Raport badawczy

Edukacja w zakresie bezpieczeństwa informacji dla MŚP
- wykorzystanie potencjału, wzrost świadomości

Funded by the
Erasmus+ Programme
of the European Union

TeBelSi

Funded by the
Erasmus+ Programme
of the European Union

Numer projektu: 2018-1-EN02-KA202-005218

Funded by the
Erasmus+ Programme
of the European Union

Spis treści

1 Wprowadzenie: Certyfikacja częściowa w zakresie bezpieczeństwa informacji 1
2 Przegląd literatury 1
3 TeBeISi – Metoda i podejście 4
3.1 Przedmiot badań 4
3.2 Metoda 5
4 Badanie: Edukacja i szkolenia z zakresu bezpieczeństwa informacji dla MŚP 7
4.1 Charakterystyka danych 7
4.2 Analiza 9
4.2.1 Kultura firmy 9
4.2.2 Kompetencje w przedsiębiorstwie 11
4.2.3 Bezpieczeństwo informacji w MŚP 14
4.2.4 Bezpieczeństwo informacji w przedsiębiorstwie: wymagania dotyczące personelu 16
4.2.5 Samoocena kompetencji 19
4.2.6 Osobowość (Wielka Piątka) 20
4.2.7 Wyniki pracy 23
4.3 Podsumowanie 24
5 Przewodnik dla MŚP 26
6 Perspektywy i zalecenia 29
7 Literatura 30

Spis wykresów

Figure 1: A way out - The TeBeISi solution to overcome the skills gap in the information security labour market. 4
Figure 2: The TeBeiSi research agenda 6
Figure 3. Competences critical for success 6
Figure 4: “Which firms participate in the survey?” 8
Figure 5: “In which branch of industry does your company operate?” 8
Figure 6: "What is your role in the company?" 8
Figure 7: "In which country does your company mainly operate?" 9
Figure 8: "How does the gender distribution look like?" 9
Figure 9: Characteristics grouped into the following categories "Strategy, Structure, Leadership, Cooperation” – all firms 11
Figure 10: Characteristics grouped into the following categories "Strategy, Structure, Leadership, Cooperation” – firms having an Information Security strategy and firms that don’t 11
Figure 11: Competences in the company – Results 13
Figure 12: Analysis of competences in SME 14
Figure 13: "What reasons have prevented your company from investing in improving information security to date?” 15
Figure 14: “Building on your experience, what type of education or training is necessary/helpful/optional for an employee tasked with ensuring information security in your organization?” 15
Figure 15: Possible options for increasing information security 16
Figure 16: “Are you aware of any information security incidents within the last 2 years or is there a suspicion of a security incident?” 16
Figure 17: “Are there employees in your company who are formally responsible for information security? (above) – If so, how many?” (below) 17
Figure 18: “How many open information security positions are there in your company?” 17
Figure 19: Business certification for information security 18
Figure 20: “How are you tackling the human resource needs in the area of information security so far?” 19
Figure 21: “How are you tackling the human resource needs in the area of information security so far?” – IS and No IS 19
Figure 22: "Please evaluate yourself: Which of the following education and training activities can you perform?" 20
Figure 23: Big-Five histograms observed for information security practitioners. 21
Figure 24: Big-Five, mean value comparison 22
Figure 25: Task Performance 23
Figure 26: Counterproductive Behavior 23
Figure 27: Contextual Performance 24
Figure 28: IWPQ results for Information security experts 24
Figure 29: Guidelines based on common problems that SME’s face in information security and data protection ....**Fehler! Textmarke nicht definiert.**

Spis tabel

Table 1: “Please indicate to what extent the following characteristics describe the company you work for or the organization you work for”. 10
Table 2: "Tasks and activities in the field of information security" 12
Table 3: Dimensions of Big-5....20
Table 4: Structure of BFI-10 21
Table 5: "Validity test: Correlation between Items and groups"....22

1 Wprowadzenie: Certyfikacja częściowa w zakresie bezpieczeństwa informacji

W ostatnich latach znaczenie bezpieczeństwa informacji gwałtownie wzrosło. W związku z rosnącą liczbą przypadków naruszenia danych, firmami, które stały się zakładnikami ataków złośliwego oprogramowania na skalę międzynarodową, oraz strategicznym wykorzystaniem cyberwojny jako środka do rozszerzenia władzy politycznej w obcych sferach, cyfryzacja nie jest już postrzegana wyłącznie jako zbawienne rozwiązanie dla borykających się z problemami firm, ale również jako istotne źródło ryzyka, które zasługuje na szeroko zakrojone środki ochrony. Ryzyko pojawia się w wielu różnych kontekstach, ale może być zakorzenione w dwóch przestrzeniach: w przestrzeni fizycznej i cybernetycznej.

Potrzebne są holistyczne podejścia do istniejących i rosnących zagrożeń. W obliczu rozproszonych i nieuchwytnych scenariuszy ryzyka, jednostki, zarówno w sferze prywatnej, jak i korporacyjnej, mają tendencję do deprecjonowania znaczenia rozpoznawania ryzyka związanego z bezpieczeństwem informacji jako środka zrównoważonego zarządzania i kierowania. Aby poradzić sobie z tym powszechnym brakiem świadomości, który przekłada się ze sfery publicznej na świat korporacyjny, należy podjąć działania mające na celu podnoszenie świadomości, uwrażliwianie i edukację. W międzyczasie, firmy muszą zrozumieć, jak mogą podejść do tematu bezpieczeństwa informacji z indywidualną strategią, która pasuje do ich własnych potrzeb i budżetu. Aby wesprzeć firmy w tym wyzwaniu, przeprowadzono badanie "Edukacja w zakresie bezpieczeństwa informacji dla MŚP". Celem badania było rzucenie światła na szkolenia i potrzeby kadrowe MŚP, aby znaleźć rozwiązania dla utrzymującego się braku wykwalifikowanych pracowników.

Podtytuł " Wykorzystanie potencjału, wzrost świadomości" zawiera tym samym wskazówkę dotyczącą najważniejszego zasobu: personelu MŚP. Wielu pracowników posiada umiejętności i wiedzę, które nabyli w trakcie swojej kariery zawodowej, a z których często nawet nie zdają sobie sprawy. Zdobywanie nieformalnego i pozaformalnego wykształcenia, szczególnie w sektorach opartych na technologii i innowacjach, takich jak bezpieczeństwo informacji, stanowi bogate zasoby, które mogą być gromadzone poprzez walidację i uznawanie kompetencji. Aby ułatwić proces uznawania, zespół projektowy TeBeISi opracował moduły edukacyjne i przy wsparciu niniejszego badania dostarcza narzędzi i zasobów dla MŚP w celu zidentyfikowania odpowiednich pracowników do podjęcia nowych obowiązków w dziedzinie bezpieczeństwa informacji.

Projekt TeBeISi stara się wnieść wkład w praktykę biznesową i sprostać codziennej rzeczywistości MŚP z całej UE. Niniejsze opracowanie pogłębia zrozumienie decydentów, osób rekrutujących i zainteresowanych w dziedzinie bezpieczeństwa informacji oraz rozwoju aktywów i wymagań w zakresie bezpieczeństwa informacji i personelu bezpieczeństwa informacji w MŚP. Aby osiągnąć ten cel, opracowanie ma następującą strukturę: rozdział drugi zawiera przegląd istniejących badań nad bezpieczeństwem informacji w MŚP i wymaganiami wobec personelu, rozdział trzeci przedstawia podstawy metodologii badawczej TeBeISi i kontekst, w którym to badanie zostało zaprojektowane, rozdział czwarty przedstawia wyniki kwestionariusza ilościowego, rozdział piąty przedstawia w skrócie najważniejsze wytyczne dla MŚP i wreszcie rozdział szósty kończy się perspektywą przyszłego rozwoju.

2 Przegląd literatury

Wdrożenie systemów informacyjnych i technologii informacyjnej stało się warunkiem koniecznym sukcesu przedsiębiorstw we wszystkich sektorach gospodarki. Bez technologii informacyjnej praca z informacją jest nie tylko nieefektywna, ale wręcz niemożliwa (Hallová et al. 2019). Co więcej, nasza zależność od tych systemów rośnie z każdym dniem. Jednak wraz z szybkim rozwojem nowoczesnych technologii i systemów informatycznych rośnie również potencjał do nadużyć (Smith, 2003; Leede i in., 2005; Kumar i in., 2011).

W dzisiejszym świecie, w którym wszystkie osoby i przedsiębiorstwa są uzależnione od technologii informacyjnej, bezpieczeństwo informacji i ochrona danych są ważnymi elementami, które wymagają szczególnej uwagi. W tym względzie istotnymi czynnikami są dyrektywa Unii Europejskiej (UE) dotycząca środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w całej Unii oraz ogólne rozporządzenie o ochronie danych (Kogenhop, 2020). Inicjatywa regulacyjna Komisji Europejskiej odzwierciedla zwiększone zapotrzebowanie na wytyczne legislacyjne, ponieważ szybki rozwój technologiczny i globalizacja stworzyły nowe wyzwania w zakresie ochrony danych osobowych i informacji (Wilkinson, 2018).

W ostatnich latach nowe formy technologii informacyjnych (np. czujniki i urządzenia mobilne) dramatycznie rozszerzyły to, co można zmierzyć i przeanalizować, stawiając zupełnie nowe wyzwania w zakresie bezpieczeństwa i prywatności (Weber, 2010; Newell & Marabelli, 2015; Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015; Lee, Cho & Lim, 2018). Potencjalny wpływ, jaki na klientów mogą mieć kwestie bezpieczeństwa i prywatności związane z systemami informacyjnymi, sprawia, że wyzwania te są kluczowe dla praktyków biznesu (Sicari et al., 2015; Sicari et al., 2016). Z drugiej strony, menedżerowie organizacji muszą wykorzystywać nowe narzędzia technologii informacyjnej do przechowywania nie tylko danych osobowych, ale także danych poufnych, aby zachować konkurencyjność w XXI wieku. Tymczasem przechowywanie danych w formie papierowej jest przestarzałe ze względu na potencjał elektronicznego przechowywania danych, organizacje szybko przyjmują nowe technologie, a elektroniczne przechowywanie danych stało się powszechne w wielu krajach (McAfee, 2010).

Rosnąca tendencja do przechowywania danych w formacie elektronicznym, a także rosnąca łączność z Internetem i wynikające z niej narażenie na cyberprzestępców, doprowadziły do opracowania konkretnych wymogów w zakresie ochrony danych (McAfee, 2010). Technologie przechowywania danych muszą być wyposażone w środki ochrony danych, a użytkownicy pracujący z danymi muszą być przeszkoleni, aby rozumieć ryzyko wycieku danych firmowych do osób nieupoważnionych. Liderzy organizacyjni muszą być świadomi poważnych konsekwencji wycieku danych elektronicznych. Tak samo jak pracownicy, którzy nie przestrzegają zasad bezpieczeństwa informacji (Siponen, Mahmood & Pahnila, 2009), menedżerowie organizacji, którzy są nieostrożni w pozyskiwaniu i zarządzaniu danymi elektronicznymi, narażają swoje firmy na ryzyko i zagrożenia (Northhouse, 2010). Menedżerowie muszą wykazać się ostrożnością i samokontrolą w celu osiągnięcia korzyści dla firmy, szczególnie w zakresie bezpieczeństwa danych (Guinote & Vescio, 2010). Jednym z kluczowych wyzwań w zarządzaniu bezpieczeństwem informacji jest zrozumienie, w jaki sposób czynniki organizacyjne, indywidualne i techniczne łączą się, aby wpłynąć na wyniki w zakresie bezpieczeństwa informacji w organizacji (Wilkinson, 2018).

Najnowsze badania pokazują, że w wielu przypadkach wyciek danych elektronicznych w małych firmach jest wynikiem złych praktyk przywódczych i zarządczych. Menedżerowie w

organizacjach podejmują najważniejsze decyzje i jeśli menedżerowie nie radzą sobie odpowiednio z kwestiami technologii informacyjnych, zagrażają one przetrwaniu przedsiębiorstwa (Davies & Hertig, 2008). Możliwy czynnik łagodzący zaproponowali Noguerol und Branch (2018), twierdząc, że menedżerowie korporacyjni mogą pozytywnie wpływać na zachowania pracowników w obszarze bezpieczeństwa danych poprzez wspieranie zdrowego środowiska pracy i pielęgnowanie relacji.

Firmy różnej wielkości na całym świecie borykają się z brakiem cyberbezpieczeństwa, a wiele z nich jest narażonych na cyberprzestępczość. Wyciek danych elektronicznych jest jednak problemem szczególnie dla mniejszych firm. MŚP mierzą się między innymi z ograniczeniami finansowymi, czasami nieefektywnymi menedżerami i brakiem uwagi dla małych zagadnień, które nie są bezpośrednio związane z biznesem (O'Rourke, 2003; Adamkiewicz, 2005; Goodwin, 2005; Baker & Wallace, 2007).

Pomimo rosnącego zagrożenia incydentami cybernetycznymi z zewnątrz, pracownicy pozostają głównym źródłem incydentów bezpieczeństwa (Richardson, 2008; PwC, 2017). Zasoby ludzkie wewnątrz organizacji mogą być bardziej niebezpieczne niż te na zewnątrz organizacji, ponieważ są zaznajomione z systemami informacyjnymi organizacji i uzyskują dostęp do danych poprzez swoje normalne czynności zawodowe (Herath & Rao, 2009a, 2009b; Bulgurcu, Cavusoglu, & Benbasat, 2010; Johnston & Warkentin, 2010; Siponen & Vance, 2010). Polityki bezpieczeństwa informacji mają zapewnić bezpieczeństwo informacji (Bulgurcu, Cavusoglu, & Benbasat, 2010), ale badania pokazują, że wiele incydentów bezpieczeństwa jest spowodowanych przez pracowników ignorujących lub nieświadomych tych zasad (Willison & Warkentin 2013, Path to Cyber Resilience, 2016).

Badacze i praktycy coraz częściej uznają organizacyjne bezpieczeństwo informacji za zagadnienie socjotechniczne, wymagające nie tylko podejścia technicznego, ale również menedżerskiego (Burns, Roberts, Posey, Bennett, & Courtney, 2018). Ze względu na powszechne wykorzystanie technologii informatycznych w firmach, pracownikom często powierza się stały dostęp do informacji firmowych i systemów informatycznych w celu wykonywania obowiązków związanych z pracą. Pomimo tej zwiększonej elastyczności operacyjnej, organizacje mają mniejsze możliwości monitorowania zachowań pracowników mających dostęp do poufnych danych (Herath & Rao, 2009). Dlatego, aby poprawić ochronę cennych aktywów informacyjnych organizacji w kontekście rozprzestrzeniania się technologii, proaktywne szkolenia pracowników w zakresie bezpieczeństwa informacji mają kluczowe znaczenie dla bezpieczeństwa informacyjnego organizacji (von Solms & von Solms, 2009; D'Arcy, Hovav & Galletta, 2009; Albrechtsen & Hovden, 2010; Puhakainen & Siponen, 2010; Karjalainen & Sipo-nen, 2011; Posey, Roberts, Lowry, Bennett & Courtney, 2013). Badania pokazują, że organizacje identyfikują programy uświadamiające pracowników jako najwyższy priorytet w swoich budżetach na bezpieczeństwo informacji (PWC, 2015), a kierownicy ds. bezpieczeństwa informacji stwierdzają, że szkolenie pracowników jest jednym z najważniejszych działań potrzebnych do wdrożenia skutecznej strategii bezpieczeństwa informacji i danych (van Zadelhoff, Lovejoy & Jarvis, 2014).

Szkolenie pracowników jest najskuteczniejszym nietechnicznym środkiem zapewnienia bezpieczeństwa informacji w organizacjach i zapobiegania ujawnianiu przez pracowników wrażliwych informacji osobom nieupoważnionym (Colwill, 2009; Peikari, Shah, & Lo, 2018). Szkolenia mogą zwiększyć wiedzę i świadomość pracowników na temat zagrożeń i konsekwencji naruszenia bezpieczeństwa oraz pomóc w zapobieganiu takim incydentom (Kluge, 2007; D'Arcy Hovav & Galletta, 2009).

Edukacja i szkolenie pracowników jest dla organizacji sposobem na zmniejszenie ryzyka niepowodzeń w zakresie bezpieczeństwa wewnętrznego (Burns, Roberts, Posey, Bennett & Courtney, 2015; Barlow, Warkentin, Ormond, & Dennis, 2018). Jest to ważny warunek wstępny i ma pozytywny wpływ na zachowania związane z bezpieczeństwem informacji. Dobrze zaprojektowane programy szkoleniowe dla pracowników mogą przyczynić się do zmniejszenia ryzyka związanego z bezpieczeństwem informacji w organizacji (Anderson & Agarwal, 2010; Liang & Xue, 2010; Bulgurcu, Cavusoglu, & Benbasat, 2010; Johnston & Warkentin, 2010; Whitman & Mattord, 2012; Jenkins & Durcikova, 2013; Johnston, Warkentin & Siponen, 2015). Według badaczy (Gardner & Thomas, 2014; Posey, Roberts & Lowry, 2015) ciągłe kształcenie i szkolenie pracowników w zakresie bezpieczeństwa danych i informacji jest skutecznym sposobem kształtowania ich zachowań w zakresie bezpieczeństwa informacji oraz zgodności z polityką bezpieczeństwa informacji organizacji. Pracownicy posiadający odpowiednią wiedzę z zakresu bezpieczeństwa informacji są w stanie zapobiegać zagrożeniom i atakom, co skutkuje zwiększeniem poufności, integralności i dostępności informacji w organizacji (Sabeeh & Lashkari, 2011). Zauważa się, że ze względu na dynamiczny charakter zagrożeń i podatności na zagrożenia bezpieczeństwa informacji, szkolenia i edukacja pracowników powinny być regularną i stałą praktyką w organizacji (Yoo i in., 2018; McConnell, 2020).

