającym stopniu bezpieczeństwo informacji jest elementem strategii biznesowej organizacji; a duży odsetek badanych organizacji w ogóle nie posiada strategii bezpieczeństwa. Duża część firm nie zdaje sobie jeszcze sprawy z zagrożeń, jakie niesie ze sobą brak spójnego podejścia do zabezpieczenia informacji – a te mogą być wielorakie – począwszy od inwestycji w tym obszarze, niewspółmiernych do rzeczywistych potrzeb, po brak skuteczności wdrażanych zabezpieczeń. Z kolei te firmy, które poczyniły już inwestycje w bezpieczeństwo informacji, planują je kon-

tynuować, pomimo światowego kryzysu i potrzeby ograniczania wydatków. Badanie zwraca również uwagę na potrzebę zwiększenia skuteczności zabezpieczeń w obszarze ochrony danych osobowych.

Najsłabszym ogniwem systemów zabezpieczeń pozostaje człowiek, w szczególności pracownicy. W przypadku naruszenia bezpieczeństwa informacji i wycieku danych, respondenci jako przyczynę najczęściej wskazują czynnik ludzki, co dowodzi, że system zabezpieczeń jest tak silny, jak jego najsłabsze ogniwo.

Jakość i dostępność informacji są kluczowymi czynnikami efektywnego zarządzania zintegrowanym łańcuchem dostaw. Zapewnienie bezpieczeństwa informacji oznacza także stabilną i bezawaryjną pracę wszystkich krytycznych systemów informatycznych, a w razie wystąpienia zagrożenia, odtworzenie systemu w krótkim czasie. Jest to możliwe dzięki wprowadzeniu odpowiednich zabezpieczeń, m.in. zapasowego centrum przetwarzania danych, procedur postępowania. Ma to fundamentalne znaczenie dla jakości świadczonych usług oraz powoduje zwiększenie bezpieczeństwa obsługi klientów, chroni przed utraconymi korzyściami w relacjach z ich partnerami biznesowymi. Jednocześnie pozwala na obniżenie kosztów obsługi, zwiększenie skuteczności planowania i podejmowania decyzji chociażby na podstawie rzetelnych i prawdziwych, dostępnych w odpowiednim czasie danych w systemach. Również w przypadku wystąpienia odchyleń, jakość informacji wpływa na szybkość właściwego rozwiązania problemu i wprowadzenia działań korygujących.

Literatura

Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2008, Cert Polska, 2009.

Borowiecki R., Jaki A., Kaczmarek J., *Metody i procedury wyceny przedsiębiorstw i ich majątku*, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 2002.

Cienińska B., Łunarski J., Perłowski R., Stadnicka D., *Systemy zarządzania bezpieczeństwem w przedsiębiorstwie*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2006.

Gierszewska G., Romanowska M., *Analiza strategiczna przedsiębiorstwa*, PWN, Warszawa 1997.

Gurgul H., *Analiza zdarzeń na rynkach akcji*, Oficyna Ekonomiczna, Kraków 2006.

Hurmphreys T., *Finding a language to address information security management*, ISO Bulletin, 2000.

Information Security Forum's (ISF) – The standard of Good Practice for Information Security.

ISO Survey 2008, ISO, Geneva 2008.

ISO/IEC 17799:2005 *Information technology — Security techniques — Code of practice for information security management*, ISO, 2005.

ISO/IEC 27001:2005 *Information technology – Security techniques – Information security management systems – Requirements*, ISO, 2005.

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

Kolegowicz K., *Nowe funkcje informacji we współczesnych koncepcjach zarządzania*, [w:] *Informacja w zarządzaniu przedsiębiorstwem*, (red.) R. Borowiecki, M. Kwieciński, Wolters Kluwer Polska, Kraków 2003.

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

Komputerowy słownik języka polskiego, WP PWN, Warszawa 1998.

Krysowaty I., Niedziejko P., *Bezpieczeństwo IT jako usługa kształtująca wartość i jakość informacji*, [w:] *Innowacyjność w kształtowaniu jakości wyrobów i usług*, (red.) J. Żuchowski, Wydawnictwo Instytutu Technologii Eksploatacyjnej, Radom 2006.

Linde S. B., *Słownik języka polskiego*, Warszawa 1951.

Zarządzanie bezpieczeństwem informacji, (red.) J. Łuczak, Oficyna Współczesna, Poznań 2004.

Moving Beyond compliance, Ernst & Young's 2008 Global, Information Security Survey, 2008.

Nogalski B., Surawski B. M., *Pozyskiwanie oraz bezpieczeństwo informacji w przedsiębiorstwie i państwie*, [w:] *Informacja w zarządzaniu przedsiębiorstwem*, (red.) R. Borowiecki, M. Kwieciński, Wolters Kluwer Polska, Kraków 2003.

PN-I-13335-1 – *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych*, PKN, 1999.

Reich L., Sawyer D., *Archiving Referencing Model*, White Book, Issue 5, CCSDS 1999.

Jacek Łuczak

INFORMATION SECURITY MANAGEMENT SYSTEM

Summary

The article focuses on selected aspects of a system approach to security management in an organization. The analysis of three qualities of information security, namely confidentiality, integrity and availability has provided a framework for the discussion. The author has put forward a number of research theses. They are related, for example, to: the frequency with which standards are used when information security is in question, significance of factors which play a decisive role in ISMS implementation, place and role of information security in management, business continuity and risk perception.

The idea underlying a practical discussion is presentation of the role of information in business. The author also discusses some possible threats and risks, resources and their vulnerability and security measures which can be taken. The practical discussion is based on the author's own research. In addition, some key requirements related to ISMSs are presented in the article. These requirements are above all based on the ISO/IEC 27001 standard. Companies tend to declare more often that they utilize the best solutions available in this respect. The solutions are determined in the ISO/IEC 27002 standard as well as by ISF. Thus, the author focuses on the best and recognized system approaches.

Based on the research, the author has been able to determine what motivates companies to implement ISMSs, what are the benefits of ISMS implementation and the main concerns related to ISMSs. Anxiety about legal consequences of incidents related to information security was one of the main motivating factors in the establishment of security policies and in the implementation of ISMSs. However, a number of respondents also stressed the significance of information security due to taking care of the good name of the company. In addition, the respondents pointed out that assuring legal compliance is crucial. As a result, organizations are well-protected against the negative effects of incidents.

At the same time it has to be stressed that the respondents declared that information security policies were usually not an integral part of the management strategy of the organization. Business Continuity Plans and their validation are very often restricted to the IT area only.

The results of the research which were fairly optimistic and were related to being aware of information security issues and at the same time taking specific activities applied only to the group of high-risk companies. Such companies declared their utmost care for information security. Unfortunately, the majority of companies did not establish and implement satisfactory information protection solutions, but they are not aware of the threats to business activity and how serious they can become.

The following article is a contribution to the discussion about the role of ISMS in organizational management.