

# **How to Manage Cybersecurity Risk**



# How to Manage Cybersecurity Risk

*A Security Leader's Roadmap with Open FAIR™*

Christopher T. Carlson



BrownWalker Press  
Irvine • Boca Raton

*How to Manage Cybersecurity Risk: A Security Leader's Roadmap with Open FAIR™*

Open FAIR is a trademark of The Open Group

Copyright © 2019 Christopher T. Carlson.

All rights reserved.

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law.

BrownWalker Press / Universal Publishers, Inc.

Irvine • Boca Raton

USA • 2019

[www.BrownWalkerPress.com](http://www.BrownWalkerPress.com)

978-1-62734-276-6 (pbk.)

978-1-62734-277-3 (ebk.)

Typeset by Medlar Publishing Solutions Pvt Ltd, India

Cover design by Ivan Popov

Publisher's Cataloging-in-Publication Data

Names: Carlson, Christopher T., 1953- author.

Title: How to manage cybersecurity risk : a security leader's roadmap with Open FAIR / Christopher T. Carlson.

Description: Irvine : BrownWalker Press, 2019. | Includes bibliographical references and index.

Identifiers: LCCN 2019034283 (print) | LCCN 2019034284 (ebook) |

ISBN 9781627342766 (paperback) | ISBN 9781627342773 (ebook)

Subjects: LCSH: Computer security--Standards. | Computer crimes--Risk assessment--Standards. | Open FAIR.

Classification: LCC QA76.9.A25 C368 2019 (print) | LCC QA76.9.A25 (ebook) | DDC 005.8--dc23

LC record available at <https://lcn.loc.gov/2019034283>

LC ebook record available at <https://lcn.loc.gov/2019034284>

For Geri



# Contents

<i>List of Tables</i>	<i>xi</i>
<i>List of Figures</i>	<i>xiii</i>
<i>Synopsis</i>	<i>xvii</i>
<i>Foreword</i>	<i>xix</i>
<i>Acknowledgements</i>	<i>xxi</i>
<i>About the Author</i>	<i>xxiii</i>
<b>I. Reactive</b>	<b>1</b>
1 Stop the Bleeding	3
2 Establish Expectations	7
3 Identify Asset Inventory	9
4 Assess Current Controls	13
5 Report Results	19
6 Manage Corrective Actions	21
<b>II. Planned</b>	<b>23</b>
7 Establish the Security Program	27
8 Protect Information	33
9 Protect Information Systems	45
10 Design Defense in Depth	49

11	Define Security Controls	61
12	Assess Compliance	77
13	Quantify Information Risk	85
14	Govern the Security Program	101
15	Deliver Security Services	105
16	Destroy Obsolete Information	109
17	Protect Assets Internationally	111
18	Ensure Supplier Security	121
19	Maintain Skills and Certifications	129
<b>III. Managed</b>		<b>131</b>
20	Document Processes	133
21	Define Risk Management Process	137
22	Define Policy Management Process	147
23	Define Assessment Management Process	157
24	Define Incident Management Process	167
25	Manage Information Security	175
26	Certify Management System	183
27	Understand Authorities and Dependencies	187
28	Manage Regulatory and Contractual Compliance	195
29	Control Access	205
30	Develop Secure Applications	219
31	Provide Metrics	241
32	Design and Implement Security Systems	251



<b>Appendices – Terminology</b>	<b>259</b>
A Who is Security	261
B What is Security	263
C Vocabulary of Risk	265
D Security Concepts	269
E What does Cybersecurity Mean	273
<i>Bibliography</i>	277
<i>Index</i>	281



# List of Tables

<b>Table 3-1</b>	Facilities Inventory	10
<b>Table 3-2</b>	Network Hardware Inventory	11
<b>Table 3-3</b>	Computing Hardware Inventory	12
<b>Table 4-1</b>	List of Findings	16
<b>Table 4-2</b>	Building Inventory	17
<b>Table 4-3</b>	Computing Equipment Inventory	17
<b>Table 4-4</b>	Network Equipment Inventory	17
<b>Table 4-5</b>	List of Findings with Corrective Actions	18
<b>Table 5-1</b>	Status of Prioritized Goals	19
<b>Table 6-1</b>	List of Findings	21
<b>Table 6-2</b>	List of Findings with Corrective Actions	22
<b>Table 11-1</b>	Controls List and Applicability	63
<b>Table 11-2</b>	Control Framework	68
<b>Table 11-3</b>	Information Protection Requirements	69
<b>Table 11-4</b>	Mapping Control Objectives and Protection Requirements	70
<b>Table 12-1</b>	Host Compliance Scorecard	81
<b>Table 12-2</b>	Summary Compliance Scorecard	82
<b>Table 13-1</b>	Green Yellow Red Risk Grid	87

