Zeszyty Teoretyczne Rachunkowości
2021, Vol. 45, Nr 2, s. 31–50
http://dx.doi.org/10.5604/01.3001.0014.9558
Stowarzyszenie Księgowych w Polsce

Cyberbezpieczeństwo i cyberryzyko w raportach zintegrowanych i sprawozdaniach zarządu operatorów usług kluczowych

Cybersecurity and cyber risk in integrated and management reports of key service operators

ALEKSANDRA FERENS *

Streszczenie

Cel: Zakres interaktywnych informacji przetwarzanych i wymienianych w cyberprzestrzeni gwałtownie wzrósł. Istnieje zatem potrzeba zbudowania obszarów cyberbezpieczeństwa chroniących tę przestrzeń przed wewnętrznymi i zewnętrznymi zagrożeniami, a także opracowanie odpowiedniego systemu raportującego model cyberbezpieczeństwa funkcjonujący w firmie. Celem artykułu jest identyfikacja i ocena zakresu ujawnień na temat cyberbezpieczeństwa i cyberryzyka w raportach zintegrowanych i sprawozdaniach zarządu wybranych spółek notowanych na GPW w Warszawie.

Metodyka: Przedmiotem badania są raporty zintegrowane oraz sprawozdania zarządu 17 wybranych spółek należących do branż wskazanych w ustawie o krajowym systemie cyberbezpieczeństwa jako operatorów usług kluczowych. Przy wyborze próby reprezentatywnej zastosowano dobór celowy. Był on poprzedzony wstępną analizą spółek wchodzących do indeksu WIG-30, co do liczby sporządzanych raportów zintegrowanych wśród operatorów usług kluczowych. W badaniach wykorzystano metodę analizy literatury, regulacji prawnych, dedukcji, analizę struktury i zakresu raportowanych informacji o cyberbezpieczeństwie.

Wyniki: Przeprowadzone analizy pokazały, że ujawnienia dotyczące cyberryzyka i cyberbezpieczeństwa w badanych przedsiębiorstwach są stosunkowo niewielkie, informacje te są rozproszone w różnych częściach sprawozdań biznesowych, a także nieporównywalne ze względu na brak jednolitej struktury danych. Ponadto wykazano, że raporty nie zawierają szczegółowych informacji o prowadzonych działaniach z zakresu cyberbezpieczeństwa, co uniemożliwia dokonanie wieloaspektowej i wielosektorowej oceny jednostki raportującej.

Oryginalność: Artykuł uzupełnia dorobek naukowy z zakresu raportowania niefinansowego, identyfikując braki związane z raportowaniem sposobu zabezpieczenia się przed ryzykiem związanym z cyberzagrożeniami w dotychczas sporządzanych raportach, a także potwierdza potrzebę doskonalenia zawartości raportów biznesowych o informacje ilościowe i jakościowe w tym zakresie.

Słowa kluczowe: cyberbezpieczeństwo, cyberryzyko, model biznesu, bezpieczeństwo informatyczne.

* Dr Aleksandra Ferens, adiunkt, Uniwersytet Ekonomiczny w Katowicach, Katedra Rachunkowości, https://orcid.org/000-0003-2346-9904, aleksandra.ferens@ue.katowice.pl

ISSN 1641-4381 *print* / ISSN 2391-677X *online*

http://www.ztr.skwp.pl

Abstract

Purpose: The scope of interactive information processed and exchanged through cyberspace has grown exponentially. Therefore, there is a need to develop cybersecurity that protects this space against both internal and external threats, as well as to work out an appropriate reporting system on the cybersecurity model operating in the company. The aim of the paper is to identify and assess the disclosures on cybersecurity and cyber risk in the integrated and management reports of selected companies listed on the Warsaw Stock Exchange.

Methodology: The study focused on the integrated and management reports of 17 selected companies identified as operators of so-called key services. The representative sample was chosen through purposive sampling. This process was preceded by a preliminary analysis of companies listed in the WIG 30 Index, drawing on the number of integrated reports prepared by the operators of key services. The research involved an analysis of the literature and legal regulations, as well as the structure and scope of information on cybersecurity reported by the surveyed companies, along with the deductive method.

The results of the analysis showed that only some companies present information on existing cyber risks and cybersecurity, while information is scattered in different parts of the business reports and non-comparable due to the lack of a unified data structure. It was noted that the reports do not contain detailed information on the activities in the field of cybersecurity, which makes it impossible to perform a multifaceted and multisectoral assessment of the results reported by the entities.

Originality: The paper builds on and thus complements the scientific achievements in the field of non-financial reporting, including the business model, by identifying the shortcomings related to reporting on how to protect companies against the risk related to cyber threats in the reports to date. The study also confirms the need to improve the content of business reports with quantitative and qualitative information in this regard.

Keywords: cybersecurity, cyber risk, business model, IT security.

Wstęp

Panująca obecnie sytuacja na międzynarodowych rynkach związana z rozbudową nowoczesnych technologii wymaga od przedsiębiorstw nieustannego rozwoju przejawiającego się w szybkim pozyskiwaniu i wdrażaniu zdobytej wiedzy. Zakres interaktywnych informacji przetwarzanych i wymienianych w cyberprzestrzeni jest tak duży i coraz bardziej zależny od sieciowych systemów komputerowych, że coraz liczniejsza grupa podmiotów postrzega kwestie bezpieczeństwa cybernetycznego za wyjątkowo istotne. Zagadnienia cyberataku i cyberbezpieczeństwa skupiają uwagę najwyższych szczebli organizacji rządowych, branżowych, wojskowych, organów regulacyjnych, którzy upatrują w wychwyceniu i przejęciu ważnych informacji duże zagrożenie. Organizacje są pod presją, aby wykazać, że zarządzają zagrożeniami dla zapewnienia cyberbezpieczeństwa oraz dysponują skutecznymi procesami kontrolnymi w celu wykrywania naruszeń i innych zdarzeń związanych z bezpieczeństwem, reagowania na nie, łagodzenia ich i odzyskiwania (Janvrin, Wang, 2019).

W systemach informacyjnych rachunkowości organizacji są zbierane, przetwarzane i przechowywane szerokie i unikatowe zbiory danych. Duża część z nich to informacje finansowe, dane osobowe, a także inne rodzaje informacji stanowiących tzw. informacje wrażliwe, w przypadku których ujawnienie mogłoby mieć negatywne konsekwencje (De Groot, 2020). Także zapewnienie bezpieczeństwa realizowanych procesów operacyjnych w cyberprzestrzeni przez różne przedsiębiorstwa, a w szczególności operatorów usług kluczowych, jest priorytetem dla tych jednostek. W związku z powyższym kadra kierownicza jest mocno zainteresowana zapewnieniem bezpieczeństwa informacji przesyłanych za pośrednictwem dowolnej sieci i innych urządzeń teleinformatycznych.

