THE ESSENTIAL SECURITY GUIDES SERIES

JUST TELL ME WHAT I NEED TO KNOW...

CYBERSECURITY

CLEAR ANSWERS. PRACTICAL INSIGHTS.
ESSENTIALS ONLY.

PROTECT WHAT MATTERS MOST

IDENTIFY THREATS

DEFEND AGAINST ATTACKS

RESPOND EFFECTIVELY

BUILD RESILIENCE. REDUCE RISK.

BELSHAW CONSULTING

Just Tell Me What I Need To Know

Cybersecurity

A Security Architect's Practical Guide

Belshaw Consulting

Copyright Notice

This book is an independent educational work. Any company names, product names, trademarks, service marks, technologies, standards, frameworks, methodologies, or registered trademarks mentioned in this publication are the property of their respective owners. Their inclusion is for identification, educational, and illustrative purposes only and does not imply any affiliation with, endorsement by, or sponsorship from the respective owners.

Technology, products, standards, regulations, certifications, security guidance, and industry best practices evolve over time. Readers should consult current vendor documentation, official standards publications, applicable regulations, and their organization's policies and procedures before implementing any recommendations or making technical, security, or business decisions.

Table of Contents

Introduction

If you are reading this book, chances are you fall into one of three groups.

Perhaps you are completely new to cybersecurity and are trying to understand what everyone is talking about. You may have accepted a new role, started a college course, or simply become curious about one of the fastest-growing professions in the world.

Perhaps you already work in Information Technology. You might be a network engineer, systems administrator, software developer, cloud engineer, project manager, or business analyst who increasingly finds cybersecurity becoming part of your daily responsibilities. Security is no longer a specialized discipline confined to a small team of experts. Today, nearly every technology decision has security implications.

Or perhaps you are already an experienced cybersecurity professional. You understand many of the concepts but want a concise reference that brings everything together, refreshes your knowledge, and helps you see how the many disciplines within cybersecurity fit together.

Regardless of which category describes you, this book was written with one simple objective:

To tell you what you really need to know.

Cybersecurity is a vast subject. Entire careers are built around identity management, cloud security, digital forensics, threat intelligence, vulnerability management, cryptography, software security, governance, and dozens of other specialties. Thousands of books have been written on these individual topics, many running to hundreds or even thousands of pages.

The problem is that most people don't need to become an expert in every subject. They need to understand enough to make informed decisions, contribute effectively to projects, communicate intelligently with colleagues, and continue learning as their careers evolve.

This book focuses on understanding rather than memorization.

Rather than overwhelming you with technical minutiae, it explains why cybersecurity exists, how organizations approach it, and how the various disciplines work together to protect modern businesses.

Whether you are preparing for your first cybersecurity interview, leading a security project, speaking with executives, or simply trying to understand today's threat landscape, this book is designed to give you the knowledge and confidence to participate in those conversations.

Who Should Read This Book?

This book was written for a broad audience because cybersecurity affects virtually every profession within Information Technology—and increasingly many outside of it.

It is ideal for:

- Individuals considering a career in cybersecurity.
- IT professionals moving into security-related roles.
- Security analysts seeking a broader understanding of the profession.
- Security engineers and architects who want to strengthen their knowledge outside their primary specialty.
- Project managers responsible for delivering technology or security initiatives.
- Managers and executives responsible for cyber risk and governance.
- Students studying cybersecurity, information assurance, or information technology.
- Anyone preparing for technical or management interviews involving cybersecurity.

You do not need an extensive technical background to benefit from this book.

Where technical concepts are introduced, they are explained in plain English before exploring more advanced ideas. Likewise, experienced professionals will find discussions on governance, architecture, management, and industry best practices that extend beyond introductory material.

This book is intentionally written to remain valuable as your career develops.

How to Get the Most from This Book

Although this book can be read from beginning to end, it is also designed to serve as a practical reference.

If you are new to cybersecurity, read the chapters in order. Each chapter builds upon the previous one, gradually introducing new concepts while reinforcing earlier material.

If you already have experience, feel free to jump directly to topics of interest. Each chapter has been written to stand largely on its own while still contributing to the overall picture of modern cybersecurity.

Throughout the book you will encounter several recurring sections.

Why This Matters

Every chapter begins by explaining why the topic is important to organizations and security professionals.

Just Tell Me What I Need to Know - This section summarizes the key concepts in a concise, easy-to-understand format. If you only have a few minutes to review a topic before a meeting or interview, this is where you should start.

