Recenzja dysertacji doktorskiej mgr inż. Estery Pietras pt. „Zarządzanie bezpieczeństwem informacji w przedsiębiorstwach branży motoryzacyjnej" napisanej pod kierunkiem dr hab. inż. Marcina Knapińskiego, prof. PCz

UWAGI OGÓLNE

Ocena potrzeby podjęcia tematu rozprawy

W gospodarce elektronicznej XXI wieku, gdzie w dużym stopniu generowanie, przesyłanie i odbiór informacji w wielu gałęziach i sektorach gospodarki odbywa się w cyberprzestrzeni za pośrednictwem Internetu, obok ewidentnych korzyści, pojawiły się też nowe zagrożenia wynikające z możliwości utraty lub przechwycenia danych elektronicznych zarówno w wyniku celowego ich zniszczenia a także kradzieży dla potrzeb np. eliminacji lub wyprzedzenia konkurentów. Szczególnie narażonymi na tego typu zagrożenia i wynikające z nich straty narażone są przedsiębiorstwa, które z uwagi na konieczność podejmowania coraz intensywniejszej współpracy z różnymi interesariuszami biznesu, (dostawcami, klientami, instytucjami publicznymi, doradczymi, itp.), w ramach klastrów, łańcuchów dostaw czy sieci biznesu nie mogą ograniczyć przepływu danych elektronicznych w przestrzeni wirtualnej. Oczywiście, podmioty gospodarcze oraz wyspecjalizowane firmy sektora IT podejmują próby przeciwdziałania zniszczeniu lub kradzieży danych, co jednak generuje dodatkowe wysokie koszty takiej ochrony wynikające nie tylko z opłacania usług związanych z podniesieniem poziomu bezpieczeństwa informacji, ale również konieczności ponoszenia dużych nakładów pracy przez własnych pracowników w tym obszarze. Słusznie podkreśla Autorka, że problematyka bezpieczeństwa informacji obejmuje także wszelkie inne wrażliwe dane zapisane w formie papierowej czy też przekazywane bezpośrednio np. w trakcie rozmów czy spotkań. Zwraca Ona słusznie uwagę, że problem ten w wielu przedsiębiorstwach nie jest dostatecznie zdiagnozowany i doceniany przez kadrę menedżerską, co powoduje, że zarządzanie bezpieczeństwem informacji nie jest profesjonalne i nie opiera się na działaniach systemowych a raczej ma charakter doraźnych i nieuporządkowanych procesów. Stad, uważam, że podjęta w opiniowanej dysertacji problematyka jest niezwykle ważna z puntu widzenia podniesienia efektywności i rozwoju przedsiębiorstw.

Cel pracy, hipotezy, metody badawcze

W. świetle sformułowanego problemu badawczego dotyczącego badania poziomu bezpieczeństwa informacji i metod jego utrzymywania przyjęta hipoteza, iż "intensywny wzrost ilości zagrożeń bezpieczeństwa informacji w przedsiębiorstwach wymaga stosowania adaptowalnych systemów zarządzania bezpieczeństwem, w których środki techniczne i proceduralne dostosowane będą do wymagań określonych aktualnymi analizami ryzyka utraty informacji,, jest jak najbardziej uzasadniona. Również sformułowany cel pracy jest spójny i w pełni koresponduje ze sformułowaną hipotezą badawczą, wskazując na konieczność opracowania i zastosowania innowacyjnej metody analizy ryzyka determinującego poziom bezpieczeństwa informacji w wybranych do badań firm z branży motoryzacyjnej, co wiąże się z koniecznością poznania źródeł zagrożeń w tym zakresie i przeanalizowania poziomu zabezpieczenia wybranej grupy przedsiębiorstw przed ryzykiem utraty informacji. Badania zostały prawidłowo

zaplanowane i wykonane. Objęci nimi zostali pracownicy administracyjno-biurowi oraz kadra zarządzająca dziewięciu przedsiębiorstw, w których gestii jest zarządzanie informacją lub/i mają oni bezpośredni wpływ na jej ochronę. Należy podkreślić kompleksowość wybranych przez Autorkę metod i technik badawczych pozwalających dogłębnie przeanalizować sformułowany problem badawczy, zweryfikować hipotezę badawczą oraz osiągnąć cel pracy. Oceniając część metodyczną pracy, docenić należy skorzystanie przez Autorkę z wielu uzupełniających się narzędzi analizy, co pozwoliło Jej na wskazanie wielu luk w systemie bezpieczeństwa informacji. W tym celu słusznie dokonano prawidłowej klasyfikacji źródeł zagrożeń zgodnie z metodą 5M, która obejmuje takie kryteria, jak: człowiek (personel), kierownictwo (zarządzanie), otoczenie (osoby trzecie), maszyna (systemy komputerowe, systemy bezpieczeństwa) oraz materiał (metodę). Zastosowany podział wskazał miejsca w organizacjach, w których w niewystarczający sposób zabezpieczono informacje oraz w szczególny sposób podatne były one na urzeczywistnienie się zagrożenia. Aparat badawczy wykorzystany w dysertacji obejmuje analizę dokumentów i literaturę przedmiotu, ankietę, obserwację oraz wywiad a także eksperyment. Wypełnione ankiety poszerzyły znacznie grono badanych respondentów, co pozwoliło zgromadzić materiał badawczy o charakterze ilościowym, natomiast zastosowana technika obserwacji postronnej, tzw. nieuczestniczącej, pozwoliła w sposób zobiektywizowany przeanalizować badane procesy i zjawiska, gdyż badacz nie brał udziału w pracach i procesach przedsiębiorstwa. Z kolei wywiad zawierający pytania problemowe pozwolił Autorce dysertacji uszczegółowić analizę badanych problemów – m.in. ustalić fakty oraz motywacje pracowników i ich poziom świadomości w zakresie przechowywanej informacji oraz stosunku i oczekiwań kadry w kwestii jej zabezpieczenia w firmie zatrudniającej. W mojej opinii przeprowadzony eksperyment, nie tak często stosowany w obszarze nauk społecznych, w jednym z 9 wybranych do badań przedsiębiorstw, pomógł poprawnie zweryfikować faktyczny stan wiedzy pracowników w zakresie ochrony informacji, którą posiadali oraz w kwestii odpowiedzi na pytanie, czy owa świadomość pozwoli im złamać obowiązujące procedury i zasady postępowania oraz czy w organizacji wskazane zabezpieczenia skutecznie zadziałały czy też nie. Na wyróżnienie zasługują przedstawione w postaci załączników kwestionariusze ankiety badawczej oraz wywiadu, arkusza obserwacji oraz oryginalny projekt Polityki Bezpieczeństwa Informacji i procedury zgodne ze schematem postępowania systemowego, co czyni wgląd czytelnika w zrozumienie omawianej w dysertacji problematyki łatwiejszym.

