Jacek Łuczak
Katedra Ekonomiki Jakości
Akademia Ekonomiczna w Poznaniu

Od zarządzana jakością (ISO 9001:2000) do zarządzania bezpieczeństwem informacji (BS 7799, ISO/ IEC 17799)

1. Wstęp

Międzynarodowe normy ISO serii 9000:2000 na trwałe wpisały się w scenariusze zarządzania organizacji, i nadal aktualny jest slogan „fenomen ISO". Setki tysięcy certyfikatów ISO 9001 na całym świecie, zainteresowanie powyższymi standardami wszystkich branż i bez mała każdej wielkości organizacji potwierdza potrzebę standaryzacji w sferze zarządzania. Potrzeba niniejsza wynika, z bardzo różnych przesłanek wewnętrznych i zewnętrznych. Niekiedy stanowi obowiązek, wynikający np. z wymagań przetargowych, innym razem związana jest z rosnącą świadomością konieczności bycia konkurencyjnym i wykorzystywania nowoczesnych metod i narzędzi w zarządzaniu.

Fakty zatem przemawiają za uznaniem pewnej koncepcji – standaryzacji w zarządzaniu. Na bazie niniejszej koncepcji powstało wiele podobnych norm sektorowych, m.in. uwzględniających wymagania branży motoryzacyjnej, telekomunikacyjnej, lotniczej, związanych z zarządzaniem jakością przy tworzeniu oprogramowania, zarządzania projektami, czy personelem[1].

Niejednokrotnie zatem zachodzi konieczność spełnienia wymagań standardów ważnych dla danego rynku, innym istotnym zagadnieniem

[1] W określonych branżach wiele wdrożeń dotyczy m.in. standardów ISO/ TS 16949, QS-9000, AS 9000, TL 9000, ISO 10006.

jest architektura systemu, która będzie odpowiadała potrzebom prowadzonej działalności. Zgodnie z podstawową koncepcją ISO 9001, system musi spełniać wymagania niniejszego standardu. Ostatecznie jednak powinien uwzględniać także inne zagadnienia, które nie są związane bezpośrednio z zapewnieniem jakości dla klienta, ale ważne z uwagi na tzw. wewnętrzne elementy zarządzania[2]. Do tych elementów bez wątpienia można zaliczyć ochronę informacji i danych, z uwagi na ich bezsprzecznie podstawową wartość w procesie zarządzania. Być może początkowo, ochrona informacji powinna być traktowana jako element system zarządzania jakością, bowiem związana jest bezpośrednio z niektórymi elementami normy. Przede wszystkim z koniecznością zapewnienia zasobów w zarządzaniu procesowym oraz z wymaganiami dotyczącymi zarządzania zasobami, w tym informacyjnymi[3]. W kolejnym kroku, zarządzanie informacją, być może powinno przybrać postać rozwiązań systemowych zgodnych z wymaganiami normy BS 7799/ ISO 17799 i zostać poddane certyfikacji.

Celem niniejszego artykułu jest zwrócenie uwagi czytelnika na systemowe rozwiązania w zakresie bezpieczeństwa informacji, mających z założenia zapobiegać zagrożeniom dotyczącym nieautoryzowanemu dostępowi, zniszczeniu, czy utracie danych informacyjnych; wskazanie konkretnych rozwiązań, jak również możliwości ich monitorowania oraz poprawnego wnioskowania. Znajduje się w nim odwołanie do podstaw systemowego zarządzania ryzykiem związanym z utratą danych, dotyczące teorii ochrony przed zagrożeniami w branży ICT (*Information and Communications Technologies*) oraz każdej organizacji dostrzegającej wartość i znaczenie informacji oraz danych.

---

[2] Obejmują one zagadnienia ważne dla prowadzenia działalności, ale nie wymagane przez dany standard, np. ISO 9001. Można do nich zaliczyć np. controlling, planowanie strategiczne, zarządzanie finansowe, działania promocyjne, benchmarking i inne.

[3] Patrz m.in. ISO 9001:2000, p. 4.1 D Wymagania ogólne, s. 8

2. Ryzyka związane z prowadzoną działalnością gospodarczą.

Ryzyko, występujące w różnych postaciach jest immanentnym elementem prowadzonej działalności gospodarczej. Zawsze istnieje możliwość pojawienia się praktycznego zagrożenia; w zależności od rodzaju i charakteru organizacji i rynku na jakim funkcjonuje będzie ono przybierało zróżnicowane postacie. W każdym przypadku ich wystąpienie jest niebezpieczne dla samej firmy, a przynajmniej spowalnia, czy ogranicza jej rozwój. Zagrożenie może się pojawić w postaci np. nieskutecznej rekrutacji, opóźnionej dostawy podzespołów od dostawcy, czy też awarii procesora wspomagającego planowanie produkcji, ale również – epidemii, włamania, ataku terrorystycznego, a coraz częściej kradzieży wartości intelektualnych firmy – różnego typu danych i informacji gospodarczych.

Konieczne jest zatem uświadomienie potrzeby systemowej ochrony informacji i traktowanie niniejszych procedur jako integralnych rozwiązań w ramach systemu zarządzania. Lekceważenie zagadnień bezpieczeństwa informacji, w pierwszej kolejności spełnienie wymagań prawnych w tym względzie, ale także celowa i świadoma ich ochrona, może sprowadzić nieoczekiwane zagrożenie i porażkę rynkową nie tylko samego przedsiębiorstwa, ale także jego klientów. Niewiele sytuacji kryzysowych formy można porównać z utratą informacji. Tym bardziej, że jak dowodzi praktyka są to przypadki coraz częstsze i niestety trudne do wykrycia. Można założyć, że każda organizacja traci na braku świadomości i nie podejmowaniu odpowiednich działań na rzecz ochrony danych. A nawet wykryte i jednoznacznie napiętnowane incydenty i niezgodności dotyczące danych, powodują nieporównywalne z innymi sytuacjami zagrożenia. Nie trudno wyobrazić sobie następstwa prawne, finansowe, czy utratę wiarygodności przedsiębiorstwa, które dopuściło do niekontrolowanego dostępu osób trzecich do bazy adresowej znaczącego klienta. Spektakularne i nagłaśniane przez media zdarzenia, mogą zobrazować powszechność incydentów tego typu skoro dochodzi do nich

w warunkach systemowych rozwiązań w tym względzie, do których zobligowane są instytucje administracyjne.

Systemowe zarządzanie bezpieczeństwem informacji (*Information Security Management Systems - ISMS)* nabiera szczególnego znaczenia w dobie informacji, kiedy zasoby informacyjne i zasoby ludzkie stanowią podstawowe filary każdej organizacji.

3. Podstawy systemowego zarządzania bezpieczeństwem informacji

Na początku lat 90-tych, Brytyjski Instytut Normalizacji BSI (*British Standards Institution*) przedstawił na forum publicznym opracowanie dotyczące zarządzania bezpieczeństwem informacji w przedsiębiorstwach, określone jako PD0003. Inicjatywa, w której popularność na początku wątpili sami twórcy wzbudziła ogromne zainteresowanie przedstawicieli wielu organizacji. Tezy i przesłanie, jakie niosła w sobie powyższa norma, skłoniły BSI do podjęcia nowych prac, w efekcie których opracowano zbiór praktycznych porad, wydany w 1995 roku jako norma BS 7799 *Code of practice for Information Security Managemen*[4].

Na poszczególnych etapach opracowania ostatecznej wersji standardu wykorzystywane były, doświadczenia i praktyki ochrony informacji stosowane w wielu znanych międzynarodowych firmach, m.in. Shell, Unilever, BT, Midland Bank, Marks and Spencer, Nationwide Building Society[5].

