

Spis treści

O autorze	19
Dedykacja	20
Podziękowania autora	21
Wprowadzenie	23
CZĘŚĆ 1: WPROWADZENIE DO CYBERBEZPIECZEŃSTWA	27
ROZDZIAŁ 1: Czym właściwie jest cyberbezpieczeństwo?	29
Cyberbezpieczeństwo oznacza co innego dla różnych osób	29
Cyberbezpieczeństwo to nieustannie uciekający cel	31
Zmiany technologiczne	31
Zmiany społeczne	35
Zmiana modelu ekonomicznego	36
Zmiany polityczne	37
Zagrożenia łagodzone przez cyberbezpieczeństwo	41
Cele cyberbezpieczeństwa: triada CIA	41
Ludzka perspektywa	43
ROZDZIAŁ 2: Typowe cyberataki	45
Ataki, które powodują szkody	45
Ataki blokady usług (DoS)	46
Rozproszone ataki blokady usług (DDoS)	46
Botnety i zombie	48
Niszczanie danych	48
Czy to naprawdę ty? Impersonacja	49
Phishing	49
Spear phishing	49
Oszustwo „na CEO”	50
Smishing	50
Vishing	50
Pharming	51
Whaling: polowanie na „grubą rybę”	51
Majstrowanie przy czyichś danych: manipulacja	51
Pozyskiwanie danych podczas przesyłania: przechwytywanie	52
Ataki typu „człowiek pośrodku”	52
Kradzież danych	53
Kradzież danych osobowych	53

Kradzież danych biznesowych	54
Eksfiltracja danych	54
Przejmowanie poświadczeń	55
Wymuszone naruszenia zasad	55
Cyberbomby przemycane do Twoich urządzeń: złośliwe oprogramowanie	55
Wirusy	55
Robaki	56
Trojany	56
Ransomware	56
Scareware	57
Spyware	57
Koparki kryptowalut	58
Adware	58
Mieszane złośliwe oprogramowanie	59
Złośliwe oprogramowanie dnia zerowego	59
Fałszywe złośliwe oprogramowanie w komputerach	59
Fałszywe złośliwe oprogramowanie w urządzeniach mobilnych	59
Fałszywe powiadomienia o odnowieniu subskrypcji	60
Zatruwanie usług internetowych	60
Zatruwanie infrastruktury sieciowej	61
Malvertising	61
Oprogramowanie pobierane „w przejeździe”	62
Kradzież haseł	62
Wykorzystywanie trudności konserwacyjnych	64
Ataki zaawansowane	64
Ataki oportunistyczne	65
Ataki ukierunkowane	65
Ataki mieszane (oportunistyczno-ukierunkowane)	66
Wybrane techniki ataków	66
Rootkity	66
Ataki typu brute-force	66
Ataki iniekcyjne	67
Przechwytywanie sesji	68
Ataki przy użyciu zdeformowanych adresów URL	68
Ataki powodujące przepełnienie bufora	68
ROZDZIAŁ 3: Złoczyńcy, przed którymi musisz się bronić	69
„Zły” i „dobry” to terminy względne	70
Ci źli, którzy mają złe zamiary	71
Skryptowe dzieciaki	71
Młodzi ludzie, którzy nie są skryptowymi dziećmi	71
Terroryści i inne zbójce grupy	72
Narody i państwa	72
Szpiedzy korporacyjni	73
Przestępcy	73
Haktywiści	74
Cybernapiści i ich kolorowe kapelusze	75

Jak cyberprzestępcy monetyzują swoje działania	75
Bezpośrednie oszustwa finansowe	76
Pośrednie oszustwa finansowe	76
Ransomware	78
Koparki kryptowalut	79
Nie tylko napastnicy: zagrożenia ze strony osób, które nie mają złych intencji	79
Ludzki błąd	79
Katastrofy zewnętrzne	81
Obrona przed napastnikami	85

