Dariusz Kralewski*

Celowa kreacja kultury bezpieczeństwa

Wstęp

W ciągu ostatnich 12 miesięcy aż 39% organizacji w Polsce padło ofiarą przestępstw gospodarczych - wynika z raportu firmy doradczej PwC (wcześniej PricewaterhouseCoopers) „Global Economic Crime Survey 2011". Najczęstszym przestępstwem była kradzież aktywów wskazywana przez 61% respondentów. Na drugim miejscu znalazła się cyberprzestępczość (26% wskazań), a na kolejnych pozycjach korupcja i przekupstwo (również 26%). Zaraz za nimi uplasowały się naruszenia prawa własności intelektualnej (23%) oraz manipulacje księgowe (kolejne 23%) [PwC, listopad 2011].

Jak wnioskować można z w powyższych badań, niezmiernie ważnym aspektem funkcjonowania współczesnych przedsiębiorstw jest bezpieczeństwo systemów informatycznych. W badaniach naukowych, literaturze, tematyce kursów poświęconych bezpieczeństwu jest ono traktowane bardzo technicznie i zwykle oderwane jest od organizacji, w której jest implementowane.

Celem artykułu jest zobrazowanie tezy autora, iż jednym z podstawowych składników świadomego, pełnego bezpieczeństwa systemów informatycznych powinna być celowo kreowana kultura bezpieczeństwa informacji. Kultura ta wspiera ochronę informacji jednocześnie wspomagając szersze cele przedsiębiorstwa. Należy tutaj podkreślić zwrot „celowo kreowana". Każda organizacja posiada kulturę bezpieczeństwa, która w różnym stopniu wspiera lub nie bezpieczeństwo informacji. Należy jednak podjąć aktywne działania w celu poprawy istniejącej kultury. W wielu firmach brak jest świadomości bezpieczeństwa informacyjnego. Niektóre firmy mają bardzo mocno ustrukturyzowane procesy bezpieczeństwa, które wyznaczają bieżące czynności pracowników. W firmach tych bezpieczeństwo najczęściej wpisane jest w misję firmy [Deloitte & Touche, 2010]. Analiza tego, czy kultura powstała

* Dr, adiunkt, Katedra Informatyki Ekonomicznej, Wydział Zarządzania, Uniwersytet Gdański, darek@univ.gda.pl, Centrum Dydaktyczno-Konferencyjne UG, ul. Piaskowa 9, 81-864 Sopot

w sposób celowy czy jest efektem „przypadku" jest kluczowym wyznacznikiem podtrzymania kultury w dłuższej perspektywie.

1. Przesłanki implementacji kultury bezpieczeństwa

W rozmowach z polskimi przedsiębiorcami i osobami odpowiedzialnymi na dział informatyczny bardzo często spotykano się z następującymi stwierdzeniami:

1. Nie zarządzamy bezpieczeństwem informacji.
2. Dział bezpieczeństwa informacji otrzymuje coraz więcej narzędzi, jako właściciel nie sądzę jednak aby nasza firma była coraz bardziej bezpieczna.
3. Polityka bezpieczeństwa to jedno, rzeczywistość to drugie.
4. Oczywiście wspieramy bezpieczeństwo, jednak w zakresie całego przedsiębiorstwa. Mój dział musi zarabiać.
5. Jestem tak przytłoczony wszystkimi tymi hasłami które muszę zapamiętać, że po prostu zapisuję je na kartce, którą pozostawiam obok komputera.
6. Wiem, że nie powinienem mieć dostępu do tych informacji. Uzyskałem dostęp do nich wcześniej na poprzednim stanowisku i zachowałem je na wszelki wypadek.
7. Zarząd zatwierdził zakup narzędzi do zabezpieczenia informacji, ale nie wydzielił żadnego budżetu dla osób niezbędnych do monitoringu.
8. Wszystkie osoby odpowiedzialne na bezpieczeństwo mówią zawsze „nie wolno". Osoby te powinny poznać zasady działania biznesu.

Powyższe opinie i wiele im podobnych usłyszeć można z pewnością w firmach na całym świecie. Dość często w czasie rozmów, co na początku wydawać się może dziwne, padające komentarze dotyczące bezpieczeństwa są wzajemnie sprzeczne. Przykładem może być choćby powyższa opinia właściciela firmy, który mimo zakupu nowoczesnych narzędzi zabezpieczających nie czuje aby informacje były bezpieczniejsze. Dłuższy wywiad z tym właścicielem firmy jak i analiza funkcjonowania organizacji potwierdziła przeczucia właściciela dając na to odpowiednie dowody. Patrząc na funkcjonowanie firmy nie zauważono znaczących zmian. Pracownicy nieskutecznie wsparli technologie informatyczne.