W obecnej chwili, pomimo ustanowienia standardu międzynarodowego ISO 17799, podstawową systemowych rozwiązań w zakresie bezpieczeństwa informacji w skali świata jest właśnie norma

---

[4] Patrz m.in. Thomas R. Peltier, Information security. Policies and Procedures. A. Practitioner`s Reference, AUERACH, CRC Press LLC, s. 234

[5] G. Bowden, I. McDonnell, J. Allen, W. O`toole, Events Management, Butterworth Heinemann, 2003, Oxford, ss. 34-40

brytyjska. Jednak wbrew powszechnej opinii nie dotyczy ona wyłącznie branży ICT (*Information and Communications Technologies*), a zgodnie z założeniami powinna spotkać się ze znacznie szerszym zainteresowaniem[6].

U źródeł opracowania założeń systemów zarządzania bezpieczeństwem informacji leżał krytyczny stosunek do stosowanych w tym względzie praktyk, w szczególności do ich powszechności. Wiodącą rolę w zakresie kreowania nowych zasad odegrał rząd brytyjski. Przeważającą większością głosów polityków brytyjskich, wszystkie organizacyjne systemy informacyjne powinny zostać objęte systemem zgodnym z BS 7799 oraz zostać poddane certyfikacji do końca 2002 roku. E-commerce przestało być teoretyczną koncepcją działalności gospodarczej, staje się aspektem gospodarki rozwijającym się szybciej i intensywniej, niż można było wcześniej przypuszczać. W Wielkiej Brytanii w 2002 roku zanotowany został 40% wzrost wykorzystania internetu w działalności gospodarczej firm i 37% w zakresie wykorzystania serwisów www (w tym samym czasie odpowiednio 7 i 11% w USA); 38% podmiotów brytyjskich deklaruje zainteresowanie e-biznesem[7]. Rząd Wielkiej Brytanii powziął ambitny cel do osiągnięcia w 2003 roku, dotyczący ustanowienia w UK najlepszego na świecie „środowiska" dla prowadzenia handlu elektronicznego.

Zgodnie ze słowami Mr Michaela Willsa, wszystkie organizacje na całym świecie będą wykorzystywały standard BS7799 – standard opracowany przez przemysł dla przemysłu[8].

---

[6] Praca zbiorowa, Asset Protection and Security Management Handbook, Auerbach Publications, A CRC Press Company, Florida, ss. 45-78

[7] Por. C.V.Brown, H.Topi, IS Magement Handbook, 8th edition, Auerbach, 2003, s. 90

[8] z wypowiedzi ministra Wielkiej Brytanii Michaela Willsa na Infosec`99

4. Normatywne podstawy systemowego zarządzania bezpieczeństwem informacji

Norma stanowiąca podstawę systemów zarządzania bezpieczeństwem informacji została opracowana przez BSI-DISC, strukturę BSI funkcjonującą pod nazwą BDD/2 Information Security Management. BDD/2 skupia przedstawicieli wielu organizacji brytyjskich, żywo zainteresowanych rozwojem e-biznesu.

BS 7799:2002 to dwuczęściowa norma:

- BS 7799-1:2002 - standardowy kodeks praktyki, katalog zagadnień, jakie należy realizować dla potrzeb bezpieczeństwa informacji (*Code of practice for Information Security Managemen)*;
- BS 7799-2:2002 - standardowa specyfikacja dla systemów zarządzania bezpieczeństwem informacji (ISMS – Information Security Management Systems).

Podstawą systemu zarządzania bezpieczeństwem informacji, która może zostać poddana akredytowanej certyfikacji jest norma BS 7799, cześć 2.

BS 7799-1:2000

BS 7799-1:2002 definiuje ponad 130 elementów kontroli i sterowania bezpieczeństwem informacji, podporządkowanych 10 grupom wymagań, co pozwala użytkownikom na zidentyfikowanie najwłaściwszych zabezpieczeń w kontekście specyfiki działalności, jaką prowadzą oraz otoczenia rynkowego i potrzeb w powyższym zakresie. Wykorzystywane narzędzia sterowania i kontroli zawierają dalsze szczegółowe techniki uznawane jako najlepsza praktyka w tym względzie.

Aktualne, drugie wydanie normy kładzie szczególny nacisk na *zarządzanie ryzykiem*, wskazuje także, że użytkownik nie jest zobowiązany do wdrażania wszystkich technik przywołanych w części

pierwszej standardu, tylko uznanych za najistotniejsze i zapewniające realizację celów. Katalog dotyczy wszystkich form informacji, w tym także ustnych i graficznych, powstających z wykorzystaniem telefonów komórkowych i faksów. Standard uwzględnia najnowsze formy działalności gospodarczej, np. e-commerce, internet, outsourcing, teleworking, mobile computing. Międzynarodowe aspiracje brytyjskiej normy podkreśla fakt, że specyfika rynku brytyjskiego została przywołana w załączniku, a nie w treści samej normy. Już na przełomie października i listopada 1999 roku rozpoczęły się formalne prace zmierzające do opracowania adekwatnego, międzynarodowego standardu (ISO), które doprowadziły w pierwszej kolejności do opracowania międzynarodowej normy ISO/ IEC 17799-1:2000[9].

BS 7799-2:2002

Zawarte w normie BS 7799-1 wymagania znalazły uznanie w wielu firmach brytyjskich. W oparciu o nabyte doświadczenie w BSI rozpoczęto prace nad kolejnym dokumentem normalizacyjnym BS 7799-2 *Information security management systems – specyfication with guidance for use*. Celem przyświecającym twórcom drugiej części standardu było stworzenie formalnych podstaw dla uruchomienia mechanizmu certyfikacji istniejących systemów ochrony bezpieczeństwa informacji. Przewiduje się, że w ramach procesu certyfikacji sprawdzany będzie aktualnie działający w danej firmie system ochrony bezpieczeństwa informacji na zgodność z sugestiami zawartymi w normie BS 7799.

BS 7799-2:2002 ilustruje, w jaki sposób zaprojektować, wdrożyć i poddać certyfikacji system zarządzania bezpieczeństwem informacji (ISMS - Information Security Management Systems). Norma wskazuje na sześcioetapowy proces kreowania i wdrożenia zaprojektowanych

[9] ISO/ IEC 17799-1 Information Technology – Code of practice for information security management.

rozwiązań (tab. 1); odwołuje się do konieczności określenia wszystkich aktywów informacyjnych i oszacowania ich istotności dla organizacji.

Tab. 1. Etapy projektowania i wdrażania ISMS

Etap	Opis
1.	Opracowanie polityki bezpieczeństwa informacji i danych, najważniejszych elementów systemu bezpieczeństwa informacji w odniesieniu do specyfiki organizacji, jej zasobów I potrzeb.
2.	Dokonanie identyfikacji ryzyk dotyczących informacji związanych z prowadzoną działalnością
3.	Ocena ryzyk – identyfikacja zagrożenia utraty aktywów informacyjnych i danych, słabości oraz nastawienia organizacji dla określania ryzyk.
4.	Zarządzanie ryzykiem z wykorzystaniem przystających elementów z BS 7799-2.
5.	Opracowanie bilansu adekwatności (Statement of Applicability) – zapisy wskazują na wybór określonych elementów BS 7799 oraz przyczyny uznania za nieodpowiednie pozostałych.
6.	Udokumentowanie procedur dotyczących zarządzania i elementów operacyjnych ISMS wskazujących na odpowiedzialności oraz podstawowe działania.