CZĘŚĆ 2: POPRAWIANIE BEZPIECZEŃSTWA OSOBISTEGO 87

ROZDZIAŁ 4: Ocena bieżącej postawy w zakresie cyberbezpieczeństwa 89

Nie bądź Achillesem: identyfikowanie obszarów, które nie są w pełni zabezpieczone	90
Komputery domowe	90
Urządzenia mobilne	91
Urządzenia internetu rzeczy (IoT)	91
Sprzęt sieciowy	92
Środowisko pracy	92
Identyfikowanie zagrożeń	92
Ochrona przed zagrożeniami	93
Obrona granic	94
Zapora/router	94
Oprogramowanie zabezpieczające	96
Twoje fizyczne komputery i inne punkty końcowe	97
Kopie zapasowe	97
Detekcja	97
Reakcja	98
Przywracanie	98
Poprawa	98
Ocena bieżących środków bezpieczeństwa	98
Oprogramowanie	98
Sprzęt	100
Ubezpieczenie	101
Edukacja	101
Podstawy prywatności	101
Pomyśl, zanim udostępnisz	102
Pomyśl, zanim opublikujesz	102
Ogólne wskazówki dotyczące prywatności	103
Bezpieczna bankowość online	105
Bezpieczne używanie urządzeń inteligentnych	107
Bezpieczeństwo kryptowalut	108

ROZDZIAŁ 5: Zwiększanie bezpieczeństwa fizycznego 111

Dlaczego bezpieczeństwo fizyczne ma znaczenie	112
Inwentaryzacja	112
Urządzenia stacjonarne	114
Urządzenia mobilne	115
Lokalizowanie wrażliwych danych	115
Tworzenie i realizacja planu bezpieczeństwa fizycznego	116
Wdrażanie bezpieczeństwa fizycznego	117
Bezpieczeństwo urządzeń mobilnych	119
Największym zagrożeniem są osoby z wewnątrz	119

ROZDZIAŁ 6: Cyberbezpieczeństwo podczas pracy w domu **121**

Bezpieczeństwo sieci	122
Bezpieczeństwo urządzeń	124
Bezpieczeństwo lokalizacji	125
Zagłądanie przez ramię	125
Podsłuchiwanie	126
Kradzież	126
Ludzkie błędy	126
Bezpieczeństwo wideokonferencji	126
Trzymaj prywatne rzeczy poza polem widzenia kamery	127
Chroń wideokonferencje przed nieupoważnionymi gośćmi	127
Kwestie socjotechniczne	128
Kwestie regulacyjne	129

CZĘŚĆ 3: JAK CHRONIĆ SIĘ PRZED SAMYM SOBĄ **131**

ROZDZIAŁ 7: Zabezpieczanie kont **133**

Uświadamianie sobie, że jesteś celem	133
Zabezpieczanie kont zewnętrznych	134
Zabezpieczanie danych związanych z kontami użytkownika	135
Kupuj u renomowanych sprzedawców	135
Używaj oficjalnych aplikacji i witryn	135
Nie instaluj oprogramowania od niezaufanych dostawców	136
Nie „rootuj” swojego telefonu	136
Nie podawaj niepotrzebnych wrażliwych informacji	136
Używaj usług płatności, które eliminują potrzebę udostępniania numerów kart kredytowych	136
Używaj jednorazowych, wirtualnych numerów kart kredytowych	137
Monitoruj swoje konta	137
Jak najszybciej zgłaszaj podejrzaną aktywność	138
Stosuj właściwą strategię wybierania haseł	138
Korzystaj z uwierzytelniania wieloskładnikowego	138
Wylogowuj się, kiedy skończysz	140
Używaj własnego komputera lub telefonu	140
Zablokuj swój komputer	140
Używaj oddzielnego komputera do wrażliwych zadań	140
Używaj oddzielnej przeglądarki do wrażliwych zadań	140

