



The Language of Cybersecurity

Compiled and edited by
Maria Antonieta Flores

Foreword by Malcolm Harkins

XML
PRESS
xmlpress.net



**The Content
Wrangler**
Content Strategy Series

The Language of **Cybersecurity**

Compiled and Edited by
Maria Antonieta Flores



The Language of Cybersecurity

Copyright © 2018 The Content Wrangler, Inc.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means without the prior written permission of the copyright holder, except for the inclusion of brief quotations in a review.

Credits

Series Producer:	Scott Abel
Copy Editor:	Trey DeGrassi
Series Cover Designer:	Marc Posch
Publishing Advisor:	Don Day
Publisher:	Richard Hamilton

Disclaimer

The information in this book is provided on an “as is” basis, without warranty. While every effort has been taken by the authors and XML Press in the preparation of this book, the authors and XML Press shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained herein.

This book contains links to third-party websites that are not under the control of the authors or XML Press. The authors and XML Press are not responsible for the content of any linked site. Inclusion of a link in this book does not imply that the authors or XML Press endorse or accept any responsibility for the content of that third-party site.

Trademarks

XML Press and the XML Press logo are trademarks of XML Press.

All terms mentioned in this book that are known to be trademarks or service marks have been capitalized as appropriate. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

XML Press
Laguna Hills, California
<http://xmlpress.net>

First Edition

ISBN: 978-1-937434-62-5 (print)

ISBN: 978-1-937434-63-2 (ebook)

This book is dedicated to my daughter Shalewa and grandson Akinsheye who make the world more beautiful through their art and to my fellow systems engineers and technical communicators who through their art make it easier for technical and not-so-technical people to understand each other.

Table of Contents

Foreword	5
Preface	7
Acknowledgments	9
Vulnerabilities	11
1. Social Engineering	14
2. Security Fatigue	16
3. Shadow Security	18
4. Data Leak	20
5. Insider Threat	22
6. Zero-day Vulnerability	24
7. Dark Web	26
Exploits	29
8. Phishing	32
9. Ransomware	34
10. Botnet	36
11. Advanced Persistent Threat	38
12. Buffer Overflow Attack	40
Defenses	43
13. Authentication	46
14. Endpoint Security	48
15. Multi-factor Authentication	50
16. Identity Management	52
17. Physical Access Control	54
18. Biometrics	56
19. Security Awareness	58
20. Situational Awareness	60
21. Behavioral Monitoring	62
22. Non-repudiation	64
23. Privilege	66
24. Firewall	68
25. Encryption	70
26. Sandboxing	72
27. Hardening	74
Planning, Management, and Controls	77
28. Governance, Risk Management, Compliance (GRC)	80
29. Application Risk Governance	82
30. Vulnerability Assessment	84
31. Business Impact Assessment (BIA)	86
32. Business Continuity Plan	88
33. Incident Response Plan	90
34. CISO	92

35. Risk Register	94
36. Kill Chain	96
37. Metrics	98
38. Audit	100
39. Threat Modeling	102
40. Static Application Security Testing	104
41. Penetration Testing	106
Compliance	109
42. Confidentiality	112
43. Integrity	114
44. Availability	116
45. Separation of Duties	118
46. Policy	120
47. Standards	122
48. Regulation	124
49. Privacy	126
50. Controls	128
51. Payment Card Industry Data Security Standard (PCI DSS)	130
52. General Data Protection Regulation (GDPR)	132
Glossary of Security Terms	135
Additional Contributors	149
References	155
Contributor Index	177
Subject Index	179

Language is a form of a
threads the needle betw
terms. This book is u

Biblioteka Główna
Akademii Sztuki Wojennej

26675/III (CB)



03-026675-000-0

The Language Cybersecurity

Compiled and edited by
Maria Antonieta Flores

The Language of Cybersecurity defines 52 terms that business professionals should know about cybersecurity, even professionals who are not specialists. Anyone who uses any kind of computing device needs to understand the importance of cybersecurity, and every business professional also needs to be able to speak intelligently with cybersecurity professionals.

The Language of Cybersecurity introduces the world of cybersecurity through the terminology that defines the field. Each of the 52 main terms contains a definition, a statement of why the term is important, and an essay that explains why a business professional should know about the term. Each term is authored by an expert practitioner.

The Language of Cybersecurity looks at vulnerabilities, exploits, defenses, planning, and compliance. In addition, there is a glossary that defines more than 80 additional terms. For those who want to dig deeper, there are more than 150 references for further exploration.

Expertly compiled and edited by Tonie Flores, this book is a useful reference for cybersecurity experts, managers, students, and anyone who uses a computer, tablet, smart phone, or other computing device

The Content Wrangler Content Strategy Book Series from XML Press provides content professionals with a road map for success. Each volume provides practical advice, best practices, and lessons learned from the most knowledgeable experts in the world



The Content Wrangler
Content Strategy Series

ISBN 978-1-937434-62-5

XML PRESS
xmlpress.net

9 781937 434625



Maria Antonieta Flores

Tonie Flores has guided systems and business professionals through the complexities of selecting and implementing leading-edge information processing solutions.

Her work as a systems engineer, instructor, change management specialist, and technical writer has helped information technology users from the shop floor and back office through the C-suite in Asia, Latin America, and the United States.