Źródło: *opracowanie na podstawie BS 7799-2:2002 Information security management systems – specyfication with quaidance for use, ss. 5–6.*

Standard zawiera także dodatkowe wymagania dotyczące struktury, zarządzania i administrowania w ramach systemu zarządzania bezpieczeństwem informacji – ISMS.

Przewodniki związane z BS 7799

Jednocześnie w ostatnim czasie dokonana została rewizja przewodników związanych z normą BS 7799:

- PD 3001:2002 – Preparing for BS 7799-2 certification;
- PD 3002: 2002 – Guide to BS 7799 Risk Assesment;
- PD 3003:2002 – Compliance assesment workbook;
- PD 3004:2002 – Guide to the implementation and auditing of BS 7799 controls;
- PD 3005:2002 – Guide on the selection of BS 7799 controls.

Zgodnie z ogólnie znanymi zasadami, opracowania o charakterze przewodników nie stanowią wymagań, przedstawiają natomiast referencyjne propozycje rozwiązań. W praktyce szacuje się możliwość ich zastosowania na poziomie 10%, z uwagi na specyfiki

5. Organizacja i wymagania BS 7799

Norma BS 7799-2 została podzielona na siedem rozdziałów, w tym cztery podstawowe części tematyczne odnoszących się do polityki i organizacji bezpieczeństwa informacyjnego w organizacji. Najważniejsze z nich to[10]:

- system zarządzania bezpieczeństwem informacji,
- odpowiedzialność kierownictwa,
- przegląd zarządzania w zakresie systemu bezpieczeństwa informacji,
- doskonalenie systemu zarządzania bezpieczeństwem informacji.

Z kolei do najważniejszych elementów wymagań należy zaliczyć::

- polityka bezpieczeństwa informacji w firmie;
- organizacja systemu bezpieczeństwa informacji;
- klasyfikacja oraz nadzór środków i zasobów wykorzystywanych dla realizacji polityki bezpieczeństwa;

[10] Praktycznie, wymagania związane z systemem zarządzania bezpieczeństwem informacji określone są w rozdziałach 4 – 7 normy BS 7799-2:2002.

- polityka bezpieczeństwa w odniesieniu do polityki kadrowej i metod rekrutacji pracowników;
- techniczne środki ochrony i kontroli dostępu do obiektów i pomieszczeń w odniesieniu do bezpieczeństwa danych i infrastuktury IT;
- formy i zasady korzystania z sieci i komputerów w firmie w odniesieniu do polityki bezpieczeństwa;
- zasady kontroli i monitorowania dostępu do systemów i informacji;
- utrzymanie, rozwój i rozbudowa systemu w odniesieniu do polityki bezpieczeństwa;
- planowanie strategii firmy wobec zagrożeń krytycznych;
- ochrona danych a regulacje prawne i wymogi formalne.

Każda z części zawiera od kilku do kilkunastu elementów odnoszących się do zakresu określonego w tytule. Dla przykładu, w części poświęconej *środkom i zasobom* norma zwraca uwagę na konieczność posiadania dokładnej informacji na temat posiadanych przez firmę komputerów czy nawet biurek. Informacja powinna zawierać szczegóły odnośnie tego, kto jest odpowiedzialny za serwis, a kto jest stałym użytkownikiem; kto może korzystać z określonych zasobów incydentalnie i w jakich sytuacjach. W normie przedstawiony został przykład, jakie środki i zasoby powinny zostać zakwalifikowane do systemu informacyjnego organizacji i jak należy je zaklasyfikować np.:

- bazy danych, kartoteki, dokumentacja systemu, podręczniki użytkownika, materiały szkoleniowe oraz procedury powinny zostać sklasyfikowane jako *informacje*;
- oprogramowanie użytkowe, systemowe oraz narzędziowe powinno zostać sklasyfikowane jako *oprogramowanie*;
- komputery, urządzenia telekomunikacyjne, drukarki, zasilacze, UPS'y, meble itp. jako *wyposażenie*;

- usługi centrum obliczeniowego, łączności czy np. służby utrzymania klimatyzacji jako *usług*.

Bazując na informacjach zebranych w trakcie inwentaryzacji środków i zasobów firmy, norma sugeruje, w jaki sposób połączyć konkretny środek lub zasób z odpowiednim poziomem jego ochrony - generalna zasada brzmi, że ochronie podlega wszystko, ale w różnym stopniu. W odniesieniu do środków i zasobów określonych jako *informacje* określony powinien ostać adekwatny poziom ochrony przy uwzględnieniu trzech potrzeb dotyczących specyfiki organizacji i rynku na jakim działa:

- *tajności* - czyli potrzeby posiadania mechanizmu utajniania wybranych, czy wszystkich informacji;
- *spójności* - czyli potrzeby posiadania mechanizmu utrzymywania starych i nowych informacji w stanie pozwalającym na zagwarantowanie ich spójności;
- *dostępności* - czyli potrzeby kontrolowanego i jednocześnie pełnego dostępu do posiadanych informacji.

Istotne jest także zwrócenie uwagi na wskazanie w normie, że nie istnieje ogólnie akceptowany standard nazywania i oznaczania informacji uznanych za *tajne* czy *poufne*, i jest to sprawa indywidualna dla każdej organizacji.

W innym fragmencie normy zwraca się szczególną uwagę na konieczność budowania świadomości wdrażanego systemu ochrony informacji wśród samych pracowników. Przedstawione tam sugestie odnośnie naboru pracowników na określone stanowiska dokładnie określają cel - minimalizację ryzyka wystąpienia zagrożenia wynikającego z błędów popełnianych przez ludzi.

Wszystkie aspekty zarządzania bezpieczeństwem informacji w firmie poruszone w standardzie i wynikające z nich problemy wymuszają na

kadrze kierowniczej bardzo dobre przygotowanie do realizacji zamierzonego celu. Z praktycznego punktu widzenia, każda z osób odpowiedzialnych za wdrożenie systemu zarządzania bezpieczeństwem informacji w danej firmie stanie przed problemem identyfikacji, definicji i analizy zagrożeń. Pełen obraz mapy zagrożeń jest etapem wstępnym przed rozpoczęciem wdrażania sugestii przedstawionych w normie BS 7799.

6. BS 7799 a międzynarodowe normy ISO

Norma brytyjska 7799-1 została zgłoszona przez BSI do Międzynarodowej Organizacji Normalizacyjnej - ISO jako podstawa ustanowienia międzynarodowego standardu zarządzania bezpieczeństwem informacji. Nadany został jej numer ISO/ IEC 17799-1 i uruchomiona została uproszczona procedura legislacyjna, tzw. *fast – track*. W tym przypadku przewidziany czas na tajne głosowanie to sześć miesięcy, który rozpoczął się 3 lutego i zakończył 3 sierpnia 2000 r. Ostatecznie w czwartym kwartale 2000 roku ustanowiony został standard ISO 17799:2000.

7. Dokumentacja systemu zarządzania bezpieczeństwem informacji – ISMS

Podobnie jak w systemach zarządzania jakością, środowiskiem czy bezpieczeństwem pracy (zgodnymi z normami ISO 9001, QS-9000, TL9000, ISO 14001, PN-N 18001 i innymi) ISMS musi być w pierwszej kolejności udokumentowany. I podobnie, najważniejszą rolę w tym względzie odgrywają procedury zarządzania. Przy tym jednak warto pamiętać, że procedura definiowana jest jako ustalony sposób przeprowadzenia działania lub procesu[11]. Dlatego właśnie mogą przybierać dowolne formy i postacie, nawet bardzo zindywidualizowane.

