Foreword

By Hugh Njemanze

By now, most of us take the Internet for granted as a useful and even indispensable part of the corporate environment. Without the Internet, many daily tasks would be a lot harder. Who would want to go back to—or even remembers—the old ways of looking up information on competitive products, or on equipment prior to purchase, or on selling off used-and-no-longer-needed equipment? Or how would you like to book business travel the way we did before Google, eBay, or Expedia came along?

But we also know that the Internet can be a dangerous place. All sorts of bad guys are out there trying to breach our networks, deface our Web sites, and disrupt the operation of our network services. However, until recently, we have mostly paid attention to the *out there* part of that last sentence. We have assumed that the main threat is from people we have never seen, people who are operating safely out of reach on the other side of the world. Or maybe we think the threat is from teenagers who have downloaded ready-made attack scripts from the web and are experimenting for bragging rights and haven't a more constructive way to occupy their time.

What Brian shows us in this unique, timely, and well-researched book filled with real-life examples and case studies, is that often you have vastly more to worry about from someone in an office down the hall or even in the next cubicle. Moreover, Brian goes way beyond just sounding the alarm bells and shows us not only what is happening, but how many organizations have woken up and are responding to *insider threats*. He also describes the tools and techniques that are being used to combat a threat that "accounts for more than 65% of monetary losses corporations experience annually through malicious network activity." It is my belief that, after reading this book, you will come away

not only with a stronger awareness of the ways our workplaces are vulnerable to disgruntled current or former employees—or even well-intentioned employees under coercion or threat from external sources—but more importantly, with a much deeper insight into strategies and techniques for preparing for, defending against, detecting, and finally responding to these threats.

Brian has been a friend and colleague for the past several years now, and I hope you get a sense of his infectious enthusiasm and deep knowledge of the subject matter from the pages you are holding in your hands.

—Hugh Njemanze,
May 2006
Los Altos, California

Hugh Njemanze is the Founder and Chief Technology Officer at ArcSight Inc, makers of the premier product suite for Enterprise Security Management. He is a frequent speaker at industry conferences. Before designing and leading the development of ArcSight products, Hugh designed, built, and/or led the construction of Search Engine products at Verity, Database Connectivity Tools at Apple Computer, and Programming Language Compilers at Hewlett Packard. In his copious free time he likes to play the bass guitar, sometimes performing in Bay Area clubs.