

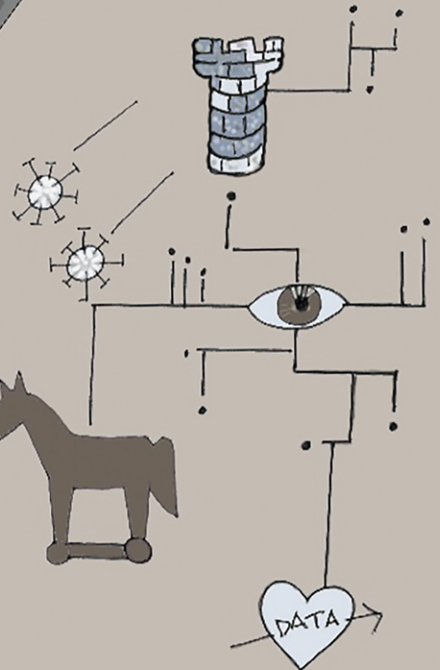


CYBERSECURITY MYTHS *and* MISCONCEPTIONS

Avoiding the Hazards and
Pitfalls that Derail Us



L33T



Illustrations by **Pattie Spafford**

Eugene H. Spafford
Leigh Metcalf
Josiah Dykstra



Foreword by **Vint Cerf**

“Many security leaders are traditionally in charge of correcting misconceptions just as much as they are in charge of building up solid security practices. We have plenty of resources on practices—but this book is the crucial guide to that essential myth busting.”

—Phil Venables
CISO, Google Cloud

“I’m writing this on my phone, over Wi-Fi, in an airplane on my way to Black Hat, one of the world’s largest security conferences. The fact that I’m able to do this at all shows how much we’ve really learned about cybersecurity over the decades. Now it’s all collected in one place for everyone to share. Thank the wise authors, and most importantly: GET OFF THEIR LAWN.”

—Wendy Nather
Head of Advisory CISOs, Cisco

“This book is astounding. A true tour de force—which I have never said about any other book. Inverting the viewpoint is a stroke of genius. This is going to be on my grabbable-at-any-time shelf. What I learned, recalled, and was refreshed on with technically astute agnosticism cannot be measured; just appreciated as a profound historical compilation of security practice and theory. Bravo!”

—Winn Schwartau
Founder and Chief Visionary Officer, The Security Awareness Company

“I am happy to endorse the central idea of this book—that cybersecurity is rife with myths that are themselves part of the problem. The brain wants to understand, the world grows ever more complicated, and the sum of the two is myth-making. As the authors say, even if some understanding is true at some time, with enough change what was true becomes a myth soon enough. As such, an acquired immunity to myths is a valuable skill for the cybersecurity practitioner if no other. The paramount goal of all security engineering is No Silent Failure, but myths perpetuate if not create silent failure. Why? Because a state of security is the absence of unmitigable surprise and you cannot mitigate what you don’t know is going on. Myths blind us to reality. Ignorance of them is not bliss. This book is a vaccine.”

—Dan Geer
CISO, In-Q-Tel

“This is a fun read for all levels. I like their rapid fire delivery and the general light they cast on so many diverse myths. This book will change the cybersecurity industry for the better.”

—Michael Sikorski
Author of *Practical Malware Analysis* & CTO, Unit 42 at Palo Alto Networks

Cybersecurity Myths and Misconceptions: Avoiding the Hazards and Pitfalls that Derail Us

Table of Contents

Cover

Half Title

Title Page

Copyright Page

Contents at a Glance

Table of Contents

Foreword

Introduction

Acknowledgments

About the Authors

Part I: General Issues

Chapter 1: What Is Cybersecurity?

Everyone Knows What Cybersecurity Means

We Can Measure How Secure Our Systems Are

Trust and Risk

Threats

Security Policy

And So...

The Primary Goal of Cybersecurity Is Security

Cybersecurity Is About Obvious Risks

Sharing More Cyber Threat Intel Will Make Things Better

Table of Contents

What Matters to You Matters to Everyone Else
Product X Will Make You Secure
Macs Are Safer Than PCs, Linux Is Safer Than Windows
Open Source Software Is More Secure Than Closed Source Software
Technology X Will Make You Secure
Process X Will Make You Secure
Færie Dust Can Make Old Ideas Magically Revolutionary
Passwords Should Be Changed Often
Believe and Fear Every Hacking Demo You See
Cyber Offense Is Easier Than Defense
Operational Technology (OT) Is Not Vulnerable
Breaking Systems Is the Best Way to Establish Yourself
Because You Can, You Should
Better Security Means Worse Privacy
Further Reading

Chapter 2: What Is the Internet?