W tym kontekście innym wymaganiem jest, i wymaga zrozumienia wynikająca z normy potrzeba ustanowienia procedur udokumentowanych. W praktyce zatem chodzi o zapewnienie adekwatności specyfiki organizacjim jej potrzeb w odniesieniu do liczby, formy i struktury procedur. W praktyce, w systemach zarządzania bezpieczeństwem informacji konieczne jest udokumentowanie:

- treści polityki bezpieczeństwa oraz cele związane z bezpieczeństwem informacji,
- opisy elementów systemu oraz procedury wsparcia w tym względzie,
- raport oceny ryzyka,
- plan bezpieczeństwa informacji
- procedury niezbędne w organizacji dla skutecznego planowania, działania i sterowania procesami bezpieczeństwa danych,
- zapisy wynikające z normy BS 7799,
- bilans adekwatności[12] (wskazania dotyczące wybór określonych elementów BS 7799 oraz przyczyny uznania za nieadekwatne pozostałych).

W trakcie realizacji założonej polityki bezpieczeństwa firmy, m. in. wszystkie operacje wykonywane przez użytkowników w czasie pracy z systemem powinny zostać precyzyjnie udokumentowane. Szczegółowość dokumentacji nie jest w normie jednoznacznie określona. Przy tym przyjmuje się jednak założenie, że powinna zostać zaprojektowana i przygotowana w taki sposób, aby po poprawnym wdrożeniu formalnych procedur gwarantowały one pełne bezpieczeństwo systemu jako całości. Formalne procedury ISMS tworzone w ramach systemu bezpieczeństwa powinny obejmować takie aktywności jak, m.in.: rozwój systemu informatycznego, jego utrzymanie w ruchu (uruchamianie oraz zatrzymywanie systemu, archiwizacja danych, zasady

---

[11] PN-EN ISO 9000:2001, System zarządzania jakością. Podstawy i terminologia, p. 3.4.5, s. 35

[12] Statement of Applicability

obsługi sprzętu itd.), ochrona i kontrola dostępu do wyznaczonych obiektów, działanie w sytuacjach awaryjnych i inne.

Procedury związane z podstawowymi działaniami obejmującymi planowanie i realizacją procesów mogą przywoływać precyzyjne instrukcje odnośnie wykonywania określonych czynności, krok po kroku, ze szczególnym uwzględnieniem:

- zasad posługiwania się i wykorzystywania wszelkich danych zawartych w systemie;
- wymagań odnośnie dokładności i regularności wykonywania powierzonych zadań wszędzie tam gdzie istnieją zależności pomiędzy różnymi systemami, procesami, aplikacjami czy procedurami;
- reakcji na sytuacje krytyczne powstałe w wyniku błędów pojawiających się w trakcie pracy systemu;
- zasad korzystania z wszelkich dostępnych w systemie aplikacji narzędziowych i wspomagających (system utilities);
- reguł tworzenia, przechowywania i usuwania wszelkich drukowanych z systemu informacji uznanych za istotne z punktu widzenia tworzonej polityki bezpieczeństwa systemu - również w przypadkach wydruków błędnych, niepełnych czy kontrolnych;
- procedur uruchamiania systemu po awarii z dokładnym opisem czynności administratorskich.

Na etapie dokumentowania ISMS konieczne jest opracowanie procedur działania przygotowujących pracowników organizacji do postępowania w sytuacjach awaryjnych. Konieczne w tym przypadku jest zwrócenie uwagi na następujące aspekty:

- awarie i uszkodzenia systemu;
- błędy wynikające z próby przetwarzania niekompletnych, niepoprawnych lub uszkodzonych danych;
- próby włamania do systemu z zewnątrz organizacji;
- próby włamania do systemu z wewnątrz firmy;

- utratę wewnętrznych mechanizmów zabezpieczeń spowodowaną awarią sprzętu lub systemu;

Przy opracowywaniu planów odbudowy systemu po awarii należy między innymi uwzględnić:

- analizę i identyfikację przyczyn awarii systemu;
- dokładną definicję przyczyny oraz określenie konkretnych planów i kroków mających w przyszłości wyeliminować skutki wystąpienia zdefiniowanej przyczyny.

Procedury opracowane na potrzeby sytuacji odbudowy bezpieczeństwa systemu po próbie włamania się do systemu powinny w przypadku ich zastosowania gwarantować, że wyłącznie uprawnieni i dokładnie zidentyfikowani użytkownicy mają dostęp do danych i zasobów systemu

- wszystkie kroki przedsięwzięte po zaistnieniu sytuacji krytycznej zostały dokładnie udokumentowane i przedstawione do wglądu kierownictwu,
- bezpieczeństwo systemu zostanie na powrót przywrócone w możliwie najkrótszym czasie.

Wymagania BS 7799 dotyczące dokumentacji są znacznie szersze, niż przedstawione powyżej. Wszystkie procedury ISMS muszą być nadzorowane, aktualne, dostępne w miejscach stosowania, autoryzowane, podobnie jak zmiany, którym podlegają.

8. Akredytowana certyfikacja – *c:cure*

Enigmatycznie brzmiąca nazwa *c:cure* jest brytyjską procedurą akredytowanej certyfikacji systemów zarządzania bezpieczeństwem informacji (ISMS) zgodnych z BS 7799-2. Procedura została pierwotnie

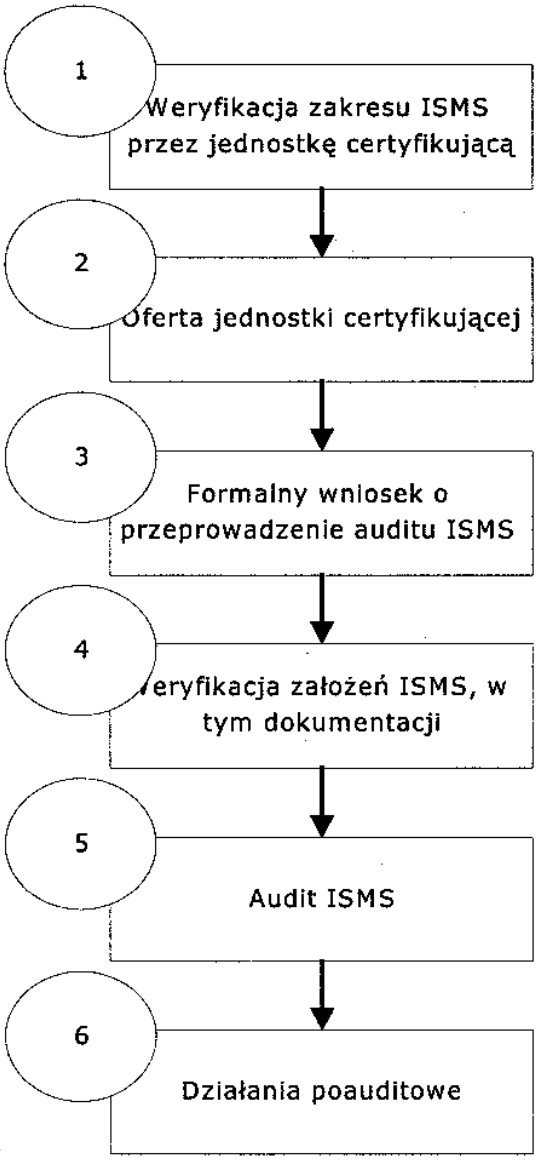
ustanowiona w 1998 przez Ministerstwo Handlu i Przemysłu Wielkiej Brytanii, jest natomiast rozwijana przez BSI-DISC[13]. Procedura zobowiązuje jednostki certyfikujące do poddania się procesowi krajowej akredytacji w zakresie realizowanej działalności. Zgodnie z założeniami *c:cure* auditorzy powoływani przez jednostki certyfikujące są wcześniej akredytowani zgodnie z określonymi kryteriami przyjętymi przez International Register of Certified Auditors (IRCA).