<b>Table 13-2</b>	Risk Grid with X*Y/IO Scores	88
<b>Table 13-3</b>	Capital Budget Return-on-Investment Analysis	99
<b>Table 14-1</b>	Summary Compliance Scorecard	102
<b>Table 18-1</b>	Supplier Access Requirement Matrix	122
<b>Table 21-1</b>	Example Risk Library	144
<b>Table 28-1</b>	Example Control Framework Mapping	199
<b>Table 28-2</b>	Control Framework Mapping Sorted by Requirement	201
<b>Table 30-1</b>	System Development Life Cycle with Security Activities	222
<b>Table 31-1</b>	Organization Security Control Implementation Status	244
<b>Table 31-2</b>	Team Security Control Implementation Status	244
<b>Table 31-3</b>	People Security Control Status	245
<b>Table 31-4</b>	Organization Security Control Status Roll-Up	246
<b>Table 31-5</b>	Technical Assessment Top Level Application Summary	247
<b>Table 31-6</b>	Technical Assessment Host Summary Drill Down	247
<b>Table 31-7</b>	Technical Assessment Protocol Summary Drill Down	248
<b>Table 31-8</b>	Technical Assessment Host Summary with Application Drill Down	248
<b>Table 31-9</b>	Technical Assessment Host Drill Down with Traffic Detail	248

# List of Figures

<b>Figure 1-1</b>	Reactive Program Process Steps	2
<b>Figure 3-1</b>	Building Layout Diagram	10
<b>Figure 3-2</b>	Logical Network Diagram	12
<b>Figure 4-1</b>	Assessment Plan Template	15
<b>Figure 5-1</b>	Information Protection Status Chart	20
<b>Figure 8-1</b>	Physical Security Diagram	40
<b>Figure 10-1</b>	Layers of Defense	50
<b>Figure 10-2</b>	IT Security Design Diagram	57
<b>Figure 11-1</b>	Change Management Example	73
<b>Figure 12-1</b>	General Assessment System	79
<b>Figure 12-2</b>	Assessment Data Collection and Reporting	80
<b>Figure 13-1</b>	Risk Definition Shown by Open FAIR Taxonomy	90
<b>Figure 13-2</b>	Open FAIR Analysis Result Illustration	90
<b>Figure 13-3</b>	Open FAIR Taxonomy	91
<b>Figure 13-4</b>	Open FAIR Tool Loss Event Frequency Input	92
<b>Figure 13-5</b>	Open FAIR Tool Loss Magnitude Input	93
<b>Figure 13-6</b>	Open FAIR Tool Output	93
<b>Figure 13-7</b>	Open FAIR Taxonomy with Control Categories	97

<b>Figure 13-8</b>	Threat Objective and Control Layers	97
<b>Figure 13-9</b>	Example Security Controls by Layer	98
<b>Figure 14-1</b>	Summary Report of Incidents	102
<b>Figure 14-2</b>	Corrective Action Plan Status Graphic	103
<b>Figure 17-1</b>	Example Global Color Scores	114
<b>Figure 17-2</b>	Headquarters and Subsidiary Policy Relationships	115
<b>Figure 17-3</b>	Policy Zone Connection Agreement Template	118
<b>Figure 20-1</b>	Example Process Flow	134
<b>Figure 20-2</b>	Example Process Step Description	135
<b>Figure 21-1</b>	FAIR ISO/IEC 27005 Risk Management Process	138
<b>Figure 23-1</b>	Example Assessment Management System Diagram	159
<b>Figure 24-1</b>	Hostile Attack Kill Chain	168
<b>Figure 25-1</b>	Information Security Management System	176
<b>Figure 25-2</b>	Example Results Chain	180
<b>Figure 27-1</b>	Policy and Authority Waterfall	190
<b>Figure 29-1</b>	Example Single System Access Request Process Flow	209
<b>Figure 29-2</b>	Tangle of Managers and Systems' Access Requests	210
<b>Figure 29-3</b>	Centralized Access Administration	211
<b>Figure 29-4</b>	Streamlined Access Administration	212
<b>Figure 29-5</b>	Maintain and Use People Data Directory	216
<b>Figure 29-6</b>	Access Decision and Control Points	217

<b>Figure 30-1</b>	System Development Life Cycle with Secure Development	220
<b>Figure 30-2</b>	Access Decision and Control Points	228
<b>Figure 30-3</b>	Application Implementation of Access Decision and Control Points	228
<b>Figure 30-4</b>	Appliance Reliance on Access Decision Point	229
<b>Figure 30-5</b>	Example Application Data Flows	233
<b>Figure 32-1</b>	Model of Security Requirements Mapped to Policy	252
<b>Figure 32-2</b>	Model of Goals by Protection Layer	252
<b>Figure 32-3</b>	Threat and Asset Added to Protection Layer Model	253
<b>Figure 32-4</b>	Security Requirements Linked to Protection Layer Model	254
<b>Figure 32-5</b>	Security Services Linked to Security Requirements	256





# Synopsis

Protecting information systems to reduce the risk of security incidents is critical for organizations today. This writing provides instruction for security leaders on the processes and techniques for managing a security program. It contains practical information on the breadth of information security topics, referring to many other writings that provide details on technical security topics. This provides a foundation for a security program that is responsive to technology developments and an evolving threat environment.