W praktyce istnieje wiele strategii i metod kontroli bezpieczeństwa danych, które firmy wdrażają w celu zmniejszenia prawdopodobieństwa ataku na systemy informatyczne funkcjonujące w jednostkach gospodarczych. Ich celem jest przede wszystkim ochrona poufnych informacji biznesowych tworzonych w systemie informacyjnym rachunkowości przesyłanych przez sieci i inne urządzenia. Zagrożenie spowodowane cyberatakiem może pojawić się na etapie realizacji podstawowych procesów operacyjnych, wprowadzania, przetwarzania, transferu i archiwizacji informacji. Wyzwaniem dla jednostek gospodarczych jest zatem wprowadzenie skutecznego systemu zabezpieczeń, które należy uwzględnić w modelu biznesowym organizacji umożliwiającym zrozumienie logiki biznesu oraz infrastruktury niezbędnej do operacjonalizacji tej koncepcji (Lambert, 2008, s. 282). Przedsiębiorstwa wchodzące lub uczestniczące w transformacji cyfrowej budują swoje modele biznesowe opierając się na nowoczesnych technologiach, dlatego uważa się za konieczne kompleksowe podejście do cyberbezpieczeństwa i wpisanie tego aspektu w model biznesu. Także organizacja National Cyber Security Alliance zaleca podejście odgórne do cyberbezpieczeństwa, w którym kierownictwo korporacji kieruje priorytetem zarządzania cyberbezpieczeństwem we wszystkich praktykach biznesowych.

Takie podejście wymaga kompleksowego ujęcia cyberbezpieczeństwa, które obejmować powinno nie tylko strategię przedsiębiorstwa, ale także jej skuteczne wdrożenie oraz monitoring ryzyka. Istnieje zatem konieczność zidentyfikowania obszarów w największym stopniu podatnych na czynniki ryzyka. Po dokonaniu szacowania i oceny cyberryzyka należy opracować i wdrożyć model zarządzania tym ryzykiem oraz zaprezentować podjęte działania w raportach biznesowych.

Celem artykułu jest identyfikacja i ocena zakresu ujawnień na temat cyberryzyka i cyberbezpieczeństwa w raportach zintegrowanych i sprawozdaniach zarządu spółek notowanych na GPW w Warszawie. Przedmiotem badania były raporty zintegrowane oraz sprawozdania zarządu celowo wybranych 17 spółek należących do branż wskazanych jako operatorzy usług kluczowych w ustawie o krajowym systemie cyberbezpieczeństwa (Ustawa o krajowym systemie, 2018) za lata 2017, 2018 i 2019. Przy wyborze próby reprezentatywnej zastosowano dobór celowy, który był poprzedzony wstępną analizą ilościową sporządzanych raportów zintegrowanych wśród operatorów usług kluczowych. Wśród spółek notowanych na giełdzie

z indeksu WIG-30 najwięcej raportów publikowały spółki branż: energetycznej, paliwowej, telekomunikacyjnej. Należy zaznaczyć, że artykuł ma także pewne ograniczenia związane z odnoszeniem wniosków do wszystkich spółek uznanych przez ustawodawcę za operatorów usług kluczowych.

Artykuł uzupełnia dorobek naukowy z zakresu raportowania niefinansowego, obejmujący model biznesowy, identyfikując braki związane z raportowaniem sposobu zabezpieczenia się przed ryzykiem związanym z cyberatakami. W badaniach wykorzystano metodę analizy: literatury, regulacji prawnych, struktury i zakresu raportowanych przez badane spółki informacji o cyberbezpieczeństwie, metodę dedukcji.

1. Zarys definicyjny cyberbezpieczeństwa

Ogólnoświatowa wymiana informacji realizowana poprzez nowoczesne techniki komputerowe, głównie sieć internetu jest łatwo osiągalną przestrzenią i najszybszym sposobem komunikacji. Temat cyberprzestrzeni oraz zagrożeń z nią związanych znany jest od momentu pojawienia się internetu, o czym świadczą liczne badania zagranicznych i polskich autorów, np.: T. Bass (2000), K.J. Knapp i in. (2009), S.W. Brenner (2010); R. Ottis, P. Lorents (2010), K.T. Smith i in. (2011), D.S. Reveron (2012), L.B.A. Rabai i in (2013); A. Rot, Olszewski B. (2017). W Polsce również od ponad 20 lat publikowane są opracowania na ten temat, np.: A. Suchorzewska (2010); M. Grzelak, K. Lieder (2012); J. Wasilewski (2013), J. Kowalewski, M. Kowalewski (2014).

Termin cyberprzestrzeń, w ostatnich latach, został użyty i zdefiniowany w literaturze i regulacjach prawnych wielu państw, a także Unii Europejskiej. W zależności od dziedziny nauki cyberprzestrzeń jest inaczej interpretowana, inne spojrzenie przedstawiają nauki techniczne, jeszcze inne nauki społeczne, socjologiczne czy psychologiczne (Marczyk, 2018, s. 60). Wiele kontrowersji i problemów sprawia sama definicja pojęcia *cyber*, którą można podzielić na pięć obszarów: 1) infrastruktura fizyczna; 2) komunikacja; 3) system; 4) urządzenia i 5) środowisko wirtualne (Azmi, Kautsarina, 2020).

W jednej z pierwszych definicji cyberprzestrzeni, wprowadzonej przez Williama Gibsona w powieści *science fiction*, określana była jako „Konsensualna halucynacja doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych […]. Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność... Świetlne linie przebiegające bezprzestrzeń umysłu, skupiska i konstelacje danych" (cyt. za: Wasilewski 2013, s. 226). Można stwierdzić, że w definicji tej zostały zaakcentowane podstawowe elementy cyberprzestrzeni, takie jak:

- ludzka percepcja nowego środowiska;
- rozległość (zasięg światowy);
- rzeczywistość wirtualna;

- przestrzeń informacyjna;
- potencjał do stworzenia nowego doświadczenia;
- spajanie wszelkich zasobów w jedną, olbrzymią całość;
- wielowymiarowość, złożoność;
- bezprzestrzenność rozumianą jako brak możliwości odniesienia cyberprzestrzeni do fizycznych (w tym geograficznych) wymiarów realnego świata.

Departament Obrony Stanów Zjednoczonych w stworzonym słowniku terminologii wojskowej (*DOD Dictionary*, 2020) traktuje wąsko cyberprzestrzeń i odnosi ją do infrastruktury sprzętowej i systemów wspomagających „cyberprzestrzeń to domena globalna w środowisku informacyjnym składająca się z współzależnej sieci infrastruktur technologii informacyjnej, w tym internetu, sieci telekomunikacyjnych, systemów komputerowych i oraz systemy kierujące procesami produkcji i kontroli w sektorach strategicznych dla bezpieczeństwa narodowego". Charakterystyczną cechą tej definicji jest zauważalny brak czynnika ludzkiego, będącego użytkownikiem cyberprzestrzeni, który jest kluczowym elementem dla innych autorów. Podkreśla się natomiast globalny zasięg, a także powiązanie infrastrukturalne łączące różne sieci.

Dynamiczny charakter cyberprzestrzeni i interakcje z czynnikiem ludzkim można zauważyć w propozycji pojęcia R. Ottisa i P. Lorentsa (2010, s. 267), według których cyberprzestrzeń to zależny od czasu zbiór wzajemnie połączonych systemów informatycznych (sprzęt, oprogramowanie, media) i ludzi, którzy wchodzą w interakcję z tymi systemami. Według autorów człowiek pozostaje ważną częścią cyberprzestrzeni, bez którego popadłaby w stagnację i w rezultacie przestałaby istnieć.

W Polsce definicję cyberprzestrzeni wprowadzono w Rządowym Programie Ochrony Cyberprzestrzeni na lata 2011–2016 (Rządowy Program, 2010): „cyberprzestrzeń to przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". Na szczególną uwagę zwrócono w tej definicji na relacje z użytkownikami, które dotyczą różnych obszarów działania przedsiębiorstwa i są narażone na niewłaściwe ich użycie.