Do końca czerwca 2001 roku akredytację United Kindom Accreditation Service zgodną z przewodnikiem ISO 62 (EN 45012) na prowadzenie certyfikacji BS 7799 uzyskało sześć organizacji, przy czym, cztery z nich uzyskały akredytację na *c:cure*:

- BSI Quality Assurance – BS 7799;
- Bureau Veritas Quality International Ltd – BS 7799 oraz c:cure;
- Lloyd`s Register Quality Assurance Ltd– BS 7799 oraz c:cure;
- Det Norske Veritas Quality Assurance Ltd – BS 7799 oraz c:cure;
- National Quality Assurance Ltd – BS 7799 oraz c:cure;
- SGS Yarsley International Certification Service Ltd – BS 7799.

[13] DISC jest strukturą wewnętrzną British Standards Institution odpowiedzialną za rozwój i publikację BS 7799 oraz sprawującą za zgodą Ministerstwa Przemysłu i Handlu Wielkiej Brytanii nadzór nad procedurą *c:cure*.

Rys. 1 Etapy certyfikacji systemu zarządzania bezpieczeństwem informacji (ISMS)



Źródło: ***materiały źródłowe BSI – DISC, 2000***

Na rysunku nr 1 przedstawione zostały typowe, formalne etapy procedury certyfikacyjnej. W swojej strukturze nie odbiega od zasad auditu jakości, czy ekoauditu[14]. Przy tym różnice związane są z istotą podstaw system, czyli wymagań BS 7799-2.

[14] Por. ISO 19011:2002 Guidelines for Quality and/ or environmental systems auditing

Przed podjęciem czynności auditowych potwierdzenia wymaga zakres ustanowionego w organizacji systemu. Na tej podstawie jednostka certyfikująca składa ofertę na przeprowadzenie certyfikacji. W przypadku jej przyjęcia dokonywana jest ocena założeń systemowych. Na tym etapie ocenie poddawane są: polityka bezpieczeństwa, cele, procedury systemowe, analiza ryzyka itd. Po skorygowaniu ewentualnych niezgodności przeprowadzany jest audit, na podstawie którego jednostka certyfikująca sporządza raport i w przypadku pozytywnej oceny rekomenduje system. Certyfikat ważny jest przez trzy lata.

9. Przeznaczenie standardu BS 7799 (ISO/ IEC 17799)

Zdecydowanie potrzeba systemowego ograniczania ryzyk związanych z niezamierzonym dostępem do zasobów informacyjnych osób trzecich dotyczy znacznie szerszego grona organizacji, niż tylko związanych z IT.

Dla zobrazowania powyższej tezy można powołać się na źródłowe informacje BSI, związane z odpowiedzią na pytanie: *Dlaczego konieczne jest zainteresowanie BS 7799*[15]:

- norma jest zbiorem praktycznych wskazówek, powstała jako odpowiedź na żądania wysuwane przez firmy różnych branż i sektorów przemysłu co do określenia metod walki z narastającą falą zagrożeń płynących z postępującej informatyzacji życia (np. szpiegostwo przemysłowe, defraudacja, zwykłe przypadki kradzieży czy awarii systemów informatycznych);
- w środowiskach otwartych systemów ICT i w dobie elektronizacji handlu standard daje możliwość wprowadzenia bardzo dobrych podstaw dla tworzenia sprawnych systemów zarządzania bezpieczeństwem informacji;

[15] www.bsi-global.com

- standard jest niezbędnym i najistotniejszym elementem, w oparciu o który buduje się bezpieczeństwo w rozproszonych i współdzielonych systemach teleinformatycznych. Standard gwarantuje partnerom, dostawcom i odbiorcom końcowym bezpieczeństwo wymienianych między sobą informacji.

Istotne jest jednak skomentowanie powyższej argumentacji, która przykłada szczególną wagę do zagrożeń zewnętrznych, powszechnie uznawanych za najbardziej niebezpieczne. W praktyce jednak, gdy system ICT łączy wiele firm w jeden organizm (systemy EDI - Electronic Data Interchange), mamy do czynienia z modelem, dla którego przede wszystkim należy mówić o analizie zagrożeń wewnętrznych. A zatem nie tylko partnerzy rynkowi, dostawcy i odbiorcy mogą stanowić potencjalne zagrożenie dla informacji gospodarczych, bowiem równie istotne są zagrożenia wewnętrzne, związane z pracownikami.

Mapy zagrożeń każdej organizacji można zbudować z czterech podstawowych elementów[16]:

- pracowników, czyli nas samych;
- procesów, którymi zarządzamy;
- technologii, które wykorzystujemy
- oraz struktury organizacyjnej, której się podporządkowujemy będąc jej elementami.

Każdy z przedstawionych elementów może stanowić dla nas potencjalne źródło zagrożeń wewnętrznych.

---

[16] Thomas R. Peltier, Information security. Policies and Procedures. A. Practitioner`s Reference, AUERACH, CRC Press LLC, 1999, s. 334

Systemy, informacyjne w tym, np. teleinformatyczne przez swoją specyfikę oraz możliwość łączenia się bez względu na odległość i porę dnia muszą być traktowane w kategorii zagrożeń wewnętrznych oraz zewnętrznych – każda organizacja musi indywidualnie zdecydować ostatecznie, jaka rola zostanie im przypisana.

Dlatego właśnie analizując istotę standardu BS 7799 można powiedzieć, że zawarte w nim regulacje powinno się traktować jako uniwersalne dla każdego typu organizacji i każdego systemu informacyjnego.

Przy tworzeniu normy założono, że będzie ona przeznaczona dla osób odpowiedzialnych za określanie, wprowadzanie i zarządzanie mechanizmami ochrony informacji w przedsiębiorstwach, a zawarte w niej informacje powinny być traktowane jako wytyczne dla określania własnych standardów ochrony. W wielu opracowaniach podkreśla się, że cechą zawartych w dokumencie wskazówek jest ich zwięzłość i uniwersalność oraz, że zakres poruszonych problemów pokrywa najczęstsze przypadki spotykane w codziennej pracy organizacji wszelkich branż.

10. Wiodące wymagania legislacyjne w zakresie ochrony danych

Ochrona danych i informacji, w tym osobowych, stała się podstawą dla opracowania wielu aktów prawnych w skali poszczególnych państw, jak również obszarów ekonomicznych czy konkretnych kontraktów handlowych. Do najbardziej znaczących w Europie na pewno zaliczyć należy Data Protection Act (1998) opracowany w Wielkiej Brytanii. Jest uznawany za najlepszy dokument tego typu na świecie, jego ustanowienie na pewno także leży także u podstaw intensyfikacji prac związanych z budową i doskonaleniem normatywnych podstaw systemowego zarządzania bezpieczeństwem informacji (BS 7799).

DPA nakłada obowiązki na pracodawców - pracowników odpowiedzialnych za nadzorowanie danych personalne, wskazuje konieczne zasady i regulacje w zakresie powyższych aktywności.

DPA określa wymagania, jakim musi sprostać pracodawca w odniesieniu do danych personalnych; restrykcyjność postępowania jakie muszą być przyjęte w praktyce są związane z rodzajem i przeznaczeniem danych, źródłem ich pochodzenia oraz procesów jakim celowo są poddawane.

Data Protection Act definiuje podstawowe zasady dotyczące bezpieczeństwa danych nakazujące postępowanie z danymi personalnymi w zgodzie z prawem. W podstawowym względzie zasady niniejsze stawiają ograniczenia, m. in.

