
Sonja Stirnimann

Der Mensch als Risikofaktor bei Wirtschaftskriminalität

Handlungsfähig bei Non-Compliance und
Cyberkriminalität

Inhaltsverzeichnis

Teil I Basis schaffen

1 Grundlagen und Theorie – eine Einführung	3
1.1 Der Weg zum Zeitalter digitaler Informationen	4
1.2 Historischer Abriss des wirtschaftlichen Zusammenlebens	8
1.2.1 Wirtschaftskriminalität und Non-Compliance – zurück zum Ursprung	8
1.2.2 Territorium Cyberspace – zurück in die Zukunft	9
1.2.3 Territorium Cyber im Zusammenhang mit Sicherheit und Kriminalität	12
1.3 Wirtschaftskriminalität und Non-Compliance – Grundlagen und Theorie	14
1.3.1 Definitionen und Begrifflichkeiten	14
1.3.2 Angriffsziele wirtschaftskrimineller Handlungen	19
1.3.3 Treiber wirtschaftskrimineller Handlungen	21
1.3.3.1 Fraud-Dreieck	24
1.3.3.2 Motiv	25
1.3.3.3 Gelegenheit	31
1.3.3.4 Rechtfertigung	32
1.3.3.5 Analyse	34
1.3.4 Muster wirtschaftskrimineller Handlungen	35
1.3.4.1 Manipulation der Jahresrechnung	36
1.3.4.2 Vermögensschädigung	42
1.3.4.3 Korruption	45
1.3.4.4 Cyberkriminalität	49
1.3.4.5 Ponzi- und Pyramiden-Schemen	58
1.3.4.6 Insiderhandel	62
1.4 Schlussfolgerungen	63

Teil II Erfolgsfaktoren erkennen

2 Risiken – eine Frage der Toleranz	67
2.1 Risiko – Relevanz der Perspektive	70
2.1.1 Evolutionsgeschichte der Risiken und des menschlichen Verhaltens	75
2.1.2 Das Individuum – Ursache für Risiko und Gefahr	78
2.2 Elemente des (Cyber-)Risikomanagements	80
2.3 Globale Risiken – Sprache der Trends	83
2.4 Schlussfolgerungen	84
3 Faktor Mensch	87
3.1 Menschliches Verhalten im Territorium „Cyberspace“	90
3.1.1 „Code of Conduct“ im Territorium „Cyberspace“	93
3.1.2 Rolle der Psychologie im Territorium „Cyberspace“	96
3.2 Profiling – die DNS der Täter	98
3.2.1 Hintergründe des Profilings	99
3.2.2 Diversität der Täterschaft	101
3.2.3 Ausprägungen in der virtuellen Welt	105
3.2.3.1 Interne Täter	109
3.2.3.2 Integration Mensch und Technik	125
3.3 Schlussfolgerungen	125
4 Social Engineering als Modus Operandi	127
4.1 Grundformen des Social Engineering	128
4.1.1 Begrifflichkeiten und Abgrenzungen	129
4.1.1.1 Phishing	129
4.1.1.2 Elizitieren am Telefon	132
4.1.1.3 Identitätsbetrug	134
4.1.1.4 Wirkung dreier Grundformen	135
4.2 Inhärenter Wert von Informationen	137
4.3 Entscheidungsfindung trifft auf Social Engineering	140
4.4 Neurowissenschaft trifft auf Social Engineering	143
4.4.1 Amygdala – die Geheimwaffe im Kopf	143
4.5 Einflussnahme und Manipulation durch Social Engineering	145
4.5.1 Beeinflussung und Manipulation – Bedeutung der Unterscheidung	148
4.5.1.1 Effektive Taktiken der Manipulation	148
4.5.1.2 Methoden der Einflussnahme	150
4.5.2 Stress und Helfersyndrom	154
4.6 Schlussfolgerungen	156

