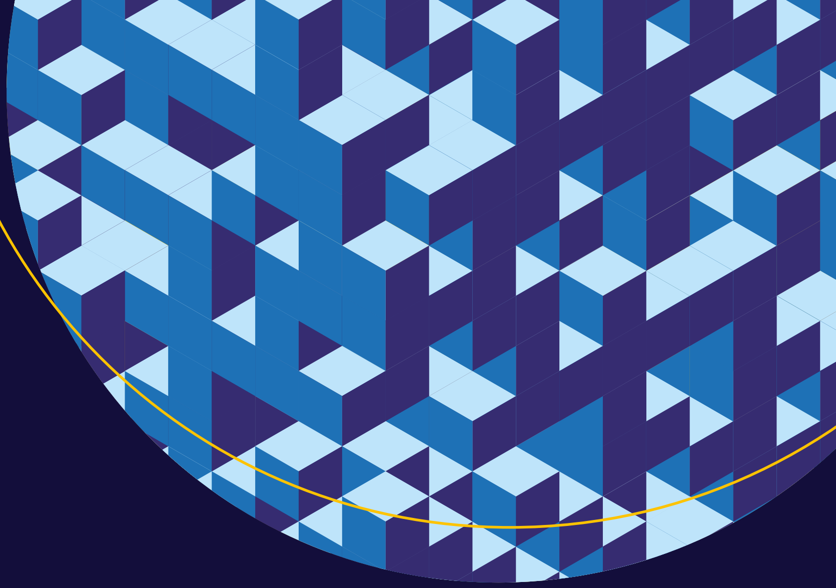

# Building a Comprehensive IT Security Program

## Practical Guidelines and Best Practices

Jeremy Wittkop

Apress®

# Building a Comprehensive IT Security Program

## Practical Guidelines and Best Practices

Jeremy Wittkop

Apress®

***Building a Comprehensive IT Security Program: Practical Guidelines and Best Practices***

Jeremy Wittkop
Boulder, Colorado, USA

ISBN-13 (pbk): 978-1-4842-2052-8 ISBN-13 (electronic): 978-1-4842-2053-5
DOI 10.1007/978-1-4842-2053-5

Library of Congress Control Number: 2016947953

Copyright © 2016 by Jeremy Wittkop

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Developmental Editor: Douglas Pundick, Laura Berendson
Technical Reviewer: Graham Laird
Editorial Board: Steve Anglin, Pramila Balen, Laura Berendson, Aaron Black, Louise Corrigan, Jonathan Gennick, Robert Hutchinson, Celestin Suresh John, Nikhil Karkal, James Markham, Susan McDermott, Matthew Moodie, Natalie Pao, Gwenan Spearing
Coordinating Editor: Rita Fernando
Copy Editor: Karen Jameson
Compositor: SPi Global
Indexer: SPi Global
Cover image designed by FreePik

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springer.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a Delaware corporation.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com.

Apress and friends of ED books may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Special Bulk Sales–eBook Licensing web page at www.apress.com/bulk-sales.

Any source code or other supplementary materials referenced by the author in this text is available to readers at www.apress.com. For detailed information about how to locate your book's source code, go to www.apress.com/source-code/.

Printed on acid-free paper

*To my Mom and Dad who never gave up on me when they probably should've, Rob and Chuck who gave me opportunities few would've, and my wife who loved me through the entire crazy journey.*

*A special thanks to Graham Laird and the Apress publishing team who made it all possible.*

# Contents at a Glance

About the Author .......................................................................................xv

About the Technical Reviewer ....................................................................xvii

Introduction ....................................................................................................xix

■Chapter 1: The Problem We Are Facing ......................................................... 1

■Chapter 2: Protecting Critical Assets ........................................................... 21

■Chapter 3: Monetizing Risk .......................................................................... 41

■Chapter 4: Security Intelligence Model ........................................................ 55

■Chapter 5: Incident Response Planning........................................................ 73

■Chapter 6: The People Problem .................................................................... 89

■Chapter 7: Assigning Accountability ........................................................... 107

■Chapter 8: Shifting the Paradigm ................................................................ 121

■Chapter 9: The Definition of Insanity ........................................................... 137

■Chapter 10: Deja Vu ..................................................................................... 153

■Chapter 11: The Information Security Community ...................................... 167

■Chapter 12: Partnering with Governments .................................................. 177

Index ................................................................................................................ 189

