PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1177 — 2007

Zarządzanie jakością i środowiskiem
jako determinanty doskonalenia działania organizacji

Bolesław Szomański

Politechnika Warszawska

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI – NOWE WYZWANIE DLA KIEROWNICTWA FIRM W DĄŻENIU DO DOSKONAŁOŚCI

1. Wstęp

Przez wiele lat XX w. jakość nie była uważana za ważny element w produkcji i sprzedaży nowych wyrobów. Sytuacja zmieniła się na skutek wspomaganych pracami Deminga i Jurana sukcesów gospodarczych Japonii. Opracowano założenia filozofii TQM, stworzono modele nagród jakości, które przekształcono w nowoczesne modele doskonałości. Podobnie przez wiele lat nie zwracano uwagi na zanieczyszczenia środowiska i problemy ekologiczne. Sprawami tymi również zaczęto się interesować dopiero w ostatnich dekadach XX w.

Na początku XXI w. opracowano najnowsze normy dotyczące zarządzania jakością serii ISO 9000:2000 i integrowano je z normami dotyczącymi zarządzania środowiskowego serii ISO 14000. Powszechnie uważano, że trzecią z norm zintegrowanych są normy związane z zarządzaniem bezpieczeństwem i higieną pracy (takie, jak PN 18000), które jednak nigdy nie uzyskały statusu norm ISO.

W roku 2000 pojawiła się jednak inna norma ISO wskazująca nowe kierunki i potrzeby w zakresie integracji systemów zarządzania. Była to norma ISO/IEC 17799 Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji [6]. Norma zawierała wytyczne, czyli stanowiła odpowiednik normy ISO 9004:2000, w zakresie zarządzania bezpieczeństwem informacji. Dopiero jednak w 2005 r. została przyjęta norma ISO/IEC 27001 Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania [8] – odpowiednik normy ISO 9001. Poprzednio funkcjonowała norma

brytyjska BS 7799-2:2002 [2], na zgodność z którą do września 2006 r. certyfikowało się ponad 2800 firm na świecie [10]. ISO/IEC 27001 bezpośrednio wywodzi się z normy BS 7799-2 [2].

Celem opracowania jest przedstawienie znaczenia bezpieczeństwa informacji jako nowego wyzwania dla kierownictwa w drodze do doskonałości. W opracowaniu przedstawiono normy serii ISO 27000 dotyczące bezpieczeństwa informacji, a także zawarte w nich wymagania dotyczące kierownictwa. Wskazano także różnice pomiędzy systemami zarządzania jakością i systemami zarządzania bezpieczeństwem informacji, z których najważniejszy jest brak wymagań przeprowadzenia analizy ryzyka w systemach zarządzania jakością. W podsumowaniu wskazano na rosnące znaczenie systemu zarządzania bezpieczeństwem informacji (SZBI) dla doskonałości firmy i zilustrowano to przykładem praktycznym.

2. Znaczenie zarządzania bezpieczeństwem informacji

Dlaczego zarządzanie bezpieczeństwem informacji stało się tak ważne, skoro informacja była wykorzystywana od niepamiętnych czasów, a przetwarzana za pomocą komputerów już co najmniej 50 lat? Sytuacja uległa zmianie, gdy firmy w sposób wydaje się nieodwracalny uzależniły się od przetwarzania komputerowego, internetu oraz komunikacji w sieciach teleinformatycznych (w tym komórkowych). Obecnie bez zapewnienia dostępności, integralności i poufności informacji firmy nie mogą przetrwać dłużej niż kilka dni.

Warto przy tym wyjaśnić, co uważane jest za bezpieczeństwo informacji według normy ISO/IEC 27001:2005: „zachowanie poufności, integralności i dostępności informacji; dodatkowo i inne własności takie, jak autentyczność, rozliczalność, niezaprzeczalność i wiarygodność, mogą być uwzględnione" [8]. Nadal jednak wiele osób niesłusznie kojarzy bezpieczeństwo informacji wyłącznie z poufnością, zapominając, że dostępność i integralność informacji może decydować o funkcjonowaniu firmy.