Globalny zasięg, potencjał do stworzenia nowego doświadczenia, bezprzestrzenność zauważyć można w definicji M. Marczyka (2018, s. 59), według którego cyberprzestrzeń jest m.in. przestrzenią komunikacyjną tworzoną przez systemy powiązań internetowych. Pozwala jej użytkownikom na komunikację, wymianę informacji za pomocą sieci i systemów komputerowych, nawiązywanie relacji w czasie rzeczywistym, a także wymiarem aktywności, w której wszelkie działania odbiegają charakterem od środowiska fizycznego. Definicja ta jest zbieżna z cybernetycznym ujęciem cyberprzestrzeni, które definiuje ją jako przestrzeń otwartej komunikacji, gdzie sprzężenie zwrotne informacji pozwala na regulację systemów, zachodzenie relacji między nimi oraz dynamiczny rozwój i wytyczanie nowych szlaków (Konieczny, 2012, s. 59).

Kontekst wymiany, gromadzenia i udostępniania informacji oraz nawiązanie do poglądu Gibsona akcentują także w swojej definicji W. Gogołek i W. Cetera

(2014), według których cyberprzestrzeń to iluzja świata rzeczywistego stworzona za pomocą metod teleinformatycznych. Ułatwia wymianę, gromadzenie i udostępnianie informacji za pośrednictwem komputerów oraz komunikację między człowiekiem i komputerem. Definicja ta podkreśla interaktywność istniejącą między informacją – człowiekiem i technologią, która powoduje, że cyberprzestrzeń dla swoich użytkowników jest nie tylko źródłem informacji, lecz także obszarem podlegającym kształtowaniu przez swoich odbiorców (Wasilewski, 2013). W psychologii pojęcie cyberprzestrzeni utożsamiane jest z wirtualną rzeczywistością, jako przestrzeń zapośredniczona w kontekście technologii informacyjnej, w której obecne są wirtualne byty, niedostępne dla człowieka w ich cyfrowym abstrakcyjnym wymiarze, zobrazowane poprzez interfejs w formie dostrzeganej wszelkimi zmysłami poprzez dźwięk lub obraz (Konieczny 2012, podano za: Marczyk 2018, s. 61). Przyjęcie określonych cech charakterystycznych dla cyberprzestrzeni oraz jego „kontekst" prezentujący zależności od splotu innych zdarzeń, wywiera wpływ na sposób wyznaczenia zakresu przedmiotowego obszaru bezpieczeństwa cyberprzestrzeni.

W kontekście definicji cyberprzestrzeni obejmującej przestrzeń wirtualną (zawarte w systemach dane, pliki, strony internetowe, aplikacje, procesy realizowane przez systemy teleinformatyczne) oraz relacje pomiędzy jej użytkownikami należy, zdaniem autorki, bezpieczeństwem cyberprzestrzeni objąć wszystko, co w tej przestrzeni się dzieje. Cyberprzestrzeń stała się podstawową cechą świata i stworzyła nową rzeczywistość dla prawie wszystkich krajów, co sprawia, że problemy z cyberprzestępczością oraz cyberbezpieczeństwem mają istotne, globalne znaczenie zarówno w wymiarze politycznym, gospodarczym, jak i ekonomicznym (Dębowski, Wrocławski, 2018). Z badania PwC wynika, że w poprzednim roku w wyniku cyberataków straty finansowe poniosło 44% polskich przedsiębiorstw, a 62% odnotowało zakłócenia i przestoje w funkcjonowaniu. Analiza ekspertów PwC pokazała dodatkowo, że jedynie 8% polskich firm jest dojrzała pod względem bezpieczeństwa cybernetycznego (Urban, 2018). Ze statystyk za 2020 rok wynika natomiast, że stwierdzonych przestępstw dotyczących cyberbezpieczeństwa było niemal 55 tys. (Business Insider). Cyberprzestrzeń to zatem duże możliwości, ale też i ryzyko.

Istnieje wiele publikacji i opracowań opisujących cyberryzyko. Nie ma jednak jednoznacznej jego definicji, dlatego należy, zdaniem autorki, to pojęcie rozpatrywać kontekstowo, co związane jest z faktem, że pojęcie ryzyka również można rozpatrywać z kilku perspektyw. Przeglądu definicji cyberryzyka dokonali C. Biener i in. (2015), z którego wynika, że w wąski sposób ujmują cyberryzyko A. Mukhopadhycy i in. (2013), według których ryzyko cybernetyczne to ryzyko wystąpienia złośliwych zdarzeń elektronicznych, które powodują zakłócenia w biznesie i straty pieniężne. Z perspektywy zarządzania ryzykiem finansowym zdefiniowali cyberryzyko F. Curti i in. (2019). Według tych autorów jest to forma ryzyka operacyjnego związanego głównie z ponoszeniem straty wynikającej z incydentów cyfrowych spowodowanych przez osoby wewnętrzne, zewnętrzne lub trzecie, w tym kradzież, naruszenie integralności i/lub uszkodzenie informacji oraz/lub zasoby technologiczne, wewnętrzne oraz oszustwa zewnętrzne i zakłócenia działalności.

Z perspektywy rynków ubezpieczeniowych i finansowych zdefiniowali cyberryzyko Biener i in. (2015). Cyberryzyko to ryzyko operacyjne, odnoszące się do zasobów informacyjnych i technologicznych, które mają konsekwencje wpływające na poufność, dostępność lub integralność informacji lub systemów informatycznych. Autorzy ci podzielili cyberryzyko na cztery grupy: działania ludzi, awarie systemów i technologii, nieudane procesy wewnętrzne oraz zdarzenia zewnętrzne. Biorąc pod uwagę szerokie ujęcie cyberryzyka zaprezentowane przez Bienera i in., fakt, że pojęcie „cyber" jest używane także jako skrót słowa cyberprzestrzeń oraz uwzględniając pojęcie ryzyka zaprezentowanego w ustawie o krajowym systemie cyberbezpieczeństwa[1], proponuje się na potrzeby niniejszego artykułu cyberryzykiem określić kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego odnoszącego się do zasobów informacyjnych i technologicznych, które mają szerokie konsekwencje dla funkcjonowania organizacji oraz pozostałych interesariuszy zewnętrznych i wewnętrznych.

Pojęcie cyberbezpieczeństwa ze względu na swoją pojemność i multidyscyplinarność jest różnie definiowane w literaturze przedmiotu (Schatz i in., 2017, s. 53–74). Czasami zamiennie używa się określenia bezpieczeństwo komputera, internetu, systemów, technologii informacyjnej (von Solms, van Niekerk, 2013, s. 101). Zależy także w dużej mierze od kontekstu, czyli okoliczności, które tworzą otoczenie wydarzenia, stwierdzenia lub idei i pod kątem których można je w pełni zrozumieć i ocenić.