- dane personalne nie mogą być wykorzystywane w żadnym innym celu poza tym dla jakich zostały zebrane,
- dane personalne powinny być wierne i utrzymywane dłużej niż jest to konieczne w związku z celem dla osiągnięcia jakiego zostały pozyskane.

Istotną cechą opracowanego w 1998 roku dokumentu jest uwzględnienie transferu danych personalnych na zewnątrz EEA (European Economic Area). Konieczne jest w powyższym zakresie zapewnienie, że dane personalne nie będą transferowane do państwa na zewnątrz Europejskiej Strefy Ekonomicznej przed zapewnieniem przez to państwo adekwatnego poziomu bezpieczeństwa oraz swobody w przetwarzaniu tego typu informacji.

DPA definiuje także wymagania w zakresie pozyskiwania, rejestracji, archiwowania oraz przetwarzania danych.

Podstawą dla opracowania DPA były doświadczenia związane z zarządzaniem bezpieczeństwem informacji i wnioskowanie w tym zakresie leży u podstaw wszystkich punktów tego dokumentu. Warto

zwrócić uwagę o uzupełnienie DPA w stosunku do poprzednich koncepcji o wymagania definiujące konieczność ustanowienia systemu monitorowania i pomiarów związanych z nieautoryzowanym i nie w pełni zgodnym z prawem działaniem na danych personalnych; związanych z utratą, zniszczeniem czy ich uszkodzeniem.

DPA w swojej treści odwołuje się do systemowego podejścia związanego z bezpieczeństwem informacji i danych. Wskazuje na konieczność wdrożenia i utrzymywania ISMS – Systemu zarządzania bezpieczeństwem informacji, odwołuje się w tym przypadku do normy BS 7799.

A zatem spełnienie wymagań normy BS 7799 może okazać się bardzo pomocnym mechanizmem demonstrowania i dowodzenia gotowości do spełnienia wymagań prawa w zakresie ochrony danych.
Prawna konieczność ochrony danych, stwarza korzystny klimat dla zainteresowania systemowym zarządzaniem bezpieczeństwem informacji (ISMS - Information Security Management System) zgodnego z normą BS 7799.
Przemawia za tym kilka argumentów:

- wymagania niniejszego standardu są związane z koniecznością systemowych działań dotyczących oceny ryzyk oraz ustanawiania adekwatnych zabezpieczeń przed realizacją działań mogących spowodować utratę czy też uszkodzenie danych organizacji,
- zobowiązanie do periodycznej weryfikacji ryzyk dotyczących bezpieczeństwa informacji, związanych ze zmianami w otoczeniu rynkowym, doświadczeń itd.,
- jest uznanym narzędziem, które z założenia zobowiązuje do respektowania wymagań prawa, prywatności danych i innych zasobów informacyjnych.

W kontekście powyższych analiz szczególnego znaczenia nabiera procedura akredytowanej certyfikacji c:cure, dzięki której organizacja

może na drodze niezależnego auditu trzeciej strony uzyskać certyfikat zgodności i demonstrować na rynku posiadanie udokumentowanego, wdrożonego i efektywnego systemu zarządzania bezpieczeństwem informacji.

Konieczne jest zwrócenie uwagi na polski obszar legislacyjny, gdzie wiodącą role odgrywają ustawy:

- Ustawa z dnia 22 stycznia 1999 o ochronie informacji niejawnych,
- Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych,
- Ustawy z dnia 6 września 2001r. o dostępie do informacji publicznej,
- Ustawa z dnia 21 sierpnia 1997 r. Prawo o publicznym obrocie papierami wartościowymi.

11. Analiza zainteresowania organizacji systemowym zarządzaniem bezpieczeństwem informacji oraz BS 7799

W 1999 roku przeprowadzone zostały w Wielkiej Brytanii badania związane przypadkami utraty informacji przez firmy oraz działań i planów związanych z ustanowieniem systemu zarządzania bezpieczeństwem informacji zgodnym z normą BS 7799 (c:cure survey 2000).
Rezultaty badań oddają obraz obaw przedsiębiorstw związanych z niekontrolowaną utratą danych oraz mogą stanowić podstawę dyskusji w tym względzie.
Ocenie poddanych zostało ponad 1000 organizacji brytyjskich, z szerokiego spektrum instytucji produkcyjnych i usługowych – począwszy od liczących mniej niż 10 pracowników (18%) do zatrudniających tysiące pracowników w różnych lokalizacjach. Badane organizacje reprezentują 10 szerokich kategorii, zawierają w sobie firmy z sektora prywatnego i publicznego, producentów i usługodawców, przedstawicieli usług profesjonalnych i innych.

Tab. 2 Respondenci c:cure survey 2000

Lp.	Sektory	udział
1.	Sektor publiczny	22%
2.	Przemysł	20%
3.	Usługi finansowe i prawne	18%
4.	IT (Information Technology)	16%
5.	Usługi serwisowe	11%
6.	Usługi przemysłowe	4%
7.	Usługi transportowe	4%
8.	Sprzedaż i dystrybucja	3%
9.	Obronność	2%

Źródło: *c:cure survey 2000, BSI – DISC, Admiral plc.*

W przypadku pytań dotyczących przypadków naruszenia zasad bezpieczeństwa większość firm odpowiadała, że nie zanotowali takich sytuacji w ogóle – szczególnie taka odpowiedź dotyczyła dużych organizacji, natomiast druga grupa organizacji wskazywała na bardzo liczne przypadki tego typu.

Zdecydowana większość badanych organizacji nie jest świadoma zagrożeń związanych z nieskutecznym systemem bezpieczeństwa informacji. Można dopatrywać się dwóch podstawowych przyczyn, dla jakich organizacje nie wykazują problemów dotyczących bezpieczeństwa informacji i danych.

Po pierwsze nie są świadome ich występowania. Jest całkiem logiczne, że jeżeli forma nie zapewniła dostępności efektywnych rozwiązań w zakresie uniemożliwienia nieautoryzowanych działań to nie jest w stanie definiować większości z takich przypadków, jeśli w ogóle jakiekolwiek.

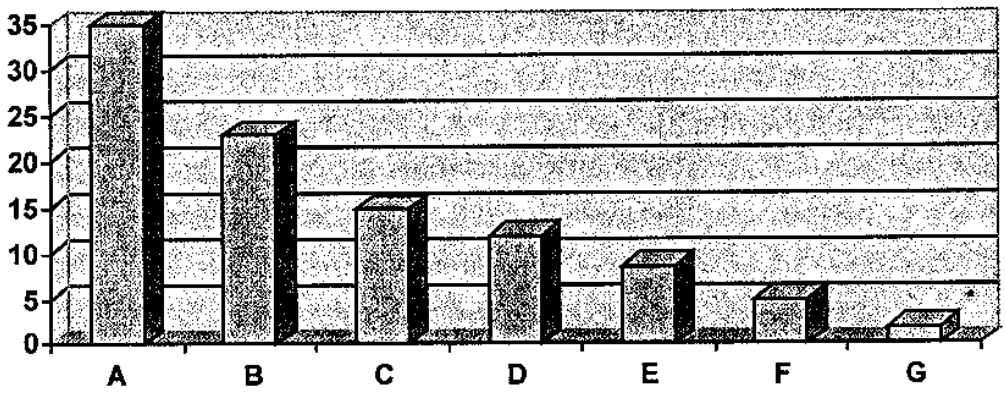
Po drugie w sytuacji, kiedy klient czy też partner rynkowy dostrzeże problemy dotyczące bezpieczeństwa, ich reputacja oraz wiarygodność zostają wystawione na wielką próbę. Na pewno także w wielu przypadkach organizacje poświęcają uwagę dyskrecji w działaniach

służących eliminowaniu skutków zdarzeń dotyczących nieskuteczności zabezpieczeń.