Obecnie coraz częściej wdraża się zintegrowane systemy zarządzania obejmujące zarządzanie jakością, środowiskiem, bhp oraz bezpieczeństwem informacji. W takich systemach bezpieczeństwo informacji nie powinno być jednak traktowane jako mniej ważne, wręcz przeciwnie, często jest dużo ważniejsze od niektórych innych systemów zarządzania.

W przypadku bezpieczeństwa informacji zwyczajowe działania nieuwzględniające niektórych wymagań bezpieczeństwa mogą w krytycznej sytuacji doprowadzić do upadłości firmy, poważnych strat finansowych, konsekwencji prawnych lub utraty wiarygodności przedsiębiorstwa. Wymagania bezpieczeństwa informacji są znacznie bardziej sformalizowane niż wymagania jakościowe i, podobnie jak wymagania norm środowiskowych i bhp, powinny być oparte na przepisach prawnych, których firma musi przestrzegać.

Systemy zarządzania bezpieczeństwem informacji nie zawsze mają tylko charakter dobrowolny, np. Unia Europejska nakazuje swoim agencjom płatniczym uzyskać certyfikat systemu zarządzania bezpieczeństwem informacji na zgodność z ISO 27001.

Trudno sobie obecnie wyobrazić doskonałą firmę bez zarządzania bezpieczeństwem informacji. Nieprzypadkowo ponad połowa certyfikatów systemów zarządzania bezpieczeństwem informacji została przyznana w Japonii, kraju, z którego wywodzi się nowoczesne podejście do zarządzania jakością. Liczbę certyfikatów w wybranych krajach przedstawiono w tab. 1.

Tabela 1. Liczba certyfikatów na zgodność z BS 7799-2:2002 i ISO 27001

Kraj	Liczba certyfikatów	Kraj	Liczba certyfikatów	Kraj	Liczba certyfikatów
Japonia	1715	Stany Zjednoczone	42	Hongkong	22
Wielka Brytania	251	Korea	31	Australia	20
Indie	201	Węgry	31	Finlandia	15
Tajwan	94	Chiny	28	Polska	15
Niemcy	60	Holandia	28	Czechy	14
Włochy	42	Singapur	24	Norwegia	14

Źródło: [10].

Systemy zarządzania bezpieczeństwem informacji są wdrażane we wszystkich działach gospodarki bez specjalnych preferencji na rzecz poszczególnych obszarów, a ich udział wynosi [3]:

- telekomunikacja 25%;
- finanse 21%;
- usługi trzeciej strony 17%;
- sektor informatyczny 15%;
- firmy produkcyjne 11%;
- agencje rządowe 7%;
- infrastruktura techniczna 4%.

Przedstawione zestawienie wskazuje wyraźnie, że ISO 27001 to nie jest kolejna norma branżowa, jak podają niektórzy, ale rozwiązanie dotyczące wszystkich dziedzin działalności gospodarczej, co najmniej tak szeroko stosowane jak zarządzanie jakością.

3. Normy dotyczące systemów zarządzania bezpieczeństwem informacji

Zarządzanie bezpieczeństwem informacji w środowiskach informatycznych powszechnie kojarzy się z normą ISO 17799 [6] (i jej brytyjskim odpowiednikiem, jakim była norma BS 7799-1 [1], a następnie norma BS 7799-2 [2]) oraz ze starymi normami związanymi z bezpieczeństwem systemów informatycznych, czyli ISO 13335 [4; 5]. Obecnie jednak to już historia. W roku 2005 podjęto decyzję, że będzie opracowana nowa seria norm związanych z bezpieczeństwem informacji – grupa norm ISO 27000 [3]:

- 27000: Information Security Management System Fundamentals and Vocabulary – wywodząca się z ISO 13335-1 [4], planowane wydanie – koniec 2007 r.;
- ISO/IEC 27001:2005 Information Security Management System (ISMS) Requirements, wkrótce ukaże się polskie wydanie;
- 27002 obecnie ISO/IEC 17799: 2005 Code of Practice for Information Security Management, 2nd Edition 2005 – od kwietnia 2007 r. będzie mieć numer ISO/IEC 27002, polskie wydanie ukaże się wkrótce;
- 27003: Information Security Management System Implementation Guidance – dalekie plany;
- 27004: ISMS Metrics & Measurements – dalekie plany;
- 27005: Information Security Risk Management – wywodząca się z ISO 13335-3 [5], planowane wydanie nastąpi pod koniec 2007 r.;
- 27006: Guidelines for the Accreditation of Bodies Operating Certification Registration of Security Management Systems Based on the Conformity Assessment Standard ISO/IEC 17021 – zaawansowane prace, wydanie polskie ukaże się w 2007 r.

