

The logo for SYNGRESS, featuring the word "SYNGRESS" in a bold, white, sans-serif font. The text is positioned on a dark background that is part of a larger image of a server room with blurred lights and racks of equipment.

**SYNGRESS**

# RESEARCH METHODS FOR CYBER SECURITY

Thomas W. Edgar | David O. Manz



# Research Methods for Cyber Security



# Research Methods for Cyber Security

Thomas W. Edgar  
David O. Manz



**SYNGRESS®**

Syngress is an imprint of Elsevier  
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, United States

Copyright © 2017 Elsevier Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: [www.elsevier.com/permissions](http://www.elsevier.com/permissions).

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

#### Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

#### British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library

#### Library of Congress Cataloging-in-Publication Data

A catalog record for this book is available from the Library of Congress

ISBN: 978-0-12-805349-2

For Information on all Syngress publications  
visit our website at <https://www.elsevier.com/books-and-journals>



Working together  
to grow libraries in  
developing countries

[www.elsevier.com](http://www.elsevier.com) • [www.bookaid.org](http://www.bookaid.org)

*Publisher:* Todd Green

*Acquisition Editor:* Brian Romer

*Editorial Project Manager:* Anna Valutkevich

*Production Project Manager:* Punithavathy Govindaradjane

*Cover Designer:* Mark Rogers

Typeset by MPS Limited, Chennai, India

# Contents

<b>ABOUT THE AUTHORS</b> .....	<b>xv</b>
<b>FOREWORD</b> .....	<b>xvii</b>
<b>PREFACE</b> .....	<b>xix</b>
<b>ACKNOWLEDGMENTS</b> .....	<b>xxiii</b>

## Part I Introduction

<b>CHAPTER 1</b> Introduction to Science .....	<b>3</b>
<i>Mark Tardiff</i>	
Chapter Objectives.....	4
What Is Science.....	4
Types of Science .....	5
Science Is Messy.....	6
Hierarchy of Evidence.....	9
From Ptolemy to Einstein—Science and the Discovery of the Nature of the Sky.....	10
A Science Continuum of Discovery.....	11
The Ptolemaic Model and Supporting Assumptions .....	13
Was the Ptolemaic Model of the Solar System Useful? .....	16
Emergence of the Heliocentric Model.....	16
Nicolaus Copernicus.....	17
Was the Copernican Model an Improvement?.....	19
Johannes Kepler .....	19
Kepler’s Contributions in the Context of the Science Continuum of Discovery.....	21
Galileo Galilei.....	21
Galileo’s Contributions in the Context of the Science Continuum of Discovery.....	23
Isaac Newton .....	23
Newton’s Contributions in the Context of the Science Continuum of Discovery.....	25
Albert Einstein.....	26
Are Einstein’s Contributions an Improvement to Understanding Planetary Motion? .....	27

	Einstein's Contributions in the Context of the Science	
	Continuum of Discovery.....	28
	Summary and Conclusions.....	29
	Discovery in the Realm of Right and Wrong.....	30
	Endnotes.....	31
<b>CHAPTER 2</b>	<b>Science and Cyber Security.....</b>	<b>33</b>
	Chapter Objectives.....	34
	Defining Cyber Space.....	34
	Data Perspective.....	34
	Technology Perspective.....	35
	Cybernetic Perspective.....	35
	Defining Cyber Security.....	36
	Attributes of Cyber Security.....	37
	Cyber Security Fundamentals.....	39
	Vulnerability.....	39
	Exploit.....	39
	Threat.....	40
	Threat Actor.....	40
	Threat Vector.....	40
	Attack.....	40
	Malware.....	40
	Secure System Design Principles.....	41
	Cyber Security Controls Overview.....	43
	Access Control.....	44
	Situation Awareness.....	45
	Cryptography.....	46
	Host Security.....	49
	Network Security.....	50
	Risk.....	50
	Defining a Science of Cyber Security.....	51
	Our Definition of a Cyber Security Science.....	52
	Challenges in Achieving Security in Cyber Space.....	55
	Further Reading.....	57
	Attack Detection.....	57
	Secure Mechanism Design.....	57
	Software Security.....	57
	Malware/Threat Analysis.....	57
	Risk Management.....	58
	Cryptography.....	58
	Endnotes.....	61
<b>CHAPTER 3</b>	<b>Starting Your Research.....</b>	<b>63</b>
	Chapter Objectives.....	65
	Starting Your Research.....	65