5 Verhaltensökonomie – ihre Rolle im Kontext der	
Wirtschaftskriminalität	159
5.1 Einführung in die Finanztheorien.	160
5.1.1 Traditionelle Finanztheorien.	161
5.1.1.1 Rationales Verhalten der Investoren	162
5.1.1.2 Effizienz des Marktes	162
5.1.2 Interaktion zweier Paradigmen.	162
5.1.2.1 Moderne Portfolio-Theorie	163
5.1.2.2 Ineffiziente Märkte und Irrationalität	163
5.2 Theorie der „Behavioral Finance“	164
5.2.1 Ziel und Absicht	166
5.2.2 Einflussfaktoren der Informationsinterpretation.	166
5.2.2.1 Selektive Wahrnehmung	168
5.2.2.2 Kognitive Dissonanz	168
5.2.2.3 Herdenverhalten und Gruppendenken.	169
5.2.2.4 Heuristiken und Befangenheit.	172
5.3 „Behavioral Finance“ und Wirtschaftskriminalität	175
5.3.1 Perspektive des Fraud-Dreiecks	176
5.3.2 Vergleich der Disziplinen	177
5.3.2.1 Zugrundeliegende Disziplinen	177
5.3.2.2 Konditionen wirtschaftskrimineller Handlungen	178
5.3.2.3 Auswirkungen und Synergien.	182
5.4 Schlussfolgerungen und Ausblick	184
5.4.1 Lernende Organisation	184
5.4.2 Zukünftige Ansätze.	185
6 Befangenheit – was wir warum glauben	189
6.1 Befangenheit und Objektivität	189
6.1.1 Befangenheit im beruflichen Umfeld	191
6.1.2 Faktoren der Befangenheit	193
6.1.2.1 Stereotypen	194
6.1.2.2 Vorurteile	194
6.1.2.3 Diskriminierung	195
6.1.2.4 Bewusste und unbewusste Befangenheit.	195
6.2 Einfluss der Befangenheit auf die professionelle Tätigkeit	198
6.3 Die Rolle des Ermittlers und des Prüfers	198
6.3.1 Einfluss unbewusster Befangenheit auf Ermittlungen und Prüfungen	200
6.3.2 Typen der Befangenheit	201
6.3.3 Befangenheit und professionelle Skepsis	211

6.4	Bewältigungsstrategien zur Minimierung der Befangenheit	215
6.4.1	Hypothesenbildung	216
6.4.2	Selbstmanagement	217
6.5	Schlussfolgerung	219
Teil III Wissen implementieren		
7	Lebenszyklus wirtschaftskrimineller Handlungen und Non-Compliance	223
7.1	Prävention – Prevention	225
7.1.1	Sensibilisierung	226
7.1.2	Hintergrundrecherche	231
7.1.2.1	Zielgruppen	233
7.1.2.2	Nutzen	235
7.1.2.3	Informationsempfänger	236
7.1.2.4	Quellen	237
7.2	Aufdeckung – Detection	240
7.2.1	Sachverhaltsermittlung	242
7.2.1.1	Ausgangslage	244
7.2.1.2	Erfolgsfaktoren – Interdisziplinarität und Heterogenität	247
7.2.1.3	Zusammenarbeit interner und externer Ermittler	251
7.3	Reaktion und Aufarbeitung – Response	252
7.3.1	Interviews im Rahmen von internen Sachverhaltsermittlungen	253
7.3.1.1	Auskunftspflicht des Mitarbeiters	253
7.3.1.2	Vorbereitung der Interviews	254
7.3.1.3	Durchführung der Interviews	256
7.3.1.4	Typologie der Fragen	257
7.3.1.5	Erfolgsfaktor „Beziehungsaufbau“	261
7.3.1.6	Königdisziplin „Zuhören“	262
7.3.2	Konsequenzen und Sanktionen aus Ereignissen	263
7.4	Schlussfolgerungen	264
8	Kommunikation – in guten wie in schlechten Zeiten	267
8.1	Abgrenzungen und Begrifflichkeiten	268
8.2	Krisenmanagement – Ereignisse erfolgreich kommunizieren	270
8.2.1	Kommunikation im Ereignisfall	271
8.2.2	Schutz der Reputation – die Macht der Krisenkommunikation	277
8.2.2.1	Krise – Bedrohung der Reputation	278
8.2.2.2	Reaktionsstrategien in der Krise	281
8.2.2.3	Implementierung der Krisenkommunikation	285
8.2.3	Zusammenarbeit interdisziplinärer Experten	289
8.3	Schlussfolgerungen	289

9	Erfolgsfaktor Handlungsfähigkeit	291
9.1	Erkennung von Frühwarnindikatoren im Rahmen des Profiling	295
9.1.1	Vier Kategorien der Frühwarnindikatoren interner Täter	297
9.1.1.1	Persönliche Veranlagung	298
9.1.1.2	Persönliche, berufliche und finanzielle Stressoren	300
9.1.1.3	Auffälliges Verhalten	301
9.1.1.4	Unternehmensinterne Reaktion auf Frühwarnindikatoren	303
9.1.1.5	Relevanz der Frühwarnindikatoren im Risikomanagement	304
9.2	Individuelle Ereignisbewältigung	304
9.2.1	Phasen der Bewältigung	305
9.2.2	Vertrauensverlust	307
9.3	Professionelle Ereignisbewältigung	312
9.3.1	Strukturiertes Vorgehen	313
9.3.1.1	Fünf Phasen des FraudAidKit™	314
9.3.1.2	Krisenmanagement bei Wirtschaftskriminalität	318
9.3.1.3	Fachkompetenz zur effizienten Umsetzung	327
9.4	Schlussfolgerungen	327
	Ausblick & Fazit	329
	Arbeitspapiere	333
	Literatur	339