Pojęcie cyberbezpieczeństwa wywodzi się z anglojęzycznego terminu *cybersecurity*, oznacza całokształt działań podejmowanych w celu urzeczywistnienia postulowanego stanu, w którym ryzyka grożące operacjom dokonywanym w cyberprzestrzeni są możliwie zminimalizowane (Cybersecurity & Infrastructure, 2009). Definicją wyznaczającą zakres cyberbezpieczeństwa oraz jej połączenie z cyberprzestrzenią prezentują L. Yang i in. (2019, s. 179), według których cyberbezpieczeństwo to ochrona samej cyberprzestrzeni, tzn. informacje elektroniczne, technologie informacyjno-komunikacyjne wspierające cyberprzestrzeń oraz użytkowników cyberprzestrzeni w zakresie ich osobistych, społecznych i krajowych możliwości, w tym ich interesów, materialnych lub niematerialnych, którzy są podatni na ataki z cyberprzestrzeni.

W sposób użyteczny ujmowane jest cyberbezpieczeństwo w ustawie o krajowym systemie cyberbezpieczeństwa[2], zgodnie z którą cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

[1] Ustawa o krajowym systemie cyberbezpieczeństwa definiuje ryzyko jako kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji.

[2] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2020 poz.1369.

Cyberbezpieczeństwo w odniesieniu do operatorów usług kluczowych[3] to zatem szeroka lista działań, które muszą być podjęte w celu ochrony danych, procesów, zasobów oferowanych przez systemy informacyjne. Zdaniem autorki, zakres koniecznych działań, które należy podjąć, dotyczy m.in. następujących kwestii:

- techniczno-organizacyjnych związanych z urządzeniami teleinformatycznymi;
- prawnymi;
- etycznymi;
- edukacyjnymi;
- organizacyjno-zarządczymi;
- monitorującymi.

Wybrane przykłady odnoszące się do powyższych zadań zawarte w ustawie o krajowym systemie cyberbezpieczeństwa zawiera tabela 1.

Tabela 1. Przykładowe działania z zakresu cyberbezpieczeństwa

Rodzaj działań	**Zakres podjętych działań**
Techniczo-organizacyjne	Wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym: • utrzymanie i bezpieczna eksploatacja systemu informacyjnego, • bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu, • bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej, • dbałość o aktualizację oprogramowania, • ochrona przed nieuprawnioną modyfikacją w systemie informacyjnym
Prawne	• wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej, • opracowanie i aktualizacja dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej
Etyczne, prewencyjne	• stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym: stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym, • oznaczenie informacji stanowiących tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa

[3] Operatorem usługi kluczowej jest podmiot, o którym mowa w załączniku nr 1 do ustawy, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej. Sektory, podsektory oraz rodzaje podmiotów określa załącznik nr 1 do ustawy.

cd. tab. 1

Rodzaj działań	Zakres podjętych działań
Edukacyjne	• zapewnienie dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową, w szczególności przez publikowanie informacji na ten temat na stronie internetowej
Organizacyjno-zarządcze	• wdrożenie systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, • zarządzanie incydentami, • wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami Krajowego systemu cyberbezpieczeństwa
Monitorujące	• prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem, • objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym, • zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, • przekazywanie organowi właściwemu do spraw cyberbezpieczeństwa danych, o których mowa w art. 7 ust. 2 pkt 8 i 9

Źródło: opracowanie własne na podstawie (Ustawa o krajowym systemie, art. 8–13).

Na podstawie zaprezentowanych działań można stwierdzić, że cyberbezpieczeństwo to zbiór zasobów, technologii, działań, procesów i praktyk zaprojektowanych w celu ochrony cyberprzestrzeni – sieci, urządzeń, programów i systemów przed zdarzeniami (atak, uszkodzenie, nieautoryzowany dostęp), które są niezgodne z faktycznymi prawami własności. Definicja ta powinna mieć bezpośrednie przełożenie na budowę systemu bezpieczeństwa w rachunkowości, który jest najważniejszym systemem informacyjnym dla każdego menedżera, wspieranym przez nowoczesne technologie informatyczne. Systemy teleinformatyczne związane z obsługą procesów operacyjnych, finansowo-księgowych przetwarzające dane szczególnie wrażliwe dla menedżerów powinny być chronione nie tylko na ataki z zewnątrz, ale także z wewnątrz. Aby skutecznie przeciwdziałać możliwym zagrożeniom, kierownictwo podmiotu musi podejmować określone działania zapewniające cyberbezpieczeństwo, czyli opracować i wdrożyć odpowiedni system zapewniający bezpieczeństwo informacji korporacyjnej, uwzględniający aktualne wymogi prawne oraz potrzeby podmiotu w tym zakresie. Z tego powodu niezwykle ważny jest wielopoziomowy system zabezpieczeń danych, który powinien być wpisany we wszystkich szczeblach (poziomach) modelu biznesowego firmy. Jednak, aby dobrze zaplanować działania zabezpieczające potrzebne są informacje kontekstowe, które umożliwią wgląd w okoliczności zdarzenia, a następnie wychwycenie i poprawną klasyfikację tego zdarzenia jako incydentu.

2. Cyberbezpieczeństwo w raportach biznesowych przedsiębiorstw

Rolę promującą oraz wspierającą inicjatywę w zakresie realizowanych działań z zakresu cyberbezpieczeństwa ma informacja z tego zakresu, która powinna być prezentowana w raportach biznesowych jednostek gospodarczych. Według E. Walińskiej (2013) istotny dla wszystkich menedżerów raport biznesowy może przybierać następującą formę:

- sprawozdanie finansowe rozszerzone o inne raporty;
- raport zintegrowany zawierający wybrane dane ze sprawozdań finansowych;
- raport zintegrowany składający się z dwóch odrębnych części: sprawozdania finansowego i pozostałych informacji biznesowych.

Zdaniem autorki szczególne znaczenie w prezentowaniu cyberbezpieczeństwa i cyberryzka powinien mieć raport zintegrowany, którego rola polega na wyraźnym i zwięzłym komunikowaniu o tym, w jaki sposób strategia organizacji, przyjęty system zarządzania, wyniki działalności i perspektywy – wraz z czynnikami zewnętrznymi środowiska – prowadzą do tworzenia wartości organizacji w perspektywie krótko-, średnio- i długoterminowej. Poza tym łączy on sprawozdanie finansowe i niefinansowe w jeden raport, co pozwala na wyeliminowanie różnic sprawozdawczych w spółkach, które sporządzają sprawozdanie według ustawy o rachunkowości, jak i te, które sporządzają go według MSR/MSSRF. Informacje w tym raporcie powinny być sformułowane pod kątem wpływu na przyszłe tworzenie wartości, które prezentuje zarówno aspekty ekonomiczne, jak i społeczne i środowiskowe (Stubbs, Higgins, 2014, s. 3). W strukturze ramowej podkreśla się, że „raportowanie zintegrowane ma być efektem zintegrowanego myślenia, polegającym na aktywnym rozpatrywaniu przez organizację zależności/relacji pomiędzy jej różnymi komórkami operacyjnymi i finansowymi oraz kapitałami, jakie organizacja wykorzystuje lub na które wpływa" (IIRC, 2013, s. 2). Zgodnie z propozycją zawartości raportu zintegrowanego uważa się, że sposób zabezpieczenia się jednostki przed cyberzagrożeniami może być opisany w różnych częściach raportu zintegrowanego (tab. 2).