Initial Question Process .....	67
Research Progression .....	68
Observational Research .....	70
Theoretical Research .....	71
Experimental Research .....	73
Applied Research .....	74
Research Before the Research .....	75
Selecting Your Research Path .....	78
Walking the Decision Tree .....	79
Observation Method Selection .....	84
Theoretical Method Selection .....	86
Experimental Method Selection .....	87
Applied Method Selection .....	89
Conferences and Journals .....	90
Endnotes .....	91

## Part II Observational Research Methods

<b>CHAPTER 4</b> Exploratory Study .....	95
Chapter Objectives .....	96
Knowledge by Inference .....	96
Types of Studies .....	98
Exploratory Study .....	98
Gathering Data .....	100
Research Questions and Datasets .....	102
Scales of Data .....	103
Sample Size .....	104
Dataset Sensitivities and Restrictions .....	109
Exploratory Method Selection .....	109
Exploratory Study Method Examples .....	111
Case-control Example .....	112
Ecological Example .....	114
Cross-sectional .....	116
Longitudinal Example .....	118
Analysis Bias .....	121
The Search for a Causal Relationship .....	123
Graph Summarization .....	123
Descriptive Statistics .....	123
Regression Analysis .....	124
Reporting Your Results .....	126
Sample Format .....	127
Endnotes .....	129
<b>CHAPTER 5</b> Descriptive Study .....	131
Chapter Objectives .....	132
Descriptive Study Methods .....	132

Observation Method Selection .....	135
Gathering Data .....	135
Data Collection Methods .....	137
Data Analysis .....	140
Coding Unstructured Data .....	141
Proportions .....	141
Frequency Statistics .....	142
Descriptive Study Method Examples .....	142
Case Study .....	143
Elicitation Studies .....	145
Case Report .....	147
Reporting Your Results .....	148
Sample Format .....	148
Endnotes .....	151
<b>CHAPTER 6</b> Machine Learning .....	153
<i>Satish Chikkagoudar, Samrat Chatterjee,</i>	
<i>Dennis G. Thomas, Thomas E. Carroll, and George Muller</i>	
Chapter Objectives .....	153
What is Machine Learning .....	154
Categories of Machine Learning .....	154
Debugging Machine Learning .....	157
Bayesian Network Mathematical Preliminaries and Model	
Properties .....	158
Strengths and Limitations .....	158
Data-driven Learning and Probabilistic Inference	
within Bayesian Networks .....	159
Parameter Learning .....	159
Probabilistic Inference .....	160
Notional Example with bnlearn Package in R .....	160
Hidden Markov Models .....	165
Notional Example with HMM Package in R .....	167
Discussion .....	169
Sample Format .....	169
Abstract .....	169
Introduction .....	170
Related Work .....	170
Approach .....	170
Evaluation .....	170
Data Analysis/Results .....	171
Discussion/Future Work .....	171
Conclusion/Summary .....	171
Acknowledgments .....	171
References .....	171
Endnotes .....	172

