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

BrownWalker Press / Universal Publishers, Inc.
Irvine • Boca Raton
USA • 2019
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://lccn.loc.gov/2019034283
LC ebook record available at https://lccn.loc.gov/2019034284

For Geri

Contents

List of Tables

List of Figures

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

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