Preface

The reports of my death are greatly exaggerated.
—Mark Twain

Throughout the 1990s, many industry pundits predicted the demise of the mainframe. It seemed that the entire information technology (IT) industry got caught up in the frenzy of client/server this and distributed that. Some lost sight of the fact that the purpose of IT is to address business problems and opportunities. Many didn't realize that, during this time, the mainframe evolved substantially with the addition of a standardized UNIX® development and execution environment, web serving capabilities, Java™, XML support, TCP/IP, firewall, and virtualization, while continuing to grow in both standalone processing power and clustering capabilities. Of course, the mainframe also maintained its traditional strengths of reliability, availability, and security.

We are at a very interesting point in the continuing evolution of the mainframe: Regulatory pressures such as the Payment Card Industry (PCI) standards and Sarbanes-Oxley mandate that companies understand their data assets and protect them properly. Cooling and power costs are driving companies to consolidate their servers, to avoid the costs of building new facilities. The rapid multiplication of servers causes substantial growth in support and software costs. All of this together explains why many companies are taking a fresh look at the mainframe to expand both existing applications and new applications. Mainframes are not appropriate to every business need, but they are optimized for high-availability and I/O-intensive applications.

That growth in the use of the mainframe drives up the need for knowledgeable security administrators. This is where this book comes in. We assume that you are already an experienced security administrator on other systems, such as UNIX, Linux®, or Windows®. We also assume that you've never logged on to TSO, the z/OS® command-line interface.

This "nuts of bolts" book will teach you how to log on, work with the mainframe's TSO and ISPF (similar to a GUI for z/OS, except that it uses text and not graphics) interfaces, and perform the major tasks of a security administrator. We are very big believers in learning by doing. Hey, that's how *we* learned! Of course, going through the exercises requires you to have access to an actual mainframe.

Chapter 1, "Introduction to the Mainframe," teaches the historical background and the basics of using a mainframe. By the end of the chapter, you will be able to log on, allocate data sets and edit their members, run JCL jobs, use UNIX System Services, and access the documentation when you need it. UNIX System Services (USS) is a version of UNIX running under z/OS.

Chapter 2, "Users and Groups," teaches users and groups. By the end of the chapter, you will be able to create, modify, and delete users and groups.

Chapter 3, "Protecting Data Sets and Other Resources," teaches resource protection. This chapter teaches you how to manipulate the profiles that protect data sets (a term that covers the rough equivalents of files and directories), the profiles that protect other permissions, and the permissions for files and directories within USS.

Chapter 4, "Logging," teaches logging. You will learn how to configure the mainframe to log security events and how to generate reports that include only the relevant log entries.

Chapter 5, "Auditing," teaches auditing. You will learn about the main weaknesses that auditors look for and will learn how to use the standard auditing tools to find those weaknesses yourself and remedy them.

Chapter 6, "Limited-Authority RACF Administrators," teaches how to create limited-authority administrators when they are appropriate, and discusses their permissions. Your first mainframe security job is likely to be as a limited-authority administrator. Unlimited access, called `system-SPECIAL`, is usually reserved for a few senior security administrators in the mainframe environment.

Chapter 7, "Mainframes in the Enterprise-Wide Security Infrastructure," teaches how the mainframe integrates into the enterprise-wide security infrastructure. In contrast to the other chapters, this chapter is very theoretical. It explains what the enterprise-wide security infrastructure does and how it relates to the mainframe, but it does not include exercises.

Time to get started. Grab a cup of coffee, fire up your terminal emulator (we explain what that is in Chapter 1), and get started!