A C T A U N I V E R S I T A T I S N I C O L A I C O P E R N I C I
DOI: http://dx.doi.org/10.12775/AUNC_ZARZ.2018.026 ZARZĄDZANIE XLV–NR 2 (2018)

Pierwsza wersja złożona 4.04.2018
Ostatnia wersja zaakceptowana 12.06.2018

ISSN (print) 1689-8966
ISSN (online) 2450-7040

Piotr Wiśniewski *

SYSTEMY ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W PRZEDSIĘBIORSTWIE

Z a r y s t r e ś c i: Celem publikacji jest wskazanie rosnącego znaczenia systemów zarządzania bezpieczeństwem informacji (ang. Information Security Management Systems, ISMS) w kontekście rozwijającego się i szybko ewoluującego czarnego rynku. Stosowanie istniejących rozwiązań w postaci standardów takich jak ISO 27000 jest niewystarczające bez szerszego zrozumienia sposobu funkcjonowania przestępców. Ponadto rozwój cyberprzestępczości doprowadził do ryzyka strat w kapitale relacyjnym i społecznym, które nabierają coraz większego znaczenia dla konkurencyjności organizacji w gospodarce opartej na wiedzy.

S ł o w a k l u c z o w e: ISMS, bezpieczeństwo, cybercrime, kapitał intelektualny,

K l a s y f i k a c j a J E L: D83;

WSTĘP

Cyberprzestępczość jest rosnącym zjawiskiem i przykładem czarnego rynku we współczesnej gospodarce. Jej wpływ na poszczególne przedsiębiorstwa jest niezaprzeczalny, jednakże nadal niezbyt dobrze zbadany. W literaturze istnieje znaczny dorobek teoretyczny dotyczący zarówno gospodarki opartej na wiedzy jak i zasobów niematerialnych przedsiębiorstw. Z tych powodów kwestia bezpieczeństwa informacji staje się coraz istotniejsza. Seria standardów ISO 27000 jest przykładem zauważenia zarówno przez naukę, jak i świat biznesu istotności wspomnianych procesów i zagrożeń. Dokumenty te posiadają liczne zalety, jednakże same w sobie są niewystarczające by stworzyć najlepszy system zarządzania bezpieczeństwem informacji w przedsiębiorstwie.

* Adres do korespondencji: Piotr Wiśniewski, Uniwersytet Mikołaja Kopernika w Toruniu, Wydział Nauk Ekonomicznych i Zarządzania, Katedra Ekonomii, ul. Gagarina 13a, 87-100 Toruń, e-mail: psw@doktorant.umk.pl

Aby osiągnąć ten cel konieczne jest zrozumienie szerszego kontekstu cyberprzestępczości i współczesnego czarnego rynku. Dopiero mówiąc o standardach ISO 27000 w wyżej wspomnianym kontekście, a także w kwestii kapitału społecznego i relacyjnego można osiągnąć optymalne rezultaty. Z tego powodu artykuł ten będzie zajmował się kwestią bezpieczeństwa informacji przedsiębiorstwa w kontekście uwarunkowań rynkowych.

