Preface

Insider threats are easy to counter. One only needs a concise model of human behaviour and its dependencies on outer and inner influences, a surveillance system in place that is able to observe in necessary detail action and influences, and an evaluation system, that can draw the necessary conclusions from its input.

Neither of the components just described is easy to realise, or desirable to have in the first place. Modelling human behaviour is close to impossible, let alone modelling how it depends on outer and inner factors. A surveillance system is heavily dependent on legal boundaries of what is allowed to be monitored or not, and the amount of data even from legal monitoring can be overwhelming at best. An evaluation system would need to be able to take all the input and models into account, and this is yet another complex task.

This book collects a series of chapters that try to map the territory between modelling, analysing, and evaluating insider threat scenarios. The chapters cover aspects from insider threats in electronic voting, over monitoring and access control systems, to legal aspects and the integration of the approaches described into Information Security Management systems.

One important and recurring theme is the question of how much surveillance is admissible and acceptable in different settings. It is this question that in the end determines the success of techniques aiming to reduce insider threats, or threats in general. This is especially true when dealing with systems *beyond* the pure technical aspects, but towards psychological aspects.

We are indebted to the participants of the Dagstuhl Seminar "*Countering Insider Threats*" (08302), during which the idea for this book was first discussed, and the staff at Schloss Dagstuhl. It has been a long road, but we believe that the result, which you are reading now, was worth it.

Kongens Lyngby, Pittsburgh, Hamburg-Harburg, and Davis   *Christian W. Probst*
January 2010   *Jeffrey Hunker*
Dieter Gollmann
Matt Bishop

Springer