Zabezpiecz swoje urządzenia dostępne	141
Aktualizuj swoje urządzenia	141
Nie wykonuj wrażliwych zadań w publicznych sieciach Wi-Fi	141
Nigdy nie używaj publicznych sieci Wi-Fi w szczególnie ryzykownych miejscach	141
Uzyskaj dostęp do swoich kont tylko w bezpiecznych miejscach	142
Używaj odpowiednich urządzeń	142
Ustaw odpowiednie limity	142
Używaj alarmów	142
Okresowo sprawdzaj listy urządzeń dostępowych	142
Sprawdzaj informacje o ostatnim logowaniu	143
Odpowiednio reaguj na alarmy o oszustwach	143
Nigdy nie przesyłaj wrażliwych informacji przez niezaszyfrowane połączenie	143
Uważaj na ataki socjotechniczne	144
Ustaw hasła do logowania głosowego	144
Chroń swój numer telefonu komórkowego	144
Nie klikaj łączy w mailach i SMS-ach	145
Zabezpieczanie danych w witrynach, z którymi wchodziłeś w interakcje	145
Zabezpieczanie danych w witrynach, z którymi nie wchodziłeś w interakcje	147
Zabezpieczanie danych przez niepodłączanie sprzętu nieznanego pochodzenia	148
ROZDZIAŁ 8: Hasła	151
Hasła: podstawowa forma uwierzytelniania	151
Unikanie zbyt prostych haseł	152
Kwestie związane z wyborem hasła	153
Łatwe do odgadnięcia hasła osobiste	153
Skomplikowane hasła nie zawsze są lepsze	153
Różne poziomy wrażliwości	154
Najbardziej wrażliwe hasła to niekoniecznie te, które za takie uważasz	154
Możesz wielokrotnie wykorzystywać to samo hasło — w pewnych okolicznościach	155
Rozważ używanie menedżera haseł	155
Tworzenie łatwych do zapamiętania, mocnych haseł	157
Kiedy zmieniać hasła	158
Zmienianie haseł po włamaniu	159
Podawanie haseł ludziom	159
Przechowywanie haseł	160
Przechowywanie haseł dla spadkobierców	160
Przechowywanie zwykłych haseł	160
Przesyłanie haseł	160
Zamienniki haseł	161
Uwierzytelnianie biometryczne	161
Uwierzytelnianie oparte na SMS-ach	163
Hasła jednorazowe generowane przez aplikację	163

Tokeny sprzętowe	164
Uwierzytelnianie oparte na urządzeniach USB	165
ROZDZIAŁ 9: Zapobieganie atakom socjotechnicznym	167
Nie ufaj technologii bardziej, niż zaufałybyś ludziom	167
Rodzaje ataków socjotechnicznych	168
Sześć zasad wykorzystywanych przez socjotechników	171
Nie przesadzaj z udostępnianiem informacji w mediach społecznościowych	172
Twój harmonogram i plany podróży	173
Informacje finansowe	173
Informacje osobiste	174
Informacje zawodowe	175
Rzekome problemy z cyberbezpieczeństwem	175
Przestępstwa i wykroczenia	175
Porady medyczne lub prawne	176
Twoja lokalizacja	176
Data urodzenia	176
Twoje „grzechy”	176
Ujawnianie informacji poprzez uczestniczenie w trendach wiralnych	177
Identyfikowanie fałszywych kontaktów w mediach społecznościowych	177
Zdjęcie	178
Weryfikacja	178
Wspólni znajomi lub wspólne kontakty	178
Odpowiednie posty	179
Liczba kontaktów	179
Branża i lokalizacja	179
Podobne osoby	180
Zduplikowany kontakt	180
Dane kontaktowe	180
Status premium	180
Potwierdzenia umiejętności na LinkedInie	181
Aktywność w grupach	181
Odpowiedni poziom użytkownika konta	181
Ludzka aktywność	181
Popularne nazwiska	182
Ograniczone informacje kontaktowe	182
Umiejętności	182
Pisownia	182
Wiek konta	183
Podejrzana ścieżka życia lub kariery	183
Szczebel zawodowy lub status celebryty	183
Używanie nieprawdziwych informacji	184
Używanie oprogramowania zabezpieczającego	185
Ogólna cyberhigiena jako sposób na zapobieganie atakom socjotechnicznym	185