Chociaż przetwarzanie danych osobowych jest nieuniknione dla wielu MŚP, często nie jest to ich podstawowa działalność i brakuje im wystarczających zasobów ludzkich lub finansowych, aby zapewnić właściwą zgodność. W szczególności MŚP nie są przygotowane do przyjęcia środków bezpieczeństwa informacji po prostu dlatego, że nie wymaga się od nich udokumentowanego bezpieczeństwa informacji ze względu na ich niewielkie rozmiary (Kuusisto, & Ilvonen, 2003; Doherty, & Fulford, 2005). MŚP są w większości świadome istnienia GDPR, ale brakuje im zasobów, aby spełnić wymagania; brakuje im zdolności organizacyjnej do wdrożenia wymagań GDPR i bezpieczeństwa informacji w organizacji. Najczęstsze wyzwania związane z ochroną danych i bezpieczeństwem informacji, przed którymi stoją MŚP, obejmują: zrozumienie, jakie zmiany należy wprowadzić, aby zachować zgodność z przepisami; projektowanie i opracowywanie nowych procesów i procedur związanych z przetwarzaniem danych osobowych; oraz świadomość pracowników w zakresie znaczenia ochrony danych. Pomimo licznych opinii i wytycznych dotyczących GDPR wydanych przez organy regulacyjne i ekspertów w dziedzinie ochrony danych, brakuje praktycznych, łatwych do zrozumienia i ukierunkowanych wskazówek dla MŚP dotyczących praktycznego wdrażania przepisów o ochronie danych (Jasmontaitė-Zaniewicz, Calvi, Nagy & Barnard-Wills, 2021). Podkreśla się, że w szczególności MŚP uświadamiają sobie potrzebę ukierunkowanych, specyficznych dla danego sektora szkoleń i porad opartych na przykładach i studiach przypadków, które odzwierciedlają specyfikę tych organizacji (Barnard-Wills, Cochrane, Matturi, & Marchetti, 2019).

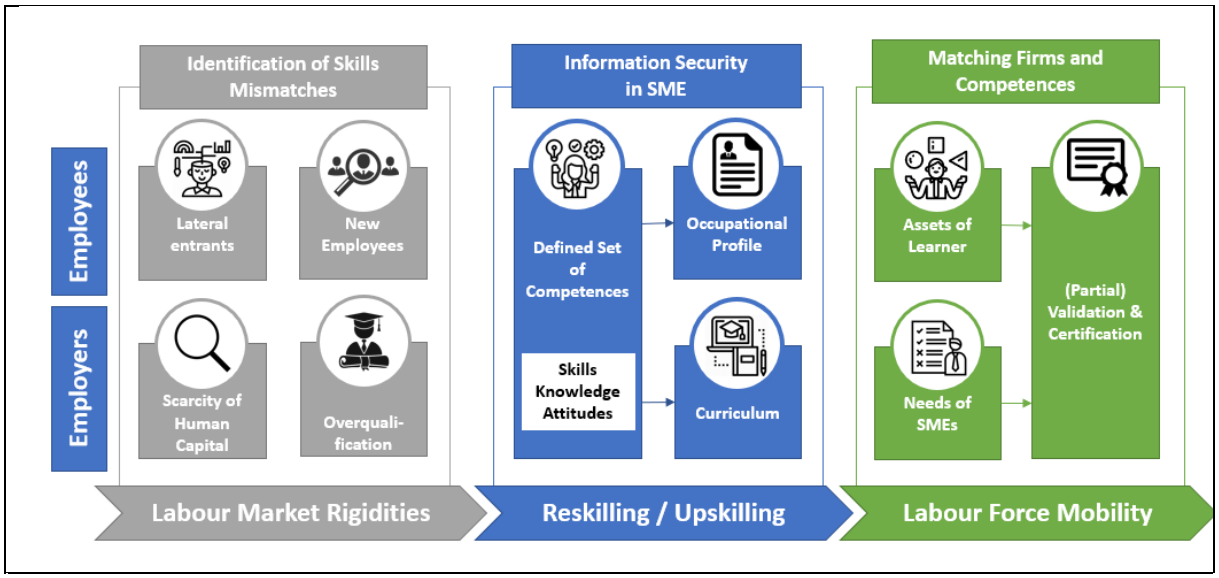
3 TeBelSi – Metoda i podejście

Bezpieczeństwo informacji w MŚP, jak dotąd, jest tematem niedostatecznie zbadanym i niewiele wiadomo na temat potrzeb i wymagań MŚP w całej UE. Tymczasem obowiązek prawny w zakresie ochrony danych (GDPR) doprowadził do gwałtownego wzrostu podejmowanych działań i świadomości wśród MŚP, bezpieczeństwo informacji było traktowane przez wiele podmiotów bardziej jako "nice to have" - i nie było realizowane z dużym wysiłkiem lub poświęceniem. Wprowadzenie Systemu Zarządzania Bezpieczeństwem Informacji, czy też certyfikacja firm i osób, dopiero powoli wkrada się do świadomości pracowników i właścicieli firm. Niemniej jednak stwierdzono, że spośród wielu czynników składających się na bezpieczeństwo firmy, czynnik ludzki, tj. pracownik, kierownictwo, a w końcu oficer bezpieczeństwa informacji, może mieć największe znaczenie.

Projekt TeBelSi- ma na celu zapewnienie wglądu w stan bezpieczeństwa informacji w MŚP oraz uzyskanie głębszego wglądu w możliwości szkoleniowe i edukacyjne dla MŚP w celu przezwyciężenia niedoboru wykwalifikowanej siły roboczej.

3.1 Przedmiot badań

Agenda badawcza, na której opiera się projekt TeBelSi, opiera się głównie na trzech iteracyjnych krokach: po pierwsze, porównanie powszechnych praktyk (IO1 i IO2), po drugie, analiza potrzeb (IO3) oraz opracowanie odpowiednich narzędzi i rekomendacji dla firm, osób indywidualnych i instytucji edukacyjnych (IO4 i IO5). Poprzez analizę sytuacji rynkowej, a w szczególności roli istniejących certyfikatów i narzędzi w kontekście uznawania kompetencji i przejrzystości. Na podstawie analizy wymagań, opracowano proces, który jest przedstawiony na wykresie 1.



Wykres 1: Wyjście z sytuacji - rozwiązanie TeBelSi w celu wypełnienia luki kompetencyjnej na rynku pracy w obszarze bezpieczeństwa informacji.

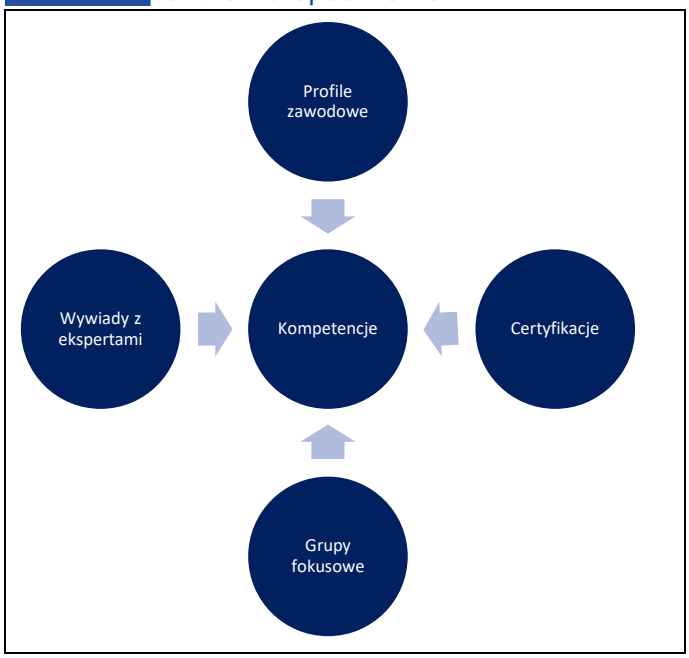
W skrócie, istniejące ograniczenia rynku pracy można opisać jako dwojakiego rodzaju: z jednej strony, istnieje po prostu niska liczba specjalistów dostępnych na rynku. Ten niedobór jeszcze bardziej pogłębia fakt, że większość dostępnych specjalistów jest wysoko wykwalifikowana -

często zbyt wysoko, ponieważ stają się oni zbyt drodzy dla MŚP, aby sobie na nich pozwolić. Obecne praktyki w firmach są podobne do tych w całym sektorze IT: wiele osób wchodzących z zewnątrz staje się aktywnych w tym sektorze, jednocześnie zupełnie nowi pracownicy rozpoczynają swoją karierę w tej obiecującej dziedzinie. Rozwiązanie opracowane w ramach projektu TeBelSi rozpoczyna się więc od analizy umiejętności, wiedzy i kompetencji wymaganych w MŚP, aby skonstruować specyficzny program nauczania dostosowany do potrzeb MŚP. Stało się oczywiste, że nie tylko z perspektywy kwalifikacji, wymagania w MŚP różnią się znacznie od wymagań w dużych korporacjach, dlatego też projekt proponuje inny profil zawodowy, aby uwzględnić te różnice. Profil zawodowy i program nauczania są oparte na kompetencjach ustalonych wśród MŚP. Wreszcie, sprawdzenie potrzeb firm i kompetencji pracowników wspiera firmy w identyfikacji odpowiednich kandydatów, którzy mają predyspozycje do pracy w dziedzinie bezpieczeństwa informacji i którzy są chętni do przekwalifikowania się i rozwijania swojej kariery w nowej dziedzinie. Inwestycje w istniejący personel i podnoszenie kwalifikacji własnej siły roboczej są zatem uważane za najbardziej efektywne ekonomicznie możliwości dla firm i pracowników, aby przezwyciężyć zapotrzebowanie na umiejętności.

Niniejsze badanie wspiera ten program na kilka sposobów: Po pierwsze, ma ono na celu identyfikację wymagań z perspektywy menedżerskiej, biorąc pod uwagę strategie zatrudniania, otwarte stanowiska, świadomość bezpieczeństwa informacji i kulturę firmy. Po drugie, oceniane są wymagania techniczne, biorąc pod uwagę przede wszystkim umiejętności społeczne, ale także techniczne. W obu tych dziedzinach pozycje zostały opracowane na podstawie serii wywiadów eksperckich i grup fokusowych. Dlatego też, po trzecie, niniejszy kwestionariusz stanowi potwierdzenie i wzajemną walidację ustaleń dokonanych w ramach mieszanego projektu badawczego.

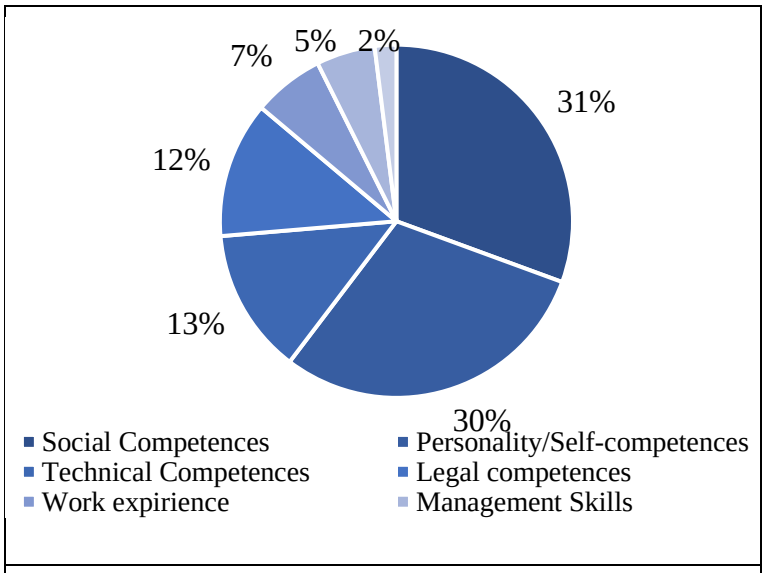
3.2 Metoda

Projekt badawczy oparty na metodzie mieszanej, mającej na celu opracowanie profili kompetencyjnych i programu nauczania TeBelSi, składającej się z czterech głównych elementów. Po pierwsze, w ramach analizy dokumentacji, przeanalizowano certyfikaty i profile zawodowe, uzyskując wgląd w nauczane kompetencje oraz kompetencje właściwe i oczekiwane od praktyków działających na rynku. Niemniej jednak, badania te były ograniczone przez ustalenie, że tylko w niewielkim stopniu uwzględniono szczególny przypadek MŚP i że nadal nie jest jasne, co odróżnia podstawowe potrzeby MŚP od bardziej zaawansowanych wymagań większych operacji.



Wykres 2: Program badań TeBelSi

Poprzez serię wywiadów eksperckich i grup fokusowych, przeprowadzonych na Litwie, we Włoszech, w Niemczech i w Polsce z pracodawcami, pracownikami i instytucjami edukacyjnymi, przeanalizowano kompetencje osób zajmujących się bezpieczeństwem informacji. Z analizy jakościowej wyodrębniono dogłębne informacje dotyczące znaczenia umiejętności technicznych, metodologicznych, społecznych i osobistych oraz zidentyfikowano konkretne elementy w każdej kategorii. Cała analiza jest dostępna w dokumencie "Kompetencje w zakresie bezpieczeństwa informacji - analiza jakościowa wywiadów ekspertów na temat wiedzy i umiejętności profesjonalistów w zakresie bezpieczeństwa informacji".



Wykres 3. Kompetencje kluczowe dla sukcesu

Poszczególne zidentyfikowane elementy zostały przeformułowane i połączone w jednostki uczenia się zgodnie ze standardem ECVET dotyczącym efektów uczenia się (por. IO4). W obecnym badaniu, jednostki te zostały poddane ocenie pod względem częstotliwości i znaczenia w firmach, tak aby końcowe wyniki dały wgląd w priorytety firm i najpilniejsze zadania, które należy wykonać.

4 Badanie: Edukacja i szkolenia z zakresu bezpieczeństwa informacji dla MŚP

W ramach projektu, grupa projektowa TeBeISi- przeprowadziła badanie "Edukacja w zakresie bezpieczeństwa informacji dla MŚP" w celu uzyskania wglądu w obecne praktyki w zakresie bezpieczeństwa informacji w małych i średnich przedsiębiorstwach, zapotrzebowania na wiedzę, umiejętności i kompetencje oraz perspektywy MŚP w zakresie radzenia sobie z istniejącymi wyzwaniami związanymi z ograniczoną dostępnością zasobów. Badanie dotyczące edukacji w zakresie bezpieczeństwa informacji dla MŚP ma na celu zidentyfikowanie wiedzy i doświadczenia w konkretnych subdziedzinach w domenie zawodowej bezpieczeństwa informacji w sferze małych i średnich przedsiębiorstw. Badanie zostało przeprowadzone za pomocą Limesurvey. W ciągu około 6 tygodni 160 uczestników, specjalistów ds. bezpieczeństwa informacji, właścicieli i dyrektorów generalnych MŚP, jak również ekspertów ds. rekrutacji i IT, odpowiedziało na ankietę online rozpowszechnioną w krajach partnerskich projektu, głównie w Polsce, Niemczech, na Litwie, we Włoszech i w Austrii.

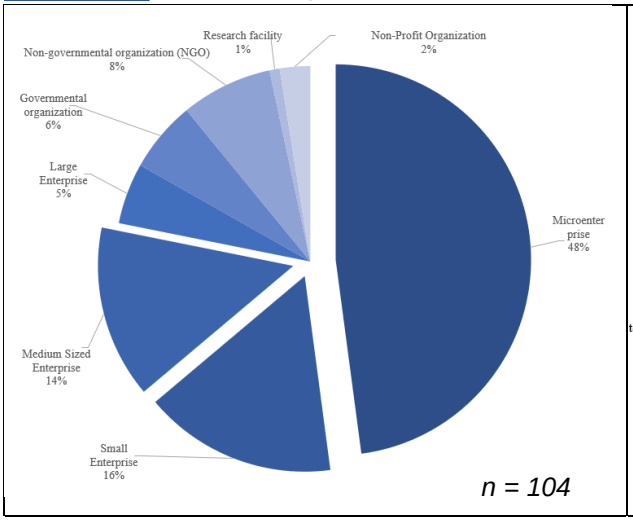
Badanie składa się z dwóch głównych aspektów: z jednej strony poszukiwano wymagań z perspektywy rekruterów, tj. działów HR i właścicieli firm, koncentrując się na głównych aspektach, które biorą pod uwagę w procesie rekrutacji. Z drugiej strony, działy IT i specjaliści ds. bezpieczeństwa informacji zostali poproszeni o przedstawienie ich opinii na temat wymagań technicznych i porównania kompetencji dla nowych pracowników w sektorze. Ponadto, obie grupy zostały poproszone o udzielenie informacji na temat kultury organizacyjnej firmy i cech osobowościowych pracowników odnoszących sukcesy. W tym celu wykorzystano zweryfikowane pozycje z Ingela et al. (2005) dla kultury firmy oraz Ramos-Villagrasa et al. (2019) dla wydajności pracy. Na potrzeby kwestionariusza skale zostały przetransformowane na 5-punktowe skale Likerta. Uczestnikom prezentowano pytania w zależności od zajmowanego stanowiska. Kwestionariusz został opracowany w ramach IO3 projektu TeBeISi i jest dostępny wraz z pozostałymi dokumentami rezultatowymi projektu.