Tabela 2. Elementy raportu zintegrowanego

Elementy raportu zintegrowanego	Charakterystyka
Informacje ogólne o organizacji i otoczeniu zewnętrznym	Co organizacja robi, czym się zajmuje i w jakich warunkach funkcjonuje? Czy jest narażona na ataki w cyberprzestrzeni?
Ład korporacyjny	W jaki sposób nadzór korporacyjny wspiera zdolność organizacji do tworzenia wartości w krótkim, średnim i długim okresie także w odniesieniu do cyberzagrożeń?
Model biznesu	Jaki jest model biznesowy organizacji? Czy uwzględnia aspekty cyberbezpieczeństwa?
Szanse i zagrożenia	Czy istnieje ryzyko cyberbezpieczeństwa i jakie są szanse, które wpłyną na zdolność organizacji do tworzenia wartości w krótkim, średnim i długim okresie?

cd. tab. 2

Elementy raportu zintegrowanego	Charakterystyka
Strategia i alokacja zasobów	Dokąd organizacja zmierza? Czy uwzględnia aspekty cyberbezpieczeństwa?
Dokonania	W jakim stopniu organizacja chce osiągnąć swoje cele strategiczne i jakie są jej wyniki w zakresie realizacji i wpływu na kapitały z uwzględnieniem cyberzagrożeń?
Perspektywy	Jakie wyzwania i niepewności może napotkać organizacja w realizacji strategii także tej dotyczącej cyberbezpieczeństwa i jakie są potencjalne implikacje dla jej modelu biznesowego i przyszłych wyników?
Podstawa sporządzenia i prezentacji	W jaki sposób organizacja określa, jakie kwestie należy uwzględnić w zintegrowanym raporcie i jak kwantyfikuje lub ocenia kwestie cyberbezpieczeństwa?

Źródło: opracowanie własne na podstawie IIRC (2013, s. 5).

Jak wynika z treści zaprezentowanej tabeli, informacje o prowadzonych działaniach z zakresu cyberbezpieczeństwa mogą pojawiać się w różnych częściach tego sprawozdania prezentując w sposób kompleksowy realizowane działania. Uważa się, że działania zabezpieczające przed cyberzagrożeniami mogą być opisane także w sprawozdaniu zarządu i obejmować informacje m.in. o:

1) zdarzeniach istotnie wpływających na działalność jednostki, jakie nastąpiły w roku obrotowym, a także po jego zakończeniu, do dnia zatwierdzenia sprawozdania finansowego;
2) przewidywanym rozwoju jednostki;
3) ważniejszych osiągnięciach w dziedzinie badań i rozwoju;
4) instrumentach finansowych w zakresie ryzyka (zmiany cen, ryzyka kredytowego, istotnych zakłóceń przepływów środków pieniężnych oraz utraty płynności finansowej, na jakie narażona jest jednostka).

Działania z zakresu cyberbezpieczeństwa wpisują się zatem w każdy z tych punktów.

3. Założenia metodyczne analizy raportów zintegrowanych i sprawozdań zarządu związane z cyberbezpieczeństwem

W celu zidentyfikowania ujawnień na temat cyberbezpieczeństwa w raportach biznesowych autorka przeanalizowała treść raportów zintegrowanych (RI) i sprawozdań zarządu (SZ) publikowanych przez spółki branży energetycznej, paliwowej, telekomunikacyjnej, notowane na GPW w ramach indeksu WIG Energia, WIG Paliwa i WIG Telekomunikacja za lata 2017–2019. Wybór tych sektorów podyktowany był największą liczebnością raportów zintegrowanych wśród spółek

notowanych na giełdzie z indeksu WIG-30. Dodatkowym argumentem przemawiającym za wyborem tych przedsiębiorstw był fakt, że branże te należą obecnie do tzw. operatorów usług kluczowych, które po spełnieniu określonych zasad obejmują przepisy ustawy o krajowym cyberbezpieczeństwie, (2018). Wybrane przykładowe ujawnienia dotyczące cyberryzyka i cyberbezpieczeństwa zidentyfikowane przez autorkę w raportach zintegrowanych i sprawozdaniach zarządu przedsiębiorstwach branży energetycznej, paliwowej i telekomunikacyjnej przedstawiono w tabeli 3.

Tabela 3. Ujawnienia dotyczące cyberryzyka i cyberbezpieczeństwa w przedsiębiorstwach branży energetycznej, paliwowej, telekomunikacyjnej w latach 2017–2019

Przedsiębiorstwo	**Kategoria ujawnień na temat cyberryzyka**	**Treść ujawnień na temat cyberbezpieczeństwa/ podjęte działania**	**Miejsce ujawnień**
Enea	Wyszczególnienie kategorii cyberryzyka: ryzyko utraty dostępności systemów bilingowych, ryzyko ataku na infrastrukturę informatyczną, ryzyko utraty ciągłości działania środowisk i infrastruktury teleinformatycznej, ryzyko braku łączności z siecią Internet	Przewiduje się dalsze doskonalenie systemu bezpieczeństwa teleinformatycznego i jego dostosowanie do nowych przepisów prawa, w szczególności do wymogów ustawy o krajowym systemie cyberbezpieczeństwa. Jednym z ważnych obszarów tego doskonalenia jest rozwój procesów reagowania na incydenty z zakresu bezpieczeństwa teleinformatycznego, jako niezwykle istotnego elementu zapewnienia ciągłości działania usług świadczonych dla Klientów. Podjęto działania związane z realizacją wymogów w zakresie analizy ryzyka w zakresie cyberbezpieczeństwa	SZ (ryzyka niefinansowe związane z działalnością)
Tauron	Zagrożenie: Rosnąca liczba cyberzagrożeń oraz infrastruktury podatnej na takie ataki	Uruchomienie projektu pn. Wdrożenie wymagań ustawy o krajowym systemie cyberbezpieczeństwa. Bezpieczeństwo: szczególny nacisk kładziemy na bezpieczeństwo przetwarzania danych osobowych w systemach IT, implementując narzędzia i procedury zwiększenia cyberbezpieczeństwa. Wdrażamy i aktualizujemy procedury, optymalizując bezpieczeństwo danych osobowych oraz szkolimy personel w tym zakresie	RZ (szanse i zagrożenia) SZ (szanse i zagrożenia)

cd. tab. 3

Przedsiębiorstwo	Kategoria ujawnień na temat cyberryzyka	Treść ujawnień na temat cyberbezpieczeństwa/ podjęte działania	Miejsce ujawnień
Energa	Ryzyko niedostosowania Grupy do nowych przepisów prawa	Utworzenie Grupy Roboczej ds. dostosowania działań Grupy do przepisów prawa (m.in. ceny cyberbezpieczeństwa). Podjęto działania związane z realizacją wymogów w zakresie analizy ryzyka w zakresie cyberbezpieczeństwa	SZ (zarządzanie ryzykiem)
Będzin	brak	brak	brak
Kogeneracja	brak	Działania: • zapewnienie odpowiedniego procesu identyfikacji i reakcji na zagrożenia związane z cyberbezpieczeństwem, • wymiana dobrych praktyk, • opracowanie i wdrożenie odpowiednich procedur, • zastosowanie odpowiednich zabezpieczeń IT oraz OT	SZ (czynniki ryzyka i działania mitygujące) Ryzyka regulacyjno-prawne
ML System	brak	brak	brak
Polenergia	brak	brak	brak
PGE	brak	Cyberbezpieczeństwo – ryzyko celowego zakłócenia prawidłowego funkcjonowania aktywów wytwórczych i dystrybucyjnych oraz systemów informatycznych funkcjonujących w GK PGE	SZ, RZ (ryzyko strategiczne)
ZEPAK	brak	brak	brak
Lotos	Ryzyko systemów IT: Zewnętrzna lub wewnętrzna ingerencja (cyberatak) w systemy informatyczne (IT) i sterowania (OT) oraz awarie w wyniku braku wystarczających zasobów i nieefektywnych procesów w obszarze IT	Implementacja wymagań ustawy o krajowym systemie cyberbezpieczeństwa: • audyty bezpieczeństwa IT, • procedury wewnętrzne dotyczące zarządzania bezpieczeństwem systemów, • regularne testy bezpieczeństwa infrastruktury teleinformatycznej, • podnoszenie świadomości pracowników w zakresie cyberbezpieczeństwa (szkolenia, informacje, testy), powołanie i rozwój Biura SOC (Security Operation Center)	SZ (ryzyko bezpieczeństwa)