Ocena merytoryczna pracy

Niniejsze opracowanie składa się z sześciu rozdziałów, podsumowania, spisu literatury, spisu rysunków, spisu tabel, załączników (kwestionariusza ankiety badawczej, arkusza obserwacji, kwestionariusza wywiadu, polityki bezpieczeństwa informacji, procedur zgodnych ze schematem postępowania systemowego) oraz streszczenia. Pierwsza część dysertacji zawiera dwa rozdziały, które podejmują problematykę bezpieczeństwa i .ochrony informacji, wskazując na system zarządzania redukujący ryzyko w przedsiębiorstwie. Natomiast w drugiej części pracy, w czterech kolejnych rozdziałach Autorka zaprezentowała tematykę bieżącego stanu bezpieczeństwa informacji w organizacjach, gdzie wykorzystano metody i techniki dotyczące ochrony przed powstającymi zagrożeniami w tym zakresie.

W pierwszych dwóch rozdziałach Autorka wyczerpująco omówiła klasyfikacje, rodzaje i ich źródła oraz skutki zagrożeń związanych z bezpieczeństwem informacji. Ponadto przedstawiła trafnie akty prawne, które regulują temat należytej ochrony informacji, przy czym mówiąc o rozporządzeniach i aktach prawnych wprowadziła nieścisłość, bo rozporządzenia to też akty prawne tylko np. o niższej randze niż np. ustawy.

Dodatkowo przedstawiła prawidłowo w tej części dysertacji poglądy autorów, którzy zajmują się tematem systemu zarządzania bezpieczeństwem informacji w artykułach naukowych, książkach, rozprawach doktorskich, wskazując na praktyczną wartość dobrych praktyk rozpatrywanych w kontekście systemowym i procesowym.
Natomiast w drugiej części rozprawy Autorka podjęła się przedstawienia problematyki obejmującej bieżący stan bezpieczeństwa informacji w organizacjach. Zaprezentowała ponadto wyniki badań, które dowiodły, że istnieje ciągła potrzeba analizy poziomu bezpieczeństwa informacji oraz opracowania systemu związanego z zarządzaniem ryzykiem jej utraty. Na podstawie badań poprawnie zdiagnozowano luki występujące w systemie bezpieczeństwa oraz podano racjonalne propozycje zmian w tym zakresie. W efekcie końcowym opracowano oryginalny projekt systemu Zarządzania Bezpieczeństwem Informacji (ZBI). W projekcie poprawnie określono założenia i przedstawiono budowę systemu ZBI. W efekcie końcowym opracowano projekt takiego systemu, w którym określono prawidłowo jego założenia i budowę. Autorka tego rozwiązania uznała, że stanowi ono gotowe do wprowadzenia narzędzie reagujące na wektor wejściowy, czyli pojawiające się zagrożenia, generując wektor wyjściowy czyli odpowiednie zabezpieczenia, które powstaną w wyniku działania ZBI rozumianego jako zbiór procedur minimalizujących wpływ zagrożeń. Być może użyte przez Autorkę skróty myślowe w tym miejscu sugerują nie do końca precyzyjnie, że te procedury będą wygenerowane automatycznie, ale w rzeczywistości system może tylko pomóc odpowiednim pracownikom w ich stworzeniu i potem wdrożeniu w praktyce działania firmy. Tu zabrakło mi trochę takiego krytycznego spojrzenia na autorski projekt ZBI, który rzeczywiście pozwala tworzyć procedury ochrony informacji wykazujące charakter uniwersalności, a które mogą być rzeczywiście stosowane w różnych obszarach organizacji. Nasuwa się tylko uwaga, którą powinna w mojej ocenie zawrzeć Autorka dysertacji, a mianowicie o konieczności dostosowania zaproponowanego narzędzia do specyficznych warunków technicznych, ekonomiczno-społecznych i organizacyjnych danego przedsiębiorstwa tak, aby rzeczywiście efekty jego wdrożenia były korzystne i dostrzegalne. Zatem użycie terminu, że opracowano „gotowe do wprowadzenia narzędzie" jest trochę na wyrost z racji tego, że każda organizacja jest bytem niepowtarzalnym i z tego względu żadne, nawet najlepsze uniwersalne procedury nie mogą uwzględnić wszystkich unikalnych procesów rzeczywistych, które w niej zachodzą, co zresztą zauważalne jest w krytycznym spojrzeniu na zarządzanie procesowe w ogóle charakteryzujące się usztywnieniem w tworzeniu i realizacji procesów w organizacjach. Nieco wagę poziomu niedostatku merytorycznego w tym względzie zmniejszają dwie cenne uwagi Autorki w podsumowaniu dysertacji iż, „...opracowany projekt ZBI jest na tyle uniwersalny, że może być wykorzystywany w innych przedsiębiorstwach, o podobnej strukturze i wielkości oraz „...W tym względzie ważnym jest zwrócenie uwagi na zaaplikowanie systemu zmniejszenia ryzyka utraty informacji, opartego o uwarunkowania i strukturę organizacji." W podrozdz. 1.1. rodz. 1 Autorka zawarła trafnie definicje i klasyfikacje ochrony i bezpieczeństwa informacji, opisała skutki braku jej bezpieczeństwa a także przedstawiła charakterystyki poszczególnych atrybutów bezpieczeństwa jak poufność, rozliczalność, autentyczność, integralność, dostępność, niezawodność, spójność, tajność oraz bezpieczeństwo informacji w pamięci jako wiedza ukryta. Omówiła w nim także szczegółowo bezpieczeństwo fizyczne, osobowo-organizacyjne, prawne i teleinformatyczne. Słusznie podsumowano podrozdz 1.1. stwierdzając, że systemy informatyczne są bezpośrednio zagrożone ze strony każdego, kto ma większy zasób wiedzy, czy też umiejętności. W podrozdz. 1.2 Autorka opisała rolę i znaczenie informacji w kontekście gospodarki opartej na wiedzy (GOW), zdefiniowała informację i scharakteryzowała trafnie jej atrybuty (aktualność, zrozumiałość, dokładność, precyzyjność, wiarygodność). Wskazała prawidłowo, czym jest wartość i jakość informacji w świetle jej klarowności, zrozumiałości i dokładności, w kontekście jej roli jako niematerialnego zasobu firmy oraz słusznie konkludując, iż informacja jest również towarem na rynku. I dalej stwierdziła logicznie, że, aby zagwarantować stan bezpieczeństwa informacji jako kluczowego zasobu firmy, winna być chroniona w aspektach przechowywania informacji, dostępu do informacji oraz transmisji informacji tak,