The security leader may be engaged by an organization that is in crisis, where the priority action is to recover from a serious incident. This work offers foundation knowledge for the security leader to immediately apply to the organization's security program while improving it to the next level, organized by development stage:

- Reactive – focused on incident detection and response
- Planned – control requirements, compliance and reporting
- Managed – integrated security business processes

The security leader must also communicate with the organization executive, whose focus is on results such as increasing revenues or reducing costs. The security leader may initially be welcomed as the wizard who applies mysterious skills to resolve an embarrassing incident. But the organization executive will lose patience with a perpetual crisis and demand concrete results. This writing explains how to communicate in terms executives understand.



# Foreword

Very few people are adequately prepared to take on their first information security leadership role. I know I wasn't. I had the appropriate professional certifications and over a decade of experience in the field, but that didn't adequately prepare me for what I faced as a newly minted CISO. Twenty years later, I can say with confidence that if this book had been available then, I would have experienced much less stress in that initial role.

The sheer complexity and speed of change within the information security landscape often aren't the greatest challenges you'll face in this role. Nor are "technology", error-prone users, or cybercriminals the greatest challenges. Organization politics, inertial resistance to change, unrealistic and sometimes illogical expectations, incomplete information, and "conventional wisdom" that often isn't particularly wise are usually more problematic. And of course, there is the immutable fact that organizations will always have many business imperatives that have to be balanced against information security concerns, because there are only so many resources to go around.

Effectively leading an information security team through this landscape requires a clear understanding of the organization's objectives, competing priorities, and limitations. It also requires clarity of thought and an ability to communicate well with senior executives, peers, those who are lower in the food chain, as well as with external stakeholders like regulators. You'll need to work with colleagues to define realistic policies that accurately reflect the capabilities and risk tolerances of the organization, and establish processes that are finely tuned to achieve their objectives without placing an unnecessary burden on the organization. At the same time, information security leaders need to help their organizations identify

and focus on the things that matter most from a risk perspective, and make smart choices about solutions to the many problems and concerns that continually crop up.

Accomplishing this is much easier with a roadmap and a mentor. That, in effect, is what this book is intended to provide. I've known Chris Carlson for over a decade, and his depth of knowledge and understanding of our field has always impressed me. Even more importantly, he always struck me as a pragmatist – which is crucial to success as a leader within the information security field. The contents of this book reflect both his vast experience and his pragmatic nature. As a result, anybody who is stepping into an information security leadership role for the first time, or who wants to prepare for such an opportunity, will benefit greatly from what Chris discusses here.

Jack Jones  
RiskLens Co-Founder and Chief Risk Scientist;  
Chairman of the FAIR Institute

# Acknowledgements

I began writing upon completion of nearly 35 years in the information system security field. The following are people who influenced me over those years as peers, managers, employees and various other relationships. They are listed roughly chronologically from my first interaction. The journey began when a job opening in the computing security organization was brought to my attention.

- |                        |                 |
|------------------------|-----------------|
| Craig Worstell         | Imre Hetenyi    |
| Chuck Carkeek          | Steve Whitlock  |
| Jed Selter             | Berne Indahl    |
| Karen Worstell         | Pam Carvey      |
| Scott Wickett          | John Roundhill  |
| Marie Olson            | Peter Rumsey    |
| Inez Briley Taylor     | John Thurlow    |
| Dennis Hill            | I4 Members      |
| Tom Nestor             | Douglas Hubbard |
| Glen Jennings          | Jack Jones      |
| Alan Mulally           | Alex Hutton     |
| Debbie Ring            | Krista Horstman |
| Carla Cummins Peterson | Sam Savage      |
| Ronald G. Smith        | Mike Jerbic     |
| Rick Carl              |                 |

This writing evolved from flow-of-consciousness fragments to an organized work. For the essential detailed review and polish I thank my friend and editor, Inez Briley Taylor.



# About the Author

Christopher T. Carlson is a pioneer, having arrived in his first computing security assignment at the dawn of the field in 1982. He created or substantially evolved practices in his security assignments including classified computing security, computing security policy and controls, security awareness, business unit security support, security assessments, access administration including role-based access, risk analysis and management, application security development life cycle, and international security. The goal of this writing is to provide lessons from the field so that those who follow need not start from scratch.





# I

## Reactive

*The situation when the first security leader arrives, often in the wake of a major incident.*

Imagine a typical medium-sized organization. The organization uses information systems for typical business functions such as product inventory, sales, finance and office automation. Perhaps they handle credit card information or personal medical histories. Maybe they create specialized products in a market where trade secrets give them a competitive edge. Possibly export-controlled information is involved, should their products be components for military products.

The information technology function will likely rely heavily on outsourced services such as datacenter or cloud services, desktop and