Brakującym elementem jest kultura bezpieczeństwa, określana jako wzorce, zachowania, przekonania, założenia, postawy i sposoby działa-

nia. Pojawiają się one w firmie lub są wyuczone i stwarzają poczucie komfortu [Eisenhauer, 2009]. Kultura rozwija się jako rodzaj wspólnej historii, jako szereg wspólnych doświadczeń jakie przechodzi firma. Te podobne doświadczenia skutkują pewnymi odpowiedziami, które stają się zestawem oczekiwanych wspólnych zachowań. Zachowania te stają się niepisanymi zasadami, te z kolei stają się wspólnymi dla ludzi o wspólnej historii normami. Ważne jest aby zrozumieć kulturę przedsiębiorstwa, ponieważ wpływa ona głęboko na to jakie informacje są uznawane, jak są interpretowane i co można z nią robić.

Tablica1. Elementy kultury bezpieczeństwa

Wzorce	Nie tylko przejściowe ale i ciągłe
Zachowania	Sposób w jaki ludzie się zachowują a nie to co twierdzą, że zamierzają zrobić
Przekonania	Podstawowe zasady, które ludzie przenoszą do świata biznesu
Założenia	Oczekiwana osobiste i społeczne dotyczące informacji i jej ochronie, które łączą przekonania i zachowania
Postawy	Perspektywy bezpieczeństwa, które są zakorzenione w człowieku w oparciu o wcześniejsze doświadczenia
Sposoby działania	Procedury bezpieczeństwa wbudowane w codzienne operacje

Źródło: opracowanie własne

Kultura pojawia się, gdy dwie lub więcej osób jest zaangażowanych we wspólnym przedsięwzięciu. W znaczeniu biznesowym są to wzorce, zachowania, przekonania, założenia, postawy, sposoby działania, które stanowią kulturę korporacyjną. Komponent kultury bezpieczeństwa informacji stanowi niezmiernie ważną część kultury korporacyjnej. W każdej firmie może być ona słaba, nieskuteczna, chaotyczna, sprzeczna, nierozpoznana, ale istnieje. Kultura bezpieczeństwa informacji istnieje w każdym przedsiębiorstwie. Kultura bezpieczeństwa powinna być silna, skuteczna, dobrze zorganizowana, spójna i wspierająca intencje tych w przedsiębiorstwie, którzy uznają że bezpieczeństwo jest strategicznym atrybutem i przyczynia się do ogólnej kondycji przedsiębiorstwa. To jest wszak celem zarządzania.

Nawet w przedsiębiorstwach, w których znajduje się wiele elementów bezpieczeństwa pracowników, oprogramowania, sprzętu, procedur, zasad i standardów, bez kultury wiążącej je z ogólną kulturą korporacyjną, w najlepszym przypadku, można mieć jedynie nadzieję na me-

chaniczną zgodność z rutynowymi wymogami związanymi z ochroną informacji [ISACA, 2009]. Jest to minimum bezpieczeństwa, które przedsiębiorstwo może tolerować, co oznacza, że wprowadzono procesy, które chciałoby się znieść lub zostały one przyjęte niechętnie. To nie jest stopień bezpieczeństwa odpowiedni dla przedsiębiorstwa funkcjonującego we współczesnym świecie. Bezpieczeństwo bez kultury stanowi niewystarczające zabezpieczenie.

Osiągnięcie odpowiedniego poziomu bezpieczeństwa nie powstaje samoistnie i niesystematycznie. Wymaga ono ciągłego zaangażowania w celu wzmocnienia kultury bezpieczeństwa do pożądanego poziomu, poziomu zamierzonego przez kierownictwo. Z tego powodu, ten artykuł koncentruje się na celowym rozwoju kultury bezpieczeństwa. Kultura bezpieczeństwa zawsze istnieje, ale celowo silna, skuteczna i stabilna kultura bezpieczeństwa wymaga pracy, zarówno w fazie budowy jak i utrzymania.