Everyone Knows What the Internet Means
An IP Address Identifies a Unique Machine
The Internet Is Managed and Controlled by a Central Body
The Internet Is Largely Static
Your Network Is Static
 You Know Your Crown Jewels and Where They Are
Email Is Private
Cryptocurrency Is Untraceable
Everything Can Be Fixed with Blockchain
The Internet Is Like an Iceberg
 The Dark Web Is Only for Criminal Activity
 Activity on the Dark Web Is Untraceable
A VPN Makes You Anonymous
A Firewall Is Enough

Table of Contents

Further Reading

Part II: Human Issues

Chapter 3: Faulty Assumptions and Magical Thinking

Humans Will Behave Rationally, So Blame the User!

We Know Everything We Need to Know About Cybersecurity Problems

Compliance Equals (Complete) Security

Authentication Provides Confidentiality

I Can Never Be Secure, So Why Bother?

I Am Too Small/Insignificant to Be a Target

Everybody Is Out to Get Me

I Engage Only with Trusted Websites, So My Data Is Safe from a Breach

Security by Obscurity Is Reasonably Secure

The Illusions of Visibility and Control

Five 9s Is the Key to Cybersecurity

Everybody Has Top-of-the-Line Technology

We Can Predict Future Threats

Security People Control Security Outcomes

All Bad Outcomes Are the Result of a Bad Decision

More Security Is Always Better

Best Practices Are Always Best

Because It Is Online It Must Be True/Correct

Further Reading

Chapter 4: Fallacies and Misunderstandings

The False Cause Fallacy: Correlation Is Causation

Absence of Evidence Is Evidence of Absence

The Straw Hacker Fallacy

Ad Hominem Fallacy

Hasty Generalization Fallacy

Regression Fallacy

Table of Contents

Base Rate Fallacy

Gamblers Fallacy

Fallacies of Anomalies

Ignorance of Black Swans

Conjunction and Disjunction Fallacies

Valence Effect

Endowment Effect

Sunk Cost Fallacy

Bonus Fallacies

- External Appeals

- Questionable Evidence

- The Loaded Question

- False Choices

- Tu Quoque

- Overloading the Question

Further Reading

Chapter 5: Cognitive Biases

Action Bias

Omission Bias

Survivorship Bias

Confirmation Bias

Choice Affirmation Bias

Hindsight Bias

Availability Bias

Social Proof

Overconfidence Bias

Zero Risk Bias

Frequency Bias

Bonus Biases

- Outcome Bias

Table of Contents

Discounting Bias
Locality Bias
Denomination Bias
Denial or Ostrich Bias
Aura or Halo Bias
One Upmanship
Anchoring Bias
Priming
Knowledge Bias
Status Quo Bias
Ism Biases
Self-Serving Bias

Further Reading

Chapter 6: Perverse Incentives and the Cobra Effect

The Goal of a Security Vendor Is to Keep You Secure
Your Cybersecurity Decisions Affect Only You
Bug Bounties Eliminate Bugs from the Offensive Market
Cyber Insurance Causes People to Take Less Risk
Fines and Penalties Cause People to Take Less Risk
Attacking Back Would Help Stop Cyber Crime
Innovation Increases Security and Privacy Incidents
Further Reading

Chapter 7: Problems and Solutions

Failure Is Not an Option in Cybersecurity
Every Problem Has a Solution
We Can Solve All Our Problems with Big Data
There Is One, and Only One, Correct Solution
Everyone Should Solve a Given Cybersecurity Problem in the Same Way
Anecdotes Are Good Leads for Cybersecurity Solutions
Detecting More Bad Stuff Means the New Thing Is an Improvement
Every Security Process Should Be Automated

Table of Contents

Professional Certifications Are Useless

To Work in Cybersecurity Does (Not) Require a College Degree in Computing

Cybersecurity Certifications Are (Not) Valuable

There Is a Shortage of Cybersecurity Talent

There Is a Disconnect Between Study and Practice

Further Reading

Part III: Contextual Issues

Chapter 8: Pitfalls of Analogies and Abstractions

Cybersecurity Is Like the Physical World

Cybersecurity Is Like Defending a Castle

Digital Theft Is Like Physical Theft

Users Are the Weakest Link

Cybersecurity Is Like Medicine and Biology

Cybersecurity Is Like Fighting a War

Cyber Pearl Harbor

Cyber Weapons

Cyber Terrorism

Cybersecurity Law Is Analogous to Physical-World Law

Tips for Analogies and Abstractions

Further Reading

Chapter 9: Legal Issues

Cybersecurity Law Is Analogous to Physical-World Law

Your Laws Do Not Apply to Me Where I Am

That Violates My First Amendment Rights!