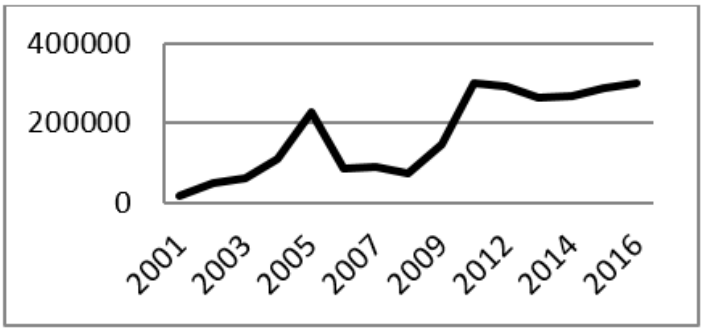
1. WPŁYW CYBERPRZESTĘPCZOŚCI NA FUNKCJONOWANIE PRZEDSIĘBIORSTWA

Rozwój techniczny doprowadził do powstania nowych szans i zagrożeń dla przedsiębiorstw. Rosnącego znaczenia nabiera „kapitał intelektualny", który jest określany jako zasoby niematerialne przedsiębiorstwa [Mroziewski, 2008, s. 28]. Efektem tego jest pojawiające się w literaturze określenie „gospodarka oparta na wiedzy", która ma być rezultatem pełnego rozpoznania roli wiedzy i technologii we wzroście gospodarczym. Wiedza jest ucieleśniona w istotach ludzkich (kapitał ludzki) i w technice, która zawsze była istotna dla wzrostu gospodarczego [The Knowledge-Based Economy, 1995, s. 9]. Oba te aspekty odzwierciedlone są w rynku cyberprzestępczym i zagrożeniach z jakimi zmaga się przedsiębiorstwo. Równolegle na gruncie socjologii rozwija się koncepcja komputerologii społecznej (social computing) [Vannoy, Palvia, 2010, s.149-150]. Według niej technologie komputerowe nie mają tylko wymiaru produktowego, lecz także wymiar społeczny. Cyberprzestrzeń jest zatem wynikiem istnienia odpowiedniej technologii i warunków społecznych [Jordan, 2011, s. 12-13]. Te aspekty rozpoznane we współczesnej gospodarce mają również wpływ na kształtowanie się przestępczości, która przybiera nowe formy, adaptując się do nowych warunków. Przykładem adaptacyjnych zachowań rynku przestępczego jest rozwój cardingu (kradzież danych z kart kredytowych), który nastąpił wraz z ich wprowadzaniem [Glenn, 2011, s. 48]. Zdolność dostosowywania się rynku przestępczego do nowych warunków doprowadziła do pojawienia się nowej wersji czarnego rynku - cyberprzestępczości. Według Jerzego Kosińskiego zjawisko to może być rozumiane w wąskim i szerokim znaczeniu. W tym pierwszym obejmuje ona każde nielegalne zachowania realizowane za pomocą działań elektronicznych nakierowanych na bezpieczeństwo systemów komputerowych i danych w nich przetwarzanych. W szerokim znaczeniu natomiast cyberprzestępczość rozumiana jest jako wszelkie nielegalne zachowania popełnione za pomocą lub względem systemu komputerowego czy sieci, w tym takie przestępstwa jak nielegalnie posiadanie, oferowanie lub rozpowszechnianie informacji za pomocą systemu komputerowego lub sieci [Kosiński, 2015, s. 13]. Dzięki tej definicji można wywnioskować, że zabezpieczenie informacji w przedsiębiorstwie przy pomocy rozwiązań technicznych jest niewystarczające. Rozwiązuje ono

problem cyberprzestępczości w wąskim rozumieniu. W przypadku innych działań przestępczych np. socjotechniki tego typu rozwiązania są niewystarczające. 66% przedstawicieli firm uważa, że to ich współpracownicy, a nie hakerzy, stanowią największe zagrożenie dla zachowania poufności danych klientów. Jedynie 10% osób wskazało hakerów jako źródło największego zagrożenia. 46% badanych zadeklarowało, że usunięcie informacji wrażliwych z firmowych baz danych byłoby dla pracowników „łatwe" lub „bardzo łatwe". 32% ankietowanych przyznało, że nie zna wewnętrznej polityki swojej firmy w zakresie ochronnych danych o klientach [Hadnagy, 2012, s. 21]. Te statystyki wskazują dlaczego konieczne jest zajmowanie się kwestiami bezpieczeństwa informacji również w zakresie zarządzania. Zarówno w przypadku zagrożeń wewnętrznych jak i zewnętrznych o charakterze nietechnicznym technologia stanowi drugorzędny problem w porównaniu do nieodpowiednich procedur.

Mając na uwadze wszystkie wymienione wcześniej aspekty rynku przestępczego należy zadać pytanie jak problem ten odnosi się do realnej gospodarki. Internet Crime Report, opracowywany przez FBI dla USA, to najdłużej publikowany raport o wiarygodnych danych statystycznych. Dane z roku 2010 były nieporównywalne z pozostałymi raportami i z tego powodu rok ten został pominięty w opracowaniu.

