# Preface

In the years since the book I coauthored, *Identity Management: A Primer*, was published, the identity and access management task has become significantly more complex, and an order of magnitude more important. It has become more complex because of the cloud and the necessity to support mobile devices. It has become more important because the networking solutions of yesteryear are no longer sufficient.

This book seeks to assist the chief information officer (CIO), or better still the chief digital officer (CDO), in grappling with this complexity and leveraging the organization's identity data to deploy an efficient and secure information technology (IT) environment. Organizations that can accomplish this can potentially realize significant benefits: better staff relations, more secure contractor engagement, more profitable customer relationships, and empowered business units that can finally get real-time information on inventory levels, production rates, market prices, and customer satisfaction. For those organizations that fail to address the identity management challenge, the term "digital transformation" will have a special meaning.

Ten years ago, identity and access management (IAM) was nicely compartmentalized and relatively easy to understand. There were a dozen vendors in the market, and after determining a company's size and propensity for an enterprise directory, as a consultant it was relatively easy for me to define a solution. I enjoyed visiting clients, listening to how vendors had bamboozled them, and explaining a succinct way forward to reach their IAM goals.

Then the "cloud" arrived.

Suddenly, it was necessary to throw out the old paradigm of enterprise directories and firewalls at the perimeter and figure out how to avoid opening up the enterprise directory to the world. At the same time, it was necessary to determine how to support software as a service (SaaS) applications without synchronizing identity data to the cloud. With the HR and identity management (IdM) systems on the internal network and the SaaS applications on the Internet, some "magic" was needed. But solutions were available, and cloud providers started supporting identity in the cloud and the SAML protocol, to varying degrees.

Then came BYOD.

All of a sudden, users were coming from anywhere with a wide variety of devices. They could no longer be relied upon to use the company's standard

operating environment (SOE). No longer were they inside the corporate network, and their devices could be used by anyone at any time of the day or night.

But solutions have developed rapidly. There are now new ways of supporting access from anywhere by anyone at any time. The development of protocols such as OpenID Connect and OAuth and initiatives such as Fast IDentity Online (FIDO) provide solid security for external access to protected corporate systems and data.

Now the Internet of Things (IoT) is upon us: how do we manage the identity of things? How do we allow secure access to corporate facilities? And what about blockchain technology? Is it appropriate for situations where components of identity can be distributed across multiple data repositories?

It is important that we keep up with technological developments and extend our frameworks to understand these challenges and take advantage of the attendant opportunities.

# Identity Management from a Business Perspective

This book seeks to make sense of identity management: where it has come from and where it's going. It's written at a business person level because it is important that business people understand identity management.

It's the level at which decisions should be made as to the strategy to follow to develop our cybersecurity infrastructure and competence. We can no longer afford to have the C-suite abrogate their responsibility and expose their organizations to unnecessary risk. Now is the time to address identity management, understand its potential, and set our organizations on a trajectory to leverage the promise it affords.

This book seeks only to make identity management understandable. It will be the CIO's responsibility to decide what this means and set their organization on a well-thought-out path to robust security at an affordable cost.

In 2002, US Secretary of Defense Donald Rumsfeld uttered a truism that is often quoted but never more appropriate to the identity and access management situation in most companies today: there are "known knowns," "known unknowns," and "unknown unknowns."

The "known knowns" are the tried and true identity management tools and standard processes, such as provisioning user accounts in Microsoft Active Directory (AD). The "known unknowns" are the issues around provisioning to

cloud applications and support for mobile devices. The "unknown unknowns" are ways to manage IoT devices to truly secure our corporate environment. We know we need to get ready to do this, we know we need to share corporate information with staff and business partners, but we don't know how to do it. Do we need to purchase a secure information sharing solution, and if so, would the staff use it? Do we need to expose an API for IoT devices; if so, who sets the guidelines for security and management? Do we need to provide better services for consumers; if so, how do we identify them and still adhere to privacy regulation?

In this book, we'll address these questions, while keeping technical detail to a minimum, and we will endeavor to appreciate the opportunities that a good identity and access management environment affords.

Chapter 1 looks at the changes that have happened and increasingly impact our security environment, and how we can leverage our IdM environment.

Chapter 2 looks at the provisioning task, so we can determine the features we need, in order to ensure correct access permissions are assigned to users.

Chapter 3 discusses directories. If there is any area of our identity management environment that is changing in the fast-paced development of IAM, it is directories.

Chapter 4 sorts out the issues affecting authorization and authentication. We'll take a look at current trends and determine what's most important in our environment.

Chapter 5 addresses the cloud and notes the impact it is having on IAM systems.

Chapter 6 discusses the use of mobile devices and investigates the wisdom, or otherwise, of supporting bring your own device (BYOD).

Chapter 7 focuses on IoT and how it impacts identity.

Chapter 8 addresses the importance of IAM for industrial computer systems and the roadblocks to exploiting corporate IAM facilities.

Chapter 9 is devoted to secure information sharing and how it should be part of an organization's data loss prevention strategy.

Chapter 10 is about consumerization, its impact on IAM, and how to "know your customer."

Chapter 11 discusses regulation and its impact on our IAM strategy.

Chapter 12 looks forward to the issues that will affect our IAM environments in the next few years and how we should prepare for them.

Each chapter consists of content on the topic in question, a use case analysis to help our understanding, and a question and answer section to promote discussion.

The expectation is that the reader will begin reading the book having some appreciation of the identity management topic, and will have a better appreciation of identity management after reading the book. The reader may not find all chapters to be equally useful, but my intent is that the majority of this book's content will provide business value. No doubt there will be areas of disagreement—but that's good. It is only after having our understanding challenged that our ideas become stronger and more actionable. That's my hope: to stimulate action in developing corporate strategy.

As one wise professor once told me, "If you're not going to do anything, you don't need a strategy."

Best wishes,

Graham Williamson