4.1 Charakterystyka danych

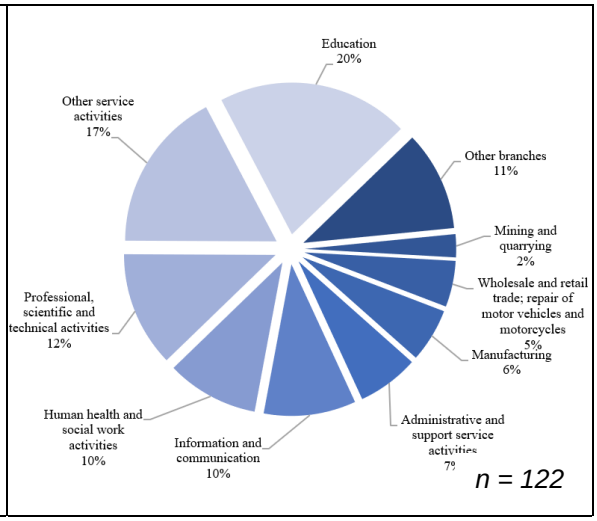
Większość firm, które wzięły udział w badaniu należy do sektora mikro-, małych i średnich przedsiębiorstw (ponad trzy czwarte). Pozostała jedna czwarta to m.in. duże przedsiębiorstwa (5 %), organizacje rządowe (6 %) i pozarządowe (8 %). Tam, gdzie było to konieczne, uwzględniono tylko wartości dla MŚP. Rysunek 4 pokazuje rozkład wszystkich uczestników według wielkości przedsiębiorstwa. Dla określenia wielkości przedsiębiorstwa zastosowano wspólną europejską definicję dotyczącą liczby pracowników i obrotu.[1]

Firmy te działają w różnych branżach, takich jak opieka zdrowotna i pomoc społeczna, edukacja lub w zakresie działalności profesjonalnej, naukowej i technicznej, zgodnie z klasyfikacją NACE Rev. 2. 10% firm działa w sektorze informacji i komunikacji (Wykres 5).

[1] European Comission 2021.

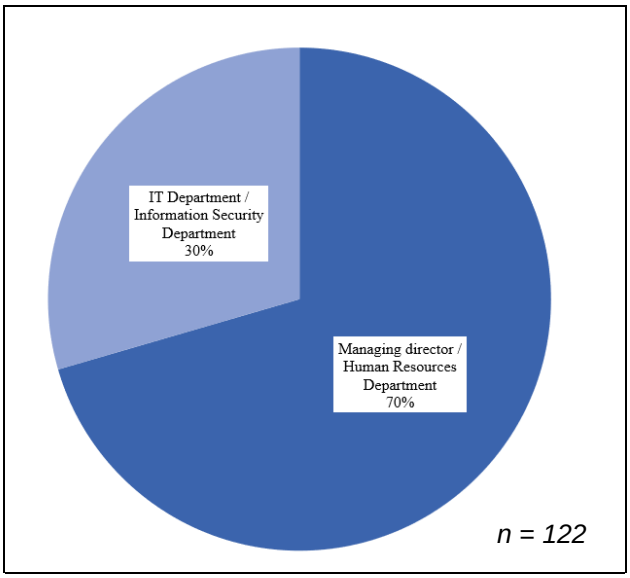


Wykres 4: "Jakie firmy biorą udział w badaniu?"



Wykres 5: "W jakiej gałęzi przemysłu działa Państwa firma?"

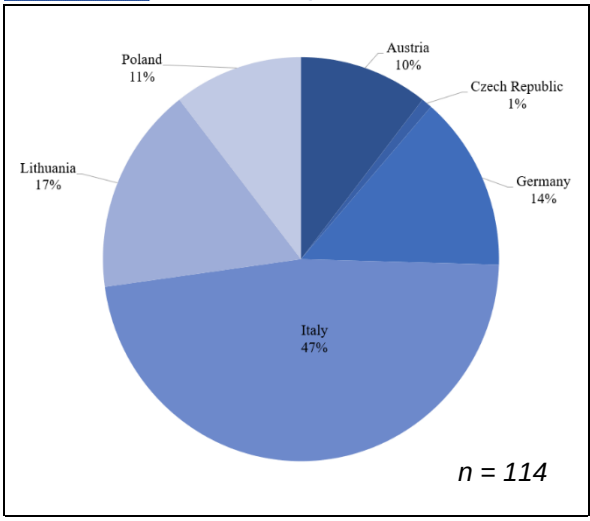
Dla przeprowadzenia ankiety ważne było poznanie rodzaju działalności uczestników w firmie, tj. albo ekspertów IT i bezpieczeństwa informacji, albo prezesa / rekrutera w MŚP, ponieważ obowiązki służbowe związane z bezpieczeństwem informacji ulegają zmianie. W zależności od udzielonych odpowiedzi, uczestnicy otrzymali różne pytania w ankiecie. Jak widać na wykresie 4 i 5, dwie trzecie uczestników pracuje jako dyrektor zarządzający lub w dziale zasobów ludzkich. Ta grupa odpowiadała na pytania związane z kulturą firmy, kompetencjami w firmie, edukacją w firmie czy technologiami stosowanymi w firmie.



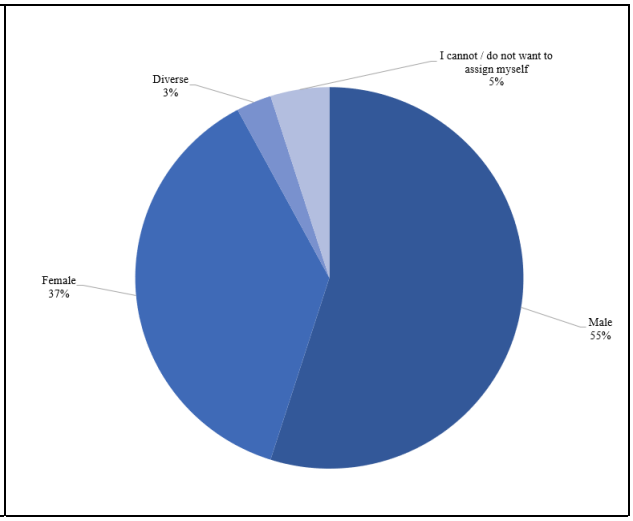
Wykres 6: " Jaka jest Twoja rola w firmie?"

Natomiast respondentom z działu IT lub bezpieczeństwa informacji zadawano pytania koncentrujące się na ich własnej pracy, cechach osobowości oraz pytaniach związanych z zarządzaniem IT w firmie. Rozróżnienie to zostało dokonane w celu uwzględnienia różnych punktów widzenia na bezpieczeństwo informacji, z naciskiem na zarządzanie ze strony właścicieli firm i naciskiem na kwestie techniczne ze strony ekspertów ds. bezpieczeństwa informacji.

Biorąc pod uwagę pochodzenie respondentów, prawie połowa uczestników wskazała, że ich firma działa głównie we Włoszech. Poza tym, firmy są również aktywne na Litwie, w Niemczech, Polsce, Austrii i Czechach (Wykres 7). Na koniec, krótkie spojrzenie na rozkład płci: Istnieje nieznaczna przewaga uczestników płci męskiej - 38 ze 102 uczestników to kobiety (Wykres 8). Niestety, rozmiar i rozmieszczenie uczestników nie pozwoliły na porównanie krajów lub płci, co należy wziąć pod uwagę przy interpretacji wyników. Wszystkie grafiki w dalszej części raportu będą ilustrować albo porównanie MŚP albo nie-MŚP. Jeśli nie zaznaczono inaczej, tylko odpowiedzi MŚP zostały przyjęte do analizy.



Wykres 7: " W jakim kraju głównie działa Państwa firma?"



Wykres 8: " Jak wygląda podział na płeć?"

4.2 Analiza

Główna część badania może być podzielona na dwie grupy: menedżerskie i techniczne aspekty bezpieczeństwa informacji w MŚP. Tymczasem pierwszy aspekt obejmuje rozdział 4.2.1 Kultura firmy, 4.2.2 Kompetencje w firmie oraz 4.2.4 Bezpieczeństwo informacji w przedsiębiorstwie: wymagania dotyczące personelu, ten ostatni aspekt obejmuje pytania dotyczące kompetencji zawarte w rozdziale 4.2.4, 4.2.5 Samoocena kompetencji, 4.2.6 Osobowość (Wielka Piątka) oraz 4.2.7 Wydajność pracy.

4.2.1 Kultura firmy

Mając na celu ujawnienie różnic pomiędzy firmami, które wdrożyły środki bezpieczeństwa informacji, a tymi, które ich nie wdrożyły, kultura firmy została uznana za kluczowy aspekt różniący firmy od siebie. W związku z tym, pierwszym krokiem dla uczestników badania było scharakteryzowanie samej kultury organizacyjnej firmy. Do analizy kultury firmy wykorzystano krótkie skale zaproponowane przez Jöns et al. (2005), używając 5-punktowej skali Likerta z 1 i 5 jako wartościami skrajnymi.

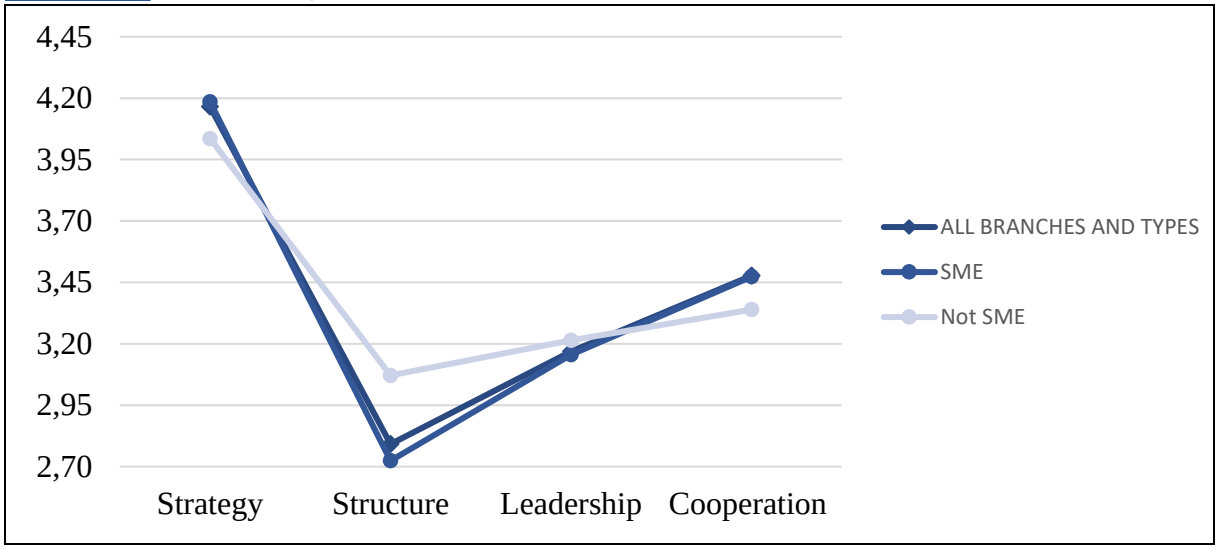
W tym kontekście respondenci zostali poproszeni o opisanie swoich firm za pomocą cech: "Strategia", "Struktura", "Przywództwo" i "Współpraca". Dla tych cech autorzy opracowali 18 pytań, które ilustruje tabela 1. Jak widać poniżej, istnieje znacząca różnica w umowach pomiędzy 18 pozycjami. Należy zatem wspomnieć, że niektóre z pozycji są sformułowane pozytywnie, a niektóre negatywnie. W konsekwencji, bezpośrednie porównanie nie daje natychmiastowych i jednoznacznych wyników. Co ważniejsze, w tym kontekście należy rozważyć agregację kategorii do czterech wyżej wymienionych dziedzin.

Question	N	Średnia	Odchylenie standardowe	Wariacja	Kurtoza	Błąd standardowy
Firma jest bardzo zorientowana na klienta.	83	4.37	0.79	0.63	3.34	0.52
Firma jest otwarta na innowacje.	83	4.19	0.82	0.67	1.73	0.52
Firma jest bardzo zorientowana na jakość.	84	4.13	0.97	0.93	0.47	0.52
Firma charakteryzuje się orientacją na pracę zespołową.	84	3.96	0.94	0.88	0.98	0.52
Firma jest silnie zorientowana na wyniki.	83	3.96	0.94	0.89	1.30	0.52
Kierownictwo pokłada duże zaufanie w pracownikach.	82	3.91	0.77	0.60	-0.19	0.53
Pracownicy pokładają duże zaufanie w kierownictwie.	84	3.87	0.89	0.79	1.32	0.52
Informacje o pracownikach mają wysoki priorytet.	82	3.76	0.90	0.80	-0.57	0.53
Pracownicy są zaangażowani w proces podejmowania decyzji.	82	3.67	0.99	0.99	0.29	0.53
Konflikty są w firmie rozwiązywane w sposób otwarty.	83	3.55	0.93	0.86	0.12	0.52
Firma jest silnie zhierarchizowana.	84	2.94	1.25	1.57	-0.98	0.52
W firmie panuje biurokratyczny styl zarządzania.	84	2.64	1.09	1.20	-0.82	0.52
Stosunki między pracownikami charakteryzuje rywalizacja.	84	2.52	1.11	1.24	-0.56	0.52
Kiedy w firmie pojawiają się błędy i problemy, w pierwszej kolejności szuka się winnych.	84	2.26	1.03	1.06	-0.27	0.52
Styl przywództwa w firmie jest autorytarny.	83	2.24	1.11	1.23	-0.52	0.52

Tabela 1: "Proszę wskazać, w jakim stopniu następujące cechy opisują firmę, dla której Pan(i) pracuje lub organizację, w której Pan(i) pracuje".

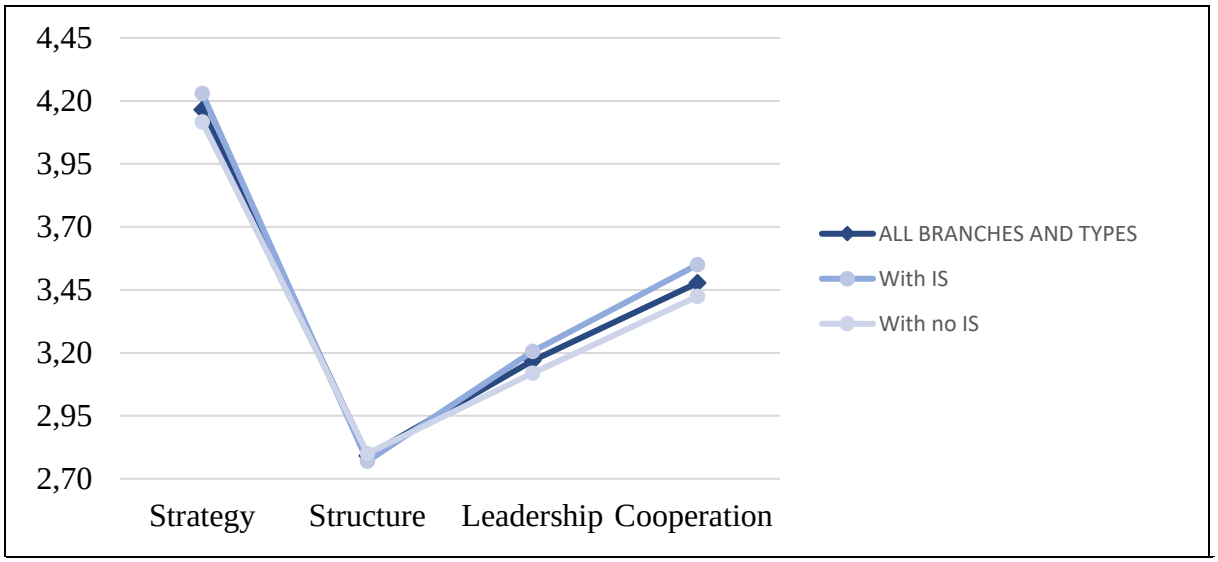
Wymienione wyżej cechy można wyróżnić ze względu na strategię, strukturę, przywództwo i współpracę. Autorzy definiują te kategorie w następujący sposób: orientacja na klienta, otwartość na innowacje, wysoka orientacja na jakość i wydajność należą do dziedziny strategii. W odniesieniu do struktury firmy ważne jest, aby wiedzieć, czy firma ma biurokratyczny styl zarządzania i czy jest silnie zhierarchizowana. Ostatni punkt prowadzi do następnej kategorii - przywództwa. W tym obszarze istotną rolę odgrywa styl przywództwa, priorytet informowania pracowników oraz zaangażowanie pracowników w podejmowanie decyzji. Ponadto, uczestnicy są pytani o sytuację, w której w firmie pojawiają się błędy i problemy. Wreszcie, takie tematy jak orientacja na zespół, zaufanie pracowników do menedżerów, radzenie sobie z konfliktami w firmie oraz relacje między pracownikami są częścią kategorii współpraca.