Powszechność normy BS 7799 oraz certyfikacji c:cure

Obecna struktura i treść BS 7799, w której wielokrotnie można odnaleźć szczególny nacisk na warunki i relacje rynkowe i jest jednoznacznym dowodem na odpowiedniość wobec współczesnych wymagań rynkowych. Jednak badania wykazały, że większość organizacji w Wielkiej Brytanii - ponad 50%, jest na bardzo zróżnicowanym poziomie zainteresowania wdrażaniem ISMS w oparciu o BS 7799 oraz certyfikacji systemu zarządzania bezpieczeństwem informacji.

Rys. 2 Powszechność normy BS 7799 oraz certyfikacji c:cure



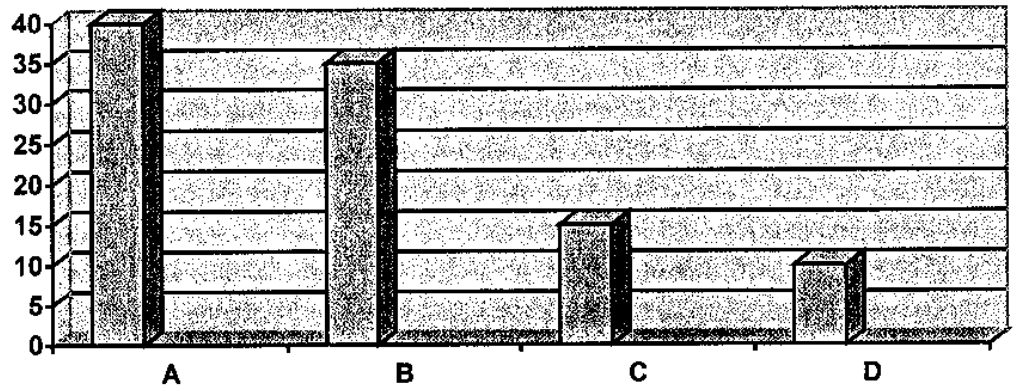
A – posiadają informacje i rozważają podjęcie projektu ISMS (64,9%)
B – świadomi istnienia BS 7799, ale nie podejmujący żadnych działań (22,9%)
C – nie posiadający żadnej wiedzy dotyczącej BS 7799 (14,9%)
D – zgodni z wymaganiami standardu BS 7799 (11,9%)
E – przeprowadzający audity wewnętrzne (8,6%)
F – rozważający z zarządem zasadność podjęcia projektu ISMS zgodnie z BS 7799 (4,9%)
G – gotowi do certyfikacji BS 7799 (1,9%)

Źródło: *c:cure survey 1999, BSI – DISC, Admiral plc.*

Korzyści związane z ustanowieniem systemu zarządzania bezpieczeństwem informacji zgodnym z BS 7799

Ponad 40% organizacji wskazuje na korzyści, jakie mogłyby być związane z ustanowieniem ISMS. W pierwszej kolejności jest wymieniana pomoc w ochronie informacji i danych i w drugiej natomiast, możliwość ustanowienia podstawy systemowych rozwiązań wewnątrz firmy.
Inna grupa organizacji postrzega BS 7799 oraz procedurę c:cure jako korzystne z uwagi na podniesienie wiarygodności w oczach klientów, pomoc w osiąganiu koniecznego poziomu bezpieczeństwa danych personalnych oraz przewagę konkurencyjną.

Rys. 3 Korzyści związane z Systemem zarządzania bezpieczeństwem informacji zgodnym z BS 7799



A – Ochrona informacji i danych (40%)
B – podstawa wewnętrznego bezpieczeństwa informacji (35%)
C – konieczny element działalności organizacji (15%)
D – Ochrona wymiany informacji rynkowej (10%)

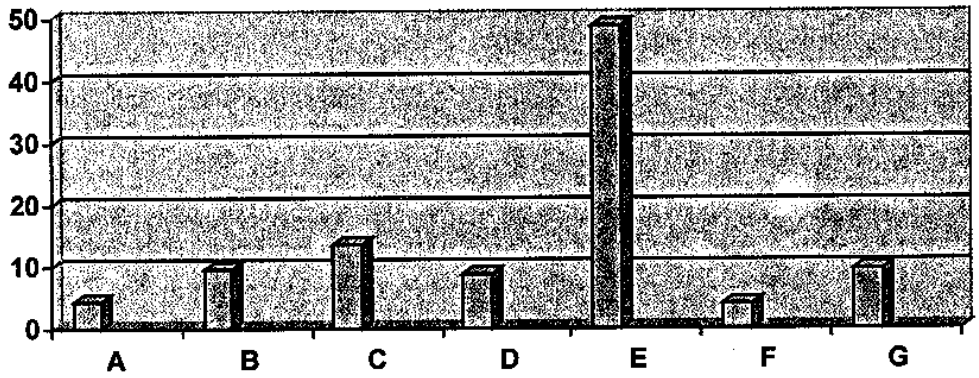
Źródło: *c:cure survey 1999, BSI – DISC, Admiral plc.*

Przygotowanie do certyfikacji

Zważywszy na fakt, że c:cure jest stosunkowo nową koncepcją weryfikacji skuteczności ISMS, 15% badanych organizacji zadeklarowało wstępnie swoją gotowość do certyfikacji w najbliższym czasie, a najdalej

w ciągu 12 miesięcy. Ponad 1/3 firm – 36% powzięło decyzję o spełnieniu wymagań BS 7799 i przystąpienie do procedury certyfikacyjnej. W kilku przypadkach firmy posiadają ustanowione systemy zarządzania bezpieczeństwem informacji lub elementy systemu oparte o inne zasady niż BS 7799. Tylko 4% firm wyraziło pogląd o nieadekwatności BS 7799 wobec prowadzonej działalności.

Rys. 4 Przygotowanie ISMS do certyfikacji



A – gotowość do certyfikacji w okresie krótszym niż 6 miesięcy (4,5%)
B – gotowość do certyfikacji w okresie 6 – 12 miesięcy (9,9%)
C – gotowość do certyfikacji w okresie 12 – 18 miesięcy (13,5%)
D – gotowość do certyfikacji w czasie dłuższym niż 18 miesięcy (8,9%)
E – zainteresowanie BS 7799 ale zbyt mało informacji (48,7%)
F – brak zainteresowania z uwagi na nieadekwatność (4,0%)
G – mało prawdopodobne wdrażanie BS 7799 i certyfikacja (9,9%)

Źródło: *c:cure survey 1999, BSI – DISC, Admiral plc.*

Można przytoczyć powtarzające się opinie przedstawicieli firm, którzy uznali, że jest mało prawdopodobne zainteresowanie BS 7799 oraz przystąpienie do procesy certyfikacji:

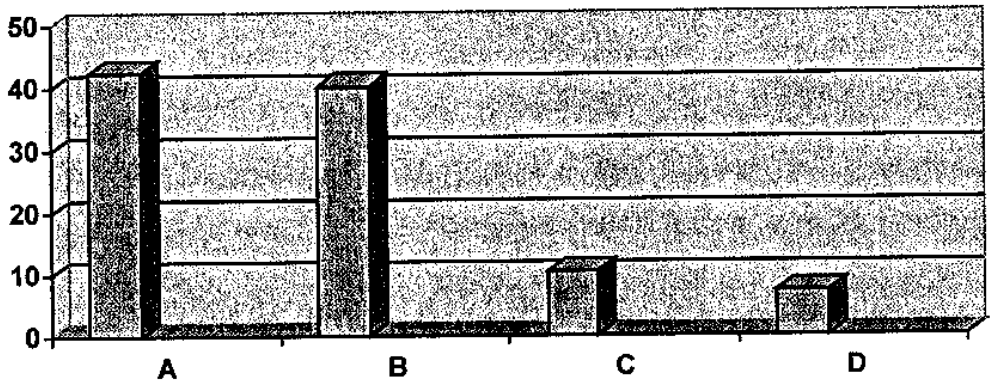
- zbyt mała firma – brak efektywności finansowej przedsięwzięcia (typowa opinia firm jednoosobowych),

- tylko w przypadku kiedy będzie to wymaganiem klientów,
- mamy inne procedury w zakresie bezpieczeństwa informacji (np. instytucje rządowe).