cd. tab. 3

Przedsiębiorstwo	Kategoria ujawnień na temat cyberryzyka	Treść ujawnień na temat cyberbezpieczeństwa/ podjęte działania	Miejsce ujawnień
Orlen	brak	brak	brak
PGNIG	brak	brak	brak
SKOTAN	brak	brak	brak
UNIMOT	brak	brak	brak
Orange	Cyberryzyko – niedostępność infrastruktury informatyczno-sieciowej, narażenie na ataki cybernetyczne. Działalność Spółki może prowadzić do utraty, ujawnienia, upublicznienia, przekazania nieuprawnionym podmiotom bądź niewłaściwej modyfikacji danych osobowych klientów. Przyczyną takiej sytuacji mogą być między innymi czyny zabronione (w tym cyberataki), zwłaszcza mające na celu kradzież danych osobowych, bądź potencjalne zaniedbania ze strony Spółki lub jej kontrahentów.	Cyberbezpieczeństwo: • aplikacje IT, • platformy usługowe, • funkcje sieciowe, • wspólny transport IP, • sieci dostępowe. Utworzenie Centrum Bezpieczeństwa Operacyjnego (SOC). Wprowadzenie usługi bezpieczeństwa dla klientów indywidualnych (CyberTarcza) i biznesowych, która zablokowała ponad 2,5 mln prób zdalnej kontroli botnetów (Command & Control). Wprowadzenie CyberTarczy w wersji mobilnej. Zespół CERT (Computer Emergency Response Team) przez całą dobę reaguje na zagrożenia, jakie napotykają użytkownicy Internetu korzystający z sieci Orange Polska. Jednostka CERT Orange Polska wchodzi także w skład krajowego ekosystemu cyberbezpieczeństwa. Nabycie udziałów spółki BlueSoft Sp. z o.o. Podejmowanie działań mających na celu zapewnienie cyberbezpieczeństwa: • odpowiednie planowanie rozwoju sieci i systemów teleinformatycznych, inwestowanie we wdrażanie rozwiązań przewidzianych na wypadek awarii, programy ubezpieczeniowe obejmujące zakresem ryzyka cybernetyczne i terrorystyczne oraz wdrażanie planów ciągłości działania i zarządzania kryzysowego • posiadanie certyfikatu zgodności z normą ISO 22301:2012 dla Sys-	RZ (model biznesowy), SZ Kluczowe czynniki ryzyka, istotne zdarzenia Ryzyka wpływające na działalność operacyjną

cd. tab. 3

Przedsiębiorstwo	Kategoria ujawnień na temat cyberryzyka	Treść ujawnień na temat cyberbezpieczeństwa/ podjęte działania	Miejsce ujawnień
		temu Zarządzania Ciągłością Działania w zakresie świadczonych usług telekomunikacyjnych, teleinformatycznych i cyberbezpieczeństwa	
Cyfrowy Polsat	brak	• rozwój usług w zakresie cyberbezpieczeństwa, • szkolenia z zakresu cyberbezpieczeństwa, • nabycie pakietu akcji Asseco (wiodący producent oprogramowania)	SZ (działalność na rynku telekomunikacyjnym, najważniejsze inwestycje)
Netia	brak	Rozwój kompetencji oraz portfolio usług z zakresu cyberbezpieczeństwa. W ramach rozwoju sprzedaży powstała inicjatywa NetiaNext. Projekt ten ma na celu zbudowanie kompetencji integratorskich i poszerzenie portfolio sprzedażowego o usługi ICT szczególnie z zakresu IT i cyberbezpieczeństwa. Szczególny nacisk kładziony jest na rozwój następujących obszarów: 1. Cyberbezpieczeństwo – usługi dedykowanej ochrony zasobów klienta, m.in ochrona przed atakami na systemy komputerowe (DDoS), usługi kopii bezpieczeństwa danych (Backup as a Service), ochrona sieci IT za pomocą urządzeń firewall/UTM, usługi Security Operations Center	SZ (model biznesowy – strategia podejście do klienta)

Objaśnienia: SZ – sprawozdanie zarządu, RZ – raport zintegrowany.

Źródło: opracowanie własne.

Wśród 17 analizowanych spółek osiem nie zamieściło informacji odnośnie do cyberzagrożeń i cyberbezpieczeństwa (PGNIG, SKOTAN, UNIMOT, MLSystem, ZEPAK, Orlen, Polenergia, Będzin). Należy podkreślić, że spółki te deklarują realizację kontroli bezpieczeństwa i dostępności informacji zawartych w systemie finansowo-księgowym na wszystkich poziomach bazy danych, aplikacji oraz systemu operacyjnego, a także na integrację systemu, która zapewniona jest przez systemy kontroli wprowadzanych danych (walidacje, autoryzacje, listy wartości) oraz dzienniki zmian. Istotne dla tych spółek jest także zagwarantowanie bieżącej weryfikacji i aktualizacji ograniczeń praw dostępu oraz poziomu zabezpieczeń

hasłowych do systemu finansowo-księgowego, jak również obowiązujące w spółce procedury tworzenia kopii zapasowych i ich przechowywania. Jest to jednak wąskie ujęcie bezpieczeństwa informacji i systemów, brakuje bowiem bezpośredniego odniesienia do szeroko ujętego cyberryzyka i cyberzagrożeń. Kolejna spółka – PGE, wymienia co prawda cyberbezpieczeństwo jako element istniejącego ryzyka, ale nie podaje żadnych podjętych działań w tym zakresie

W sprawozdaniach zarządu w części dotyczącej przyjętych przez jednostkę celów i metod zarządzania ryzykiem cztery spółki: ENEA, Tauron, Lotos, Orange wyodrębniły kategorię cyberryzyka. Prezentowane przez nie informacje dotyczące cyberzagrożeń pozwalają ustalić zakres cyberryzyka, do którego zalicza się:

- cyberzagrożenia związane z infrastrukturą informatyczną, systemami sterowania;
- ryzyko utraty ciągłości działania środowisk;
- brak łączności z siecią Internet;
- kradzież lub przekazanie nieupoważnionym podmiotom danych osobowych klientów.

Wyniki pokazują, że dwa najczęściej ujawniane zagrożenia cyberbezpieczeństwa to ryzyko przerwania usług/operacji oraz ryzyko naruszenia danych, co potwierdza badanie dokonane przez Gao, Calderon, Tang (2020).

Można zatem stwierdzić, że wymienione spółki nie podchodzą w sposób interaktywny do cyberryzyka, ponieważ w swoich planowanych działaniach uwzględniają tylko wybrane aspekty, a powinny uwzględnić zarówno część technologiczną, operacyjną, jak i relacje z interesariuszami oraz wymianę informacji.