Jak wynika z wykresu 9, badane firmy charakteryzują się relatywnie wysoką orientacją strategiczną, niskim stopniem struktury hierarchicznej oraz niskim stopniem przywództwa dyrektorskiego. Widoczne jest, że firmy nienależące do sektora MŚP mają nieco wyższą wartość w obszarze struktury. Można przyjąć, że szczególnie duże firmy są bardziej zorganizowane hierarchicznie niż firmy małe i średnie. W zakresie strategii, przywództwa i współpracy można zaobserwować jedynie marginalne różnice między MŚP a firmami spoza sektora MŚP.



Wykres 9: Cechy pogrupowane w następujące kategorie "Strategia, Struktura, Przywództwo, Współpraca" - wszystkie firmy

Odnosząc się do początkowego pytania tej części ankiety można zauważyć, że istnieje niewielka różnica w stopniu współpracy, strategii i przywództwa, który jest wyższy w firmach, które podjęły działania w zakresie bezpieczeństwa informacji w porównaniu z firmami, które tego nie zrobiły. Biorąc pod uwagę aspekty leżące u podstaw tych kategorii,



Wykres 10: Cechy charakterystyczne pogrupowane w następujące kategorie "Strategia, Struktura, Przywództwo, Współpraca" - firmy posiadające strategię bezpieczeństwa informacji i firmy nieposiadające takiej strategii

4.2.2 Kompetencje w przedsiębiorstwie

W ramach badania, głównym celem było uzyskanie głębszego wglądu w najważniejsze kompetencje z zakresu bezpieczeństwa informacji, jakie powinni posiadać pracownicy zatrudnieni w MŚP. Respondenci zostali poproszeni o bliższe przyjrzenie się strategii bezpieczeństwa informacji w ich firmie oraz zadaniom, które są szczególnie istotne. Tabela 2 przedstawia przegląd różnych zadań i działań. Ważność danej czynności jest mierzona w

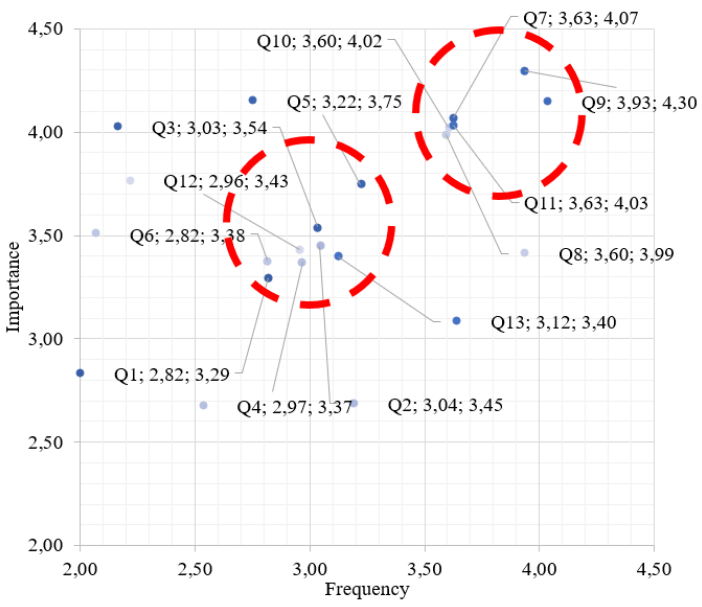
przedziale od "5 - bardzo ważne" do "1 - wcale", a częstotliwość od "5 - bardzo często" do "1 - nigdy".

Pytanie	Kod
Analiza procesów biznesowych i przygotowywanie raportów strategicznych z zakresu ochrony danych i bezpieczeństwa informacji	Q1
Śledzenie i raportowanie zmian wewnątrz i na zewnątrz organizacji, które mają wpływ na strategię bezpieczeństwa organizacji	Q2
Tworzenie polityki firmy w zakresie systematycznego postępowania z niektórymi informacjami i danymi	Q3
Opracowanie rekomendacji dotyczących zamawianego sprzętu, z uwzględnieniem wymogów firmy w zakresie bezpieczeństwa informacji i ochrony danych	Q4
Prowadzenie działań (informacyjnych) mających na celu zwiększenie świadomości pracowników w zakresie zagrożeń dla bezpieczeństwa w ich codziennej pracy oraz rozpowszechnianie wiedzy na temat bezpieczeństwa wśród pracowników	Q5
Tworzenie planów szkoleniowych dla firmy w celu regularnego szkolenia pracowników w zakresie bezpieczeństwa informacji i ochrony danych	Q6
Instalowanie oprogramowania typu firewall i antywirusowego. Przeprowadzanie aktualizacji i stosowanie elementarnych metod sprawdzania bezpieczeństwa oprogramowania używanego w firmie oraz sporządzanie odpowiedniej dokumentacji.	Q7
Zabezpieczanie urządzeń mobilnych, kanałów komunikacyjnych i przechowywania danych za pomocą haseł lub innych środków uwierzytelniania	Q8
Wykonywanie rutynowych kopii zapasowych danych oraz stosowanie właściwych metod postępowania zgodnie z GDPR w zakresie przetwarzania danych w firmie	Q9
Tworzenie kont administratorów i ograniczanie praw dostępu dla pracowników zgodnie z ustalonymi poziomami bezpieczeństwa	Q10
Ustalenie haseł dostępu dla poszczególnych pracowników oraz bezpiecznego procesu przechowywania i odzyskiwania danych.	Q11
Tworzenie polityk i procesów dotyczących występowania wszelkich roszczeń	Q12
Koordynowanie potrzeb menedżerów i pracowników firmy oraz dostarczanie obu stronom informacji i spostrzeżeń z firmy	Q13

Tabela 2: " Zadania i działania w dziedzinie bezpieczeństwa informacji "

Wykres 11 przedstawia wyniki w tabeli krzyżowej (częstotliwość jest wyświetlana na osi x; ważność jest wyświetlana na osi y). Ogólnie rzecz biorąc, żadne z wymienionych działań nie wykazuje niskiego stopnia ważności lub częstotliwości. Można jednak wyraźnie wyróżnić dwie grupy działań, jedna z nich charakteryzuje się zarówno wysoką częstotliwością, jak i znaczeniem, druga zaś średnią częstotliwością i znaczeniem. Grupy te zostały zakreślone kolorem czerwonym na poniższym rysunku.

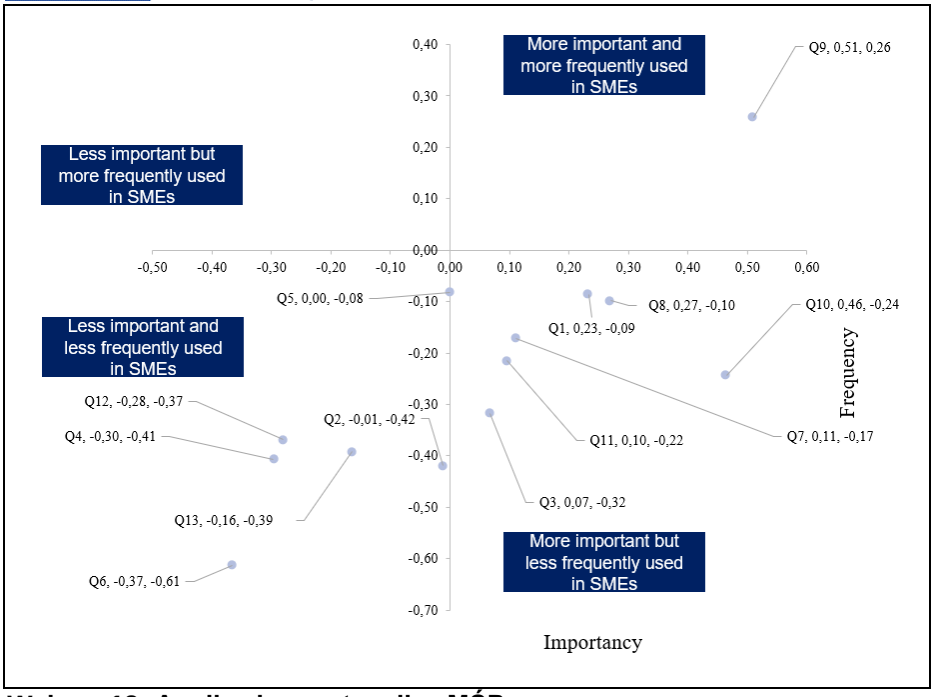
Pierwsza grupa kompetencji wykazuje wysokie wartości zarówno pod względem częstotliwości, jak i ważności. Do tej grupy należą kompetencje dotyczące "testów bezpieczeństwa", "kodowania", "zarządzania hasłami" i "kontroli dostępu opartej na rolach". W ramach tej grupy "zarządzanie danymi", tj. wykonywanie rutynowych kopii zapasowych danych oraz stosowanie właściwych metod postępowania zgodnie z GDPR przy przetwarzaniu danych, charakteryzuje się najwyższą ogólną wartością dotyczącą ważności i częstotliwości (Q9: 3,93; 4,30). Z drugiej strony, działania w obszarze "zarządzania procesami/interesariuszami/zgodnością", "zamówień w zakresie technologii informacyjno-komunikacyjnych", "uwrażliwiania i wywierania wpływu" oraz "edukacji i szkoleń" można zgrupować razem. Wszystkie kompetencje są uważane za raczej ważne, jednak ich częstotliwość nie może być określona jako szczególnie częsta. Jako najmniej ważny i najrzadziej występujący respondenci określają obszar "zarządzanie procesami". Obszar ten dotyczy analizy procesów biznesowych oraz przygotowywania raportów strategicznych z zakresu ochrony danych i bezpieczeństwa informacji. Niemniej jednak, wartość 2,82 wskazuje, że temat ten zdecydowanie cieszy się zainteresowaniem w firmach.



Moduły szkoleniowe	Kod
Zarządzanie procesem	Q1
Ocena ryzyka w zakresie technologii informacyjno-komunikacyjnych	Q2
Zarządzanie zgodnością	Q3
Zamówienia w dziedzinie technologii informacyjno-komunikacyjnych	Q4
Uwrażliwianie i wpływanie	Q5
Edukacja i szkolenie	Q6
Badanie bezpieczeństwa	Q7
Kodowanie	Q8
Zarządzanie danymi	Q9
Kontrola dostępu oparta o role	Q10
Zarządzanie hasłami	Q11
Zarządzanie ciągłością biznesu	Q12
Mediacje i zarządzanie interesariuszami	Q13

Wykres 11: Kompetencje w firmie - Wyniki

Poniższy wykres koncentruje się na analizie kompetencji w MŚP (Wykres 12). Dane opisują różnicę ważności pomiędzy MŚP a podmiotami spoza sektora MŚP: im wartość jest bliższa zeru, tym różnica jest mniejsza. Dlatego większe wartości oznaczają większe różnice. Wartości dodatnie oznaczają, że kompetencje są ważniejsze i częściej wykorzystywane w MŚP, podczas gdy wartości ujemne stanowią przeciwieństwo. Wszystkie wymienione wcześniej kompetencje można znaleźć w tabeli krzyżowej. Jeśli chodzi o opis osi, to należy zwrócić uwagę na to, że są to osie: w tym przypadku oś x pokazuje ważność; oś y pokazuje częstotliwość. Można wspomnieć, że zarządzanie danymi w domenie jest uważane za ważniejsze i częściej stosowane w MŚP. Wykres 11 pokazał już wysokie znaczenie zarządzania danymi (patrz Q9). Poniższy aspekt jest szczególnie interesujący w kontekście częściowej certyfikacji w zakresie bezpieczeństwa informacji: Kod Q6 opisuje kompetencje i działania w zakresie edukacji i szkoleń. Jak pokazuje wykres 12, kod Q6 można znaleźć w obszarze, który charakteryzuje się kompetencjami, które są mniej ważne i rzadziej stosowane w MŚP. Tworzenie planów szkoleniowych w celu regularnego szkolenia pracowników w zakresie bezpieczeństwa informacji i ochrony danych jest oczywiście mniej ważne dla MŚP.



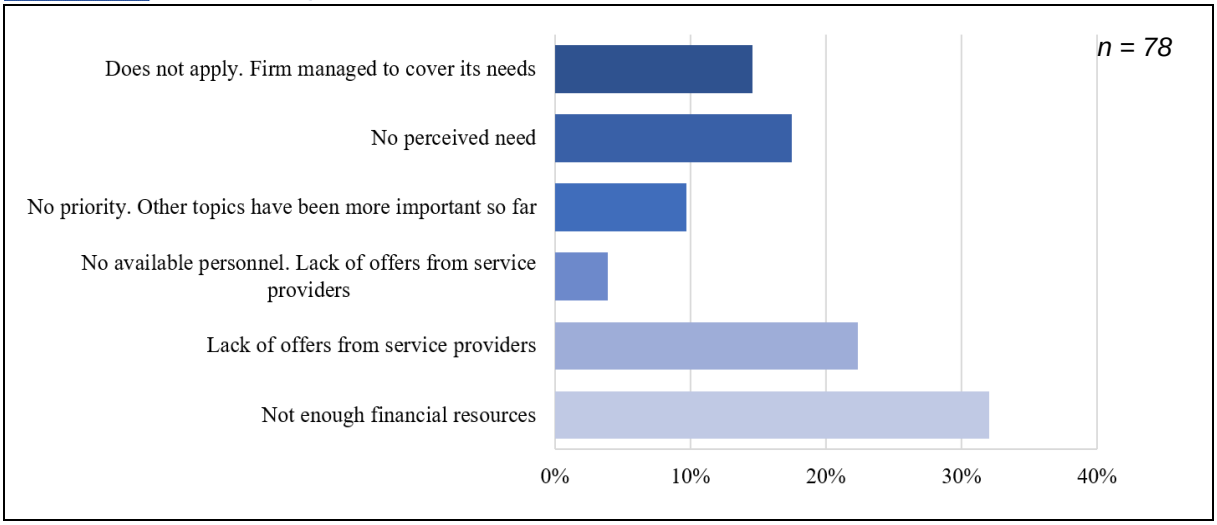
Wykres 12: Analiza kompetencji w MŚP

Okazuje się, że wszystkie kompetencje są dość ważne (średnia > 3,3) i często używane (średnia > 2,8). Najważniejsze i najczęściej wykorzystywane kompetencje to typowe zadania przeciętnego administratora systemu, np. tworzenie kopii zapasowych, instalacja oprogramowania antywirusowego i firewalli czy ustalanie indywidualnych haseł.

4.2.3 Bezpieczeństwo informacji w MŚP

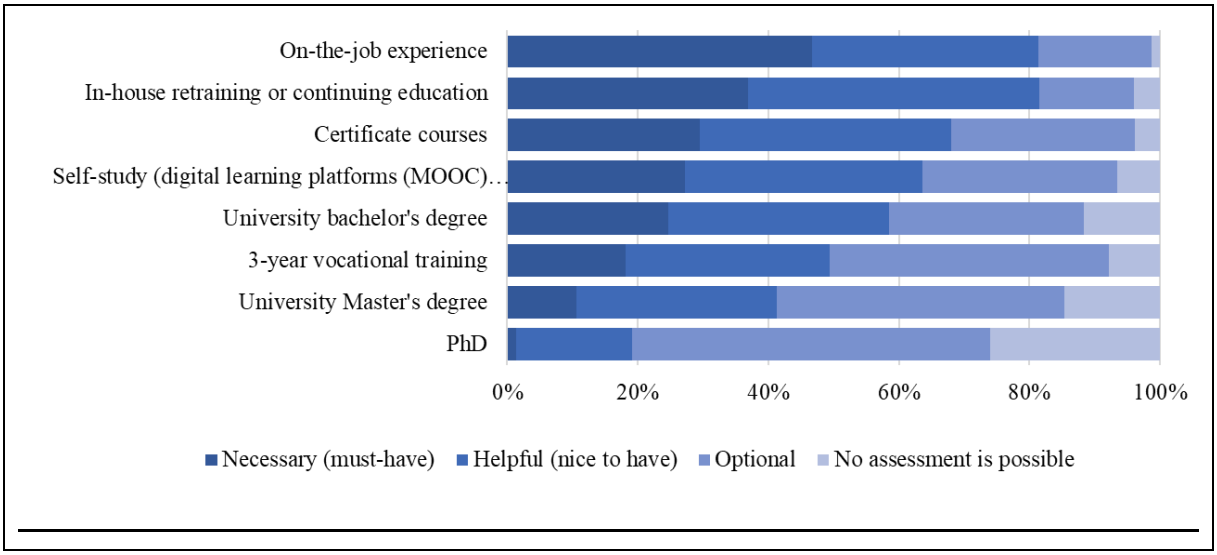
W tej części respondenci odpowiadali na bardziej szczegółowe pytania związane z bezpieczeństwem informacji w ich firmach. Badana kwestia dotyczy powodów, które powstrzymywały firmę przed inwestowaniem w poprawę bezpieczeństwa informacji (wykres 13). W badaniu biorą udział tylko te osoby, które jako typ firmy wybrały MŚP.