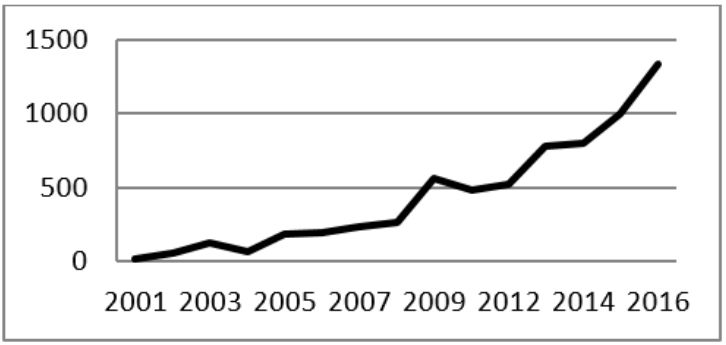
Wykres 1. Liczba zgłoszeń przestępstw internetowych w USA w latach 2001-2016



Źródło: Opracowanie własne na postawie IFCC 2001 Internet Fraud Report 2001-2016

Wykres 1 wskazuje wzrost ilości zgłoszeń przestępstw internetowych między latami 2001-2005 i 2008-2011. Po roku 2011 nastąpiła stabilizacja liczby zgłoszeń. Jednocześnie na wykresie 2 dostrzec można trend rosnący łącznej straty z tytułu przestępczości.

Wykres 2. Łączna strata z tytułu cyberprzestępczości (w milionach USD) w USA w latach 2001-2016



Źródło: Opracowanie własne na postawie IFCC 2001 Internet Fraud Report 2001-2016

2. ROLA KAPITAŁU INTELEKTUALNEGO W PRZEDSIĘBIORSTWIE

Zmiany w funkcjonowaniu czarnego rynku nie są jedynymi na które musi zwrócić uwagę przedsiębiorstwo pod względem ochrony informacji i danych. Jednym z istotnych elementów są efekty traktowania wiedzy jako ważnego zasobu, z których wynikają następujące procesy:

- przekształcenie się struktur społecznych i organizacyjnych sieci,
- tworzenie się: nowych sił politycznych i ekonomicznych, nowych relacji i więzi, nowego klimatu działania, nowej kultury, nowej polityki, nowej filozofii zarządzania przedsiębiorstwami,
- zmiany w kierunkach badań nauk społecznych, w tym nauk o zarządzaniu; głównym problemem stają się zasoby informacyjne i intelektualne,
- zmiany ładu organizacyjnego w systemach gospodarczych w kierunku decentralizacji,
- zmiany norm moralnych, w tym zmiany w podziale dochodów i przywilejów na rzecz redukowania stopni asymetrii organizacyjnej,
- zmiany mentalności członków społeczności doceniających wiedzę, która przynosi realną poprawę jakości życia [Mroziewski, 2008, s. 22].

Następuje zmiana całego szeregu uwarunkowań, w których działa przedsiębiorstwo. O kwestii przekształcenia się struktur społecznych i sieci była mowa w ramach „social computing". Zmianie ulega także powiązanie przedsiębiorstwa z otoczeniem, zarówno z innymi organizacjami jak i klientami. Obecnie większość przedsiębiorstw posiada dość znaczące bazy danych związane ze swoimi klientami oraz innymi formami np. dostawcami. Wyciek tych danych, mimo że może nie zaszkodzić bezpośrednio przedsiębiorstwu, będzie zagrożeniem dla

powiązanych podmiotów. To spowoduje straty w kapitale relacyjnym, który jest częścią kapitału intelektualnego przedsiębiorstwa. Kapitał relacyjny to kategoria ekonomiczna, która zdefiniowana jest przez uzyskiwanie korzyści z sieci powiązań z wewnętrznymi i zewnętrznymi interesariuszami przedsiębiorstwa. Powiązanie, które istnieje między organizacją i bytami w jej środowisku, współzależność i interakcja między powiązanymi podmiotami są esencją kapitału relacyjnego. Utrata wartościowych informacji na temat członków tej sieci może ograniczyć ich zaufanie i chęć utrzymywania relacji. Przedsiębiorstwo w ich oczach może wydać się niegodne zaufania. To spowoduje znaczącą stratę w kapitale intelektualnym którym dysponuje przedsiębiorstwo, a który to - jak wcześniej wspominano - nabiera coraz większego znaczenia. Relacje te są budowane w procesie ciągłego, stopniowego rozwoju w długim okresie czasu opierając się na wzajemnym zaufaniu i zaangażowaniu [Lenart-Gansiniec, 2015, s. 62]. Z tego powodu odbudowanie tych relacji będzie czasochłonne i kosztowne, a bardzo często niemożliwe.