CZĘŚĆ 4: CYBERBEZPIECZEŃSTWO W FIRMACH, ORGANIZACJACH I INSTYTUCJACH RZĄDOWYCH **187**

ROZDZIAŁ 10: Zabezpieczanie małej firmy **189**

Osoba odpowiedzialna	189
Pilnowanie pracowników	190
Motywuuj pracowników	191
Nie rozdawaj kluczy do bram zamku	191
Przydziel każdemu oddzielne poświadczenia	191
Ogranicz dostęp administracyjny	192
Ogranicz dostęp do kont firmowych	192
Wprowadź regulamin pracy	194
Egzekwuj zasady korzystania z mediów społecznościowych	196
Monitoruj pracowników	197
Bezpieczeństwo pracy zdalnej	197
Używaj urządzeń służbowych i oddzielnych sieci służbowych	198
Skonfiguruj wirtualne sieci prywatne	199
Stwórz standardowe procedury komunikacji	199
Używaj znanej sieci	200
Określ sposób zarządzania kopiami zapasowymi	200
Uważaj, gdzie pracujesz zdalnie	200
Bądź szczególnie wyczulony na socjotechnikę	201
Ubezpieczenie od naruszenia cyberbezpieczeństwa	201
Regulacje i przepisy	202
Ochrona danych pracowników	202
PCI DSS	203
Obowiązek ujawniania naruszeń bezpieczeństwa	204
RODO	204
HIPAA	204
Dane biometryczne	205
Przepisy przeciwdziałające praniu pieniędzy	205
Sankcje międzynarodowe	205
Dostęp do internetu	205
Oddzielanie dostępu urządzeń osobistych	205
Zasady używania urządzeń osobistych do celów zawodowych (BYOD)	206
Prawidłowa obsługa ruchu przychodzącego	206
Ochrona przed atakami blokady usług	208
Używanie protokołu https	208
Korzystanie z VPN	209
Testy penetracyjne	209
Urządzenia IoT	209
Podział sieci na wiele segmentów	209
Płatności kartą	210
Problemy z zasilaniem	210

ROZDZIAŁ 11: Cyberbezpieczeństwo w dużych przedsiębiorstwach **211**

Złożoność technologiczna	212
Zarządzanie niestandardowymi systemami	212
Planowanie ciągłości działania i przywracania awaryjnego	213
Spojrzenie na regulacje	213
Ustawa Sarbanesa-Oxleya	213
Bardziej rygorystyczne wymagania PCI	214
Zasady ujawniania danych przez spółki publiczne	215
Ujawnianie naruszeń bezpieczeństwa	215
Przepisy i regulacje branżowe	215
Zobowiązania powiernicze	216
Głębokie kieszenie	217
Głębsze (i ubezpieczone) kieszenie	217
Pracownicy, konsultanci i partnerzy	217
Polityka wewnętrzna	218
Szkolenia w zakresie bezpieczeństwa informacji	218
Zreplikowane środowiska	219
Rola głównego dyrektora ds. bezpieczeństwa informacji	219
Zarządzanie ogólnym programem bezpieczeństwa	219
Testowanie i mierzenie programu bezpieczeństwa	220
Zarządzanie ryzykiem ludzkim	220
Klasyfikowanie i kontrolowanie zasobów informacyjnych	220
Bieżące zarządzanie bezpieczeństwem	220
Strategia bezpieczeństwa informacji	220
Zarządzanie tożsamością i dostępem	221
Zapobieganie utracie danych	221
Zapobieganie oszustwom	221
Plan reakcji na incydenty	222
Plan przywracania awaryjnego i ciągłości działania	222
Zgodność z przepisami	222
Dochodzenia	222
Bezpieczeństwo fizyczne	223
Architektura bezpieczeństwa	223
Zagrożenia geopolityczne	223
Możliwość audytu administratorów systemu	223
Zgodność z ubezpieczeniem od skutków naruszenia cyberbezpieczeństwa	224

CZĘŚĆ 5: CO ROBIĆ, KIEDY (NIE: JEŚLI!) DOJDZIE DO INCYDENTU

ROZDZIAŁ 12: Identyfikowanie naruszeń bezpieczeństwa	227
Identyfikowanie jawnych włamań	228
Ransomware	228
Zeszpecenie	229
Rzekome zniszczenie danych	230
Wykrywanie ukrytych włamań	230
Twoje urządzenie wydaje się wolniejsze niż wcześniej	231