# Contents

**About the Author** .......... xv

**About the Technical Reviewer** .......... xvii

**Introduction** .......... xix

■ **Chapter 1: The Problem We Are Facing** .......... 1

ThreatCon .......... 1

A Question of Motive .......... 3

Spies and Nation-States .......... 4

Organized Criminals .......... 4

Terrorists .......... 4

Hacktivist Groups .......... 4

Electronic Espionage .......... 5

Spies and Nation-States Modus Operandi .......... 6

Espionage Use Case Example: Anthem .......... 7

If Al Capone Owned a Computer .......... 9

Organized Crime Example Case Study: Target .......... 12

Terrorism 2.0 .......... 14

Example Case Study: Saudi Aramco .......... 16

Example Case Study: Sony .......... 17

Shades of Gray .......... 18

Anatomy of an Anonymous Attack .......... 18

Hacktavist Example Case Study: Federal Reserve .......... 19

Conclusion .......... 20

Chapter 2: Protecting Critical Assets ........................................................ 21

Three Wise Men........................................................ 21

Rob Eggebrecht ........................................................ 22

Chuck Bloomquist........................................................ 22

Ryan Coleman........................................................ 23

What Is a Critical Information Asset? ........................................................ 24

Data Life Cycle Elements........................................................ 25

Creation ........................................................ 25

Storage ........................................................ 26

Usage........................................................ 26

Transmission........................................................ 27

Vertical Challenges........................................................ 27

Law Firms and Other Service Providers ........................................................ 27

Oil and Gas ........................................................ 28

Health Care........................................................ 29

Manufacturing ........................................................ 29

Financial Services ........................................................ 30

Retail ........................................................ 30

Publicly Traded Companies........................................................ 31

Needles in the Haystack........................................................ 31

Content Analytics........................................................ 31

Data in Motion ........................................................ 32

Data in Use ........................................................ 32

Data at Rest........................................................ 33

The Future of Content Analytics........................................................ 33

Context Analytics ........................................................ 34

Evolution of Context Analytics ........................................................ 35

Types of Events........................................................ 36

Content, Community, and Channel ........ 36
Content ........ 37
Community ........ 37
Channel ........ 37
A Proper Response ........ 38
Conclusion ........ 39
**Chapter 3: Monetizing Risk ........ 41**
Calculating Annual Loss Expectancy ........ 42
Example Case Study: Hurricane Katrina ........ 44
Risk Treatment Strategies ........ 45
Risk Acceptance ........ 45
Risk Mitigation ........ 46
Risk Transference ........ 46
Risk Avoidance ........ 46
Real-World Example ........ 47
A Different Approach ........ 47
Indirect Costs of Breaches ........ 48
Modeling Risk ........ 49
Conclusion ........ 53
**Chapter 4: Security Intelligence Model ........ 55**
How the Security Intelligence Model Works ........ 56
The Business ........ 57
Intelligence Layer ........ 60
Strategy Layer ........ 62
Tactical Layer ........ 63
Technology Layer ........ 65
Event Layer ........ 66
Program Results ........ 67

Case Study: Mastering the Model .......... 69
Conclusion .......... 71
**Chapter 5: Incident Response Planning .......... 73**
Elements of an Incident Response Plan .......... 74
Preparation .......... 75
Detection and Analysis .......... 77
Containment, Eradication, and Recovery .......... 78
Post-Incident Activity .......... 81
Testing the Plan .......... 82
Red Team Exercises .......... 82
Purple Team Exercises .......... 83
Tabletop Exercises .......... 83
Security Assessments .......... 84
Vulnerability Scanning .......... 84
Vulnerability Assessments .......... 85
Penetration Testing .......... 85
The Erosion of the Perimeter .......... 85
Next-Generation Firewalls .......... 86
The Cloud .......... 86
Evolving Infrastructure .......... 86
Digital Protectionists .......... 87
Conclusion .......... 87
**Chapter 6: The People Problem .......... 89**
What Would You Do for a Klondike Bar? .......... 90
Why Don't They Get It? .......... 91
The Insider Threat .......... 92
Malicious Insider .......... 92
Misguided Insiders .......... 93
Well-Meaning Insiders .......... 94
Internal and External Threats .......... 94