aby dane były chronione przed ujawnieniem, modyfikacją czy też zniszczeniem. Podkreślając fakt, iż aż 70% poufnych informacji w spółkach USA było ujawnianych, udało się Autorce dowieść, że rola bezpieczeństwa informacji w organizacjach jest obecnie tak newralgiczna. W podrozdz. 1.3 stanowiącym logiczny wywód treści zwartych wcześniej w dysertacji scharakteryzowano elementy bezpieczeństwa informacji, na których opiera się zarządzanie tym aspektem działalności organizacji zgodnie z treściami zawartymi w normie PN-I-13335-1, a do których należą zasoby, zagrożenia, podatność, następstwo, ryzyko, zabezpieczenia i ryzyko szczątkowe. Trafnie zaakcentowano, że nadrzędnym celem zarządzania jest proces minimalizowania ryzyka wystąpienia zagrożenia i wprowadzenia skutecznych zabezpieczeń informacji. Następnie podkreślono celnie, że przy identyfikacji zasobów należy również wziąć pod uwagę ich atrybuty takie, jak: ich wartość, wrażliwość oraz podatność na określone zagrożenie, definicje zagrożeń w ogóle i w kontekście bezpieczeństwa, także ryzyko. Należy także uwzględnić podatności na zagrożenie utraty informacji związane ze sprzętem, oprogramowaniem personelem, siedzibą, organizacją, siecią, zabezpieczeniami administracyjno-technicznymi oraz dotyczących aspektów zarządczych lub prawnych. W dalszej części dysertacji przedstawiono podstawowe zastosowania zabezpieczeń obejmujących ochronę przed zagrożeniami; redukcję podatności, odtwarzanie zasobów po incydentach, wykrywanie niepożądanych zagrożeń, ograniczenie następstw oraz ryzyko szczątkowe, które można zredukować jedynie częściowo poprzez zastosowanie zabezpieczeń. Ważne jest zwrócenie przez Autorkę uwagi, iż w każdej sytuacji pozostaje ryzyko szczątkowe, które należy zaakceptować. Prawidłowo sformułowana konkluzja, iż osoby, które przetwarzają, przechowują i tworzą informacje zobowiązane są do znajomości istoty zasobu, podatności, zagrożenia, następstwa oraz zabezpieczenia, kończy podrozdział. W kolejnym podrozdziale Autorka podkreśla trafnie, że liczba zagrożeń dla bezpieczeństwa danych wzrasta proporcjonalnie do rozwoju technologii informacyjno-komunikacyjnej i upowszechniania rozmaitych rozwiązań informatycznych wykorzystywanych w przedsiębiorstwach. Dobrze byłoby powiązać ten fakt z argumentem lawinowego wzrostu liczby gromadzonych, przetwarzanych i przesyłanych danych liczonych już w zettabajtach. Dalej Autorka przedstawia wymagania dla klasyfikacji zagrożeń i oczekiwania z tym związane, aby klasyfikacja wnosiła do systemu bezpieczeństwa określoną wartość, wyłączność, powtarzalność, akceptowalność, jednoznaczność a kryteria klasyfikacji powinny być jasne, czytelne i oczywiste dla wszystkich identyfikujących zagrożenie, tak, aby osoba dokonująca klasyfikacji nie miała wątpliwości co do sposobu zaklasyfikowania zagrożenia. Wymieniono i scharakteryzowano wiele podziałów zagrożeń, takich jak: cywilizacyjne i naturalne, wewnętrzne i zewnętrzne, techniczne, pierwotne i wtórne, przedmiotowe i podmiotowe oraz militarne i niemilitarne. Dalej Autorka trafnie usystematyzowała opisane zagrożenia wg takich kryteriów, jak dotkliwość określona poprzez zakres szkodliwości, motywacja, częstotliwość pojawienia się oraz rodzaj szkody, np. czasowa powodująca tylko przerwę w dostępie do zasobu, ale też stała, która może zniszczyć całkowicie zasoby. O dociekliwości badawczej Autorki świadczy ważkie stwierdzenie, iż uwarunkowania kulturowe i środowiskowe oraz koniunktura i otoczenie, w których funkcjonuje dana jednostka organizacyjna mogą znacząco wpływać na sposób postępowania z zagrożeniem. W dalszej części podrozdziału słusznie wskazano, że zagrożenia mogą mieć bardzo różnorodne pochodzenie a ich analiza z wiarygodnych źródeł wskazuje na częste występowanie przestępczości komputerowej, włamań komputerowych, metod phishingowych, oszustw, kradzieży, szpiegostwa gospodarczego, wyłudzania informacji, błędów pracowników oraz awarii technicznych, złośliwego oprogramowania czy klęsk żywiołowych. Zagrożenia te mogą mieć charakter środowiskowy, ludzki przypadkowy oraz rozmyślny. W podrozdz. 1.5 Autorka przeanalizowała wpływ zagrożeń socjotechnicznych na bezpieczeństwo informacyjne firmy bardzo trafnie podsumowując go cytowaną bezpośrednią dość pesymistyczną dla właścicieli przedsiębiorstw konkluzją mówiącą, iż „W miarę wymyślania coraz to nowych technologii zabezpieczających, utrudniających znalezienie technicznych luk w systemie, napastnicy będą zwracać się w stronę ludzkich słabości. Złamanie ludzkiej bariery jest o wiele prostsze i często wymaga jedynie inwestycji rzędu kosztu rozmowy telefonicznej…".