Tendencję wzrostową w zakresie prezentowanych informacji o cyberryzyku i cyberbezpieczeństwie podczas przeprowadzanej analizy sprawozdań można było zauważyć w roku 2019, co wiązać się może m.in. z wprowadzeniem w roku 2018 ustawy o krajowym cyberbezpieczeństwie obowiązującej większość operatorów usług kluczowych od roku 2019, a także wzrostem zainteresowania informacjami z tego zakresu przez interesariuszy zewnętrznych. Na aspekt ciągłego niedostatecznego dostosowania do wymogów nowych przepisów prawa zwracają jednak uwagę spółki Energa, Enea, natomiast spółki Tauron, Energa, Enea, Lotos podjęły konkretne działania w tym obszarze.

Prezentowane informacje o cyberbezpieczeństwie mają charakter jakościowy, a w realizacji strategii cyberbezpieczeństwa największe znaczenie nadaje się konieczności zapewnienia odpowiedniego procesu identyfikacji zagrożeń i rozwoju procesów i kompetencji reagowania na incydenty z zakresu cyberbezpieczeństwa, które jest podstawą zapewnienia ciągłości działania usług świadczonych dla klientów (Enea, Kogeneracja, Lotos, Netia, Cyfrowy Polsat, Orange). W realizacji cyberbezpieczeństwa niektóre z analizowanych spółek podjęły konkretne działania mające na celu nie tylko realizację wymogów ustawy, a także zapobiegnięcie możliwemu ryzyku. W tym celu spółka Lotos utworzyła m.in. Biuro Security Operation Center (SOC), które odpowiada za budowę centralnego systemu zgłaszania, monitorowania i koordynacji poważnych incydentów bezpieczeństwa, nadzoruje całokształt działań związanych z monitorowaniem, wykrywaniem oraz koordynacją

i obsługą incydentów bezpieczeństwa informacji w Grupie. Ponadto spółki podjęły następujące działania z zakresu cyberbezpieczeństwa:

- podnoszenie świadomości pracowników w zakresie cyberbezpieczeństwa (szkolenia, informacje, testy –Tauron, Cyfrowy Polsat, Lotos);
- wymianę dobrych praktyk (Kogeneracja);
- zastosowanie odpowiedniej jakości i poziomu zabezpieczeń systemów informacji (Kogeneracja, Lotos);
- audyty bezpieczeństwa IT;
- wprowadzenie procedur wewnętrznych dotyczących zarządzania bezpieczeństwem systemów (Lotos);
- regularne testy bezpieczeństwa infrastruktury teleinformatycznej (Lotos);
- działania optymalizujące bezpieczeństwo danych osobowych (Tauron).

Na szczególne uznanie zasługują działania spółki Cyfrowy Polsat, która w celu realizacji zasad cyberbezpieczeństwa wykupiła pakiety akcji w spółkach będących wiodącymi producentami oprogramowania z tego zakresu. Jedna ze spółek w ramach kategorii podejście do klienta podjęła natomiast decyzję o rozszerzeniu swojej oferty sprzedażowej o produkty mające zapewnić cyberbezpieczeństwo obejmujące m.in ochronę przed atakami na systemy komputerowe, usługi kopii bezpieczeństwa danych, ochronę sieci IT itp.

Podsumowanie

Tempo zmian technologiczno-informatycznych wymaga od przedsiębiorstw, aby nieustannie modyfikowały swoją dotychczasową strategię i podejmowały decyzje związane z poprawą jakości oferowanych usług, produktów, dające przewagę na konkurencyjnym rynku, co jest ściśle powiązane z zaufaniem do sposobu zarządzania bezpieczeństwem informacji i procesów. Istnieje zatem konieczność przyjęcia określonej sekwencji działań, których celem jest utworzenie indywidualnego modelu reagowania na incydenty z zakresu bezpieczeństwa teleinformatycznego i prezentowanie informacji z tego obszaru interesariuszom zewnętrznym.

Zagadnienie cyberbezpieczeństwa i cyberryzyka stanowi szczególne znaczenie dla jednostek będących operatorami usług kluczowych, których wpływ na prawidłowe funkcjonowanie państwa jest niezwykle silne. Przedstawione badania pokazały, że ujawnienia na temat cyberryzyka i cyberbezpieczeństwa w analizowanych przedsiębiorstwach są stosunkowo niewielkie, mimo że raporty zintegrowane i sprawozdania zarządu są bardzo obszerne.

Informacje te są rozproszone w różnych częściach tych sprawozdań, najczęściej pojawiały się w rozdziałach dotyczących zarządzania ryzykiem, szans i zagrożeń, a tylko dwie spółki – Orange i Netia wpisały ten aspekt w część dotyczącą modelu biznesu. Taki stan powoduje, że informacje z tego zakresu, ze względu na brak jednolitej struktury danych, nie mogą być porównywane. Różnią się także zakresem i formą prezentacji, co zdecydowanie uniemożliwia dokonanie wieloaspektowej i wielosektorowej oceny podejmowanych działań przez badane jednostki raportujące.

Należy zaznaczyć, że istotnym ograniczeniem jest odnoszenie wniosków przedstawionych w artykule do wszystkich spółek uznanych przez ustawodawcę za operatorów usług kluczowych, co ma związek z reprezentatywnością badania i jego wstępnym charakterem. Stosunkowo nieliczna grupa badawcza jest spowodowana faktem, że ustawa o krajowym systemie cyberbezpieczeństwa została wprowadzona dopiero w 2018 roku, dlatego, zdaniem autorki, liczba raportujących spółek, informacji o cyberbezpieczeństwie i cyberryzyku jest niewielka.

Brak informacji o modelach zabezpieczania się przed możliwymi cyberzagrożeniami w dotychczas sporządzanych raportach biznesowych potwierdzają potrzebę doskonalenia zawartości raportów zintegrowanych o informacje ilościowe i jakościowe w tym zakresie.

Autorka proponuje uzupełnienie i ustrukturyzowanie dotychczas raportowanych informacji niefinansowych o informacje dotyczące cyberbezpieczeństwa, a także rekomenduje zbudowanie „modelu biznesowego" przedsiębiorstwa, który obejmowałby aspekty bezpieczeństwa cybernetycznego. Informacje te powinny być ujmowane w raportach zintegrowanych spółek, które stosują przepisy ustawy o rachunkowości, jak i MSR. Takie podejście do prezentowania tych informacji poprawiłoby porównywalność dostarczanych informacji i zmniejszyłoby istniejący dualizm sprawozdawczy w Polsce wynikający m.in. z odmiennego zakresu sprawozdań sporządzanych według ustawy o krajowym systemie cyberbezpieczeństwa i MSR, różnych metod grupowania i wyceny poszczególnych informacji. Ważne jest, aby podmioty objęte ustawą o krajowym systemie cyberbezpieczeństwa, wprowadziły aspekt zarządzania cyberbezpieczeństwem do obecnie funkcjonującego modelu biznesowego przedsiębiorstwa, ponieważ:

1) model biznesu traktowany jest jako nośnik różnych rodzajów innowacji procesowych (np. nowe technologie wytwarzania, zabezpieczeń przed cyberatakami) i jako architektura działalności biznesowej wzmacnia cyberbezpieczeństwo;
2) model biznesu jest odpowiedzią na wymagania przepisów prawnych w zakresie krajowego systemu cyberbezpieczeństwa;
3) model biznesu to ścieżka biznesu, stanowiącego propozycję dla potencjalnych inwestorów i kredytodawców chcących współpracować z przedsiębiorstwami, dla których cyberbezpieczeństwo odgrywa pierwszorzędną rolę.