Nie działa Menedżer zadań	231
Nie działa Edytor rejestru	231
Urządzenie zaczyna wykazywać problemy z opóźnieniami	232
Urządzenie zaczyna wykazywać problemy z komunikacją i buforowaniem	233
Zmieniają się ustawienia Twojego urządzenia	233
Twoje urządzenie wysyła lub odbiera dziwne wiadomości e-mail	234
Twoje urządzenie wysyła lub odbiera dziwne SMS-y	234
Na Twoim urządzeniu pojawiają się nowe programy (w tym aplikacje), których nie instalowałeś	234
Bateria Twojego urządzenia szybciej się wyczerpuje	235
Twoje urządzenie bardziej się nagrzewa	235
Zmienia się zawartość plików	235
Brakuje niektórych plików	235
Witryny wyglądają inaczej niż wcześniej	235
W Twoich ustawieniach internetowych jest serwer proxy, którego nie konfigurowałeś	236
Niektóre programy (lub aplikacje) przestają poprawnie działać	236
Programy zabezpieczające są wyłączone	237
Zwiększone użycie danych lub wiadomości tekstowych (SMS)	237
Zwiększony ruch sieciowy	237
Nietypowe otwarte porty	238
Twoje urządzenie zaczyna się zawieszać	238
Na Twoim rachunku telefonicznym pojawiają się nieoczekiwane opłaty	239
Nieznane programy żądają dostępu	239
Urządzenia zewnętrzne włączają się nieoczekiwanie	239
Twoje urządzenie działa tak, jakby używał go ktoś inny	239
Nowa wyszukiwarka domyślna w przeglądarce	239
Zmieniło się hasło do Twojego urządzenia	240
Zaczynają pojawiać się wyskakujące okna	240
Pojawiają się nowe dodatki do przeglądarki	240
Nowa strona główna przeglądarki	240
Wiadomości e-mail z Twojego urządzenia są blokowane przez filtry spamu	241
Twoje urządzenie próbuje uzyskać dostęp do „złych” witryn	241
Doświadczasz nietypowych zakłóceń usług	241
Zmieniają się ustawienia językowe Twojego urządzenia	241
Dostrzegasz nieoczekiwaną aktywność w urządzeniu	242
Dostrzegasz nieoczekiwaną aktywność online	242
Twoje urządzenie nagle uruchamia się ponownie	242
Widzisz oznaki włamania i (lub) wycieku danych	242
Jesteś kierowany do niewłaściwej witryny	242
Wskaźnik aktywności Twojego dysku twardego lub stacji SSD nigdy nie gaśnie	243
Dzieją się inne nietypowe rzeczy	243
ROZDZIAŁ 13: Postępowanie w razie naruszenia bezpieczeństwa	245
Gram profilaktyki jest wart wielu ton lekarstwa	245

Zachowaj spokój i działaj roztropnie	246
Zatrudnij specjalistę	246
Usuwanie skutków włamania bez pomocy specjalisty	247
Etap 1. Odkryj, co się stało lub dzieje	247
Etap 2. Powstrzymaj atak	248
Etap 3. Przerwij atak i wyeliminuj jego skutki	249
Ponownie zainstaluj uszkodzone oprogramowanie	252
Ponownie uruchom system i przeprowadź zaktualizowane skanowanie	253
Usuń wszystkie potencjalnie problematyczne punkty przywracania systemu	253
Przywróć zmodyfikowane ustawienia	254
Odbuduj system	255
Co robić w przypadku kradzieży informacji	255
Płacenie okupu	256
Nauka na przyszłość	258
Co robić, jeśli bezpieczeństwo Twoich danych zostanie naruszone w systemach stron trzecich	258
Przyczyna wysłania powiadomienia	258
Oszustwa	259
Hasła	260
Informacje o kartach płatniczych	260
Dokumenty wystawione przez rząd	261
Dokumenty wystawione przez szkołę lub pracodawcę	261
Konta w mediach społecznościowych	261

CZĘŚĆ 6 KOPIE ZAPASOWE I PRZYWRACANIE **263**

ROZDZIAŁ 14: Kopie zapasowe	265
Backup to konieczność	265
Kopiowanie danych z aplikacji i kont online	266
Wiadomości SMS	266
Media społecznościowe	267
WhatsApp	267
Zdjęcia Google	268
Inne aplikacje	268
Kopie zapasowe danych ze smartfona	268
Android	268
Apple	269
Kopie zapasowe kryptowalut	270
Kopie zapasowe haseł	271
Różne typy kopii zapasowych	271
Pełny backup systemu	271
Oryginalne obrazy systemu	272
Późniejsze obrazy systemu	273
Oryginalne nośniki instalacyjne	273
Pobrane oprogramowanie	273
Pełny backup danych	274