Istotna zmiana następuje również w kwestii kapitału społecznego. Kapitał ten to wielowymiarowy koncept, który może być powiązany zarówno z normami społecznymi, dzielonymi wartościami jak i interpersonalnymi relacjami [Castelfranchi et. al, 2014, s. 181]. Obejmuje on zarówno relacje formalne jak i nieformalne między samodzielnymi podmiotami [Walkiewicz, 2012, s. 26]. Z punktu widzenia podejmowanego tematu kapitał społeczny ma kilka istotnych efektów. Przede wszystkim istnieje oczekiwanie pewnej poufności między uczestnikami relacji rynkowych. Można mówić zatem o presji utrzymania poufności informacji wynikającej z istnienia kapitału społecznego. Ma ona swoje odzwierciedlenie w prawie, które jest jej formalnym wyrazem, jak również w konsekwencjach na gruncie nieformalnym, gdzie przedsiębiorstwo można określić jako niegodne zaufania. Kapitał społeczny ma również znaczenie dla sposobu działania wewnątrz organizacji i będzie pełnił pewną rolę w przypadku modelu akceptacji technologii. Ostatnia rola tego rodzaju kapitału związana jest z mediami społecznościowymi (social media). Dowody empiryczne wskazują, że social media zmieniają strukturę i naturę społecznych relacji, a tym samym zmieniają kapitał społeczny. Badania dowiodły, że social media pozwalają na szukanie szerszego wsparcia społecznego i powiązań. Istnieje powiązanie między zachowaniami offline, które mają wpływ na kapitał społeczny [Zuniga et. al. 2017, s. 46]. To w połączeniu ze wzrostem obecności przedsiębiorstw online sprawia, że konieczna jest ochrona także tych zasobów. Wraz z rozwojem gospodarczym i postępującą globalizacją należy spodziewać się również, że rola i wartość tych zasobów także będzie rosła. To oznacza, że potencjalne straty w tym aspekcie funkcjonowania przedsiębiorstwa będą coraz bardziej dotkliwe.

3. SYSTEMY BEZPIECZEŃSTWA INFORMACJI W PRZEDSIĘBIORSTWIE

Mając na uwadze powyższe uwarunkowania, w których zarówno IT jak i zarządzanie są istotnymi tematami dla praktyków jak i badaczy, nie dziwi fakt, że następuje rozwój w zakresie ISMS. Pomimo to szczegółowy opis interakcji między procesami związanymi z zarządzaniem bezpieczeństwem informacji w przedsiębiorstwie, a innymi procesami zarządczymi nie istnieje [Brandis et. al. 2016, s. 28]. Jedną z metod odpowiedzi na to zapotrzebowanie jest seria standardów ISO 27000. Celem tych standardów jest między innymi zapewnienie bezpieczeństwa kluczowym zasobom, zarządzanie ryzykiem, stosowanie najlepszych praktyk, uniknięcie szkód dla marki, straty zysków i potencjalnych kar i rozwój systemów informacyjnych. Ponadto standardy ISO są kompatybilne względem siebie i możliwe do użycia w tym samym czasie. Nie należy tego jednak mylić z ich zintegrowaniem. Kluczowym wśród tych standardów jest ISO 270001, który zawiera wymagania dla planowania, implementowania, działania i ulepszania ISMS. Wymagania są sformułowanie w ogólny sposób, by pasowały do wszystkich organizacji niezależnie od ich rozmiaru, celów, modelu biznesowego, lokalizacji itd. W standardzie nie znajdują się wymogi dotyczące konkretnej technologii, ale są wymagania odnoście procesów ISMS. Oprócz ISO 27001 istnieje cały szereg procesów w tej serii. Są to:

- ISO 27000 – ISMS – Overview and vocabulary;
- ISO 27003 – ISMS implementation guidance;
- ISO 27004 – Information security management – Measurement;
- ISO 27005 – Information security risk management;
- ISO 27006 – Requirements for bodies providing audit and certification of ISMS;
- ISO 27007 – Guidelines for ISMS auditing;
- ISO 27008 – Guidance for auditors on ISMS controls;
- ISO 27010 and following – sector specific standards;
- ISO 27030 and following – standards for technical controls and guidelines for controls of ISO 27002 [Brandis et. al. 2016, s. 29].