Autorka proponuje zbudowanie modelu cyberbezpieczeństwa opartego na założeniach ustawy o krajowym systemie cyberbezpieczeństwa, a następnie uwzględnienie jego elementów w modelu biznesowym przedsiębiorstwa, co spowoduje bezsprzeczny wzrost ochrony systemów związanych z obsługą rachunkowości i finansów. Uwzględnienie w modelu biznesowym firmy aspektów cyberbezpieczeństwa, a następnie raportowanie o nim to propozycja, która zapewni szereg korzyści w postaci podwyższenia transparentności koncepcji tworzenia wartości, zarówno dla klienta, jak i dla właścicieli przedsiębiorstwa, osiągnięcie przewag konkurencyjnych, wśród których coraz większą rolę odgrywają cechy jakościowe (np. niezawodność sieci teleinformatycznych i bezpieczeństwa relacji między różnymi użytkownikami informacji) wzmocnienie istniejących i budowania nowych trwałych relacji z interesariuszami.

Literatura

Azmi R., Kautsarina K., Apriany I., Tibben W.J. (2020), *Revisiting „Cyber" Definition: Context, History, and Domain*, [w:] W. Yaokumah W., Rajarajan M., Abdulai J., Wiafe I., Apietu. Katsriku F. (eds.), *Modern Theories and Practices for Cyber Ethics and Security Compliance*, IGI Global, Hershey, PA, s. 1–17.

Bass T. (2000), *Intrusion detection systems and multisensor data fusion: Creating cyberspace situational awareness*, „Communications of the ACM", 43 (4), s. 99–105.

Biener C., Eling M., & Wirfs J.H. (2015), *Insurability of cyber risk: An empirical analysis*, „The Geneva Papers on Risk and Insurance-Issues and Practice", 40 (1), s.131–158.

Brenner S.W. (2010), *Cybercrime: criminal threats from cyberspace*, ABC-CLIO Corporate, Santa Barbara, CA.

Curti F., Gerlach J., Kazinnik S., Lee M.J., Mihov A. (2019), *Cyber risk definition and classification for financial risk management*, Working Paper, Federal Reserve Bank of Richmond, August (mimeo).

Dębowski T.R., Wrocławski U. (2018), *Cyberbezpieczeństwo wyzwaniem XXI wieku*, Wydawnictwo Naukowe ArchaeGraph Diana Łukomiak, Łódź.

Gao L., Calderon T.G., Tang F. (2020), *Public companies' cybersecurity risk disclosures*, „International Journalof Accounting Information Systems", 38.

Gogołek W., Cetera W. (2014), *Leksykon tematyczny. Zarządzanie, IT*, Wydawnictwo Wydziału Dziennikarstwa i Nauk Politycznych UW, Warszawa.

Grzelak M., Liedel K. (2012), *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe", 22, s. 125–139.

Janvrin D.J., Wang T. (2019), *Implications of Cybersecurity on Accounting Information*, „Journal of Information Systems", 33 (3), s. A1–A2.

Knapp K.J., Morris R.F, Marshall T.E., Byrd T.A. (2009), *Information security policy: An organizational-level process model*, „Computer & Security", 28 (7), s. 493–508.

Konieczny M. (2012), *Poszukiwanie tożsamości w cyberprzestrzeni. Implikacje pedagogiczne*, VULCAN, Wrocław.

Kowalewski J., Kowalewski M. (2014), *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki Informacyjne", 1–2, s. 24–32.

Lambert S. (2008), *A conceptual framework for business model Research*, 21st Bled eConference eCollaboration: Overcoming Boundaries through Multi-Channel Interaction, Bled, Slovenia.

Marczyk M. (2018), *Cyberprzestrzeń jako nowy wymiar aktywności człowieka: analiza pojęciowaobszaru*, „Przegląd Teleinformatyczny", 6, s. 59–72.

Mukhopadhyay A., Chatterjee S., Saha D., Mahanti A. and Sadhukan S.K. (2013), *Cyber-Risk Decision Models: To Insure IT or Not?*, Decision Support Systems 56 (1), s. 11– 26.

Ottis R., Lorents P. (2010), *Cyberspace: Definition and implications*, 5 th International Conference on Cyber Warfare and Security, Dayton, OH, Academic Publishing Limited, s. 267–270.

Rabai L.B.A., Jouini M., Aissa A.B., Mil A. (2013), *A cybersecurity model in cloud computing environments*, „Journal of King Saud University-Computer and Information Sciences", 25 (1), s. 63–75.

Reveron D.S. (ed.) (2012), *Cyberspace and national security: threats, opportunities, and power in a virtual world*, Georgetown University Press, Washington, DC.

Rot A., Olszewski B. (2017), *Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection*,Position Papers on Federated Conference on Computer Science and Information Systems, Prague, s. 113–117.

Schatz D., Bashroush R., Wall J. (2017), *Towards a more representative definition of cyber security*, „Journal of Digital Forensics, Security and Law", 12 (2), s. 53–74.
Smith K.T, Smith L.M., Smith J.L. (2011), *Case Studies of Cybercrime and The Impact on Marketing Activity and Shareholder Value*, „Academy of Marketing studies Journal", 15 (2), s. 67–86.
Stubbs W., Higgins C. (2014), *Integrated reporting and internal mechanisms of change*, „Accounting, Auditing & Accountability Journal", 27 (7), s. 1068–1089.
Suchorzewska A. (2010), *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wolters Kluwer, Warszawa.
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2020 poz. 1369.
Von Solms R., Van Niekerk J. (2013), *From information security to cyber sec*urity, „Computers and Security", 38, s. 97–102.
Walińska, E. (2013), *Sprawozdanie finansowe a raport biznesowy – głos w dyskusji*, „Przegląd Organizacji", (10), s. 40–45.
Wasilewski J. (2013), *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego", 5 (9), s. 225–234.
Yang L., Lau L., Gan H. (2020), *Investors' perceptions of the cybersecurity risk management reporting framework*, „International Journal of Accounting & Information Management", 28 (1), s.167– 183.

Źródła internetowe

Business Insider, https://businessinsider.com.pl/technologie/nowe-technologie/cyberprzestepstwa-w-polsce-statystyki/zrn11l7 (dostęp 11.05.2021).
Cybersecurity & Infrastructure Security Agency, Security Trip (2009), https://us-cert.cisa-.gov/ncas/tips/ST04-001
De Groot (2020), *What is Cyber Security? Definition, Best Practices & More*, https://digitalguardian.com/blog/what-cyber-security (dostęp 26.11.2020).
DOD Dictionary of Military and Associated Terms (2020), https://www.jcs.mil/Portals/36/-Documents/Doctrine/pubs/dictionary.pdf (dostęp 17.12.2020).
https://www.pwc.pl/pl/publikacje/2018/cyber-ruletka-po-polsku-5-edycja-badania-stanu-bezpieczenstwa-informacji-pwc.html (dostęp 11.05.2021).
Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej polskiej na lata 2011–2016 (2010), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map-/Poland_Cyber_Security_Strategy.pdf