W podrozdz. 1.6 dysertacji obszernie omówiono bezpieczeństwo teleinformatyczne rozumiane jako całokształt przedsięwzięć zmierzających do zapewnienia bezpieczeństwa systemów i sieci teleinformatycznych tj. ochrony danych wytwarzanych, przetwarzanych i przechowywanych w systemach i sieciach przed przypadkowym bądź celowym ujawnieniem, modyfikacją czy zniszczeniem, w wyniku czego uniemożliwione jest ich przetwarzanie poprzez zastosowanie technicznych, programowych czy kryptograficznych i organizacyjnych środków oraz metod zapobiegających ujawnieniu. Naświetlono też kluczowe znaczenie BI w XXI wieku, wskazując prawidłowo jego istotę oraz rodzaje zagrożeń w tym zakresie m. in. ich klasyfikację i przewidywane skutki wystąpienia oraz wskazując szczegółowo rodzaje bezpieczeństwa teleinformacyjnego. Autorka także trafnie podkreśliła rangę tego problemu jako zbioru zagadnień z dziedziny telekomunikacji i informatyki bezpośrednio związanych z monitorowaniem ryzyka, wynikającego z korzystania z komputerów, sieci teleinformatycznych czy przesyłania danych.
W podrozdz. 1.7. Autorka szczegółowo opisała obowiązujące uregulowania prawne dotyczące bezpieczeństwa informacji od najwyższej ich rangi a więc Konstytucji RP, RODO, kolejnych adekwatnych do tego obszaru ustaw a na Kodeksie Pracy oraz Kodeksie Karnym kończąc. W sposób logiczny kontynuuje swój wywód oceniając w podrozdz. 1.8. zalecenia zawarte w obowiązujących normach z zakresu bezpieczeństwa informacji w związku z ich przestrzeganiem, np. zasad prywatności oraz omawia wytyczne dla szacowania ryzyka w tym zakresie i doboru zabezpieczeń.
Raczej w podrozdziale 1.9 nie powinno się używać tytułu „wnioski", gdyż taki tytuł nie jest spójny ze strukturą pracy jako całości i nazewnictwem poszczególnych jej elementów. Podsumowując rozdz. 1 Autorka zwraca celnie czytelnikowi szczególną uwagę na zaistnienie problemu wielości ustaw, norm czy rozporządzeń powodujących, że przedsiębiorca nie jest w stanie zaznajomić się z nimi wszystkimi. Słusznie też akcentuje Ona częste zmiany przepisów powodujące chaos informacyjny powodujący, że przedsiębiorcy nie wiedzą, gdzie szukać uregulowań prawnych oraz czy są one jeszcze aktualne. Z drugiej strony prawidłowo konkluduje, iż zmiany przepisów uwarunkowane są rosnącą liczbą nowych zagrożeń, więc ich katalog powinien być ciągle aktualizowany a działania zabezpieczające muszą ciągle być doskonalone i uaktualniane zgodnie zasadą cyklu Deminga: Planuj-Wykonuj-Sprawdzaj –Działaj.
W rozdziale 2 zaprezentowano Systemy Zarządzania Bezpieczeństwem Informacji (SZBI) jako systemy redukujące ryzyko utraty informacji w przedsiębiorstwie. Zdefiniowano je poprawnie jako rozwiązania do ZBI czyli „część całościowego systemu zarządzania, opartego na podejściu wynikającym z ryzyka biznesowego, dotyczącego ustanawiania, wdrożenia, eksploatacji, monitorowania, utrzymania i doskonalenia systemów bezpieczeństwa informacji". Autorka pokazuje znaczenie SZBI w sytuacji coraz częstszych włamań do wewnętrznych systemów informacyjnych przedsiębiorstw, również przez swoich pracowników i niefrasobliwości menedżerów, którzy nie reagują na skutki takich zagrożeń. Dalej słusznie podkreśla, iż postanowienie o wprowadzeniu SZBI jest decyzją strategiczną dla każdego przedsiębiorstwa. Taki wysoki status tej decyzji w firmie wyznaczają takie uwarunkowania, jak wpływ jej potrzeb i celów biznesowych, wymagania bezpieczeństwa, realizowane procesy oraz sama wielkość i struktura organizacji. Z uwagi na fakt, że turbulentnym zmianom podlegają obecnie wszystkie obszary działalności w każdej organizacji, stąd konieczne jest modernizowanie systemów je wspomagających. Wdrożenie SZBI jest wynikiem potrzeb organizacji, dlatego też wymaga się, aby system zarządzania był rozpatrywany w kontekście systemowym lub procesowym. W następnym kroku Autorka prezentuje zobowiązania wynikające z Normy z serii 27000. Należą do nich wymagania z serii ISO/IEC, 27001, które zostały podzielone na zobowiązania obejmujące odpowiedzialność kierownictwa, audyty wewnętrzne i zewnętrzne, przeglądy SZBI realizowane przez kierownictwo, działania doskonalące system ZBI i jego dokumentowanie. Dalej opisuje w podrozdz. 2.3 zagadnienia dotyczące klasyfikacji informacji oraz różnych aspektów polityki bezpieczeństwa informacji a szczegółowo omawia zabezpieczenia techniczne, fizyczne, administracyjne, organizacyjne, sprzętowo-programowe, zarządzanie IT oraz zarządzanie bezpieczeństwem IT. W rozważaniach na temat klasyfikowania informacji słusznie Autorka rozprawy akcentuje konieczność