Niewątpliwie najważniejszą normą spośród norm serii 27000 jest norma ISO/IEC 27001, stanowiąca wymagania do projektowania systemów zarządzania bezpieczeństwem informacji. Budowa tej normy jest zbliżona do innych norm dotyczących systemów zarządzania i składa się z wprowadzenia i definicji, rozdziałów merytorycznych (4. System zarządzania bezpieczeństwem informacji; 5. Odpowiedzialność kierownictwa; 6. Wewnętrzne audyty SZBI; 7. Przeglądy SZBI realizowane przez kierownictwo; 8. Doskonalenie SZBI) oraz załączników, w tym normatywnego załącznika A [8].

Jak widać z przedstawionego zestawienia, budowa normy opiera się na ISO 9001, ale z jedną istotną różnicą: konieczność spełnienia wymagań normatywnego załącznika A, zawierającego 134 przeznaczonych do wdrożenia zabezpieczeń (znacznie więcej niż wymagania ISO 9001 i samej normy ISO 27001); które powoduje, że pracochłonność przygotowania SZBI jest znaczna.

4. Rola i znaczenie kierownictwa firm w odniesieniu do SZBI

Norma ISO 27001 określa rolę i odpowiedzialność kierownictwa w odniesieniu do SZBI, podobnie jak ISO 9001 w rozdziale 5:

„5. Odpowiedzialność kierownictwa

5.1. Zaangażowanie kierownictwa

Kierownictwo powinno zapewnić świadectwo swojego zaangażowania w ustanowienie, wdrożenie, eksploatację, monitorowanie, przegląd, utrzymanie i doskonalenie SZBI przez ..." [8].

Przedstawione w tym rozdziale wymagania nie różnią się znacznie od wymagań w odniesieniu do kierownictwa w systemie zarządzania jakością (SZJ) i określają działania niezbędne do zbudowania i funkcjonowania SZBI. Istnieje jednak jedna zasadnicza różnica wynikająca ze sformułowania: „f) podejmowanie decyzji o kryteriach akceptacji ryzyka i akceptowalnym poziomie ryzyka" [8].

Sformułowanie to określa, że kierownictwo odpowiada za podejście do bezpieczeństwa informacji oparte na zarządzaniu ryzykiem, musi być świadome istniejących rodzajów ryzyka i podejmować decyzje, jaki poziom ryzyka może zaakceptować. Równocześnie jednak wskazuje, że SZBI, podobnie zresztą jak system zarządzania bezpieczeństwem i higieną pracy (SZBHP), jest oparty nie tylko na podejściu procesowym, ale przede wszystkim na działaniach związanych z ryzykiem biznesowym.

Wymagania dotyczące kierownictwa i ogólnie przywództwa są określone także w załączniku A: „A.6.1.1. Kierownictwo powinno aktywnie wspierać bezpieczeństwo informacji całej organizacji poprzez wskazanie wyraźnego kierunku działania, demonstrowanie zaangażowania, jednoznaczne przypisanie i przyjmowanie odpowiedzialności w zakresie bezpieczeństwa informacji" [8].

W normie ISO/IEC 17799:2005 [7], stanowiącej wytyczne do wdrożenia SZBI, zaleca się, aby za bezpieczeństwo informacji odpowiadał zarząd lub specjalnie powołane do tego celu ciało zarządzające, takie jak forum bezpieczeństwa informacji. Oznacza to, że najlepiej, żeby działania były koordynowane przez grupę ludzi, a nie nadzorowane przez jednego człowieka, jak to jest w zarządzaniu jakością. Wyraźne wskazanie potrzeby kolektywnego nadzoru nad bezpieczeństwem informacji jest ujęte w wymaganiach pkt A.6.1.2: „A.6.1.2. Działania w zakresie bezpieczeństwa informacji powinny być koordynowane przez reprezentantów różnych części organizacji z odpowiednimi rolami i funkcjami" [8].