Digging a Little Deeper - For readers who want additional context, this section expands on important concepts without becoming overly academic.

Real-World Example - Cybersecurity is most easily understood through practical examples. Real-world scenarios illustrate how organizations apply the concepts discussed throughout the chapter.

Common Mistakes - Many cybersecurity failures occur because of misunderstandings rather than technology limitations. Learning from common mistakes can often be as valuable as learning best practices.

Interview Insight - Many readers use books like this while preparing for new opportunities. These sections explain how interviewers commonly approach a topic and what distinguishes an average answer from an exceptional one.

What Every Professional Should Remember

Each chapter concludes with a concise summary of the most important points that every cybersecurity professional should know.

Finally, you'll find references to other books in the Just Tell Me What I Need to Know... series whenever a subject deserves deeper coverage.

How This Book Fits into the Series

Cybersecurity is an incredibly broad discipline. No single book can thoroughly cover every specialty without becoming either too large or too superficial.

This book serves as the foundation of the Just Tell Me What I Need to Know... series.

It explains the core concepts that every cybersecurity professional should understand before diving into more specialized subjects.

Several books in the series explore specific disciplines in greater depth, including:

- Cloud Security – Designing, securing, and managing cloud environments.
- Threat Management – Vulnerability management, threat detection, incident response, and security operations.
- Zero Trust – Identity-centric security architecture and modern access control.
- DevSecOps – Integrating security into software development and deployment pipelines.
- Risk Assessment – Identifying, analyzing, and managing organizational risk.

- Security & Privacy Metrics – Measuring cybersecurity effectiveness and communicating with leadership.
- Writing Policies & Procedures – Developing governance documentation that supports business objectives.
- F5 BIG-IP Security – Securing enterprise application delivery and network services.
- Artificial Intelligence in Cybersecurity – Understanding how AI is transforming both cyber defense and cyber-attacks.
- Machine Learning in Cybersecurity – Applying machine learning techniques to modern security challenges.

If you find yourself particularly interested in one of these areas, each specialized title expands significantly on the concepts introduced here.

To reinforce your understanding, this book also has a companion volume:

- Just Tell Me What I Need to Know... Cybersecurity Q&A Workbook

The workbook contains hundreds of review questions, detailed explanations, and interview-style scenarios that help reinforce the concepts presented in this book and prepare readers for professional interviews and certification studies.

Together, these books provide both the knowledge and the practice needed to build confidence in cybersecurity.

THE ESSENTIAL SECURITY GUIDES SERIES

JUST TELL ME WHAT I NEED TO KNOW... CYBERSECURITY

CLEAR ANSWERS. PRACTICAL INSIGHTS. ESSENTIALS ONLY.

Cybersecurity is complicated. This book makes it understandable.

Cybersecurity is no longer the responsibility of one technical team. It affects executives, managers, architects, engineers, developers, auditors, project leaders, business owners, and anyone responsible for protecting information or keeping an organization operating.

The problem is not a shortage of information.

The problem is knowing what actually matters.

Just Tell Me What I Need to Know... Cybersecurity provides a practical, business-focused introduction to the concepts every cybersecurity professional should understand. It explains how security technologies, governance, risk, architecture, operations, resilience, and leadership fit together in real organizations—without unnecessary jargon or dependence on a particular vendor.

INSIDE, YOU WILL LEARN:

- How cybersecurity supports business objectives
- How governance, risk, and compliance work together
- How identity, cryptography, networks, endpoints, cloud, and applications are protected
- How security operations detect and respond to threats
- How to design secure and resilient systems
- How to build and manage cybersecurity programs and projects
- How artificial intelligence, automation, Zero Trust, and quantum computing may shape the future
- How to prepare for cybersecurity interviews and build a long-term career

The book also includes practical checklists, interview guidance, quick-reference material, and recommendations for continuing your professional development.

Whether you are entering cybersecurity, expanding into a new specialty, preparing for an interview, or moving toward architecture and leadership, this book gives you the foundation you need to understand the profession as a whole.

YOU DO NOT NEED TO KNOW EVERYTHING.
YOU NEED TO UNDERSTAND THE PRINCIPLES, ASK THE RIGHT QUESTIONS, AND KNOW HOW THE PIECES FIT TOGETHER.

PROTECT WHAT MATTERS MOST | IDENTIFY THREATS | DEFEND AGAINST ATTACKS | RESPOND EFFECTIVELY | BUILD RESILIENCE. REDUCE RISK.

BELSHAW CONSULTING