Jak widać na poniższym wykresie, głównym powodem jest brak wystarczających środków finansowych w firmach (ponad 30% respondentów podało ten powód). Poza tym, brak ofert ze strony dostawców usług jest również ważnym aspektem w odniesieniu do problemu inwestycji w dziedzinie bezpieczeństwa informacji. Z jednej strony, około 15% stwierdziło, że problem ten nie występuje w ich firmie, lub że firmy zdołały zaspokoić swoje potrzeby: jest to aspekt, który można uznać za dość pozytywny. Z drugiej strony, prawie jedna trzecia uczestników nie dostrzega żadnej potrzeby lub raczej nie widzi priorytetu i stwierdza, że inne tematy były do tej pory ważniejsze. Jest to dość poważna kwestia, która pokazuje, że temat bezpieczeństwa informacji nie jest jeszcze centralnym zagadnieniem we wszystkich firmach. Wreszcie, aspekt dotyczący dostępnego personelu wydaje się odgrywać raczej mniej istotną rolę. Tylko około 4 uczestników wskazało na związek pomiędzy brakiem personelu a problemem inwestycji w bezpieczeństwo informacji.



Wykres 13: " Jakie powody powstrzymywały do tej pory Państwa firmę przed inwestowaniem w poprawę bezpieczeństwa informacji?"

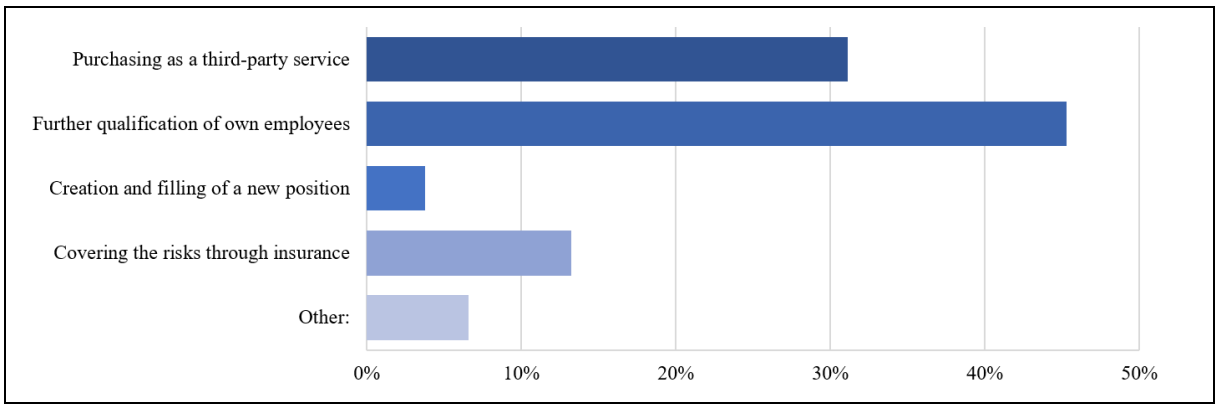
Respondenci podkreślają znaczenie poszczególnych rodzajów wykształcenia niezbędnego do zapewnienia bezpieczeństwa informacji w firmie. W tym kontekście zadano pytanie o to, jakiego rodzaju wykształcenie jest niezbędne/pomocne/ itp. dla pracownika odpowiedzialnego za zapewnienie bezpieczeństwa informacji w firmie. Należy zaznaczyć, że istnieje różnica pomiędzy umiejętnościami lub szkoleniami niezbędnymi ("must-have") a umiejętnościami lub szkoleniami przydatnymi ("nice-to-have"). Wykres 14 pokazuje, że duże znaczenie ma doświadczenie w pracy. Prawie połowa uczestników uważa ten punkt za "must-have". Ponadto, szkolenia wewnętrzne lub kształcenie ustawiczne są również istotne i pomocne. Generalnie widać, że respondenci wolą mieć pracownika z doświadczeniem niż z wykształceniem. Wszystkie formy studiów nieklasycznych są nieco mniej istotne i ważniejsze niż wykształcenie wyższe.



Wykres 14: "Opierając się na Pana/Pani doświadczeniu, jakiego rodzaju wykształcenie lub szkolenia są niezbędne/pomocne/opcjonalne dla pracownika odpowiedzialnego za zapewnienie bezpieczeństwa informacji w Pana/Pani organizacji?"

W ramach badania respondenci zostali również zapytani o możliwe opcje zwiększenia bezpieczeństwa informacji (wykres 15). Największą popularnością cieszy się możliwość podniesienia kwalifikacji pracowników, która została wybrana w prawie 50% przypadków. Drugą opcją jest zakup usługi zewnętrznej, która została wybrana w 30% przypadków.

Natomiast utworzenie i obsadzenie nowego stanowiska lub zabezpieczenie ryzyka poprzez ubezpieczenie nie jest już tak popularne.

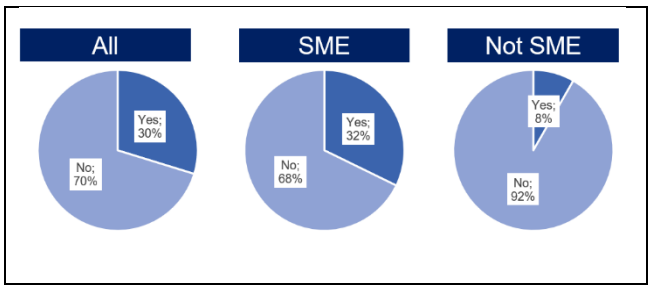


Wykres 15: Możliwe opcje zwiększenia bezpieczeństwa informacji

Badanie dotyczące bezpieczeństwa informacji w MŚP pokazuje, że brak środków finansowych i usług firm trzecich w zakresie bezpieczeństwa informacji to główne przyczyny problemu inwestycyjnego w tym obszarze. Jest to szczególnie ważne, ponieważ respondenci chcą korzystać z usług firm zewnętrznych w celu poprawy bezpieczeństwa informacji w ich firmie. Ze względu na brak finansów i podaży na rynku usług bezpieczeństwa, wydaje się, że nasi respondenci wolą podnosić kwalifikacje swoich pracowników, aby utrzymać rozrywkowy poziom bezpieczeństwa informacji. Jest to zbieżne z wymaganiami edukacyjnymi: respondenci wolą zatrudniać osoby z doświadczeniem niż z wykształceniem.

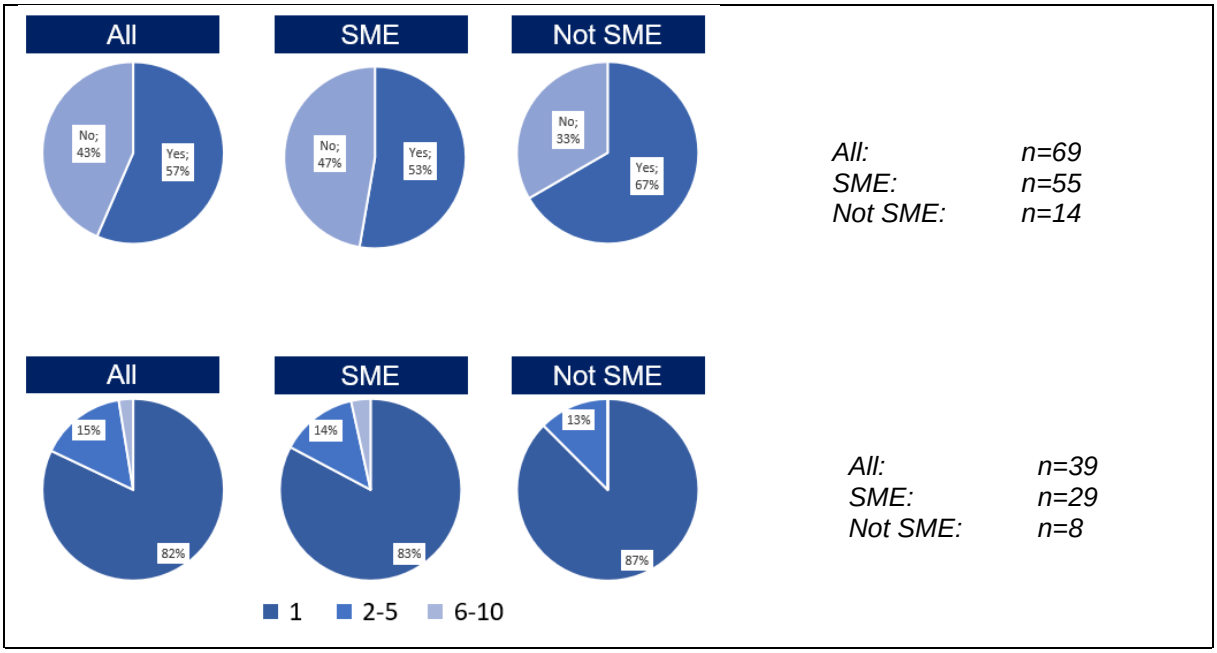
4.2.4 Bezpieczeństwo informacji w przedsiębiorstwie: wymagania dotyczące personelu

Kolejną kwestią, która została przeanalizowana w ramach badania, były wymagania dotyczące personelu w zakresie bezpieczeństwa informacji w firmie. W tym celu przeanalizowano nie tylko zróżnicowanie pomiędzy MŚP i firmami spoza sektora MŚP, ale także różne sytuacje firm pod względem występowania incydentów związanych z bezpieczeństwem informacji. Szczególnie ta ostatnia kwestia daje jasny obraz zmieniających się postaw firm wobec bezpieczeństwa informacji i wydatków na bezpieczeństwo informacji. Występowanie incydentów bezpieczeństwa informacji przedstawiono na wykresie 16.



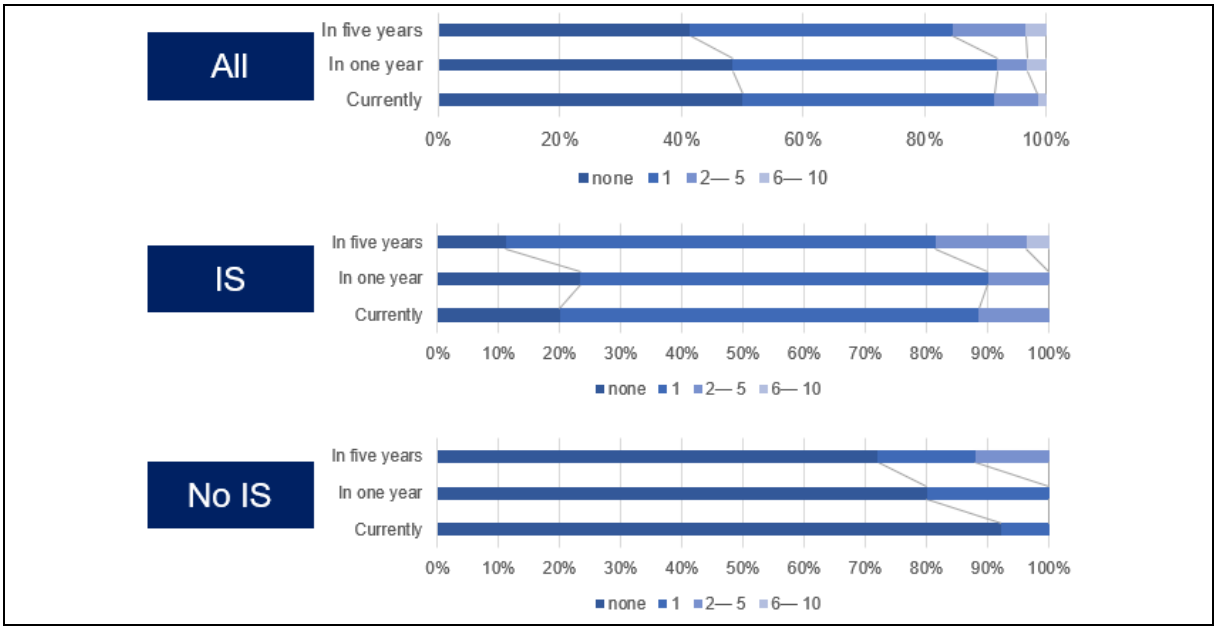
Wykres 16: " Czy wiedzą Państwo o jakichkolwiek incydentach związanych z bezpieczeństwem informacji w ciągu ostatnich 2 lat lub istnieje podejrzenie, że taki incydent miał miejsce?"

W celu lepszego zrozumienia realiów kadrowych w firmach, respondenci zostali zapytani o to, ilu pracowników zatrudniają obecnie, których głównym zadaniem jest zapewnienie bezpieczeństwa informacji, oraz ilu pracowników planują zatrudnić w najbliższych latach. Okazuje się, że w większości firm jest zwykle jeden pracownik, który formalnie odpowiada za bezpieczeństwo informacji. Nawet w firmach nie będących MŚP zwykle nie ma większej liczby pracowników odpowiedzialnych za ten obszar działalności (Wykres 17). Powyżej pokazano, czy jest zatrudniony personel, poniżej można zobaczyć równoważne liczby firm, które odpowiedziały na pierwsze pytanie.



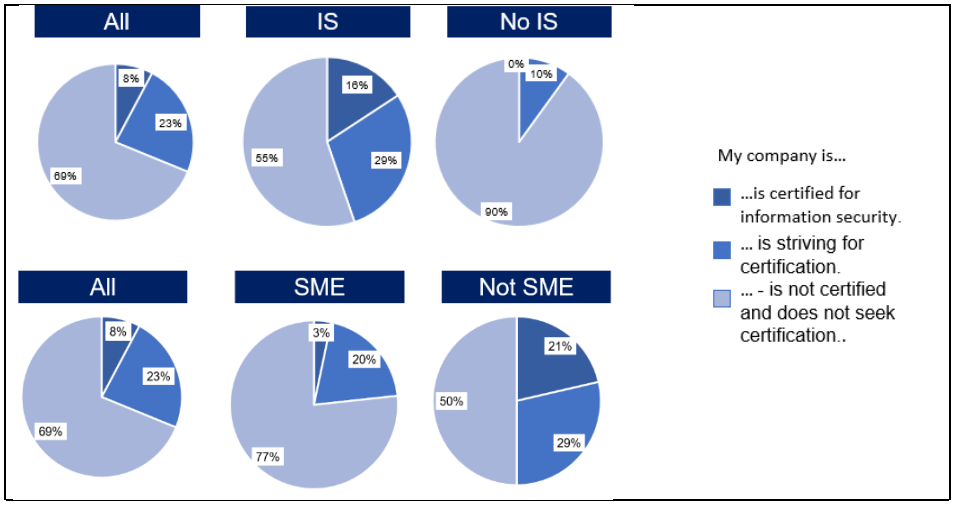
Wykres 17: " Czy w Państwa firmie są pracownicy, którzy są formalnie odpowiedzialni za bezpieczeństwo informacji? (powyżej) - Jeśli tak, to ilu?" (niżej)

Następnie zapytano, ile jest w firmie otwartych stanowisk związanych z bezpieczeństwem informacji. Jak wynika z wykresu 18, około 50% respondentów odpowiedziało, że w ich firmie nie ma obecnie otwartych stanowisk związanych z bezpieczeństwem informacji. Biorąc pod uwagę wystąpienie incydentu związanego z bezpieczeństwem informacji (IS), można zauważyć gwałtowny wzrost liczby tworzonych stanowisk. Wśród firm, w których nie wystąpił incydent bezpieczeństwa informacji (NO IS), około 90% nie posiada żadnego konkretnego stanowiska związanego z bezpieczeństwem informacji. Liczba ta spada do zaledwie 20% w porównaniu z firmami, które doświadczyły incydentu. Porównywalne liczby zostały odnotowane w przypadku istnienia więcej niż jednego stanowiska, co ilustruje inicjatywę, jaką firmy podejmują po ataku.



Wykres 18: "Ile jest wolnych stanowisk związanych z bezpieczeństwem informacji w Państwa firmie?"

W tym kontekście, respondenci zostali dodatkowo zapytani o to, w jaki sposób radzą sobie z potrzebami kadrowymi w zakresie bezpieczeństwa informacji. Wykres 20 pokazuje, że szczególnie firmy spoza sektora MŚP przywiązują dużą wagę do doskonalenia zawodowego pracowników. Jeśli chodzi o MŚP, można zauważyć, że zakup usług z zakresu "bezpieczeństwa informacji" od zewnętrznych dostawców jest w przybliżeniu równoważny z dalszym szkoleniem pracowników. Z kolei zatrudnianie nowych pracowników jest mniej istotne dla firm. Można więc stwierdzić, że ogólnie rzecz biorąc, rozwój wewnętrznego potencjału i dalsze szkolenie własnych pracowników jest uważane za najbardziej odpowiednie rozwiązanie dla większości firm. Niemniej jednak istnieje pewne zastrzeżenie co do wiarygodności przedstawionych danych, które staje się oczywiste, gdy weźmie się pod uwagę firmy, które doświadczyły incydentu związanego z bezpieczeństwem informacji oraz firmy, które tego nie zrobiły. Jak widać na rys. 21, pozycja "brak środków" zmniejsza się z 31% (najczęściej wymieniana) wśród firm, w których nie wystąpił incydent bezpieczeństwa informacji do zaledwie 10% (najrzadziej wymieniana) wśród firm, w których wystąpił incydent bezpieczeństwa informacji.