## Part III Mathematical Research Methods

<b>CHAPTER 7</b>	Theoretical Research .....	177
	<i>Thomas E. Carroll</i>	
	Chapter Objectives.....	177
	Background.....	177
	Characteristics of a Good Theory .....	179
	Challenges in Development of Cyber Security Science Theory.....	180
	Identify Insight.....	181
	Determine Relevant Factors .....	182
	Formally Define Theory.....	182
	Test for Internal Consistency.....	183
	Test for External Consistency.....	183
	Refute.....	184
	Continue to Seek Refinements.....	184
	Example Theoretical Research Construction.....	184
	Reporting Your Results .....	188
	Sample Format.....	188
	Endnotes.....	191
<b>CHAPTER 8</b>	Using Simulation for Research.....	193
	Chapter Objectives.....	194
	Defining Simulation .....	194
	When Should Simulation Be Used .....	196
	Theoretical Simulations.....	196
	Simulation for Decision Support.....	197
	Empirical Simulation .....	197
	Synthetic Conditions.....	198
	Cautions of Simulation Use.....	199
	Defining What to Model.....	199
	Model Validity .....	201
	Instantiating a Model.....	202
	Types of Simulation.....	203
	Example Use Case.....	207
	Paper Format.....	210
	Endnotes.....	210

## Part IV Experimental Research Methods

<b>CHAPTER 9</b>	Hypothetico-deductive Research.....	215
	Chapter Objectives.....	215
	Purpose of Hypothesis-Driven Experimentation .....	215

Turn Inductive Process Into Deductive Process ..... 216

Reject a Theory or Build Evidence Strengthening ..... 217

Specify What You Think is Involved; Challenge Assumptions .... 217

Define a Process by Which Others can Replicate and  
Reproduce the Effect; to Test and Ensure that Your  
Own Approach is Valid. .... 218

The Goal of Hypothetico-deductive Experimentation  
is Different than Applied Experimentation ..... 218

A Proper Hypothesis ..... 219

Observable and Testable ..... 219

Clearly Defined ..... 220

Single Concept ..... 221

Predictive ..... 222

Generating a Hypothesis from a Theory ..... 222

Experimentation ..... 224

Dependent Variables (Measured Variables) ..... 226

Independent Variables (Controls) ..... 228

Experimental Design ..... 232

Analysis ..... 239

Hypothesis Testing ..... 239

Integrating the Theory with Results ..... 244

Reporting Your Results ..... 245

Sample Format ..... 245

Endnotes ..... 248

**CHAPTER 10** Quasi-experimental Research ..... 251

Chapter Objectives ..... 252

True versus Quasi-experiment ..... 252

Cyber Drivers for Quasi-experimental Design ..... 253

Quasi-experiment Research Methods ..... 255

    Difference-of-differences Design ..... 255

    Time Series Design ..... 260

    Cohort Design ..... 264

Reporting Your Results ..... 268

Endnotes ..... 268

## Part V Applied Research Methods

**CHAPTER 11** Applied Experimentation ..... 271

Chapter Objectives ..... 272

Building From a Theory ..... 272

Methods of Applied Experimentation ..... 273

Benchmarking ..... 274

    Collecting or Defining a Benchmark ..... 276

    Running the Benchmark ..... 279

	Analyzing the Results .....	280
	Problems With Benchmarking.....	283
	Reporting Your Results .....	284
	Sample Format.....	284
	Validation Testing .....	287
	Independent Variables.....	289
	Dependent Variables .....	289
	Experimental Design .....	290
	Problems With Validation Testing.....	292
	Reporting Your Results .....	293
	Sample Format.....	294
	Endnotes.....	297
<b>CHAPTER 12</b>	<b>Applied Observational Study.....</b>	<b>299</b>
	Chapter Objectives.....	300
	Applied Study Types .....	300
	Applied Exploratory Studies .....	301
	Applied Descriptive Study.....	304
	Applied Observation Method Selection .....	306
	Data Collection and Analysis .....	306
	Applied Exploratory Studies .....	306
	Applied Descriptive Studies.....	307
	Applied Exploratory Study: Stress Test .....	307
	System.....	308
	Behavior .....	308
	Testing Methodology .....	309
	Applied Descriptive Study: Case Study .....	311
	Reporting Your Results .....	313
	Sample Format.....	314
	Endnote.....	317
 <b>Part VI Additional Materials</b>		
<b>CHAPTER 13</b>	<b>Instrumentation .....</b>	<b>321</b>
	Chapter Objectives.....	322
	Understanding Your Data Needs.....	322
	Fidelity.....	323
	Types .....	326
	Amount.....	326
	Source location.....	327
	Difference between Operational and Scientific Measurements.....	327
	Overview of Data and Sensor Types.....	328
	Host-based Sensors.....	328
	Network-based Sensors .....	330