Przedsiębiorstwo, które uznaje, że nie posiada skutecznej kultury bezpieczeństwa, ale chce ją utworzyć musi sporządzić systemowy punkt widzenia całego przedsiębiorstwa w odniesieniu do ochrony informacji. Firma musi pogodzić wszystkie sprzeczne impulsy w ramach przedsiębiorstwa, które hamują wzrost bezpieczeństwa. Kultura nie może być ustanowiona szybko, jak można zaimplementować techniczne aspekty bezpieczeństwa. Nie ma wszak tutaj żadnego urządzenia do instalacji lub oprogramowania do wdrożenia. Implementacja kultury bezpieczeństwa polega na kreowaniu mentalności wśród ludzi, którzy tworzą przedsiębiorstwo i wśród tych, z którymi firma wchodzi w kontakt tj. dostawcami, klientami, innymi zainteresowanymi stronami i społeczeństwem. Sposoby myślenia, światopoglądu i postaw, które kierują zachowaniem są istotą kultury, która musi zostać wprowadzona, pielęgnowana i akceptowana stopniowo. Nie może być ona narzucona z góry, chociaż przewodnictwo organizacyjne może przyspieszyć implementację.

Gdy celowo stworzona zostanie kultura bezpieczeństwa, fakt kreacji wydaje się być zapominany. W tym momencie pewne zachowania stają się nieodłączną częścią przedsiębiorstwa i sposobu prowadzenia działalności gospodarczej. Na przykład, w sektorze prywatnym, nie ma potrzeby umyślnego tworzenia kultury sprzedaży w firmie handlowej, ponieważ pracownicy czynią to na bieżąco. Uznajemy, że w firmie takiej, bez sprzedaży nie ma biznesu, a ludzie realizują kulturę sprzedaży

w sposób poprawny. Przesada w kulturze sprzedaży, może być niekorzystna dla obsługi klienta, kalkulacji zysków i bezpieczeństwa. W skrajnych przypadkach, kulturę sprzedaży może przytłoczyć etyka i aspekty zgodności z prawem. Podobnie, kultura bezpieczeństwa, zbyt ciężka może być przeszkodą dla wzrostu i realizacji misji. Ciężka kultura bezpieczeństwa może być osłabiać działalność gospodarczą firmy, jeżeli nie jest odpowiednio dostosowana do misji organizacji i funkcji biznesowych. Kultura bezpieczeństwa musi mieścić się w ramach ogólnej kultury przedsiębiorstwa i stać się ledwie zauważana.

2. Bezpieczeństwo twarde i miękkie

Nieporozumieniem wydaje się uznawanie technologii i mechanicznych czynników bezpieczeństwa metodami twardym, natomiast aspekty, które dotyczą czynników ludzkich, takie jak planowanie, zarządzanie, motywowanie i nagradzanie, jako miękkie strony bezpieczeństwa. Słowo "twarde" ma wiele konotacji tj.: hermetyczność, trudność, zwartość, faktyczność, realizm i surowość [Ross, 2004]. Na wszystkich poziomach rozwój kultury bezpieczeństwa jest aspektem twardym:

1. Aby być niezawodna, kultura bezpieczeństwa musi dostosowywać się do zmieniającego się środowiska i zawartości, szczególnie w momencie, gdy firma się rozbudowuje lub zmniejsza, pracownicy przychodzą lub odchodzą, kierownictwo organizuje lub reorganizuje procesy a technologia wspiera lub hamuje innowacje. Żadna technologia nie jest niezawodna, ponieważ wszystkie technologie są obsługiwane przez ludzi. Skuteczność każdej realizacji opiera się na wnikliwości i spójności tych, którzy nią zarządzają, innymi słowy, przez kulturę, w której funkcjonuje.
2. Dla osób bez umiejętności technicznych, mogą być one trudne do zdobycia. Można jednak pracowników, poprzez szkolenia, ich nauczyć. Kultura musi zostań wykreowana i stać się żywym tworem a to jest znacznie trudniejsze od zdobycie umiejętności technicznych.
3. Technologia może wydawać się trwała i niezmienna: pakiet oprogramowania zawsze funkcjonuje tak samo a sprzęt zawsze tak samo działa. Czasami sprzęt i oprogramowanie odmawia jednak działania. Oprogramowanie i sprzęt są zaprojektowanymi obiektami, z których każdy ma swoje wady. Oczywiście, kultura może być także zawodna, ale jest znacznie łatwiej zmienić ją i dostosowywać niż złamać.