Zainteresowanie procesem certyfikacji

Podstawową przyczyną, dla jakich organizacje podejmują decyzje o certyfikacji ISMS w oparciu o normę BS 7799, jest bezpieczeństwo prowadzonej działalności oraz podążanie za najlepszymi i sprawdzonymi koncepcjami w tym zakresie. W dalszej kolejności przedsiębiorcy zwracają uwagę na przewagę konkurencyjną z jaką wiążą posiadanie certyfikatu. Na ostatnim miejscu zainteresowania pozostaje zainteresowanie partnerów handlowych oraz wymagania klientów.
Spośród innych przyczyn, na jakie zwracali uwagę przedstawiciele badanych firm można przytoczyć także: dowodzenie zgodności z wymaganiami legislacyjnymi (Data Protection Act), osiągnięcie poziomu bezpieczeństwa w standardzie jakim to realizują najlepsze firmy.

Rys. 5 Zainteresowanie procesem certyfikacji *c:cure*



A – najlepsza praktyka w zakresie zarządzania bezpieczeństwem informacji (42,3%)
B – bezpieczeństwo prowadzonej działalności (40,1%)

C – przewaga konkurencyjna (10,4%)
D – wymagania klientów (7,2%)

Źródło: *c:cure survey 1999, BSI – DISC, Admiral plc.*

12. Podsumowanie

Błędy w zakresie ochrony danych popełniane są na każdym kroku: nie uporządkowanie biurka po dniu pracy, nie wykorzystywanie niszczarek dokumentów, lekceważenie rotacji haseł i zachowania ich tajności, niekontrolowany dostęp pracowników do internetu, niesprawdzeni pracownicy służb czyszczących i inne. Upowszechniającą się plagą są wirusy komputerowe. Szczególnie niepokojąca jest globalizacja problemu; np. wirus *I love you*, Czernobyl, Michał Anioł czy MyDoom

Z założenia system zarządzania jakością powinien osiągać cele zewnętrzne – zadowolenie klientów jak również wewnętrzne – zróżnicowane w zależności od charakteru organizacji oraz rynku, na jakim działa. ISMS jest mechanizmem pozwalającym zarządzać oraz chronić wszystkie aktywa informacyjne poprzez zapewnienie ich poufności, integralności oraz dostępności danych i informacji. Wdrażanie systemu zarządzania bezpieczeństwem informacji związane jest w pierwszej kolejności z dbałością o zapewnienie podstaw bezpiecznego funkcjonowania firmy. I tak np. czy jest możliwe wprowadzenie nowej technologii bez dokonania analizy ryzyka, jakie z tym przedsięwzięciem się wiążą. Na takich samych zasadach niezbędne wydaje się dokonanie analizy ryzyka związanego z utratą różnego typu danych i informacji. Powyższe założenia w istotny sposób wpływają również na satysfakcję klienta, bowiem tylko systemowe rozwiązania w zakresie bezpieczeństwa informacji mogą spowodować, że firma zrealizuje postanowienia umowne. Co więcej w wielu przypadkach dane powierzone przez

klientów, stanowią znacznie większą wartość niż samo zlecenie. Tak jest np. w przypadku firm pracujących na bazach danych klientów.

A zatem za powzięciem decyzji o ustanowieniu systemu zarządzania bezpieczeństwem informacji przemawia kilka argumentów, m.in.:

- wymagania niniejszego standardu są związane z koniecznością systemowych działań dotyczących oceny ryzyk oraz ustanawiania adekwatnych zabezpieczeń przed realizacją działań mogących spowodować utratę czy też uszkodzenie danych organizacji,
- standard stanowi zobowiązanie do periodycznej weryfikacji ryzyk dotyczących bezpieczeństwa informacji, związanych ze zmianami w otoczeniu rynkowym, doświadczeń itd.
- BS 7799 uznanym narzędziem, które z założenia zobowiązuje do respektowania wymagań prawa, prywatności danych i innych zasobów informacyjnych.

W kontekście powyższych rozważań szczególnego znaczenia nabiera procedura akredytowanej certyfikacji c:cure, dzięki której organizacja może na drodze niezależnego auditu trzeciej strony uzyskać certyfikat zgodności i demonstrować na rynku posiadanie udokumentowanego, wdrożonego i efektywnego systemu zarządzania bezpieczeństwem informacji.

Prawdziwość powyższych argumentów potwierdza coraz szersze grono certyfikowanych brytyjskich organizacji, m. in. Insight Consulting, Wright Publications, Logica pic, Business Link London City Partners.

Bibliografia:

1. BS ISO/ IEC 17799–1 Information Technology – Code of practice for information security, 2000.
2. BS 7799–2 Information Security Managemet Systems – Specyfication with guidance for use, 2002.

3. Materiały szkoleniowe BS 7799 Risk Assesment Workshop, ODI 2000.
4. M. Oldegard, Applying the management system approach to information security and working conditions in Sweden, ISO News, vol. 9, no. 3 may/ June 2000.
5. Forrester Research Raport 1999.
6. PD 3001:2002 Preparing for BS 7799-2 certification.
7. PD 3002:2002 Guide to BS 7799 Risk Assesment
8. PD 3003:2002 Compliance assessment workbook
9. PD 3004:2002 Guide to the implementation and auditing of BS 7799 controls
10. Pd 3005:2002 Guide on the selection of BS 7799 controls
11. ISO/IEC/TR 13335 Technika informatyczna – wytyczne do zarządzania bezpieczeństwem systemów informatycznych
12. c:cureworld newsletter, BSI – DISC, summer 99.
13. The c:cure survey 2000, BSI – DISC – Admiral plc, 2000.
14. E. Stankunowicz, Nie śpij bo cię okradną, Businessman Magazine, sierpień 2000.
15. J. Stokłosa, T. Bilski, T. Pankowski, Bezpieczeństwo danych w systemach informatycznych, Wydawnictwo Naukowe PWN Warszawa, Poznań 2001.
16. Thomas R. Peltier, Information security. Policies and Procedures. A. Practitioner`s Reference, AUERACH, CRC Press LLC, 1999
17. Maria Parlińska, Dystrybucja informacji w wirtualnym środowisku, Wydawnictwo SGGW, Warszawa, 2002
18. G. Bowden, I. McDonnell, J. Allen, W. O`toole, Events Management, Butterworth Heinemann, Oxford, 2003
19. V. Milak (editor), Foundamentals of Risk Analysis and Risk Management, Lewis Publishers, 1997
20. P. Gerrard, N. Thompson, Risk – Based E-Business Testing, Artech Hose, 2002
21. Praca zbiorowa, Asset Protection and Security Management Handbook, Auerbach Publications, A CRC Pres Company, Florida, 2003
22. C.V.Brown, H.Topi, IS Magement Handbook, 8th edition, Auerbach, 2003
23. A.R.Simon, S.L.Shaffer, Hurtownie danych i systemy informacji gospodarczej, Oficyna Ekonomiczna, 2002