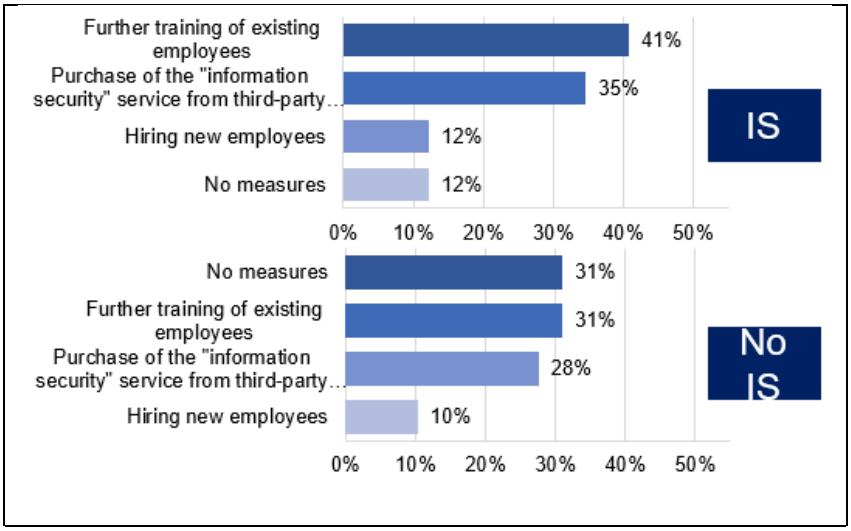


Wykres 19: Certyfikacja biznesowa w zakresie bezpieczeństwa

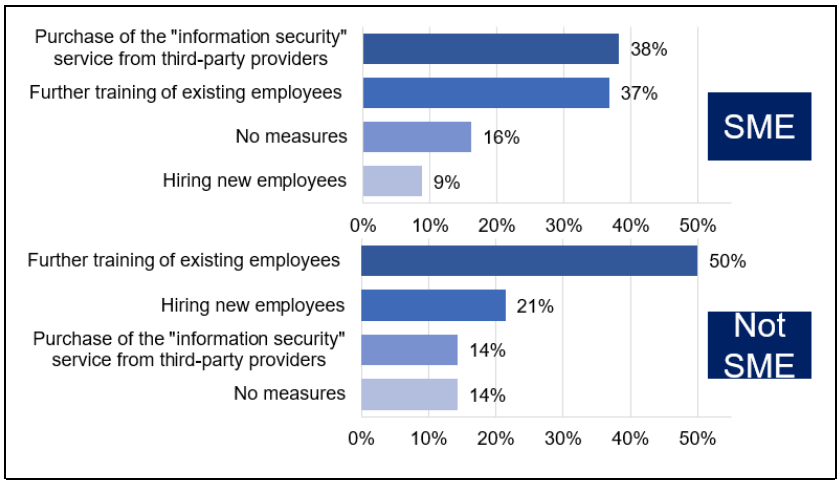
Analogiczne liczby można zaobserwować w przypadku certyfikacji wśród MŚP i firm spoza sektora MŚP, a także wśród firm, w których wystąpił incydent związany z bezpieczeństwem informacji. Podczas gdy certyfikaty są ledwie widoczne wśród MŚP (3%), są one całkowicie nieobecne wśród MŚP, w których nie wystąpił incydent związany z bezpieczeństwem informacji. W przypadku firm, w których wystąpił incydent, liczba zarówno istniejących, jak i planowanych certyfikacji znacząco wzrasta.

Biorąc pod uwagę zakres tego badania, ważne jest nie tylko zrozumienie sytuacji w zakresie certyfikacji i inwestycji, ale także działań już podjętych w celu sprostania wyzwaniom związanym z bezpieczeństwem informacji.

Jak widać na poniższym wykresie, dwie trzecie respondentów odpowiedziało na to pytanie przecząco.



Wykres 21: " Jak do tej pory radzą sobie Państwo z potrzebami kadrowymi w obszarze bezpieczeństwa informacji?" – IS i brak IS



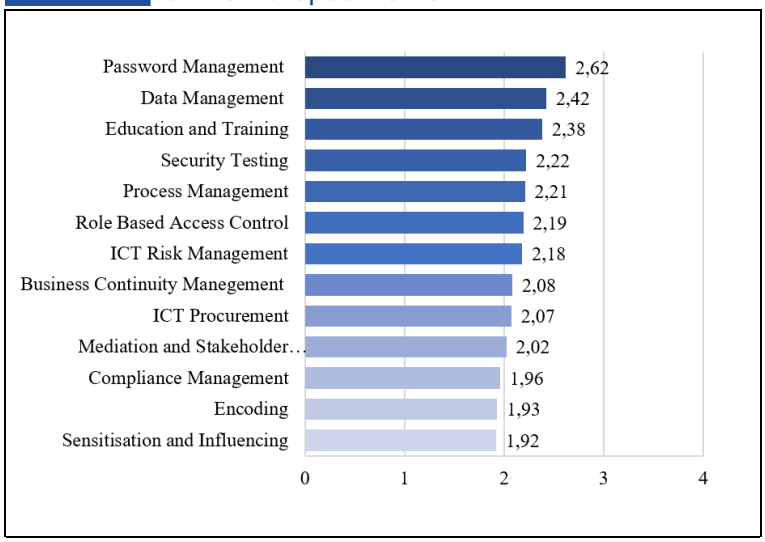
Wykres 20: "Jak do tej pory radzili sobie Państwo z zapotrzebowaniem na personel w obszarze bezpieczeństwa informacji"

Oznacza to jednak również, że około 30 % odpowiedziało twierdząco.

Biorąc pod uwagę wnioski z wykresów 18 i 21, oczywisty staje się pogląd, że firmy podejmują aktywność dopiero po ataku. Firmy nie tylko widzą potrzebę utworzenia etatowego stanowiska, ale również szukają możliwości poprawy bezpieczeństwa informacji wszelkimi możliwymi sposobami. Można stwierdzić, że istniejące wśród praktyków bezpieczeństwa informacji i społeczności zajmującej się bezpieczeństwem informacji przekonanie, że "nauka przez ból" jest dokładnym opisem rzeczywistości panującej w większości firm. Zrozumienie dla podejmowania ostrych środków i inwestowania zasobów w pracowników rośnie najczęściej dopiero po ataku - kiedy szkody są już wyrządzone.

4.2.5 Samoocena kompetencji

W ramach badania respondenci zostali poproszeni o ocenę samych siebie w odniesieniu do odpowiednich działań edukacyjnych i szkoleniowych w zakresie bezpieczeństwa informacji. Poniższy wykres pokazuje, że zarządzanie hasłami i danymi było często wymieniane. Obejmuje to na przykład ustanawianie haseł lub wykonywanie rutynowych kopii zapasowych danych.



Wykres 22: " Proszę ocenić siebie: Które z poniższych działań edukacyjnych i szkoleniowych możesz wykonać?"

4.2.6 Osobowość (Wielka Piątka)

W trakcie wielu dyskusji z ekspertami, stało się jasne, że zawód związany z bezpieczeństwem informacji stawia przed praktykami specjalne wymagania dotyczące ich umiejętności społecznych. Stało się jednak oczywiste, że w większości przypadków, w sposób dorozumiany, odnosi się to również do cech osobowych. W związku z tym, "właściwa postawa" nie ogranicza się do postępowania z pracownikami i w sferze miejsca pracy, ale do postępowania w ogóle, biorąc pod uwagę dyspozycje charakterologiczne. Dlatego też celem niniejszego badania jest rzucenie pewnego światła na dyspozycje cech charakteru i wydajność pracy wśród ekspertów ds. bezpieczeństwa informacji. Wyniki mogą być postrzegane jako wskazanie korzystnych warunków wstępnych dla nowych pracowników w miejscu pracy. W tym celu zastosowano Wielką Piątkę cech osobowości (Rammstedt et al. 2013), dostarczającą pięcioczynnikowego modelu grupowania cech osobowości. Zgodnie z tym modelem, pięć następujących podstawowych czynników opisuje większość cech osobowości w sposób dychotomiczny, gdzie każda cecha pociąga za sobą dwie skrajności:

Cecha	Wysokie wyniki	Niskie wyniki
Otwartość	pomysłowy/ciekawy	konsekwentny/ostrożny
Sumienność	skuteczny/zorganizowany	ekstrawagancki/nieostrożny
Ekstrawersja	uczuciowy, wesoły, gadatliwy, kochający zabawę, aktywny, pełen pasji	powściągliwy, zamknięty w sobie, cichy, trzeźwy, pasywny, nieczuły
Ugodowość	przyjazny/ współczujący	krytyczny/racjonalny
Neurotyzm	wrażliwy/ nerwowy	odporny/pewny siebie

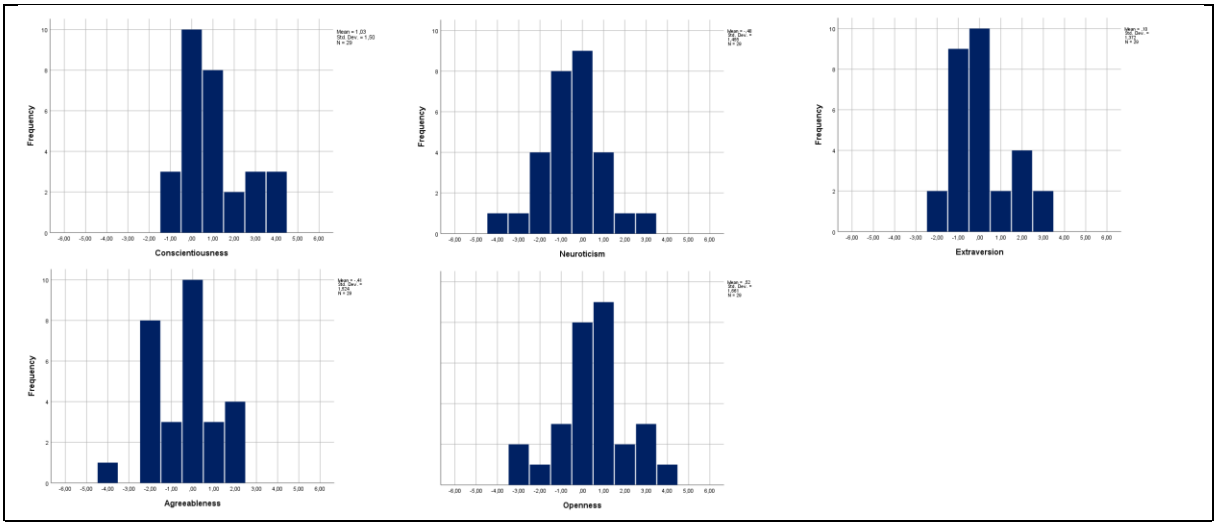
Tabela 3: Wymiary Wielkiej Piątki.

BFI-10 jest 10-stopniową skalą mierzącą wyżej wymienione cechy. Skala ta została opracowana w taki sposób, aby była krótka i przeznaczona do sytuacji, w których respondenci mają ograniczony czas. Każda skala BFI-10 składa się z jednej pozycji ocenianej prawdziwie i jednej ocenianej fałszywie, np. aby uzyskać pomiar otwartości, wartość z pytania szóstego jest wyodrębniana z wartości pytania dziesiątego. Im wyższy wynik, tym bardziej pomysłowa/ciekawska jest dana osoba.

Nr.	Pozycje	Po-laryzacja	Podskala
1	Widzę siebie jako kogoś, kto jest powściągliwy.	-	Ekstrawersja
2	Postrzegam siebie jako osobę, która jest ogólnie ufna.	+	Ugodowość
3	Postrzegam siebie jako kogoś, kto ma tendencję do bycia leniwym.	-	Sumienność
4	Postrzegam siebie jako osobę, która jest zrelaksowana, dobrze radzi sobie ze stresem.	-	Neurotyczność
5	Postrzegam siebie jako osobę, która ma niewiele zainteresowań artystycznych.	-	Otwartość
6	Postrzegam siebie jako kogoś, kto jest otwarty, towarzyski.	+	Ekstrawersja
7	Postrzegam siebie jako osobę, która ma tendencję do szukania wad u innych.	-	Ugodowość
8	Postrzegam siebie jako kogoś, kto wykonuje dokładną pracę.	+	Sumienność
9	Łatwo się denerwuję.	+	Neurotyczność
10	Mam aktywną wyobraźnię.	+	Otwartość

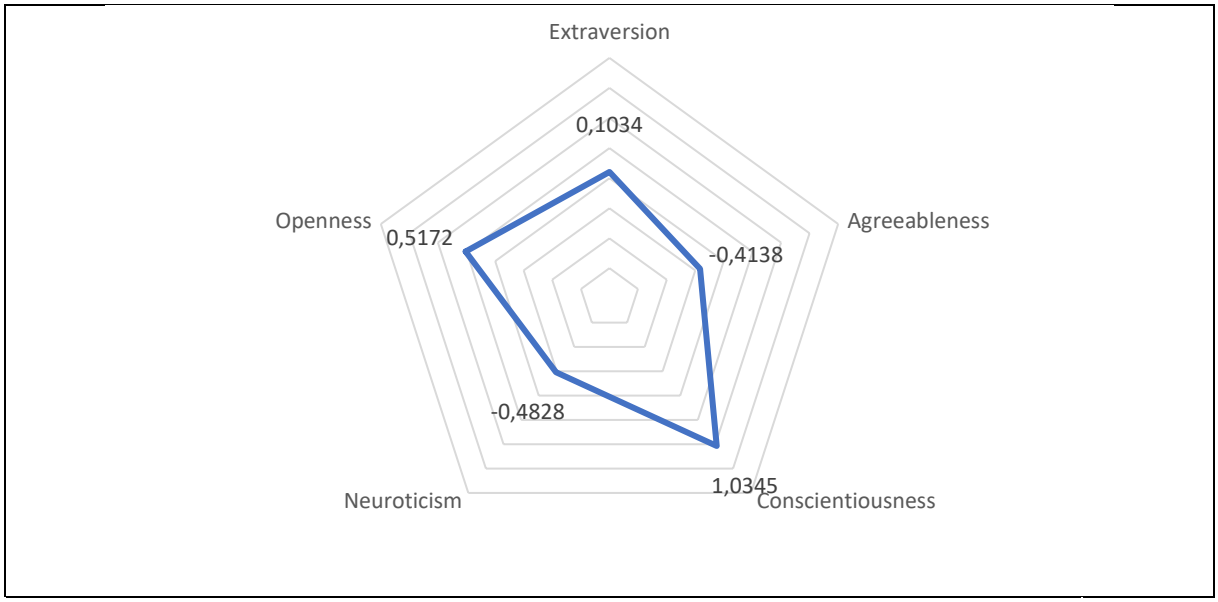
Tabela 4: Struktura BFI-10

Z poniższych histogramów można wywnioskować, że wśród wszystkich respondentów przeważają osoby wydajne/zorganizowane, a nie ekstrawaganckie/nieostrożne (zob. sumienność). Odpowiedzi rozkładają się dodatnio również w przypadku otwartości; widzimy, że więcej respondentów identyfikuje się jako pomysłowi/ciekawscy niż konsekwentni/ostrożni (zob. otwartość). Odpowiedzi niemal równo rozkładają się w definicjach ekstrawersji, z marginalną pozytywną pobłażliwością, tzn. respondenci są uważani za bardziej wybiegających/energetycznych niż samotnych/rezerwowych (w bardzo ograniczonym zakresie). Odwrotną sytuację można zaobserwować w przypadku neurotyczności i ugodowości. W tym przypadku respondenci są bardziej odporni/pewni siebie i krytyczni/racjonalni niż odpowiednio wrażliwi/ nerwowi i przyjaźni/współczujący. Ogólną pobłażliwość można zauważyć na wykresie 24..



Wykres 23: Histogramy Wielkiej Piątki odnotowane przez praktyków bezpieczeństwa informacji.

Z łagodnego traktowania można wywnioskować kilka istotnych założeń dotyczących cech charakteru ekspertów ds. bezpieczeństwa informacji. Najbardziej dominującym czynnikiem jest dodatnia wartość dla sumienności, pociągająca za sobą silne dyspozycje do efektywnego i zorganizowanego postępowania. Ujemne wartości neurotyczności potwierdzają opinię ekspertów, że odporność i wiara we własną pracę odgrywają ważną rolę w pracy. Ponadto, eksperci mogą być scharakteryzowani jako konsekwentni i ostrożni (otwartość), krytyczni i racjonalni (ugodowość) oraz w ograniczonym stopniu powściągliwi (ekstrawersja).



Wykres 24: Wielka Piątka, porównanie średnich wartości

Jak widać z macierzy wagowej przedstawionej w tabeli 5, generalnie wszystkie pozycje wykazują najwyższy ładunek na odpowiadającym im czynniku, zgodnie z hipotezami. Przemawia to na korzyść słuszności tego podejścia w naszym przypadku.