Backupy przyrostowe	274
Backupy różnicowe	275
Backupy mieszane	275
Backupy ciągłe	275
Backupy częściowe	276
Backupy folderów	276
Backupy dysków	277
Backupy dysków wirtualnych	277
Wyjątki	278
Kopie zapasowe w aplikacji	279
Jak często należy robić kopie zapasowe?	280
Narzędzia do backupu	280
Oprogramowanie do backupu	281
Oprogramowanie do backupu dołączane do dysków	281
Backup w Windowsie	282
Backup smartfona lub tabletu	282
Ręczne kopiowanie plików lub folderów	283
Zautomatyzowane zadania kopiowania plików lub folderów	283
Tworzenie dysku rozruchowego	283
Gdzie przechowywać kopie zapasowe	284
Kopia lokalna	284
Kopia zdalna	284
Chmura	285
Sieciowa pamięć masowa	285
Mieszanie lokalizacji	286
Gdzie nie przechowywać kopii zapasowych	286
Szyfrowanie kopii zapasowych	287
Testowanie kopii zapasowych	288
Pozbywanie się kopii zapasowych	288
ROZDZIAŁ 15: Resetowanie urządzenia	291
Dwa typy resetowania	291
Miękki reset	292
Twardy reset	294
Odtwarzanie zawartości urządzenia po twardym resecie	300
ROZDZIAŁ 16: Przywracanie z kopii zapasowej	301
Kiedyś będziesz musiał przywrócić dane	301
Zaczekaj! Jeszcze nie przywracaj!	302
Przywracanie danych aplikacji	302
Przywracanie pełnego backupu systemu	303
Przywracanie na urządzeniu, z którego pochodzi backup	303
Przywracanie na urządzeniu innym niż to, z którego pochodzi backup	303
Oryginalne obrazy systemu	304
Późniejsze obrazy systemu	305
Instalowanie oprogramowania zabezpieczającego	305
Oryginalne nośniki instalacyjne	305

Pobrane oprogramowanie	306
Przywracanie pełnego backupu danych	306
Przywracanie backupu przyrostowego	307
Przyrostowe backupy danych	308
Przyrostowe backupy systemu	308
Backupy różnicowe	308
Backupy ciągle	309
Backupy częściowe	309
Backupy folderów	310
Backupy dysków	311
Backupy dysków wirtualnych	311
Usunięte pliki	312
Wykluczanie plików i folderów	312
Archiwa	313
Wiele plików przechowywanych w jednym pliku	313
Stare aktywne dane	314
Stare wersje plików, folderów lub kopii zapasowych	315
Przywracanie z wykorzystaniem narzędzi do backupu	315
Przywracanie z backupu Windows	316
Przywracanie do punktu przywracania systemu	316
Przywracanie backupu smartfona/tabletu	316
Przywracanie ręcznie skopiowanych plików lub folderów	317
Używanie backupów przechowywanych u dostawców zewnętrznych	317
Odkładanie backupów na właściwe miejsce	318
Sieciowa pamięć masowa	318
Przywracanie z wielu różnych lokalizacji	318
Przywracanie do lokalizacji innych niż pierwotne	319
Nigdy nie zostawiaj podłączonych kopii zapasowych	319
Przywracanie zaszyfrowanych kopii zapasowych	319
Testowanie kopii zapasowych	320
Przywracanie kryptowalut	320
Uruchamianie systemu z dysku rozruchowego	321

CZĘŚĆ 7: SPOJRZENIE W PRZYSZŁOŚĆ **323**

ROZDZIAŁ 17: Kariera w cyberbezpieczeństwie **325**

Zawody związane z cyberbezpieczeństwem	325
Inżynierowie bezpieczeństwa	326
Kierownik ds. bezpieczeństwa	326
Dyrektor ds. bezpieczeństwa	326
Główny dyrektor ds. bezpieczeństwa informacji (CISO)	326
Analitik bezpieczeństwa	327
Architekt bezpieczeństwa	327
Administrator bezpieczeństwa	327
Audytor bezpieczeństwa	327
Kryptograf	327
Analitik podatności	328