skupienia uwagi na tym, jakie dokumenty i systemy zawierają informacje ważne ze względu na atrybuty bezpieczeństwa, ponieważ poziom ochrony informacji określany jest też przez analizę pod kątem jej poufności, integralności oraz dostępności. Dalej słusznie konkluduje, że klasyfikacja informacji jest jak najbardziej potrzebna w celu zidentyfikowania jej najistotniejszej wartości dla jednostki gospodarczej, które w dalszej kolejności należy poddać precyzyjnie obserwacji, a także dotyczy takich danych, które w danym momencie nie wymagają ochrony, ale powinny być śledzone z punktu widzenia możliwych zmian.
Podrozdział 2.4. zawiera zagadnienia zarządzania ryzykiem w SZBI a więc, np. ryzyko związane z bezpieczeństwem informacji definiowane jest, jako „potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywów lub grupy aktywów, powodując szkodę dla organizacji". Mierzone ono może być przy pomocy metod opisowych czy skomplikowanych modeli matematycznych. W teorii i w praktyce znane są metody ilościowe, jakościowe oraz mieszane oceny ryzyka. Natomiast zwięźlej można istotę ryzyka wyrazić dwoma następującymi parametrami: P-prawdopodobieństwo wystąpienia zdarzenia i S-skutki konsekwencji zdarzenia jako iloczyn tych dwóch wielkości. Autorka szczegółowo charakteryzuje różne miary oceny ryzyka słusznie eksponując miarę ryzyka jako podstawę rankingu zagrożeń, czy metodę CRAMM w szczególności dedykowaną organizacjom rządowym lub też stosowaną często w przemyśle. Prezentuje dalej ocenę ryzyka poprzez szacowanie częstotliwości zagrożeń a wśród metod jakościowych szczegółowo m. in. charakteryzuje takie podejścia, jak: FMEA, HOZOP, COBRA, CRAMM, MEHARI, MARION i OCTAVE. Następnie Autorka trafne zauważyła, iż charakter i kierunek ryzyka w każdej jednostce gospodarczej jest inny i wymaga dostosowania metody łagodzenia ryzyka do specyfiki przedsiębiorstwa, rodzajów realizowanych przez nią operacji oraz istotności występujących zagrożeń. Przedstawione w pracy klasyfikacje i podziały ryzyka wg różnych kryteriów jak np. ryzyko właściwe (np. klęski żywiołowe), subiektywne, (które jest przewidywalne) oraz obiektywne, (można ocenić przy pomocy danych z ostatniego zdarzenia czy zdarzenie się powtórzy), czy też ryzyka charakterystyczne w prowadzonym biznesie jak ryzyko gospodarcze, ryzyko finansowe, ryzyko niewypłacalności czy ryzyko handlowe wskazują, że ocena ryzyka utraty bezpieczeństwa informacji jest bardzo ważna. Wszelkie zagrożenia, jak konstatuje słusznie Autorka, mogą być minimalizowane poprzez efektywne zarządzanie ryzkiem w przedsiębiorstwie, kiedy to podejmowane są działania w zakresie ciągłego monitorowania i analizy ryzyka oraz przeciwdziałania nowym zagrożeniom oraz podatnościom wykorzystanym poprzez zagrożenie a głównym elementem zarządzania ryzykiem w BI jest ukierunkowanie całego procesu na rozpoznanie okoliczności i czynników, istotnie wpływających na odpowiednie zabezpieczenie cennych aktywów chronionych w przedsiębiorstwie. Bardzo klarownie zależności między ryzykiem a zagrożeniami, podatnościami, zabezpieczeniami, zasobami oraz wymaganiami w zakresie ochrony i wartości pokazano na rys. 23. Bardzo ważne jest trafne holistyczne ujęcie przez Autorkę problemu ryzyka w firmie poprzez rzeczowe uargumentowanie, iż zarządzanie ryzykiem powinno się rozpatrywać, jako całość, czyli jako integralną część całego cyklu życia organizacji a nie jako osobno traktowany obszar zarządzania tą organizacją. Przedstawiony w podrozdz. 2.5 cykl zarządzania ryzykiem w obszarze bezpieczeństwa informacji został także w sposób logiczny i przejrzysty opisany jako proces obejmujący ustanowienie kontekstu, szacowanie ryzyka, estymowanie oraz ocenę i jego akceptację, wreszcie postępowanie z ryzykiem i przegląd oraz monitorowanie ryzyka. Trafnym podsumowaniem podrozdz. 2.5 może być stwierdzenie, iż skutecznym zabezpieczeniem firmy przez zagrożeniami może być wdrożenie procesu zarządzania ryzykiem w sposób dopasowany do charakteru i specyfiki prowadzonej działalności oraz tak, aby właściwie rozpoznać podatności i słabości mechanizmów kontroli, gdyż mogą one stanowić o zakłóceniach pracy w organizacji. Charakteryzując System Zarządzania Bezpieczeństwem Informacji (SZBI) Autorka słusznie podkreśla, że choć przedsiębiorstwa nie wykazują zbyt dużych chęci do wdrożenia tego typu rozwiązań, to istniejąca norma 27001: 2017 może być przydatnym drogowskazem w budowaniu bezpiecznej jednostki organizacyjnej, ponieważ zaproponowany w niej model może być stosowany w każdej organizacji, niezależnie od rodzaju prowadzonej działalności, wielkości organizacji, statusu