Podkreślone jest to także w normie ISO/IEC 17799:2005 [7], zalecającej, kto powinien koordynować działania: „Zazwyczaj koordynacja bezpieczeństwa informacji wymaga współdziałania kierownictwa, użytkowników, administratorów, projektantów aplikacji, audytorów i pracowników działu bezpieczeństwa oraz specjalistycznych umiejętności z takich dziedzin, jak ubezpieczenia, prawo, zarządzanie zasobami ludzkimi, informatyką lub ryzykiem" [7].

W kolejnym punkcie wymaga się uświadamiania pracowników i przeprowadzenia odpowiednich szkoleń, co stawia kolejne wymagania względem kierownictwa. Przedstawione w rozdziale 4 artykułu wymagania i zalecenia wskazują, jak ważna jest rola kierownictwa i jego działania dla bezpieczeństwa informacji. Wskazują też pewne różnice podejścia w odniesieniu do systemów zarządzania jakością, które zostaną szerzej omówione w rozdziale 5.

5. Różnice między zarządzaniem jakością a zarządzaniem bezpieczeństwem informacji

Podstawową różnicą pomiędzy SZJ a SZBI jest inne rozumienie komunikacji międzyludzkiej: w SZJ – co nie jest zakazane, jest dozwolone, w SZBI – co nie jest dozwolone, jest zakazane. Ma to swoje istotne konsekwencje w pracochłonności opracowania SZBI i odpowiedzialności oraz zadaniach kierownictwa, wymaga bowiem starannego przygotowania struktur zarządzania, odpowiedzialności i dokumentacji.

W SZBI, w przeciwieństwie do SZJ, za jedno z podstawowych zagrożeń uważa się działania ludzkie, w tym działania pracowników i współpracowników organizacji, w związku z tym system wymaga odpowiednich zabezpieczeń, polegających na wzajemnej kontroli pracowników i członków zarządu. Wyjaśnia to, dlaczego w SZBI nie jest zalecany jeden przedstawiciel kierownictwa, ale ciała kolegialne.

Kolejną fundamentalną różnicą jest sprawa analizy ryzyka i zarządzania ryzykiem, co nie występuje w SZJ (projektowanym zgodnie z ISO 9001:2000), aczkolwiek występuje także w SZBHP. W przeciwieństwie do SZJ, w których najważniejsi są klienci, w SZBI najważniejsze są bezpieczeństwo i ciągłość funkcjonowania firmy oraz właściwa współpraca z zainteresowanymi stronami. Klienci oczywiście też są zainteresowaną stroną, ale równocześnie mogą stanowić zagrożenie dla bezpieczeństwa informacji.

Następną kwestią, za którą odpowiedzialność ponosi kierownictwo, jest zarządzanie incydentami i zarządzanie ciągłością działania. Znane z SZJ postępowanie z wyrobem niezgodnym to tylko szczególny przypadek zarządzania incydentami.

Zakres SZBI obejmuje całą firmę ze szczególnym uwzględnieniem działów informatycznych, ekonomicznych, ochrony fizycznej, spraw kadrowych, działów umów oraz zarządu. Wymagania dotyczące dokumentacji są również szersze niż w SZJ i uwzględniają wiele różnorodnych dokumentów: metodykę postępowania z ryzykiem, raport z szacowania ryzyka, plan postępowania z ryzykiem oraz deklarację stosowania. Norma wymaga tzw. polityki szczegółowej (9), procedur (20), procesów (6), planów (4), zasad (1), metod (2), schematów (1). Nie ma natomiast potrzeby wykonywania księgi jakości, gdyż jej odpowiednikiem jest deklaracja stosowania. Wszystko to stwarza dodatkowe obowiązki dla kierownictwa w obszarze przeglądu SZBI i zarządzania audytem.

