

JUST TELL ME WHAT I NEED TO KNOW...

SECURITY & PRIVACY METRICS

MEASURE WHAT MATTERS. IMPROVE WHAT COUNTS. PROTECT WHAT'S IMPORTANT.

SECURITY METRICS

- ✓ RISK EXPOSURE
- ✓ THREAT DETECTION
- ✓ INCIDENT RESPONSE
- ✓ VULNERABILITIES
- ✓ COMPLIANCE

PRIVACY METRICS

- ✓ DATA PROTECTION
- ✓ ACCESS CONTROL
- ✓ PRIVACY COMPLIANCE
- ✓ DATA BREACHES
- ✓ USER RIGHTS

78%

RISK REDUCTION
Year Over Year



TURN DATA INTO INSIGHT

Track. Analyze. Act.
Continuously Improve.

92%

POLICY COMPLIANCE
On Time



MEASURE

Define meaningful
metrics aligned to
business goals.



MONITOR

Continuously collect
and validate accurate
security & privacy data.



ANALYZE

Identify trends,
anomalies, and
areas for improvement.



REPORT

Communicate clear,
actionable insights
to stakeholders.



IMPROVE

Drive data-informed
decisions and reduce
risk over time.

Just Tell Me What I Need To Know
Security & Privacy Metrics

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.

Copyright © 2026 Belshaw Consulting

All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, transmitted, or distributed in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher, except for brief quotations used in reviews or scholarly works as permitted by applicable copyright law.

Table of Contents

Introduction	5
Part I — Foundations of Security Metrics.....	7
Chapter 1 — Introduction to Security Metrics	7
Chapter 2 — Metric Types	42
Chapter 3 — Building a Metrics Program	77
Part II — Operational Security Metrics	88
Chapter 4 — Vulnerability Management Metrics	88
Chapter 5 — Threat Detection & Response Metrics	96
Chapter 6 — Identity & Access Metrics.....	105
Chapter 7 — Infrastructure & Cloud Metrics	114
Part III — Governance, Risk & Compliance Metrics	124
Chapter 8 — Risk Metrics	124
Chapter 9 — Compliance Metrics	132
Chapter 10 — Privacy Metrics.....	140
Part IV — Executive Reporting & Decision Support.....	149
Chapter 11 — Security Dashboards	149
Chapter 12 — Measuring Security Program Effectiveness.....	156
Chapter 13 — Security Scorecards	165
Part V — Advanced Analytics	174
Chapter 14 — Security Analytics.....	174
Chapter 15 — AI and Automation for Metrics	182
Chapter 16 — Continuous Improvement	189
Part VI — Building a Metrics-Driven Security Program	198
Chapter 17 — Developing a Security Metrics Strategy	198
Chapter 18 — Case Studies.....	205
Chapter 19 — Creating a Culture of Measurement	216
Appendices	224
Appendix A — Security Metrics Review Checklist	224
Appendix B — KPI, KRI & KCI Quick Reference	230
Appendix C — Executive Dashboard Templates	237
Appendix D — Security Scorecard Examples	247

Appendix E — CISO Monthly Report Template	258
Appendix F — Board Cybersecurity Report Template.....	268
Appendix G — SOC Metrics Cheat Sheet	277
Appendix H — Cloud Security Metrics Checklist	285
Appendix I — Privacy Metrics Checklist	295
Appendix J — Benchmarking Worksheet.....	304
Appendix K — Metrics Catalog (100+ Example Metrics)	314
Appendix L — Security Metrics Interview Questions	322
Appendix M — Recommended Reading.....	329

Introduction

You can't improve what you don't measure.

Organizations invest millions of dollars in cybersecurity technologies, privacy programs, and compliance initiatives, but one question continues to challenge executives and security leaders:

Are we actually becoming more secure?

Answering that question requires more than intuition or isolated technical reports. It requires meaningful metrics that measure security performance, identify trends, communicate risk, and support informed decision-making. Good metrics help organizations prioritize investments, demonstrate the value of security programs, satisfy regulatory requirements, and continuously improve their defenses.

Unfortunately, measuring security and privacy isn't as simple as counting vulnerabilities or reporting the number of blocked attacks. Many organizations collect vast amounts of data but struggle to turn it into useful information. Others overwhelm leadership with technical details while failing to answer the business questions that matter most.

That's where this book comes in.

The Just Tell Me What I Need to Know... series is designed to cut through the complexity and focus on the knowledge professionals actually need. Rather than overwhelming you with academic research or complex statistical models, each book delivers practical, real-world concepts in a clear, concise, and easy-to-understand format.

This book focuses on Security & Privacy Metrics—the discipline of measuring the effectiveness, efficiency, maturity, and business value of cybersecurity and privacy programs. You'll learn how to develop meaningful Key Performance Indicators (KPIs), Key Risk Indicators (KRIs), and operational metrics; build dashboards and executive scorecards; measure compliance, resilience, and privacy performance; and communicate results in ways that support better business and technical decisions.