prawnego, realizowanych systemów czy struktury organizacyjnej w systemie zarządzania bezpieczeństwem informacji. Zastosowanie doskonalącego modelu Planuj-Wykonuj-Sprawdzaj-Działaj (PDCA: Plan-Do-Check-Act) w odniesieniu do SZBI obejmuje przebieg procesów i systemów w całej strukturze SZBI, opierając się o szacowanie ryzyka w projektowaniu, wdrażaniu oraz zarządzaniu bezpieczeństwem informacji, które można wykorzystać we wszystkich systemach zarządzania BI. Podejście procesowe modelu jest podyktowane stosowaniem czterech struktur procesowych pochodzących z modelu Deminga, które obejmują takie etapy, jak: Planowanie – opracowanie założeń SZBI, procedur, procesów oraz celów ważnych z punktu zarządzania ryzykiem; Wykonuj – eksploatacja i wdrożenie polityki SZBI, działania ochronne i połączone z zabezpieczeniami, Sprawdzaj – monitorowanie i przegląd systemu oraz inne zabezpieczenia w celu szybkiego wykrycia błędów podczas przetwarzania informacji (tworzenie raportów dla kierownictwa). Autorka trafnie akcentuje, że na etapie ustanawiania SZBI ważnym etapem w jego wdrażaniu jest identyfikacja ryzyka, która bazuje na wskazaniu zasobów oraz przypisaniu do nich zagrożeń, podatności oraz skutków wystąpienia niebezpieczeństwa. Omawiając szczegółowo kolejne działania na etapie wdrożenia, SZBI, monitorowania i przeglądu oraz utrzymania i doskonalenia polityki bezpieczeństwa Autorka wyeksponowała celnie rolę szkoleń jako jednego z kluczowych czynników sukcesu poprawy polityki bezpieczeństwa informacji. W końcowej części podrozdz. 2.5 Autorka wymienia ważne korzyści wewnętrzne i zewnętrzne wdrożenia SZBI w firmie a w szczególności eksponuje słusznie te, które podnoszą jej prestiż i zaufanie w oczach kontrahentów. Nie kwestionując ww. korzyści , w mojej opinii zabrakło jednak tutaj spojrzenia krytycznego wskazującego np. podmioty, dla których koszty opracowania i wdrożenia takiego systemu mogłyby być niewspółmiernie duże w stosunku do potencjalnych korzyści z jego zastosowania. Myślę, że w literaturze jakieś opinie krytyczne na ten temat można by znaleźć. W podrozdz. 2.6 prezentującym przykłady bezpieczeństwa informacji Autorka omówiła kilka opracowań dotyczących przedsiębiorstw i jednostek samorządowych przybliżających tematykę zarządzania bezpieczeństwem informacji wskazując m. in. na autorski model opierający się na normie ISO 27001 oraz pokazując pewne ciekawe innowacyjne rozwiązania w sferze zarządzania kulturą bezpieczeństwa informacji czy też zarządzania nadużyciami. W mojej opinii jednak, mankamentem tej części dysertacji jest wysoki poziom ogólności prezentowanych przykładów. Merytorycznie podrozdział 2.6 zyskałby na wartości, gdyby Autorka chociażby wycinkowo przedstawiła dla każdego z podanych przykładów konkretne problemy zagrożeń informacji i metody ich łagodzenia lub eliminacji.

W rozdziale 3 Autorka wyczerpująco i logicznie omówiła cel i zakres rozprawy dobrze argumentując genezę podjęcia tematu pracy i przedmiot badań jak również sformułowała cele badań hipotezę badawczą. Opisała także wybrane metody, techniki i narzędzia badawcze jak również organizację i przebieg badań. Do tych zagadnień odniesiono się już merytorycznie w pierwszej części recenzji, natomiast należy bardzo pozytywnie ocenić szczegółową charakterystykę grupy badawczej zamieszczoną w rodz. 3 dysertacji, w której Autorka opisała atrybuty wybranych do badań przedsiębiorstw, trafnie argumentując, że do próby badawczej wybrano te przedsiębiorstwa, które są liderami wśród dostawców na rynku motoryzacyjnym w Europie, zaznaczając swoją pozycję na rynku zbytu, jako potentata i wyróżniając się pod względem przetwarzania grupy informacji określonych jako tajemnica przedsiębiorstwa. Co więcej, celnie uwypuklono, że wybrane obiekty badawcze jako dostawcy przemysłu motoryzacyjnego są często w posiadaniu informacji poufnych, dotyczących części stosowanych w nowych rozwiązaniach konstrukcyjnych, wykorzystywanych przez kontrahentów. Tutaj można by tylko dodać wzmiankę o tym, że przemysł motoryzacyjny w wymiarze globalnym stanowi swoiste „koło zamachowe" postępu technologicznego, gdzie koncentrują się najnowsze odkrycia z wielu dziedzin nauki i są to najczęściej innowacje o charakterze unikalnym, które muszą być szczególnie chronione. Stąd, uważam wybór przedsiębiorstw z branży motoryzacyjnej jako obiektów do badań z obszaru bezpieczeństwa informacji za bardzo trafny. Zaprezentowano także prawidłowo organizację i przebieg badań, co także wydaje się logiczne w świetle zaprezentowanych w rozdziale 4 wyników badań w postaci diagnozy analizy ryzyka