Ignorance of the Law

Jurisdictional Differences

Legal Code Supersedes Computer Code

Laws Can Simply Be Converted to Computer Code

Legislators/Regulators/Courts Know Enough About Technology to Regulate It

Laws and Courts Unduly Constrain Developers

Law Enforcement Will Never Respond to Cyber Crimes

Table of Contents

You Can Always Hide Information by Suing
Suing to Suppress a Breach Is a Good Idea
Terms and Conditions Are Meaningless
The Law Is on My Side, So I Do Not Need to Worry
Further Reading

Chapter 10: Tool Myths and Misconceptions

The More Tools, The Better
 Every New Threat Needs a New Tool
Default Configurations Are Always Secure
A Tool Can Stop All Bad Things
Intent Can Be Determined from Tools
Security Tools Are Inherently Secure and Trustworthy
Nothing Found Means All Is Well
 Nothing Found by the Scanners Means We Are Secure
 No Alarms Means We Are Secure
 No Vulnerability Reports Means No Vulnerabilities
Further Reading

Chapter 11: Vulnerabilities

We Know Everything There Is to Know About Vulnerabilities
Vulnerabilities Are Sparse
Attackers Are Getting More Proficient
Zero-Day Vulnerabilities Are Most Important
 Zero-Days Are the Scariest
 Zero-Days Mean Persistence
All Attacks Hinge on a Vulnerability
Exploits and Proofs of Concept Are Bad
Vulnerabilities Happen Only in Complex Code
First Movers Should Sacrifice Security
Patches Are Always Perfect and Available
Defenses Might Become Security Vulnerabilities with Time

Table of Contents

All Vulnerabilities Can Be Fixed

Scoring Vulnerabilities Is Easy and Well Understood

Because You Can, You Should Vulnerabilities Edition

Vulnerability Names Reflect Their Importance

Further Reading

Chapter 12: Malware

Using a Sandbox Will Tell Me Everything I Need to Know

Reverse Engineering Will Tell Me Everything I Need to Know

Malware and Geography Are/Are Not Related

I Can Always Determine Who Made the Malware and Attacked Me

Malware Is Always a Complex Program That Is Difficult to Understand

Free Malware Protection Is Good Enough

Only Shady Websites Will Infect Me

Because You Can, You Should Malware Edition

Ransomware Is an Entirely New Kind of Malware

Signed Software Is Always Trustworthy

Malware Names Reflect Their Importance

Further Reading

Chapter 13: Digital Forensics and Incident Response

Movies and Television Reflect the Reality of Cyber

Incidents Are Discovered as Soon as They Occur

Incidents Are Discrete and Independent

Every Incident Is the Same Severity

Standard Incident Response Techniques Can Deal with Ransomware

Incident Responders Can Flip a Few Switches and Magically Everything Is
Fixed

Attacks Are Always Attributable

Attribution Is Essential

Most Attacks/Exfiltration of Data Originate from Outside the Organization

The Trojan Horse Defense Is Dead

Table of Contents

Endpoint Data Is Sufficient for Incident Detection
Recovering from an Event Is a Simple and Linear Process
Further Reading

Part IV: Data Issues

Chapter 14: Lies, Damn Lies, and Statistics

Luck Prevents Cyber Attacks
The Numbers Speak for Themselves
Probability Is Certainty
Statistics Are Laws
 We Need Context
 Forecasting an Inference with Statistics
 Correlation Implies Causation
 Errors in Classification Are Insignificant
Data Is Not Important to Statistics
Artificial Intelligence and Machine Learning Can Solve All Cybersecurity Problems
Further Reading

Chapter 15: Illustrations, Visualizations, and Delusions

Visualizations and Dashboards Are Inherently and Universally Helpful
Cybersecurity Data Is Easy to Visualize
 Visualizing Internet Geolocation Is Useful
 Visualizing IPs and Ports Is Clear and Understandable
Further Reading

Chapter 16: Finding Hope

Creating a Less Myth-Prone World
The Critical Value of Documentation
Meta-Myths and Recommendations
 Meta-Myths
 Meta Recommendations
Avoiding Other and Future Traps
Parting Thoughts

Table of Contents

Appendix: Short Background Explanations

Acronyms

Index