Pozycja	E	A	C	N	O
Postrzegam siebie jako kogoś, kto jest powściągliwy.	**,411***	0.067	0.212	-0.264	-0.169
Postrzegam siebie jako osobę, która jest ogólnie ufna.	**-,422***	**-,572****	-0.054	-0.081	0.210
Postrzegam siebie jako kogoś, kto ma tendencję do bycia leniwym.	-0.163	0.138	**-,597****	0.097	0.294
Postrzegam siebie jako osobę, która jest zrelaksowana, dobrze radzi sobie ze stresem.	0.193	0.039	0.113	**-,379***	-0.233
Postrzegam siebie jako osobę, która ma niewiele zainteresowań artystycznych.	-0.101	-0.006	**-,375***	0.089	**,670****
Postrzegam siebie jako kogoś, kto jest otwarty, towarzyski.	**-,635****	**-,401***	-0.194	0.067	0.095
Postrzegam siebie jako osobę, która ma tendencję do szukania wad u innych.	0.091	**,538****	-0.154	0.283	-0.026
Postrzegam siebie jako kogoś, kto wykonuje rzetelną pracę.	0.281	0.039	**,566****	-0.335	-0.264
Postrzegam siebie jako osobę, która łatwo się denerwuje.	-0.137	0.350	-0.271	**,678****	0.000
Postrzegam siebie jako kogoś, kto ma aktywną wyobraźnię.	0.191	0.267	0.175	-0.137	**-,493****

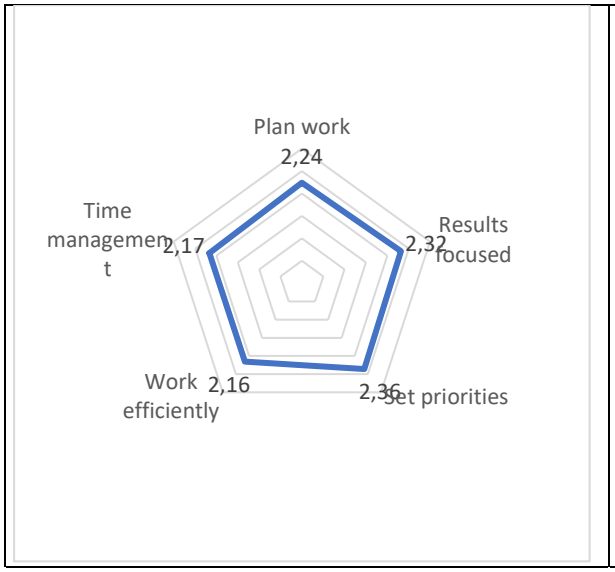
Tabela 5: " Badanie poprawności: Korelacja między pozycjami i grupami "

Respondenci powściągliwi myślą o sobie jako o osobach zrelaksowanych. Uważają też, że wykonują rzetelną pracę i mają aktywną wyobraźnię. Respondenci, którzy określili się jako ogólnie ufni, są też bardziej otwarci i towarzyscy. Leniwi respondenci mają mało zainteresowań artystycznych, są towarzyscy, ale też doszukują się wad u innych. Zrelaksowani uważają, że wykonują rzetelną pracę i mają aktywną wyobraźnię. Ci, którzy mają skłonność do doszukiwania się wad u innych, łatwo się denerwują i widzą siebie jako kogoś, kto ma aktywną wyobraźnię. Wreszcie, respondenci "dokładni" mają aktywną wyobraźnię.

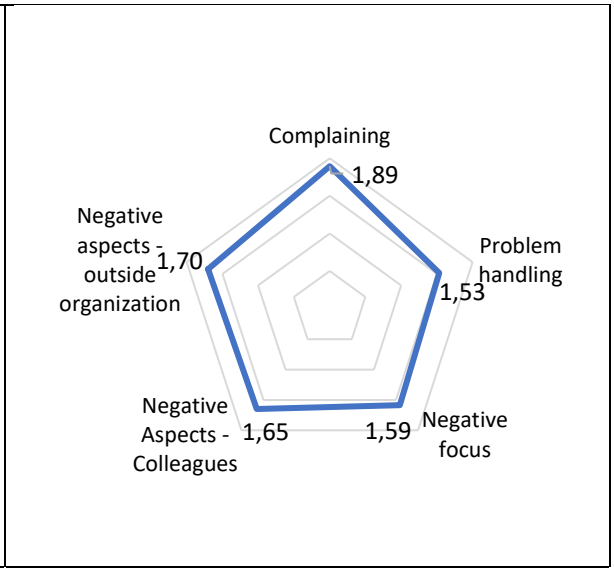
4.2.7 Wyniki pracy

- Ta część oparta jest na Kwestionariuszu Indywidualnej Wydajności Pracy (IWPQ). IWPQ to 18-pozycyjna skala opracowana przez Ramos-Villagrasa i wsp. (2019) do pomiaru trzech głównych wymiarów wydajności pracy:
- wydajność zadaniowa (5 pozycji)
- wydajność kontekstowa (8 pozycji)
- kontrproduktywne zachowanie w pracy (5).

Wszystkie pozycje mają trzymiesięczny okres przywoływania i 5-stopniową skalę ocen (0 = rzadko do 4 = zawsze dla wykonania zadania i zachowania w kontekście; oraz 0 = nigdy do 4 = często dla zachowań kontrproduktywnych w pracy). W przypadku zachowań kontrproduktywnych skala ma biegunowość ujemną, a więc niższe wartości są bardziej pożądane, ponieważ przekłada się to na ogólnie niższy poziom zachowań kontrproduktywnych. Odpowiednie wartości przedstawiono na wykresach od 25 do 27, a ostateczny profil połączony na wykresie 28.

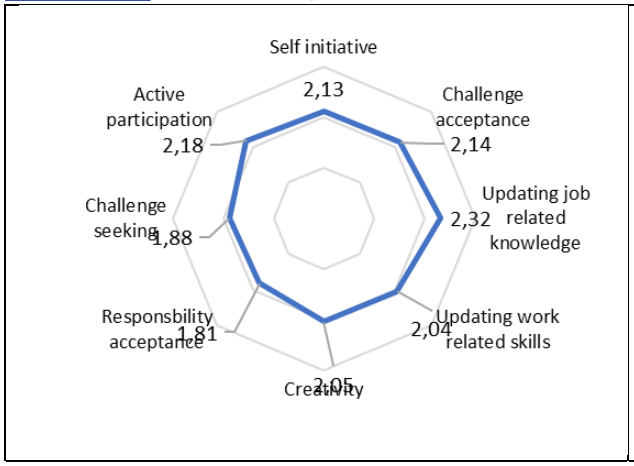


Wykres 25: Wykonywanie zadań

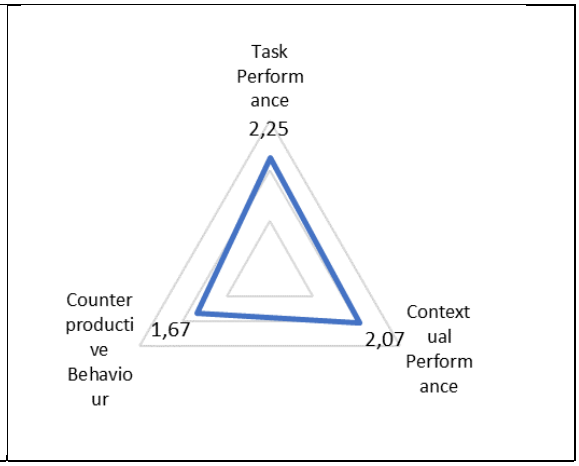


Wykres 26: Zachowania kontrproduktywne

Zwraca uwagę fakt, że uczestnicy uzyskali niski wynik dla zachowań kontrproduktywnych, co potwierdza wynik z testu BIG.5, że odporność i wysoki wskaźnik tolerancji są ważnymi aspektami w pracy praktyka bezpieczeństwa informacji. Patrząc na poszczególne kategorie, najbardziej wyróżniającymi się czynnikami są "aktualizowanie wiedzy związanej z pracą" (2,32) i "aktywne uczestnictwo" wśród zachowań kontekstowych, słaba "koncentracja na negatywnych aspektach pracy" (1,59) i silna orientacja na "radzenie sobie z problemami" (1,53) wśród zachowań kontrproduktywnych oraz wysoka koncentracja na "ustalaniu priorytetów" (2,36) i "koncentracja na wynikach" (2,32) wśród zachowań zadaniowych.



Wykres 27: Wydajność kontekstowa



Wykres 28: Wyniki IWPQ dla ekspertów ds. bezpieczeństwa informacji

Jak pokazano na wykresie 28, miara wydajności zadaniowej jest wyższa niż inne miary, a miara wydajności kontekstowej jest wyższa niż miara zachowań kontrproduktywnych. Wyniki te są zgodne z poprzednimi badaniami. Mimo to, wykonanie zadania jest znacząco niższe niż wyniki bazowe z innych artykułów, co wskazuje na problemy w tej dziedzinie - wyższe miary dla zachowań kontrproduktywnych potwierdzają to ustalenie. Pomiar wydajności kontekstowej jest również niższy niż ten z innych badań, ale nie znacząco.

Podsumowując, można powiedzieć, że uczestnicy z branży IT i bezpieczeństwa informacji są mniej produktywni niż ci, których zwykle obserwuje się w odpowiednich badaniach.

4.3 Podsumowanie

Ogólnie rzecz biorąc, badanie dostarcza ważnych spostrzeżeń na temat bezpieczeństwa informacji w MŚP. Jeśli chodzi o sytuację na rynku pracy i możliwości w firmach, należy wspomnieć, że w ponad 50% firm nie ma pracownika, który byłby formalnie odpowiedzialny za bezpieczeństwo informacji. Jeśli uczestnicy badania odpowiedzieli twierdząco, to w większości przypadków tylko jeden pracownik jest odpowiedzialny za ten obszar działalności. Patrząc na rozwój ofert pracy można zaobserwować niewielkie zmiany. Ułamek firm stworzy około sześciu do dziesięciu miejsc pracy w obszarze bezpieczeństwa informacji w ciągu najbliższych pięciu lat.

Wyniki badań potwierdzają istniejące przekonanie o "uczeniu się przez ból", tzn. że najpierw musi dojść do incydentu, zanim firmy podejmą działania związane z bezpieczeństwem. Stwierdzenie to jest poparte spójnymi ustaleniami dotyczącymi certyfikacji, tworzenia określonych stanowisk i ogólnie podejmowanych działań w zakresie bezpieczeństwa informacji.

Jeśli chodzi o wymagany rodzaj wykształcenia i szkoleń, można wskazać na duże znaczenie doświadczenia zawodowego. Prawie połowa uczestników stwierdziła, że jest to szczególnie istotne. Ogólnie rzecz biorąc, respondenci wolą mieć pracownika z doświadczeniem niż z wykształceniem. W świetle istniejącego niedoboru możliwości zatrudnienia na rynku pracy, firmy uważają, że podnoszenie kwalifikacji obecnych pracowników jest najbardziej realną opcją pokrycia zapotrzebowania na zasoby ludzkie.

Wreszcie, ocena charakterystycznych cech za pomocą testu osobowości Big 5 i IWPQ, pozwoliła zidentyfikować ważne cechy pracowników, które mogą być określone wśród nowych pracowników w tej dziedzinie. Wśród silnych dyspozycji odpornościowych w obu testach,

szczególnie dobrze zorganizowana rutyna pracy oraz krytyczne i analityczne podejście zostały określone jako cechy charakterystyczne dla specjalistów ds. bezpieczeństwa informacji.

5 Przewodnik dla MŚP

Ochrona danych i bezpieczeństwo informacji nabrały istotnego znaczenia wraz ze wzrostem intensywności stosowania ICT w procesach organizacji i zarządzania w MŚP. Presja MŚP na lepsze zarządzanie bezpieczeństwem informacji i ochroną danych wynika z kilku czynników. Po pierwsze, zarządzanie procesami i danymi w MŚP stało się w dużym stopniu zależne od infrastruktury ICT. Po drugie, ustawodawstwo dotyczące prywatności i ochrony danych zostało wzmocnione i skodyfikowane w sposób bardziej szczegółowy. Po trzecie, wzrosła świadomość społeczna w zakresie prawa do prywatności i odpowiedzialności za wykorzystanie danych osobowych. Kilka incydentów związanych z wyciekiem danych na całym świecie również przyczyniło się do uświadomienia sobie, że bezpieczeństwo informacji jest kwestią priorytetową przy korzystaniu z usług cyfrowych. MŚP zostały dotknięte digitalizacją w mniejszym stopniu niż duże przedsiębiorstwa. Jednak znaczna część z nich pracuje z osobistymi dokumentami cyfrowymi. Niektóre z nich zarządzają danymi wrażliwymi. Wszystkie te czynniki stanowią podstawę do lepszego uregulowania i zapewnienia bezpieczeństwa informacji i ochrony danych w MŚP. Zaktualizowane regulacje Unii Europejskiej sprawiły, że niektóre MŚP mają problemy ze znalezieniem lub przygotowaniem odpowiedniego personelu, który mógłby spełnić bardziej rygorystyczne wymagania w zakresie bezpieczeństwa informacji i ochrony danych.

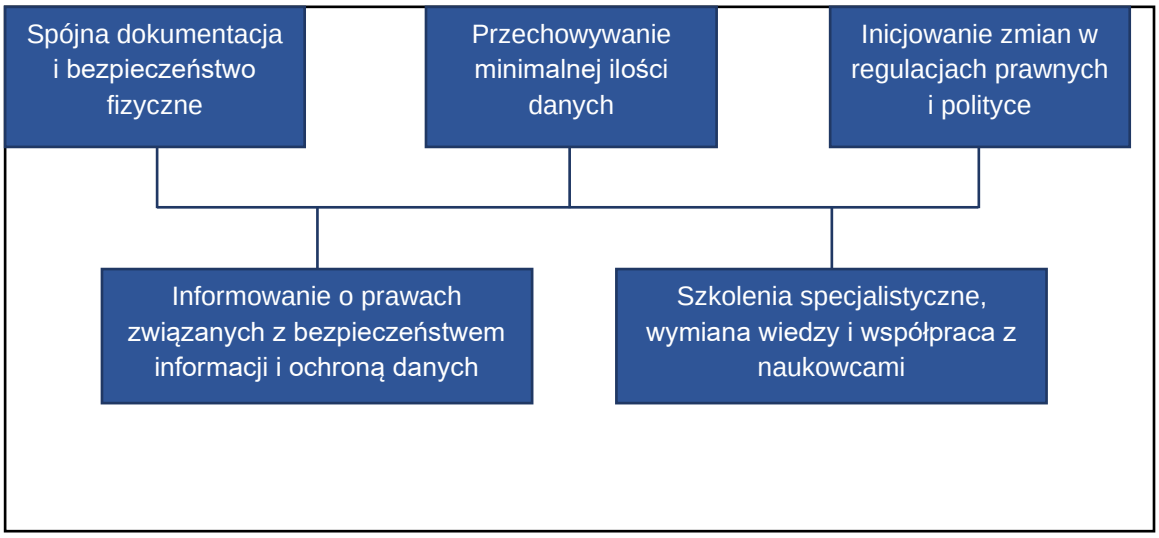
W oparciu o przegląd literatury oraz informacje zebrane podczas wydarzeń związanych z upowszechnianiem wyników projektu, można stwierdzić, że istnieje wiele obszarów dla MŚP, w których kwestie bezpieczeństwa informacji i ochrony danych wymagają dodatkowej uwagi. Poniższe wytyczne podkreślają główne względy i możliwe rozwiązania dla kwestii związanych z bezpieczeństwem informacji i ochroną danych, przed którymi stoją MŚP.

1. Wdrożenie GDPR spowodowało znaczące zmiany w cyfrowych i fizycznych praktykach zarządzania dokumentacją dla MŚP. Niektóre organizacje nie posiadały odpowiedniej infrastruktury fizycznej i cyfrowej, aby spełnić nowe wymagania. W większości przypadków okres przejściowy przed wdrożeniem GDPR był wykorzystywany do kompensowania braków infrastrukturalnych. Jednym z najbardziej wymiernych działań dla MŚP jest audyt stanu infrastruktury fizycznej i usunięcie braków, które uniemożliwiają spełnienie wymagań dotyczących zapewnienia bezpieczeństwa informacji i ochrony danych w organizacji. Po pierwsze, należy opracować wewnętrzny dokument, który będzie określał procedury i regulacje związane z bezpieczeństwem informacji i ochroną danych (w tym wiążące reguły korporacyjne w przypadku przekazywania danych do krajów spoza UE). Po drugie, należy wprowadzić fizyczne ograniczenia dostępu do dokumentacji fizycznej (szafy, sejfy, strefy ograniczonego dostępu). Personel musi być poinformowany o procedurach związanych z zarządzaniem danymi (ograniczenia w ujawnianiu informacji, zamknięcie rejestrów przed dostępem publicznym, polityka zgody na wykorzystanie danych, polityka bezpieczeństwa haseł i miejsca pracy, zarządzanie prawami użytkowników)..
2. Osoby, których dane dotyczą (klienci) muszą być informowani o praktykach zarządzania danymi w obszarach, w których ich dane są wykorzystywane. Klientom należy udzielić upoważnienia do dostępu do danych osobowych, a także poinformować ich o prawie do żądania korekty danych, sprzeciwu wobec przetwarzania, wycofania zgody na dostęp do danych, złożenia skargi, żądania usunięcia zapisów, sprzeciwu wobec transakcji danych z innymi podmiotami zarządzającymi danymi.