istniejącego stanu bezpieczeństwa i wykrytych istotnych luk w systemie BI oraz oryginalnych rozwiązań usprawniających w tym zakresie.
W rozdziale 4 rozprawy Autorka przedstawiła wyniki badań własnych uzyskanych z badanych 9 przedsiębiorstw w działach: księgowo-finansowym, płacowo-kadrowym, kontrolingu, sprzedaży, technologicznym, marketingu, IT, badawczo-rozwojowym oraz w dziale BHP a przeprowadzonych wśród pracowników zatrudnionych w ww. działach, które są w posiadaniu aktywów informacyjnych, do których zaliczamy wszelkiego rodzaju zbiory danych i środki do ich gromadzenia, przetwarzania i transmisji. Najpierw oceniła stopień wdrożenia normy ISO 27001 dotyczącej bezpieczeństwa informacji wg kryterium potwierdzenia luba zaprzeczenia takiego procesu a także świadomości badanych pracowników w tym zakresie. Następnie zdiagnozowała świadomość pracowników w zakresie opracowania i wdrożenia polityki bezpieczeństwa informacji (PBI) wg kryterium uszeregowania stanowisk pracy w drabinie hierarchii badanych organizacji. Kolejnym etapem badań było przenalizowanie dostępu do różnych grup informacji, (danych osobowych, tajemnic zawodowych, tajemnic przedsiębiorstwa, tajemnic prawnie chronionych), kierowników niższego szczebla oraz pracowników na stanowiskach niekierowniczych. Następnie zbadano znajomość zapisów dotyczących poufności informacji w realizowanych projektach, umowach z kontrahentami wg wykształcenia i oceny stopnia składania podpisów na oświadczeniach o zachowaniu poufności informacji. Kolejny przekrój analityczny prowadzonych badań własnych dotyczył oceny sposobu utylizacji sprzętu komputerowego w organizacjach, detekcji organizacji wyrzucających do śmieci np. nośniki danych wg grupy stanowisk, a także stopnia udostępnienia swojego służbowego loginu lub hasła innemu współpracownikowi lub stażyście wg wykształcenia i zajmowanych stanowisk pracowniczych oraz stażu pracy. Kolejnym etapem analizy bezpieczeństwa informacji była ocena świadomości respondentów w kwestii identyfikowania i analizy w ich firmach ryzyka w tym zakresie oraz częstotliwości tego typu działań. Następnie zdiagnozowano stopień przestrzegania zasad prawidłowego przechowywania dokumentów w firmach i wiedzy pracowników w tym zakresie. W dalszym etapie sprawdzono częstotliwość aktualizacji oprogramowania antywirusowego i świadomości znaczenia aktualizacji automatycznej takiego oprogramowania. Autorka w kolejnym etapie badań ankietowych oceniła bezpieczeństwo informacji związane z ochroną budynków oraz swobodą poruszania się po terenie przedsiębiorstw. Także w tym aspekcie oceniła znaczenie prowadzenia rejestru osób z zewnątrz i kontroli ich wejść i wyjść oraz stosowanych zabezpieczeń fizycznych (ogrodzeń, drzwi, itp.) na podstawie opinii respondentów wypowiadających się na ten temat np. wg zajmowanych stanowisk pracy. Dalej dokonała analizy korzystania ze stron internetowych, działań związanych z ochroną nośników pamięci zewnętrznej czy też z zagubieniem sprzętu komputerowego czy wykorzystywania sprzętu lub oprogramowania firmowego do celów prywatnych. Zdiagnozowała również poziom reakcji kadr zarządczych firm na wystąpienie ww. zagrożeń i wyciągania konsekwencji w stosunku do osób lekceważących zasady zachowania bezpieczeństwa informacji.
W ostatniej części dysertacji, co trzeba podkreślić pozytywnie, udało się Autorce z powodzeniem przeprowadzić szczegółową i kompleksową analizę wyników badań i przedstawić propozycje rozwiązań na ich podstawie, co zawarto w rozdziale 5 i 6. Jeśli chodzi o prezentację wyników badan ankietowych, to kolejność ich prezentacji powinna być logicznie wg mnie uprządkowania nieco inaczej, lub też Autorka powinna wyraźniej określić, czy kolejność ocenianych aspektów bezpieczeństwa informacji jest prowadzona wg zapisów w jakiejś konkretnej polityce bezpieczeństwa, np. wg zabezpieczeń organizacyjnych, administracyjnych, sprzętowo-programowych i zarządzania IT, technicznych czy fizycznych. Moje wątpliwości w tym zakresie związane są z pewnym przemieszaniem dostrzeżonym w toku zadawania respondentom pytań i analiz z nimi związanych, gdyż dotyczą one np. raz zabezpieczeń niematerialnych typu oprogramowania antywirusowego, potem materialnych typu ochrona budynków, a potem znowu niematerialnych np. oceny korzystania ze stron internetowych w godzinach pracy dla celów prywatnych. W prezentacji wyników badań własnych Autorka stwierdza słusznie, że odpowiedzialność za

bezpieczeństwo informacji w firmie ponosi kierownictwo, ale zasadne byłoby dodać, że przy tak rozbudowanej kontroli nie jest ono w stanie kontrolować skutecznie wszystkich procedur BI bezpośrednio tylko za pośrednictwem upoważnionych pracowników, którym deleguje się wtedy uprawnienia. W dobrej atmosferze w firmie oraz przy okazywaniu szacunku zaufanym pracownikom jest to możliwe i skuteczne.
Bardzo dobrym i syntetycznym a jednocześnie wnikliwym i klarownym podsumowaniem przeprowadzonych badań własnych, zarówno ankietowych, wywiadów jak i obserwacji, jest treść diagramu Ishikawy przedstawiająca stan bezpieczeństwa informacji w badanych firmach w formie utraty bezpieczeństwa informacji związanych z przyczynami i skutkami określonymi w tzw. szkieletach. Dotyczą one po pierwsze zachowania personelu i jego działań zarówno celowych jak i przypadkowych, obrazują zarządzanie dokumentami wewnętrznymi, nadzór nad pracownikami, odpowiedzialność osobową i organizację kontroli dostępu jak również systemy komputerowe, systemy bezpieczeństwa, metody, osoby trzecie oraz złe zarządzanie sprzętem. Rekomendowany oryginalny projekt Autorki w zakresie SZBI oceniam merytorycznie bardzo wysoko jako skuteczne rozwiązanie, które po spełnieniu warunków efektywnego wdrożenia, może bardzo istotnie podnieść poziom bezpieczeństwa informacji w wielu organizacjach, w tym firm produkcyjnych.
W mojej opinii, zabrakło w podsumowaniu rozprawy choćby krótkiej dyskusji wyników z rekomendowanym oryginalnym projektem Autorki w zakresie SZBI na tle innych metod stosowanych w zarządzaniu bezpieczeństwem informacji. Dobrze byłoby także przedstawić przyszłościowe kierunki badań w analizowanym obszarze, np. odpowiadających na pytanie, czy wszystkie firmy ponoszą takie samo ryzyko wynikające z utraty lub kradzieży informacji np. z punktu widzenia unikalności danych i jak metodycznie takie różnice w tych ryzkach pomierzyć.
Niemniej, mimo dostrzeżonych nielicznych mankamentów dysertacji w jej ocenie merytorycznej, oceniam jej wartość pod tym względem bardzo wysoko z uwagi na kompleksowość przeprowadzonej analizy bezpieczeństwa informacji jak również pragmatyzm zaproponowanego rozwiązania usprawniającego w tym zakresie.