	Hardware Sensors .....	331
	Physical Sensors .....	332
	Honeypots .....	333
	Centralized Collectors .....	334
	Data Formats .....	334
	Sensor Calibration .....	337
	Controlled-Testing Environments .....	338
	Conclusion .....	342
	Endnotes .....	342
<b>CHAPTER 14</b>	<b>Addressing the Adversary .....</b>	<b>345</b>
	Chapter Objectives .....	346
	Defining Adversary .....	346
	The Challenge of Adversarial Research .....	348
	Adversaries in Other Fields of Study .....	353
	Different Ways to Think About Threats .....	356
	Adversary Perspective .....	357
	Defining Adversaries as Threats .....	358
	Attribution .....	359
	Integrating Adversary Models into Research .....	359
	Approaches .....	360
	Challenges .....	361
	Conclusions .....	365
	Endnotes .....	365
<b>CHAPTER 15</b>	<b>Scientific Ethics .....</b>	<b>367</b>
	Chapter Objectives .....	367
	Ethics for Science .....	367
	History of Ethics in Cyber Security .....	371
	Ethical Standards .....	374
	Association for Computing Machinery .....	374
	Institute of Electrical and Electronics Engineers .....	376
	IEEE Code of Ethics .....	376
	Ten Commandments of Computer Ethics .....	377
	Certification Bodies Ethics .....	378
	Cyber Security Expert Classification .....	378
	Cyber Security and the Law .....	379
	United States .....	379
	Canada .....	380
	United Kingdom .....	381
	France .....	381
	European Union .....	381
	Japan .....	381
	South Korea .....	382

Human Subjects Research.....	382
Institutional Review Board .....	383
Ethical Use of Data .....	384
Consent .....	385
Criminally Released Data .....	386
Individual Responsibility.....	387
Plagiarism.....	387
Authorship.....	388
Conclusion.....	389
Endnotes.....	389
<b>INDEX .....</b>	<b>393</b>



## A systematic methodology for improving cyber security research

*Research Methods for Cyber Security* teaches scientific methods for generating impactful knowledge, validating theories, and adding critical rigor to the cyber security field. This book shows how to develop a research plan, beginning by starting research with a question, then offers an introduction to the broad range of useful research methods for cyber security research: observational, mathematical, experimental, and applied. Each research method chapter finishes with recommended outlines and suggested templates for submission to peer reviewed venues. This book concludes with information on cross-cutting issues within cyber security research.

Cyber security research contends with numerous unique issues, such as an extremely fast environment evolution, adversarial behavior, and the merging of natural and social science phenomena. *Research Methods for Cyber Security* addresses these concerns and much more by teaching readers not only the process of science in the context of cyber security research, but providing assistance in execution of research as well.

### Key features

- Presents research methods from a cyber security science perspective
- Catalyzes the rigorous research necessary to propel the cyber security field forward
- Provides a guided method selection for the type of research being conducted, presented in the context of real-world usage

**Thomas W. Edgar**, Senior Cyber Security Scientist, Pacific Northwest National Laboratory

**David O. Manz**, Senior Cyber Security Scientist, Pacific Northwest National Laboratory

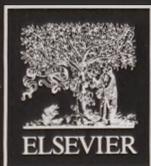
COMPUTER SECURITY

ISBN 978-0-12-805349-2



58995

9 780128 053492

**SYNGRESS**

elsevier.com/books-and-journals