

Spis treści

Wstęp	7
Rozdział 1	
Wprowadzenie do zarządzania cyberbezpieczeństwem	
w przedsiębiorstwie	23
1.1. Koncepcje zarządzania przedsiębiorstwem	23
1.2. Definicje i kluczowe pojęcia w zakresie cyberbezpieczeństwa	54
1.3. Zarządzanie cyberbezpieczeństwem	72
1.5. Wymagania w zakresie cyberbezpieczeństwa	84
1.6. Podsumowanie i wnioski	93
Rozdział 2	
Zagrożenia w cyberprzestrzeni i przeciwdziałanie nim	95
2.1. Rodzaje zagrożeń i aktorów w cyberprzestrzeni	95
2.2. Wybrane modele zarządzania bezpieczeństwem IT	112
2.3. Zarządzanie kosztami cyberbezpieczeństwa przedsiębiorstwa	133
2.4. Podsumowanie i wnioski	143
Rozdział 3	
Zarządzanie cyberbezpieczeństwem państw Trójkąta Weimarskiego	145
3.1. Charakterystyka państw Trójkąta Weimarskiego	145
3.2. Nakłady państw Trójkąta Weimarskiego na cyberbezpieczeństwo	147
3.3. Ramy prawne w zakresie cyberbezpieczeństwa w Unii Europejskiej	167
3.4. Analiza strategii cyberbezpieczeństwa państw Trójkąta Weimarskiego	177
3.5. Podsumowanie i wnioski	183

Rozdział 4

Wpływ cyberataków na zarządzanie przedsiębiorstwem	185
4.1. Wprowadzenie do krajobrazu zagrożeń według analiz raportów firm audytorsko-doradczych	185
4.2. Przegląd ataków hakerskich w Europie i na świecie	201
4.3. Wpływ cyberataku typu <i>ransomware</i> na zarządzanie przedsiębiorstwem ..	212
4.4. Wpływ cyberataku typu wyciek danych na zarządzanie przedsiębiorstwem	224
4.5. Podsumowanie i wnioski	237

Rozdział 5**Praktyczne aspekty zarządzania cyberbezpieczeństwem**

w przedsiębiorstwie - wyniki badań	238
5.1. Wyniki badań ankietowych i ich analiza	238
5.1.1. Charakterystyka próby badawczej	241
5.1.2. Zagadnienia dotyczące zarządzania cyberbezpieczeństwem w przedsiębiorstwie	242
5.1.3. Zagadnienia dotyczące zarządzania nakładami finansowymi na cyberbezpieczeństwo	263
5.2. Trudności i wyzwania w zakresie zarządzania cyberbezpieczeństwem w przedsiębiorstwie	269
5.2.1. Zagadnienia dotyczące problemów przedsiębiorców w obszarze zarządzania bezpieczeństwem informacji	269
5.2.2. Zagadnienia w zakresie wystąpienia cyberataków w ciągu roku do pięciu lat	274
5.2.3. Zagadnienia dotyczące sztucznej inteligencji w odniesieniu do zarządzania cyberbezpieczeństwem	278
5.3. Determinanty i model zarządzania cyberbezpieczeństwem w przedsiębiorstwie	282
5.4. Podsumowanie i wnioski	290
Zakończenie	296
Bibliografia	301
Załączniki	315
Załącznik 1. Słownik pojęć	315
Załącznik 2. Kwestionariusz ankiety	323
Załącznik 3. Kwestionariusz wywiadu eksperckiego	329
Spis tabel i rysunków	330