Ocena formalnej strony pracy

W ocenie redakcyjnej strony pracy należy podkreślić bardzo wysoką jakość aż 76 rysunków, (w tym wykresów i schematów), zamieszczonych w pracy, które w sposób bardzo klarowny i przejrzysty prezentują informacje przekazywane odbiorcy dysertacji, co czyni przekaz jej treści komunikatywnym.
Wśród spostrzeżonych mankamentów należy wymienić takie nieprawidłowości, jak:
- nieuprawnione skróty myślowe np. „…bieżący stan w organizacjach…" s. 4 w. 5 od dołu", stan czego?
- użycie skrótu w tytułach lub podtytułach, np. po raz pierwszy wystąpił skrót „ZBI", s. 5 w. 1 od góry, "BI firmy…", s. 33, w. 1 od góry, „SZBI" s. 86 w. 3 od dołu bez ich objaśnienia. Stąd, albo w dysertacji powinien być załączony osobno wykaz skrótów, lub wszędzie tam, gdzie skrótu używa Autorka po raz pierwszy, musi się znaleźć jego pełne objaśnienie,
- wielokrotnie bł. interpunkcyjne – nadmiarowość przecinków np. s. 10, w. 11 od góry, s. 202, w. 1 od góry
- bł. stylistyczne i gramatyczne — „..Z znacznie…" a powinno być "… ze znacznie…", s. 10, w. 9. od dołu, „Z kolei słabością tej metody to kosztowne szkolenia…"– powinno być „Z kolei słabością tej metody są kosztowne szkolenia…" s. 89, w. 5 od góry, „…z wszystkich organizacjach…„ powinno być „…z wszystkich organizacji…" s. 163, 8 w. od dołu, tab. 1 „zakresu działań jednego podmiotu" a powinno być „…zakresu działań jednemu podmiotowi…", „…uczulając o…" a powinno być uczulając na…"– s. 164, w. 1 od góry,
- pisownia wyrazów z partykułą „nie" razem a nie osobno: „nie wprowadzenie" s. 3 w. 10 od dołu, „nie ujawnianiem", nie udostępnianiem", s. 163 w. 16 od góry, „..nie odpowiednio…", s. 165 w. 2 od góry, „…nie bagatelne…" s. 165, w. 1 od dołu, „…nie świadomie…"s. 167, w. 13 od dołu, rys. 67 „nie

zachowanie, rys. 69. „nie przestrzeganie", „nie podpisania" „…w skutek…" s. 172 w. 16. od dołu, „.. nie przestrzeganiem…", s.172 w. 1. od dołu, tab. 13 z.23 „nie podpisania",
- liczne błędy literowe, np. „..wynikającego z korzystania komputerów, sieci.." powinno być „…wynikającego z korzystania z komputerów, sieci", s. 41, w. 14 od dołu,
Przytaczane są niekiedy wielkości w procentach bez odniesienia liczby względnej do wielkości, którą opisują – są to nieuprawnione skróty, np. „…jedynie 27%...." s. 164 w. 4 od góry
- błędy pojęciowe np. jest „koniunktura, otoczenie, w którym obraca się organizacja…", s. 30, w. 2 od dołu, a powinno być „koniunktura, otoczenie, w którym funkcjonuje organizacja…" jest „…metodologii…", s. 221. , w. 9 od dołu, a powinno być „…metodyki…", bo metodologia jest nauką o metodach
- zdanie niezrozumiałe: „…ponadto z powodzeniem autorka pracy weszła na teren organizacji niezidentyfikowanym…" s. 181, w.11-12 od dołu
Z uwagi na, z jednej strony, zauważone błędy językowe, ale z drugiej strony na bardzo starannie opracowaną stronę graficzną pracy, całość dysertacji pod względem formalnym oceniam na poziomie zadawalającym.

Podsumowanie

Uwzględniając wszystkie powyższe opinie, oceny i uwagi stwierdzam, że recenzowana rozprawa doktorska stanowi oryginalne rozwiązanie problemu naukowego, ponieważ rzeczywiście wypełnia w pewnym stopniu zdefiniowane luki poznawcze w zakresie zarządzania bezpieczeństwem informacji w przedsiębiorstwach. Autorka wykazała bardzo gruntowną ogólną wiedzę teoretyczną w dyscyplinie pn. „Nauki o zarządzaniu i jakości" oraz umiejętność samodzielnego prowadzenia pracy naukowej.

W mojej opinii dysertacja doktorska mgr inż. Estery Pietras pt. „Zarządzanie bezpieczeństwem informacji w przedsiębiorstwach branży motoryzacyjnej" napisanej pod kierunkiem dr hab. inż. Marcina Knapińskiego, prof. PCz spełnia wymagania stawiane rozprawom doktorskim określone w odnośnej ustawie.

Wnoszę, więc o jej przyjęcie przez Radę Dyscypliny Naukowej Nauki o Zarządzaniu i Jakości Wydziału Zarządzania Politechniki Częstochowskiej i dopuszczenie do publicznej obrony.

Bydgoszcz dn. 14. 02. 2022 r.

dr hab. inż. Waldemar Bojar, prof. PBŚ