Unlike books that focus only on compliance reporting or audit metrics, this book emphasizes measurement as a management tool. Effective metrics help leaders identify weaknesses, justify investments, monitor progress, and continuously improve security and privacy programs across the enterprise.

Whether you're an engineer, analyst, architect, ISSO, manager, privacy professional, executive, student, or cybersecurity leader, understanding how to measure security and privacy performance is essential to building programs that deliver measurable results.

Most cybersecurity books discuss metrics as a few pages near the end. In reality, metrics are what separate a mature security program from one that's simply "busy." Executives don't ask, "How many vulnerabilities did you scan?" They ask, "Are we becoming more secure, and how do you know?"

This book should answer:

"How do I measure, communicate, and continuously improve cybersecurity and privacy performance?"

It should bridge the gap between technical operations and executive decision-making.

Our goal is simple:

Give you the knowledge you need, without making you read three books to get it.

So, let's get started.

IF YOU CAN'T MEASURE SECURITY, YOU CAN'T IMPROVE IT.

Organizations invest millions in cybersecurity technologies, privacy programs, and compliance initiatives—but how do you know whether any of it is actually making your organization more secure? Data alone isn't enough. What matters is turning that data into meaningful metrics that support better decisions.

The problem? Most books on security metrics are either filled with statistical theory, focused solely on compliance reporting, or assume you're building enterprise dashboards from scratch.

This book is different.

Just Tell Me What I Need To Know... Security & Privacy Metrics provides a practical, business-focused guide to measuring the effectiveness, efficiency, maturity, and value of cybersecurity and privacy programs. You'll learn how to develop meaningful Key Performance Indicators (KPIs), Key Risk Indicators (KRIs), and Key Control Indicators (KCIs); build executive dashboards and scorecards; measure operational performance, risk, resilience, compliance, and privacy; and communicate results in language that business leaders understand. Rather than simply collecting numbers, you'll learn how to use metrics to improve security, justify investments, demonstrate progress, and drive continuous improvement across the enterprise.



METRICS THAT DRIVE RESULTS



ALIGN

Align security metrics with business objectives.



INFORM

Provide clear insights that support better decisions.



IMPROVE

Continuously measure, refine, and get better.

INSIDE YOU'LL LEARN HOW TO:

- ✓ Build a meaningful security and privacy metrics program
- ✓ Develop KPIs, KRIs, KCIs, and executive scorecards
- ✓ Measure security performance, effectiveness, and business risk
- ✓ Create dashboards that support executive decision-making
- ✓ Measure vulnerability management, incident response, identity, cloud security, privacy, and compliance
- ✓ Communicate security performance in business terms
- ✓ Avoid common metrics pitfalls and misleading measurements
- ✓ Build a mature, data-driven cybersecurity program focused on continuous improvement

RISK SCORE

2.4

↓ 18%

INCIDENTS

37

↓ 24%

MTTR

3.6 hrs

↓ 31%

COMPLIANCE

92%

↑ 12%

TRAINING

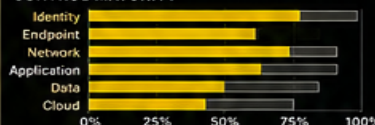
88%

↑ 9%

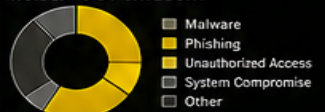
RISK TREND



CONTROL MATURITY



INCIDENTS BY CATEGORY



TOP RISKS

RISK	RATING	TREND
Third-Party Risk	High	↑
Ransomware	High	↑
Data Breach	High	↑
Privilege Misuse	Medium	→
Cloud Misconfiguration	Medium	→

BUILD A STRONGER, DATA-DRIVEN PROGRAM



MEASURE WHAT MATTERS

Focus on metrics that drive security and business value.



IMPROVE DECISIONS

Use data to prioritize investments and manage risk.



DEMONSTRATE VALUE

Show progress, justify budgets, and build confidence.



DRIVE ACCOUNTABILITY

Hold teams and processes accountable with clear metrics.



CONTINUOUS IMPROVEMENT

Refine metrics and programs to evolve with the business.



REDUCE RISK AND COST

Improve security outcomes while reducing exposure.



RISK MANAGEMENT



VULNERABILITY MANAGEMENT



INCIDENT RESPONSE



IDENTITY SECURITY



CLOUD SECURITY



DATA PROTECTION



PRIVACY & COMPLIANCE



THIRD-PARTY RISK



Whether you're a CISO, security architect, engineer, ISSO, analyst, auditor, privacy professional, manager, consultant, or aspiring cybersecurity leader, this book gives you the practical knowledge needed to **measure what matters—and use those measurements to make better security decisions.**



BETTER METRICS. BETTER INSIGHTS. BETTER SECURITY.
MEASURE WHAT MATTERS. IMPROVE WHAT COUNTS.

B E L S H A W C O N S U L T I N G