4. Technologia nie zawsze opiera się o fakty. To, że urządzenie przekazuje wynik nie oznacza, że jest to właściwy wynik. Oddźwięk kultury musi opierać się na faktach: w jaki sposób ludzie faktycznie pracują, wartość informacji z którą pracują i uwzględniać sprzeczne impulsy którymi się kierują.
5. Niepoprawne jest myślenie, że fakty są elementem „twardym" a opinie i emocje są „miękkie", gdy w rzeczywistości wiele osób, jeśli nie większość ludzi działa w reakcji na bodźce swoich emocji i opinii, a nie w oparciu o otaczającą rzeczywistość. Kultura bezpieczeństwa może być stosowana do kształtowania opinii w całym przedsiębiorstwie oddziałując bardziej realnie na ryzyko działalności przedsiębiorstwa i środowisko funkcjonowania.
6. Kultura bezpieczeństwa jest dokładnie tak restrykcyjna w danym przedsiębiorstwie, jak organizacja zakłada. Jedynie kilka typów organizacji, takie jak agencje wywiadowcze lub banki, wymuszają ścisłe przestrzeganie bezpieczeństwa. Fakt ten jest naturalną konsekwencją czynników biznesowych, które obejmują zapewnienie zysku i obsługi klienta, ale również zarządzanie ryzykiem, realizację misji organizacji i działania zgodnego z etyką.

W literaturze funkcjonuje pojęcie bezpieczeństwa, jako funkcja do odparowania ataku [Hofstader, Douglas]. Zabezpieczenia nie powinny być uciążliwe, niepozwalające na pracę, zniechęcające lub kłopotliwe. Bezpieczeństwo nie powinno niekorzystne wpływać na realizację misji przedsiębiorstwa. W organizacjach, w których to występuje istnieje wyraźny dowód, że bezpieczeństwo jest słabym ogniwem ogólnej kultury korporacyjnej. To stwarza opinie, że bezpieczeństwo należy traktować jako zakaz, a nie wsparcie. Wśród zadań kultury bezpieczeństwa jest dostosowanie się bezpieczeństwa i firmy jako całości. Niedogodności związane z bezpieczeństwem typu zamki, barykady, kary itp. osłabiają jej skuteczność. Kultura bezpieczeństwa jest niezbędna do przezwyciężenia przeszkód tego rodzaju.

Kultura bezpieczeństwa może być postrzegana jako element miękki, gdyż jest ona mniej namacalna. Brak wyrazistości nie należy mylić z nieścisłością. Kultura dotyczy percepcji, szacunków, przewagi i kierunków, a nie uporządkowanych liczb, które można znaleźć, np. w księgowości lub finansach. Jednak poglądy i kierunki są często wskaźnikami rzeczywistości, lepszymi niż pozornie „twarde" liczby, które przy głębszej analizie mogą być postrzegane jako zasłona dymna

mająca na celu ukrycie rzeczywistości. Kultura określa co przedsiębiorstwo faktycznie robi w zakresie bezpieczeństwa (lub w zakresie jakiegoś innego celu), a nie co mówi, że zamierza zrobić.

3. Odpowiedzialność za kulturę bezpieczeństwa

Tematyka kultury bezpieczeństwa nie należy do Działu Ochrony Informacji bardziej niż kultura etyczna należy do departamentu prawnego. Kultura jest rozproszona w całym przedsiębiorstwie, wśród kadry zarządzającej, rady nadzorczej, personelu, wśród działów wykonawczych i wsparcia oraz sprzedawców, pracowników działu IT, personelu sprzątającego, itp. Jest to organizacyjny duch czasu, w którym przedsiębiorstwo funkcjonuje. Kultura bezpieczeństwa jest w stanie się zmienić, ale to zależy od samego przedsiębiorstwa.

Niektóre funkcje firmy, takie jak np. bezpieczeństwo informacji, audyt wewnętrzny, zarządzanie ryzykiem i bezpieczeństwo korporacyjne, może posiadać bardziej wiodącą rolę w kreowaniu kultury [Ross, 2010]. Funkcje te działają i są promowane za to, że zdają sobie sprawę z potrzeby bezpieczeństwa i ogólnie są korzystne dla silniejszej kontroli. Istnieje pułapka, w postrzeganiu tych funkcji jako właścicieli kultury bezpieczeństwa, jakby usprawiedliwiając innych pracowników od konieczności zwracania na to uwagi. Należy osiągnąć równowagę w poziomie, w jakim niektóre funkcje są bardziej zaangażowane w bezpieczeństwo niż inne. Wszyscy, którzy chcą być częścią przedsiębiorstwa muszą dostosować się do jego kultury i nikt nie może sobie pozwolić na wyróżnianie się w tej kwestii i przejęcie odpowiedzialności za jej rozwój. Kultura bezpieczeństwa jest i musi być wspólnym przedsięwzięciem.

