

Spis treści

<i>Przedmowa do drugiego wydania Jack Jones</i>	7
<i>Podziękowania</i>	10
<i>Przedmowa</i>	12
Wstęp	13
CZĘŚĆ I	
DLACZEGO CYBERBEZPIECZEŃSTWO WYMAGA LEPSZYCH POMIARÓW RYZYKA	17
ROZDZIAŁ 1. Ta jedna najbardziej potrzebna látka w cyberbezpieczeństwie	19
ROZDZIAŁ 2. Elementarz pomiarowy dla cyberbezpieczeństwa	33
ROZDZIAŁ 3. Szybki audyt ryzyka: zacznij od prostego ilościowego modelu ryzyka	55
ROZDZIAŁ 4. Najważniejszy pomiar w cyberbezpieczeństwie	87
ROZDZIAŁ 5. Macierze ryzyka, czynniki kłamstwa, błędne przekonania i inne przeszkody przy pomiarze ryzyka	116

CZĘŚĆ II	EWOLUCJA MODELU RYZYKA CYBERBEZPIECZEŃSTWA	151
ROZDZIAŁ 6.	Rozłóż to: analiza szczegółów	153
ROZDZIAŁ 7.	Skalibrowane oszacowania: ile teraz wiesz?	173
ROZDZIAŁ 8.	Redukcja niepewności metodami bayesowskimi	201
ROZDZIAŁ 9.	Niektóre potężne metody oparte na regule Bayesa	211
CZĘŚĆ III	ZARZĄDZANIE RYZYKIEM CYBERBEZPIECZEŃSTWA DLA PRZEDSIĘBIORSTW	253
ROZDZIAŁ 10.	Dojrzałość pomiarów bezpieczeństwa	255
ROZDZIAŁ 11.	Jak dobrze współpracują moje inwestycje w bezpieczeństwo?	281
ROZDZIAŁ 12.	Wezwanie do działania: jak wdrożyć zarządzanie ryzykiem cyberbezpieczeństwa	301
DODATEK A	Wybrane rozkłady prawdopodobieństwa	315
DODATEK B	Wykłady gościnne	322