

Inhaltsverzeichnis

Vorwort	VII
Abstract	IX
Inhaltsverzeichnis	XI
Abkürzungsverzeichnis	XV
Abbildungsverzeichnis	XIX
Tabellenverzeichnis	XXI
1 Einleitung und theoretische Grundlagen	1
1.1 Problemstellung	1
1.2 Stand der Forschung und Forschungsbeitrag	4
1.3 Erklärung abweichenden Verhaltens	8
1.4 Aufbau der Arbeit	14
2 Wirtschaftskriminalität	19
2.1 Historische Entwicklung	19
2.1.1 Zwischen Mittelalter und Moderne	20
2.1.2 ‚Entdeckung‘ der White-Collar Kriminalität durch Sutherland	21
2.1.3 Die Zeit nach Sutherlands Pionierrede	23
2.1.4 Ansteigende Aufmerksamkeit	24
2.1.5 Die Moderne	25
2.2 Merkmale	27
2.2.1 Situative Tatmerkmale	27
2.2.2 Täterprofil	30
2.2.3 Rationalisierung wirtschaftskrimineller Handlungen	32
2.3 Definitoriale Eingrenzung und Entstehung	35
2.3.1 Definitionszweck und Konkretisierungsgrad	35
2.3.2 Problematik einer Legaldefinition	37
2.3.3 Occupational Crime als Makrophänomen	38
2.3.4 Logik der Aggregation	39
2.4 Bedeutung aus gesellschaftlicher Sicht	42
2.4.1 Kriminalität im Hell- und Dunkelfeld	43
2.4.2 Schadensarten und Problematik von Schadensschätzungen	45
2.4.3 Schadensumfang	47
3 Computerkriminalität	51
3.1 Historische Entwicklung	51
3.1.1 Anbruch des Computerzeitalters	52
3.1.2 Entdeckung des Makrophänomens	54
3.1.3 Die Hacker-Subkultur	55
3.1.4 Ansteigende Aufmerksamkeit und Kriminalisierung	56
3.2 Sicherheitseigenschaften von ITK-Systemen	60
3.2.1 Die EDV im Kriminalitätsgeschehen	60
3.2.2 Bedeutung von Informationen	63
3.2.3 Sicherheitsgrundlagen in der Informationstechnologie	65
3.2.4 Strukturelemente	68

3.3 Merkmale	71
3.3.1 Vorsätzlichkeit der Handlung	72
3.3.2 Tätertypologie	73
3.3.3 Täterbezogene Merkmale	75
3.3.4 Systembezogene Merkmale	77
3.3.5 Merkmale des Tathergangs	78
4 Computer Related Occupational Deviance	83
4.1 Betrachteter Gegenstandsbereich	83
4.1.1 Abweichendes und kriminelles Verhalten	84
4.1.2 Zusammenhang zwischen Wirtschafts- und Computerkriminalität	86
4.1.3 Empirische Indikatoren der Konvergenz beider Deliktformen	87
4.1.4 Definition von CROD	89
4.1.5 CROD als Mesophänomen	91
4.2 Deliktformen	94
4.2.1 Kategorisierung	94
4.2.2 Betrug	97
4.2.3 Verrat von Geschäftsgeheimnissen	98
4.2.4 Missbräuchliche Nutzung von ITK-Diensten	102
4.2.5 Sabotage	106
4.2.6 Diebstahl von Hardware	109
4.2.7 Diebstahl von Software	110
4.2.8 Taxonomie	112
4.3 Bedeutung aus Unternehmenssicht	114
4.3.1 Ausgaben für IT-Sicherheit	114
4.3.2 Verzerrte Wahrnehmung von Insiderdelikten	116
4.3.3 Strategische Bedeutung von Informationen und ITK-Systemen	118
4.3.4 Kosten und Häufigkeit von Schadensfällen	119
4.3.5 Ansprüche der Stakeholder	121
5 Handlungstheorie	123
5.1 Bewertungskriterien	123
5.1.1 Anforderungen an eine Handlungstheorie	123
5.1.2 Menschenmodelle	124
5.2 Verschiedene kriminologische Theorien im Vergleich	125
5.2.1 Theorieklassen	126
5.2.2 Soziale Lern-, Anomie- und Straintheorien	126
5.2.3 Rationalistische Theorien	128
5.2.4 Vorbehalte gegenüber rationalistischen Theorien	130
5.3 Rational Choice Ansatz	132
5.3.1 Ökonomische Grundlagen	132
5.3.2 Rationalität menschlichen Verhaltens – Erklärungsgehalt der Theorie	134
5.3.3 Beitrag zur Erklärung abweichenden Verhaltens	138

6.1.4 Beschränkte Rationalität	151
6.2 Missbrauchsgelegenheiten (Mesoebene)	154
6.2.1 IT-Sicherheitsverantwortliche	154
6.2.2 Transaktionskostenökonomik	156
6.2.3 Organisatorische Reibungsverluste	157
6.2.4 Opportunismus und Spezifität	161
6.2.5 Komplexität und beschränkte Rationalität	163
6.2.6 Informationsverteilung	166
6.3 Gesamtgesellschaftliche Rahmenbedingungen (Makroebene)	168
6.3.1 Individualisierung und Rationalisierung	168
6.3.2 Markt- und Wettbewerbsdruck	170
6.3.3 Technologisierung	171
6.4 Das Gesamtmodell im Überblick	174
7 Prävention	175
7.1 Notwendigkeit aus Unternehmenssicht	176
7.1.1 Gesellschaftliche Träger der Verbrechenskontrolle	176
7.1.2 Arten der Verbrechensbekämpfung	177
7.1.3 Grenzen staatlicher Präventionsbemühungen	178
7.2 Risikoanalyseverfahren	180
7.2.1 Klassische Analyseverfahren	181
7.2.2 Bewertung klassischer Verfahren	182
7.2.3 Alternative Verfahren	186
7.2.4 Szenarioanalyse	189
7.3 Grundschutzmaßnahmen	191
7.3.1 Information technology – Code of practice for information security management	192
7.3.2 IT-Grundschutzhandbuch	193
7.3.3 Grundschutz im Kontext von CROD	194
7.4 Reduktion von Tatgelegenheiten	195
7.4.1 Komplexitätsabbau	195
7.4.2 Spezifitätsreduktion	199
7.4.3 Zentralisierung der Datenhaltung	201
7.4.4 Sicherheitsschulungen	205
7.5 Nutzenreduktion	209
7.5.1 Vertrauensaufbau	209
7.5.2 Vermeidung arbeitsplatzbezogener Risiken	213
7.6 Kostenerhöhung	216
7.6.1 Sicherheitspolicy	216
7.6.2 Sicherheitsgrundsätze	219
7.6.3 Beschämstechniken	220
8 Schlussbetrachtung	223
8.1 Zusammenfassung	223
8.2 Ausblick	226
Literaturverzeichnis	229