Zakończenie

Aspekty techniczne (sprzętowe i programowe) dotyczące bezpieczeństwa (ściany ogniowe, strefy zdemilitaryzowane, programy antywirusowe itp.) są niezwykle ważną częścią zarządzania bezpieczeństwem informatycznym. Technologie te są na bieżąco rozwijane i wspierane poprzez wytwórców. Firmy, jak i dział IT najczęściej ograniczają się do implementacji „nowinek technologicznych" dotyczących zabezpieczeń. Słaba kultura bezpieczeństwa nie pozwala, mimo dużych nakładów inwestycyjnych, na osiągnięcie określonego poziomu bezpieczeństwa. Dopiero podniesienie kultury bezpieczeństwa poprzez jej celową kreację podnosi poziom bezpieczeństwa całego przedsiębiorstwa i przyczynia się do skutecznego wykorzystania zasobów sprzętowo-programowych.

Gdy przedsiębiorstwo „żyje" bezpiecznie, powiedzieć można iż jest bezpieczne. Kreacja bezpieczeństwa informacyjnego jest zadaniem niezwykle skomplikowanym i czasochłonnym jednak aktywny udział w tym przedsięwzięciu powinno wziąć całe przedsiębiorstwo. Wbrew powszechnym opiniom, kultura bezpieczeństwa jest czynnikiem twardym przedsiębiorstwa.

Literatura

1. PwC, *Badanie przestępczości gospodarczej Polska 2011, Cyberprzestępczość rosnącym zagrożeniem w biznesie*, listopad 2011, http://www.pwc.pl/pl/publikacje/PwC_Crime_Survey_2011.pdf
2. ISACA, *An Introduction to the Business Model for Information Security*, 2009,
3. *The Security—Privacy Paradox: Issues, Misconceptions, and Strategies*; A Joint Report by The Information and Privacy Commissioner/Ontario and Deloitte & Touche, Canada, 2010,
4. Hofstader, Douglas F. (2009), *Escher Godel Bach: An Eternal Golden Braid*, Basic Books, USA.
5. Ross, Steven (2010), *Information Security Matters: Boston, Berlin, Baghdad and Bora Bora,* ISACA Journal, vol. 4, USA.
6. Ross, Steven (2004), *IS Security Matters: Frameworkers of the World, Unite*, Information Systems Control Journal, vol. 6, USA.
7. Ross, Steven J. (2010), *IS Security Matters?*, ISACA Journal, vol. 2, USA.
8. Eisenhauer, Margaret P. (2009), *The Privacy Case Book: A Global Survey of Privacy and Security Enforcement Actions with Recommendations for Reducing Risks*, USA.

Streszczenie

Niezmiernie ważnym aspektem funkcjonowania współczesnych przedsiębiorstw jest bezpieczeństwo systemów informatycznych. W badaniach naukowych, literaturze, tematyce kursów poświęconych bezpieczeństwu jest ono traktowane bardzo technicznie i zwykle oderwane jest od organizacji, w której jest implementowane. Zdaniem autora jednym z podstawowych składników świadomego, pełnego bezpieczeństwa systemów informatycznych powinna być celowo kreowana kultura bezpieczeństwa informacji. Kultura ta wspiera ochronę informacji jednocześnie wspomagając szersze cele przedsiębiorstwa. Należy tutaj podkreślić zwrot „celowo kreowana". Każda organizacja posiada kulturę bezpieczeństwa, która w różnym stopniu wspiera lub nie bezpieczeństwo informacji. Należy jednak podjąć aktywne działania w celu poprawy ist-

niejącej kultury. Wbrew powszechnym opiniom kultura bezpieczeństwa powinna być rozważana jako czynnik twardy przedsiębiorstwa, a za jej kreację i utrzymanie odpowiedzialność bierze całe przedsiębiorstwo.

Słowa kluczowe
zarządzanie kulturą firmy, kultura bezpieczeństwa, bezpieczeństwo systemów informatycznych, bezpieczeństwo informacji

Intentional creation of a culture of security summary

An extremely important aspect of modern business is security systems. In scientific studies, literature, courses on security issues it is treated very technical and is usually separated from the organization in which it is implemented. According to the author one of the basic components of a conscious, full security of information systems should be intentionally created culture of information security. This culture supports the protection of information while supporting the wider objectives of the company. It should be noted the phrase "intentionally created". Each organization has a culture of safety, which in varying degrees of support or information security. It should, however, to take active steps to improve the existing culture. Contrary to widespread opinion, the culture of security should be considered as a hard factor in the company, and responsibility for the creation and maintenance takes the whole company.

Keywords
managing corporate culture, culture of security, security of information systems, information security