User-Generated and System-Generated Events ........ 94
The Evolution of Attacks ........ 95
Security Humanistics ........ 96
People, Process, and Technology ........ 96
People – What Would You Do for a Klondike Bar? ........ 97
Process ........ 99
Technology ........ 101
A Different Approach ........ 102
Business Requirements ........ 102
Functional Requirements ........ 102
Technology Selection ........ 102
Back to Basics ........ 103
eBay and Concept of Least Privilege ........ 103
Sony Pictures and Records and Information Management ........ 103
Target and Third-Party Access Control ........ 103
Saudi Aramco and Separation of Duties ........ 104
Conclusion ........ 105
■ **Chapter 7: Assigning Accountability ........ 107**
Who Is Responsible for Security? ........ 107
The Rise of Data Classification ........ 108
Shifting Accountability ........ 110
Establishing Mandates Using Earnings Reports ........ 111
It's MY Problem, Now What? ........ 111
Flexibility within a Framework ........ 112
Using a RACI Matrix ........ 112
Responsible ........ 112
Accountable ........ 113
Consulted ........ 114
Informed ........ 114
Building a Matrix ........ 114

Effective Leadership .......... 115

Setting Proper Expectations .......... 116

Communication .......... 116

Delegation .......... 117

Millennials .......... 117

Privacy in the New Millennium .......... 120

Conclusion .......... 120

**Chapter 8: Shifting the Paradigm .......... 121**

Education Reforms .......... 122

Traditional Information Security Professionals and Effective Information Security Teams .......... 124

Traditional Information Security Professionals .......... 124

Effective Information Security Teams .......... 125

The History of Software Development .......... 129

Secure Business Process Design .......... 129

Reactive vs. Proactive Security .......... 130

Traditional Reactive Security Models .......... 132

Adaptive Security .......... 132

Behavioral Analytics .......... 133

Workflow Automation .......... 135

Conclusion .......... 135

**Chapter 9: The Definition of Insanity .......... 137**

Pickett's Charge .......... 138

Planning to Fail .......... 140

Check Box Compliance .......... 142

The Ostrich Approach .......... 143

Silos in Security .......... 144

Destroying Barriers to Communication .......... 144

Red Herrings .......... 146

Example: Mobile Device Security .......... 146

Persistent Areas of Vulnerability ........ 146

Single-Factor Authentication Servers ........ 147

Social Engineering ........ 148

Back to Basics ........ 148

Concept of Least Privilege and Need to Know ........ 149

Separation of Duties and Job Rotation ........ 150

Vulnerability Scanning and Patching ........ 151

Engaging the Business ........ 151

■ **Chapter 10: Deja Vu ........ 153**

The Wild West ........ 154

Evolving the Approach ........ 155

Lessons from History ........ 155

Creation of the Federal Bureau of Investigation – 1908 ........ 156

The Federal Deposit Insurance Corporation (FDIC) – 1933 ........ 157

Anti-Bank Robbing Technology ........ 157

The Evolution of an Outlaw ........ 161

Nineteenth-Century Outlaws ........ 161

Twentieth-Century Outlaws ........ 162

Outlaws in the New Millennium ........ 162

Conclusion ........ 164

■ **Chapter 11: The Information Security Community ........ 167**

Sharing Information ........ 168

The Elderwood Framework ........ 169

Creating a Framework for Sharing Information ........ 169

Industry Alerting ........ 170

The Role of Security Vendors ........ 171

Protecting Participants ........ 171

The Rise of the Platform ........ 172

Rich Correlation ........ 173

Ease of Operational Management ........ 173

Monitoring and Auditing ........ 174
Access Control ........ 174
Platform Conclusion ........ 174
The End-User Paradigm ........ 174
Respect the End User ........ 175
Dunning–Kruger Effect ........ 175
Building Internal Bridges ........ 176
Conclusion ........ 176
■ Chapter 12: Partnering with Governments ........ 177
Apple and San Bernardino ........ 177
Gas Station Sushi ........ 178
A Question of Trust ........ 179
The Role of Government and the Private Sector ........ 179
Partnerships That Work ........ 180
InfraGard ........ 180
Defense Industrial Base ........ 181
National Cybersecurity Center ........ 182
National Vulnerability Database ........ 183
CREST ........ 183
Regulations ........ 183
What Should Be the Role of Government? ........ 184
Effective Public Partner Partnership Opportunities ........ 185
Counterattacks and Hacking Back ........ 185
Militaries and Corporations Working Together ........ 186
You Are Not a Number! ........ 186
Conclusion ........ 188
Index ........ 189