Etyczny haker	328
Badacz bezpieczeństwa	328
Haker ofensywny	328
Inżynier bezpieczeństwa oprogramowania	329
Audytór bezpieczeństwa kodu źródłowego	329
Konsultant ds. bezpieczeństwa	329
Biegli sądowi ds. bezpieczeństwa	329
Specjalista ds. bezpieczeństwa	329
Członek zespołu ds. reakcji na incydenty	329
Analityk kryminalistyczny	330
Znawca regulacji w dziedzinie cyberbezpieczeństwa	330
Znawca regulacji w dziedzinie prywatności	330
Ścieżki kariery	330
Ścieżka kariery: starszy architekt bezpieczeństwa	330
Ścieżka kariery: CISO	331
Początki kariery w bezpieczeństwie informacji	332
Popularne certyfikaty	333
CISSP	334
CISM	334
CEH	335
Security+	335
GSEC	336
Weryfikacja	336
Etyka	336
Problemy z karalnością	336
Problemy z oceną kredytową	337
Inne zawody związane z cyberbezpieczeństwem	337

ROZDZIAŁ 18: Nowe technologie, nowe zagrożenia **339**

Internet rzeczy	340
Zagrożenia dla infrastruktury krytycznej	341
Komputery na kółkach: nowoczesne samochody	341
Używanie kryptowalut i technologii blockchain	342
Chmurowe aplikacje i dane	344
Optymalizacja sztucznej inteligencji	345
Większa potrzeba cyberbezpieczeństwa	346
Użycie AI jako narzędzia zabezpieczającego	347
Użycie AI jako narzędzia hakerskiego	347
Gdzie naprawdę wyprodukowano ten laptop? Zagrożenia w łańcuchu dostaw	347
Nie ufaj niczemu: zero zaufania	348
Nadchodzą genialne komputery: supremacja kwantowa	349
Rzeczywistość wirtualna	350
Nowe doświadczenia w rzeczywistości rozszerzonej	351

CZĘŚĆ 8: DEKALOGI **353**

ROZDZIAŁ 19: Dziesięć sposobów na poprawienie cyberbezpieczeństwa bez wydawania majątku	355
Uświadom sobie, że jesteś celem	356
Używaj oprogramowania zabezpieczającego	356
Szyfruj wrażliwe informacje	356
Często rób kopie zapasowe	358
Nie dziel się poświadczeniami logowania	358
Używaj odpowiedniego uwierzytelniania	359
Rozsądnie używaj mediów społecznościowych	359
Segreguj dostęp do internetu	359
Bezpiecznie używaj publicznych sieci Wi-Fi (a najlepiej nie używaj ich w ogóle!)	360
Zatrudnij profesjonalistę	360
 ROZDZIAŁ 20: Dziesięć wniosków z głośnych naruszeń bezpieczeństwa	 361
Marriott	361
Target	363
Sony Pictures	363
Office of Personnel Management	364
Anthem	365
Colonial Pipeline i JBS S.A.	365
Colonial Pipeline	366
JBS	366
 ROZDZIAŁ 21: Dziesięć sposobów bezpiecznego używania publicznych sieci Wi-Fi	 367
Używaj telefonu komórkowego jako mobilnego hotspotu	368
Wyłącz obsługę łączności Wi-Fi, kiedy nie używasz sieci Wi-Fi	368
Nie wykonuj wrażliwych zadań w publicznej sieci Wi-Fi	369
Nie resetuj haseł podczas używania publicznej sieci Wi-Fi	369
Używaj usług VPN	369
Używaj sieci Tor	369
Używaj szyfrowania	370
Wyłącz udostępnianie	370
Zainstaluj oprogramowanie zabezpieczające we wszystkich urządzeniach, które łączą się z publicznymi sieciami Wi-Fi	370
Zrozum różnicę między naprawdę publiczną siecią Wi-Fi a współdzieloną siecią Wi-Fi	370