Mówiąc o ISMS i ISO 27000 warto zwrócić uwagę na kwestię integracji aspektu technicznego i ludzkiego w implementacji jakichkolwiek systemów mających wesprzeć bezpieczeństwo informacji. Użyteczny przy planowaniu i zarządzaniu systemem bezpieczeństwa informacji jest model akceptacji technologii. Został on zaproponowany w 1989 roku przez Davisa w celu wyjaśnienia i przewidzenia zachowań użytkowników podczas wykorzystania technicznych innowacji, a bardziej precyzyjnie - akceptacji technologii informacyjnych [Deneen et. al., s. 603]. Model ten jest bardzo istotny, gdyż stworzenie nawet najbardziej zaawansowanego i skutecznego systemu pod względem technicznym

nie gwarantuje pełnego bezpieczeństwa bez uwzględnienia ludzi, którzy będą tego systemu używać. Podobnie planując procedury w organizacji należy wziąć pod uwagę wykorzystane technologię i sposób w jaki ludzie z nich naturalnie korzystają. Oba te elementy mają swoje odzwierciedlenie w TAM (Technology Adaptation Model) w postaci postrzeganej przydatności (Perceived Usefulness) i postrzeganej łatwości użycia (Perceived Ease of Use) [Dornodulu, 2016, s. 1].

Projektując procedury i procesy, ale także wdrażając rozmaite technologie dotyczące bezpieczeństwa informacji, należy wziąć pod uwagę powyższy model. Niezależnie od ilości szkoleń i doskonałości procedur realne bezpieczeństwo informacji będzie zależne od realizowania wskazanych zadań i metod postępowania. Z racji tego, że ISO 27000 nie ma scharakteryzowanych konkretnych technologii TAM może służyć jako metoda ich wyboru i wdrażania w celu uzyskania najlepszych rezultatów. Ma to znaczenie również z powodu istotności czynnika ludzkiego w zapewnieniu bezpieczeństwa informacji. Według raportu „Efektywne zarządzanie bezpieczeństwem informacji" oprócz braku regulacji i narzędzi największym zagrożeniem dla ochrony danych jest właśnie czynnik ludzki. Szczególnie zagrożenie wiąże się z menedżerami średniego szczebla, gdyż mają oni szerszy dostęp do ważnych informacji. Człowiek działający nieświadomie bądź przez łamanie zasad związanych z bezpieczeństwem informacji może spowodować całkowitą kompromitację systemu bezpieczeństwa - np. karteczka z zapisanym hasłem pozostawiona na biurku, bądź przylepiona do monitora [Efektywne zarządzanie bezpieczeństwem informacji, 2013, s. 11]. Według publikacji Hadnagy'ego, do najbardziej kosztownych rodzajów ataków należą ataki internetowe oraz ataki wywołane przez złośliwy kod lub złośliwe działania pracowników. Łącznie przekładają się one na ponad 90% kosztów spowodowanych działaniami cyberprzestępców w przeliczaniu na jedną organizację w jednym roku [Hadnagy, 2012, s. 29]. Oczywiście stosowanie metod powiązanych i uwzględniających TAM nie daje gwarancji pełnego bezpieczeństwa, gdyż coś takiego nie istnieje, jednakże zmniejsza zawodność czynnika ludzkiego.

Ostatnim faktem na który warto zwrócić uwagę jest pytanie czy każdej organizacji opłaca się wprowadzać skomplikowaną procedurę ochrony danych i w jakim stopniu należałoby ją wprowadzić. Pomocny ku temu może być wskaźnik ROSI (Return of Security Investments).

ALE (Annual Loss Expectancy)- oczekiwana roczna strata. ALE liczone jest za pomocą wzoru:

RS - to procentowy wskaźnik efektywności określonego rozwiązania z zakresu bezpieczeństwa [Brangetto, Kert-Saint, 2015, s. 12-14].

Oczywiście ROSI jest bardzo prymitywnym wskaźnikiem pomijającym wiele wcześniej omawianych aspektów, między innymi kwestie kapitału relacyjnego. Ponadto stosunkowo trudne może być określenie efektywności

poszczególnych rozwiązań z racji błyskawicznie zmieniającego się rynku i metod działania przestępców.