3. Innym obszarem, w którym MŚP napotykają na niezgodności z przepisami dotyczącymi bezpieczeństwa informacji i ochrony danych jest gromadzenie danych, które nie powinny być gromadzone lub przechowywane. Dane te są zazwyczaj gromadzone z powodu przestarzałych procesów przepływu pracy. W niektórych przypadkach, dane są powiązane z systemami informatycznymi lub innymi cyfrowymi środkami identyfikacji. Aby uniknąć takich przypadków MŚP powinny skupić się na przechowywaniu minimalnej ilości niezbędnych danych i usuwaniu danych, jeśli cel ich wykorzystania jest nieistotny. Istniejące zapisy powinny być przechowywane i zarządzane w oparciu o przejrzyste algorytmy i procedury. Takie polityki bezpieczeństwa jak "czyste biurko", czy "zablokowany ekran" powinny być traktowane jako domyślne w MŚP.

4. Czwarta wytyczna związana jest z jakością kształcenia i certyfikacji. Analiza literatury oraz bezpośrednie wypowiedzi pracowników MŚP pokazują, że dla małych i średnich organizacji certyfikacja nie jest najbardziej optymalnym sposobem wyboru kandydatów do pracy z informacjami poufnymi. Głównym kryterium jest wiedza i kompetencje, które obejmowałyby domenę ICT i prawną, a także inne bardziej interdyscyplinarne umiejętności społeczne. MŚP zazwyczaj nie mają odpowiednich zasobów, aby zatrudnić dobrze wyszkolonych specjalistów do utrzymania infrastruktury informacyjnej. Ponadto, obszary działania różnych MŚP są bardzo zróżnicowane. Stwarza to problem, w którym uniwersalne kursy szkoleniowe lub certyfikaty nie wyposażają pracowników w specyficzną wiedzę, możliwą do zastosowania w wąskich domenach. MŚP wymagają szkoleń praktycznych, opartych na scenariuszach i przykładach z życia wziętych. Jednym ze sposobów zapewnienia dostępności tych informacji jest dokumentowanie procesów zachodzących w organizacji, a następnie dzielenie się doświadczeniami poprzez profesjonalne sieci lub wydarzenia społeczne. Alternatywnie, MŚP mogą zainicjować współpracę z instytucjami szkolnictwa wyższego, które mogłyby naukowo analizować przypadki wzbogacając istniejący zasób wiedzy w określonych domenach.

5. Ostatnia wytyczna związana jest z niespójnością lub niedoskonałością regulacji prawnych. Dla niektórych instytucji ograniczenia w wymianie informacji i danych osobowych mogą stanowić poważne obciążenie w celu zabezpieczenia interesów ich klientów. Na przykład, w domu spokojnej starości mieszka stały pensjonariusz, któremu nie pozostała żadna rodzina. W nagłych przypadkach, gdy pensjonariusz jest zabierany do szpitala, obecna instytucja nie przekazuje informacji prywatnych osobom trzecim (w tym domowi spokojnej starości). Jeśli podopieczny jest przewożony do innego szpitala, dom starców musi przeprowadzić własne dochodzenie w celu odnalezienia swojego podopiecznego. W tym przypadku obie instytucje przestrzegają prawa, ale sytuacja stwarza luki prawne, które wymagają naprawy. MŚP powinny zainicjować korektę lub zainicjować (poprzez przedstawicieli politycznych) normy prawne, które obejmowałyby takie kwestie.



Wykres 29: Wytyczne oparte na wspólnych problemach, z jakimi spotykają się MŚP w zakresie bezpieczeństwa informacji i ochrony danych

6 Perspektywy i zalecenia

W trakcie realizacji projektu TeBeISi działania ujawniły, że zapotrzebowanie na szkolenia z zakresu bezpieczeństwa informacji i ochrony danych osobowych dla małych i średnich przedsiębiorstw oraz instytucji społecznych jest duże. Organizacje te często borykają się z niedogodnościami finansowymi związanymi z zatrudnieniem profesjonalnego inspektora ochrony danych, dlatego często funkcje te powierzane są innemu pracownikowi. Celem jest spełnienie wymogów GDPR i zapewnienie ochrony danych osobowych zarówno klientów, jak i pracowników firmy. Projekt pokazał również, że szkolenia z zakresu bezpieczeństwa informacji i ochrony danych osobowych są stosunkowo drogie i że MŚP bardzo chętnie korzystają z wysokiej jakości bezpłatnych szkoleń z zakresu stosowania GDPR (szkolenia wspierane w ramach projektu Erasmus plus) oraz z podnoszenia kompetencji pracowników w zakresie bezpieczeństwa informacji i ochrony danych osobowych.

Opracowany w ramach projektu kwestionariusz pozwolił pracownikom małych i średnich przedsiębiorstw ocenić swoje dotychczasowe kompetencje w zakresie bezpieczeństwa informacji i ochrony danych osobowych. Stworzony w ramach projektu program nauczania daje interesariuszom możliwość wyboru odpowiedniego szkolenia. W trakcie realizacji projektu nie planowano opracowania pakietu materiałów dydaktycznych, które umożliwiłyby interesariuszom samodzielne podnoszenie kompetencji w zakresie bezpieczeństwa informacji i ochrony danych osobowych. Dlatego też partnerzy projektu planują kontynuację wspólnych działań oraz opracowanie i przetestowanie pakietu szkoleniowego we wszystkich krajach partnerskich projektu podczas kolejnego projektu.

Zrealizowane działania projektowe pozwalają rekomendować firmom zwrócenie większej uwagi na komunikację wewnętrzną i szkolenia (zarówno poprzez organizowanie szkoleń w firmach, jak i wysyłanie pracowników na szkolenia). Wszyscy pracownicy, zwłaszcza ci, którzy mają bezpośredni kontakt z danymi osobowymi w środowisku pracy, powinni być świadomi wymogów ochrony danych osobowych, być stale szkoleni z tego, czym są dane osobowe, jak je rozpoznawać, co można, a czego nie można robić z danymi osobowymi. Konieczne jest również realistyczne oszacowanie potrzeb związanych z gromadzeniem danych osobowych, tj. utrzymywanie funduszu nadwyżkowego, niezbędnego tylko dla gromadzonych danych osobowych. Małe i średnie przedsiębiorstwa, a także instytucje świadczące usługi społeczne powinny ocenić wpływ GDPR i zidentyfikować obszary problematyczne, co dałoby czas na szkolenia pracowników i podnoszenie świadomości.

Sugeruje się również, aby przedsiębiorstwa najpierw przeprowadziły audyt gromadzonych i przechowywanych przez siebie danych osobowych w celu określenia, na których operacjach przetwarzania danych należy się skupić. Pomogłoby to ujawnić, które procesy związane z zarządzaniem danymi osobowymi i bezpieczeństwem informacji wymagają dodatkowej uwagi i poprawy kompetencji pracowników. Z przeprowadzonego kwestionariusza można wywnioskować, że MŚP są najbardziej zadowolone z inwestycji w obecnych pracowników, co daje najbardziej opłacalny kompromis w odniesieniu do potrzebnych zasobów i bezpieczeństwa.

7 Literatura

Adamkiewicz, S. L. (2005). *The correlation between productivity and the use of information security controls in small businesses.* Dissertation Abstracts International, 66(03), 1541B. (UMI No. 3167184).

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. Anintervention study. *Computers & Security, 29*(4), 432–445. doi: 10.1016/j.cose.2009.12.005

Anderson, C. L. & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613-643.

Baker, W. H., & Wallace, L. (2007). Is information security under control? *IEEE Security & Privacy,* 5, 36-44. doi:10.1109/MSP.2007.11.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance. *Journal of the Association for Information Systems*, *19*(8), 689–715. doi: 10.17705/1jais.00506

Barnard-Wills, D., Cochrane, L., Matturi, K. & Marchetti, F. (2019). *Report on the SME experience of the GDPR*. https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. doi: 10.2307/25750690

Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2018). Intentions to Comply Versus Intentions to Protect: A VIE Theory Approach to Understanding the Influence of Insiders' Awareness of Organizational SETA Efforts. *Decision Sciences*, *49*(6), 1187–1228. doi:10.1111/deci.12304

Burns, A.J., Roberts, T.L., Posey, C., Bennett, R.J., & Courtney, J.F. (2015). Assessing the role of security education, training, and awareness on insiders' security related behavior: An expectancy theory approach. *Proceedings of the IEEE 48th Hawaii International Conference on Systems Sciences, HI.* doi:10.1109/HICSS.2015.471

Colwill C. (2009). Human factors in information security: the insider threat–who can you trust these days? Information Security Technical Report, *14*(4),186–96. doi:10.1016/j.istr.2010.04.004

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security counter measures. *Journal of Business Ethics*, *89*(1),59–71. doi:10.1007/s10551-008-9909-7

D'Arcy, J., Hovav, A, Galletta, D. (2009). User awareness of security counter measures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, *20*(1), 79-98. doi: 10.1287/isre.1070.0160

Davies, J. S., & Hertig, A. C. (2008). *Theory and practice of asset protection. Security, supervision and management*. Burlington, MA: Elsevier.

Doherty, N. F., & Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. *Information Resources Management Journal, 18*, 20-38.

Easttom, C. (2006). *Computer security fundamentals*. Upper Saddle River, NJ: Prentice Hall.

Path to Cyber Resilience: Sense, Resist, React. EY's 19th Global Information Security Survey 2016-17. https://www.ey.com/Publication/vwLUAssets/EY-giss-india/$FILE/EY-giss-india.pdf

Gardner, B., & Thomas, V. (2014). *Building an information security awareness program: Defending against social engineering and technical threats*. New York, NY: Elsevier.

Goodwin, B. (2005, February 14). *Big guns target supply chain threat. Computer Weekly*. http://www.computerweekly.com/.

Guinote, A., & Vescio, K. T. (2010). *The social psychology of power*. New York, NY. The Gilford Press.

Hallová, M., Polakovič, P., Šilerová, E., & Slováková, I. (2019). Data Protection and Security in SMEs under Enterprise Infrastructure. *Agris On-Line Papers in Economics & Informatics*, *11*(1), 27–33. doi:10.7160/aol.2019.110103

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. doi: 10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. doi: 10.1057/ejis.2009.6

Yoo, C.W., Sanders, G.L., & Cerveny, R.P. (2018). Exploringthe influence of flow and psychological ownership on security education, training, and awareness effectiveness and security compliance. *Decision Support Systems*, *108*, 107-118. doi: https://doi.org/10.1016/j.dss.2018.02.009

Jasmontaitė-Zaniewicz, L., Calvi, A., Nagy, R. & Barnard-Wills, D. (2021). *The GDPR Made Simple(r) for SME's*. doi: 10.46944/9789461171092

Jenkins, J. L. & Durcikova, A. (2013). What, I shouldn't have done that?: The influence of training and just-in-time reminders on secure behavior. *Proceedings of the International Conference on Information Systems*. AIS. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.661.9290&rep=rep1&type=pdf

Johnston, A. C. & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34(*3), 549-566. doi: 10.2307/25750691

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113-134. doi: 10.25300/MISQ/2015/39.1.06

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, *12*(8), 518–555.

Kluge, EH. (2007). Secure e-health: managing risks to patient health data. International Journal of Medical Informatics**,** *76* **(**5–6**)**, 402-406**.** doi: 10.1016/j.ijmedinf.2006.09.003

Kogenhop, G. (2020). Tooling for optimal resilience. *Journal of Business Continuity & Emergency Planning*, *13*(4), 352–361.

Kumar, V., Batista, L. & Maull, R. (2011). The Impact of Operations Performance on Customer Loyalty. *Service Science*, *3*(2), 158-171. doi:10.1287/serv.3.2.158

Kuusisto, T., & Ilvonen, I. (2003). Information Security Culture in Small and medium size enterprises. *Frontiers of e-business research*, 431-439.

Lee, J. K., Cho, D., & Lim, G. G. (2018). Design and validation of the Bright Internet. *Journal of the Association for Information Systems*, 19(2), 63-85.

Leede, J. & Looise, J. K. (2005). Innovation and HRM: Towards an integrated framework. *Creativity and Innovation Management, 14* (2), 108-117. doi: 10.1111/j.1467-8691.2005.00331.x.

Leilanie Del Prado-Lu, J. (2005). *Gender, information technology, and health*. Quezon City, Philippines: The University of the Philippines Press.

Liang, H. & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394-413.

McAfee, I. (2010). *A good decade for cyber crime*. http://www.mcafee.com/ca/resources/reports/rp-good-decade-for-cyber crime.pdf.

McConnell, J. P. (2020). *UNIX Administrator Information Security Policy Compliance: The Influence of a Focused SETA Workshop and Interactive Security Influence of a Focused SETA Workshop and Interactive Security Challenges on Heuristics and Biases Challenges on Heuristics and Biases*. https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2127&context=gscis_etd.

Mohjel Eghdam, A., Khameneh, S., Hasankhni, H, Moghadam, S., Zamanzadeh V. (2013). Nurses' performance on Iranian nursing code of ethics from Patients' perspective. *26*(84),1–11. doi: 10.5681/jcs.2013.027

Newell, S., & Marabelli, M. (2015). Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of datification. *The Journal of Strategic Information Systems, 24*(1), 3-14. doi: 10.2139/ssrn.2644093

Noguerol, L. O., & Branch, R. (2018). Leadership and Electronic Data Security within Small Businesses: An Exploratory Case Study. *Journal of Economic Development, Management, IT, Finance & Marketing*, *10*(2), 7–35.

Northouse, P. G. (2010). *Leadership: Theory and practice* (5th ed.). Thousand Oaks, CA: Sage.

O'Rourke, M. (2003). Cyber attacks prompt response to security threat. *Risk Management, 50*(1), 8.

Peikari, H. R., T., R., Shah, M. H., & Lo, M. C. (2018). Patients' perception of the information security management in health centers: the role of organizational and human factors. *BMC Medical Informatics & Decision Making*, *18*(1), 1–13. doi:10.1186/s12911-018-0681-z

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of asystematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly, 37*(4), 1189–1210. doi: 10.25300/MISQ/2013/37.4.09

Posey, C., Roberts, T., & Lowry, P.B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179–214. Doi: 10.1080/07421222.2015.1138374

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quar-terly*, *34*(4), 757–778. doi: 10.2307/25750704

Richardson, R. (2008). *CSI computer crime and security survey*. http://www.cse.msstate.edu/~cse6243/ readings/CSIsurvey2008.pdf.

Sabeeh, A., and Lashkari, A. H. (2011). *Users' Perceptions on Mobile Devices Security Awareness in Malaysia.* International Conference for Internet Technology and Secured Transactions, Abu Dhabi: IEEE, 428-435.

Sicari, S., Cappiello, C., De Pellegrini, F., Miorandi, D., & Coen-Porisini, A. (2016). A security-and quality-aware system architecture for Internet of Things. *Information Systems Frontiers*, *18*(4), 665-677.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146-164. doi: doi.org/10.1016/j.comnet.2014.11.008

Siponen, M., & Vance, A.O. (2010). Neutralization: New insights into the problem of employee systems security policy violations. *MIS Quarterly*, *34*(3), 87–502.

Siponen, M., Mahmood, M., & Pahnila, S. (2009). Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, *52*(12), 145-147. doi: 10.1145/1610252.1610289

Smith, M. (2003). Business process design: correlates of success and failure. *The Quality Management Journal, 10* (2) 38-49. doi: 10.1080/10686967.2003.11919062.

The European Parliament and the Council of the European Union (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high*

common level of security of network and information systems across the Union. https://eur-lex.europa.eu/eli/dir/2016/1148/oj (accessed 31st January, 2020).

The European Parliament and the Council of the European Union (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.* https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed 31st January, 2020).

van Zadelhoff, M., Lovejoy, K., & Jarvis, D. (2014). *Fortifying for the future: Insights from the 2014 IBM Chief Information Security Officer Assessment*. https://www.ibm.com/smarterplanet/us/en/centerforappliedinsights/article/ciso_insights.html.

von Solms, S. H., & von Solms, R. (2009*). Information security governance*. NewYork, NY: Springer.

Weber, R. H. (2010). Internet of Things: New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23-30. doi: 10.1016/j.clsr.2009.11.008

Whitman, M.E., & Mattord, H.J. (2012). *Principles of Information Security* (4thed.). Boston, MA: Course Technology.

Wilkinson, G. (2018). General Data Protection Regulation: No silver bullet for small and medium-sized enterprises. *Journal of Payments Strategy & Systems*, *12*(2), 139–149.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *Management Information Systems Quarterly*, *37* (1): 1–20. doi:10.25300/MISQ/2013/37.1.01

Raport badawczy

Dziękujemy współautorom i redaktorom:

Simon Rath

Prof. Irena Žemaitaitytė

Mgr. Agata Katkonienė

Assoc. Prof. Marius Kalinauskas

Prof. Odeta Merfeldaitė

Assoc. Prof. Asta Railienė

Ivan Karitonov

Teresa Rauenbusch

Teilzertifizierung im Berufsfeld Informationssicherheit - TeBeISi

Finansowane przez program Erasmus+ Unii Europejskiej

https://information-security-in-sme.eu/.