6. Podsumowanie

Można obecnie stwierdzić, że nie ma doskonałego zarządzania bez bezpieczeństwa informacji i powinno być to uwzględnione przy ocenie kierownictwa w tym zakresie. Samo kierownictwo może także spowodować zagrożenia dla bezpieczeństwa informacji zarówno poprzez działania celowe, jak i niefrasobliwość, np. utratę notebooka z ważnymi informacjami.

Zarządzanie bezpieczeństwem informacji stanowi nowe wyzwanie dla kierownictwa firm. Minęły bezpowrotnie czasy, gdy sprawami bezpieczeństwa w firmie zajmował się jeden pracownik, który był za to odpowiedzialny. W przypadku zarządzania bezpieczeństwem normy wyraźnie podają, że o ile można delegować zagadnienia związane z bezpieczeństwem, o tyle nie można delegować odpowiedzialności za bezpieczeństwo. Oznacza to, że kierownictwo firmy jest odpowiedzialne za bezpieczeństwo informacji i pojawiające się ryzyko. Zmniejszenie ryzyka może zapewnić m.in. wdrożenie systemu zarządzania bezpieczeństwem informacji oraz stosowanie odpowiednich zabezpieczeń.

Obecnie bez właściwego podejścia do bezpieczeństwa informacji nie ma już mowy o prawdziwym dążeniu do doskonałości.

Przykładem problemów kierownictwa w zakresie bezpieczeństwa informacji jest przypadek zarządu firmy HP. Stwierdzono przecieki z posiedzeń zarządu firmy. W celu wykrycia ich źródła zaangażowano firmę detektywistyczną, a rok później kolejną. Druga firma, stosując metody niezgodne z prawem (w tym przechwytując wykazy rozmów telefonicznych i próbując zainstalować „konia trojańskiego" w komputerze dziennikarki), wykryła sprawcę. Wybuchł jednak skandal związany z nielegalnymi działaniami; w wyniku którego trzech członków zarządu HP (ale nie osoba, która była odpowiedzialna za przeciek) podało się do dymisji, rozpoczęły się przesłuchania w senacie USA i śledztwo prokuratorskie [9].

Literatura

[1] BS 7799-1:1999 Code of Practice for Information Security Management.
[2] BS 7799-2:2002 Information Security Management System (ISMS) Requirements.
[3] Humpreys T. *ISMS Standards The ISO 27000 Family and BS7799-2/ISO/IEC 27001*, konferencja „Wyzwania dla bezpieczeństwa informacji", Warszawa 2006.
[4] ISO/IEC 13335-1:2004 Information Technology – Guidelines for the Management of IT Security – Part 1 Concepts and Models for Information Security Management.
[5] ISO/IEC 13335-3 Information Technology – Guidelines for the Management of IT Security – Part 3 Techniques for the Management of IT Security.
[6] ISO/IEC 17799: 2000 Code of Practice for Information Security Management.
[7] ISO/IEC 17799: 2005 Code of Practice for Information Security Management, 2nd edition 2005.

[8] ISO/IEC 27001:2005 Information Security Management System (ISMS) Requirements.
[9] www.gazeta.pl, 28.09.2006.
[10] www.xisec.com, 20.08.2006.

INFORMATION SECURITY MANAGEMENT – A NEW CHALLENGE FOR COMPANY EXECUTIVES IN ASPIRATIONS FOR PERFECTION

Summary

Contemporary dependence on computers, Internet and teleinformatic networks has caused that any disruption of integrity, availability or confidentiality of information can bring on serious consequences to the company. Since 2005 ISO 27000 standards on information security management have essentially supplemented and even changed the principles of aspirations for perfection binding in the 1980s.

Executives should support all activities connected with preparation and implementation of information security management, provide adequate management structures assuring effective control, technical means and increase staff awareness. They should undertake their activities basing on a risk analysis and prepare their company in case of failure of operation continuity. Executives can pose a serious danger to the security of information through their unaware or deliberate actions.

As long as the activities connected with security of information can be delegated, the responsibility for security cannot. Currently, without executives' proper approach to security of information, the aspiration for perfection is out of the question.