PODSUMOWANIE

Niniejszy artykuł zwraca uwagę na kilka istotnych aspektów związanych z ochroną informacji w przedsiębiorstwie. Przede wszystkim tak zwana „gospodarka oparta na wiedzy" wpływa nie tylko na szanse przedsiębiorstwa, ale także zagrożenia z jakimi musi się zmagać. Wynika to z ewolucji czarnego rynku i sposobu działania przestępców. Ci ostatni zagrażają najcenniejszym zasobom jakimi dysponuje we współczesnej gospodarce organizacja tj. kapitałowi intelektualnemu, z szczególnym naciskiem na kapitał społeczny i relacyjny przedsiębiorstwa. Wskazana została rola standardów ISMS, takich jak ISO 27001 i ich braków. Konieczne jest zdanie sobie sprawy, że normy tego typu są dość ogólne pod względem wykorzystanych technologii, jak również zawierają wskazówki, a nie ścisłe procedury. Menedżerowie, którzy próbują je wprowadzić, często nie znają szerszego kontekstu czarnego rynku przez co nie są w stanie ich skutecznie wdrożyć, a następnie rozwijać. Z tego powodu konieczne jest wykorzystanie teorii takich jak TAM, który pozwoli obniżyć zawodność czynnika ludzkiego w organizacji. Ten z kolei został wskazany jako najsłabsze ogniwo ISMS. Prócz tego warto zwrócić uwagę na metody kalkulowania ponoszonych na bezpieczeństwo wydatków i zdać sobie sprawę z ich niedoskonałości. Należy stwierdzić, że rola zarządzania bezpieczeństwem informacji będzie rosła wraz z rozwojem czarnego rynku i rozwojem gospodarki opartej na wiedzy. Przyszłe badania powinny skupić się na integracji ISMS z innymi systemami zarządzania przedsiębiorstwem i procesami. Obecnie badanie bezpieczeństwa danych i informacji w przedsiębiorstwie jest nieco oderwane od innych części zarządzania. Bezpieczeństwo informacji powinno być przede wszystkim przeanalizowane w powiązaniu społecznej odpowiedzialności biznesu i kapitału relacyjnego nie tylko w sferze B2B, ale również kontaktów z klientami.

LITERATURA

Brandis K. et. al. (2016), *A process framework for information security management* "International Jurnal of Information Systems and Project Management", Vol 4, No 4.

Brangetto, P., Kert-Saint M. (2015), *Economic aspects of national cyber security strategies Project Report*, Tallinn.

Castelfranchi C., Falcone R., Marzo F. (2006), *Trust and relational capital* "Computational and Mathematical Organization Theory", Vol 17, Issue 2.

Deneen C. C., Ng E. M., Shroff R. H. (2011), *Analysis of the technology acceptance model in examining students' behavioural intention to use an eportfolio system* "Australasian Jurnal of Educational Technology", No 27(4).

Durodolu, O. (2016), *Technology Acceptance Model as a predictor of using information system' to acquire information literacy skills* "Library Philosophy and Practice", November.

Glenny M. (2011), *Mroczny Rynek. Hakerzy i nowa mafia*. Wydawnictwo W.A.B, Warszawa.
Hadnagy, C. (2012), *Socjotechnika. Sztuka zdobywania władzy nad umysłami,* Wydawnictwo Helion.
IFCC 2001 Internet Fraud Report 2001-2016.
Jordan T. (2011), *Hakerstwo*, Wydawnictwo Naukowe PWN, Warszawa.
Kosiński J. (2015), *Paradygmat cyberprzestępczości*, Wydawnictwo Difin, Warszawa.
Lenart-Gansiniec R. (2015), *Relational Capital for Managing the Uncertainty of the Environment,* "Jurnal of Science of the Military Academy of Land Forces, Volume 47 Number 1 (175).
Mroziewski M. (2008), *Kapitał intelektualny współczesnego przedsiębiorstwa. Koncepcje, metody wartościowania i warunki jego rozwoju*, Wydawnictwo Difin, Warszawa.
Raport Efektywne zarządzanie bezpieczeństwem informacji, 2013.
Vannoy S., Palvia P. (2010), *The social influence model of technology adoption* "Communications of the ACM", Volume 53 Issue 6, June.
Walukiewicz S. (2012), *Kapitał społeczny*, Instytut Badań Systemowych Polskiej Akademii Nauk, Warszawa.
Zuniga H., Barnidge M., Scherman A. (2017), *Social Media Social Capital, Offline Social Capital and Citizenship: Exploring asymmetrical Social Capital Effects* [w:] "Political Communication", No 34.
The Knowledge-Based Economy, Paryż, 1995.

INFORMATION SECURITY MANAGEMENT SYSTEMS IN ENTERPRISE

Abstract: The main goal of this publication is to point out rising importance of Information Security Management Systems (ISMS) in context of developing black market. Using existing solutions like ISO 27000 standard is insufficient without understanding of criminal modus operandi. Development of cybercrime leads to risk of losing relational and social capitals. Both of them grain more and more meaning for competitiveness of organisations in knowledge-based economy.

Keywords: ISM, security, cybercrime, intellectual capital,