



COMPUTER SECURITY HANDBOOK

Fifth Edition

SEYMOUR BOSWORTH, MS CDP
M. E. KABAY, PhD, CISSP-ISSMP
ERIC WHYNE

ISBN13: 978-0-471-71652-5

Paper, Cons. Rel. Date: January 26, 2009

Price: ~~\$210.00~~ \$189.00

Order now and
get a 10% discount using
promo # 2-4182

Computer Security Handbook, Fifth Edition provides comprehensive coverage of the broad scope of issues relating to computer security in a well-organized, easy-to-follow format. Each chapter is written by one or more outstanding security experts. By following the practices and procedures described in this Handbook, professionals can minimize the possibilities of losses over their organization's computer system that can arise due to computer hacking and fraud, human error, or natural disasters. Practitioners and managers will find a wealth of accessible, thorough analysis and recommendations that they can apply right away to their organizations. Educators will find the two volumes an excellent basis for undergraduate and graduate courses in

information assurance and in management of information assurance.

SEYMOUR BOSWORTH, MS CDP, is president of S. Bosworth & Associates, Plainview, New York, a management consulting firm active in computing applications for banking, commerce, and industry. Since 1972 Bosworth has been a contributing editor to all five editions of the *Computer Security Handbook*, and he has written many articles and lectured extensively about computer security and other technical and managerial subjects. He has been responsible for design and manufacture, system analysis, programming, and operations of both digital and analog computers.

M. E. KABAY, PhD, CISSP-ISSMP, is Associate Professor of Computer Information Systems at Norwich University, where he is also director of the graduate program in Information Assurance. During his career, he has worked as an operating systems internals and database performance specialist for Hewlett-Packard, an operations manager at a large service bureau, and a consultant in operations, performance, and security.

ERIC WHYNE is a Captain in the United States Marine Corps. He joined the Marine Corps in the Signals Intelligence field and received two meritorious promotions before being selected for an officer candidate program and finally commissioning into the communications occupational specialty. Eric holds a BS in Computer Science from Norwich University as well as minor degrees in Mathematics, Information Assurance, and Engineering. He has presented about communications security and other technology topics at many forums, and worked as a researcher for the National Center for Counter-Terrorism and Cyber Crime Research.

To order online: www.wiley.com

or Call: 1-800-225-5945

 **WILEY**
Now you know.
wiley.com

TABLE OF CONTENTS

Part I. Foundations Of Computer Security

- Chapter 1. Brief History and Mission of Information System Security (Seymour Bosworth and Robert V. Jacobson)
- Chapter 2. History of Computer Crime (M. E. Kabay)
- Chapter 3. Toward a New Framework for Information Security (Donn B. Parker, CISSP)
- Chapter 4. Hardware Elements of Security (Sy Bosworth and Stephen Cobb)
- Chapter 5. Data Communications and Information Security (Raymond Panko)
- Chapter 6. Network Topologies, Protocols, and Design (Gary C. Kessler and N. Todd Pritsky)
- Chapter 7. Encryption (Stephen Cobb and Corinne Lefrançois)
- Chapter 8. Using a Common Language for Computer Security Incident Information (John D. Howard)
- Chapter 9. Mathematical Models of Computer Security (Matt Bishop)
- Chapter 10. Understanding Studies and Surveys of Computer Crime (M. E. Kabay)
- Chapter 11. Fundamentals of Intellectual Property Law (William A. Zucker and Scott J. Nathan)

Part II. Threats And Vulnerabilities

- Chapter 12. The Psychology of Computer Criminals (Q. Campbell and David M. Kennedy)
- Chapter 13. The Dangerous Information Technology Insider: Psychological Characteristics and Career Patterns (Jerrold M. Post, M.D.)
- Chapter 14. Information Warfare (Seymour Bosworth)
- Chapter 15. Penetrating Computer Systems and Networks (Chey Cobb, Stephen Cobb, and M. E. Kabay)
- Chapter 16. Malicious Code (Robert Guess and Eric Salveggio)
- Chapter 17. Mobile Code (Robert Gezelter)
- Chapter 18. Denial-of-Service Attacks (Gary C. Kessler and Diane E. Levine)
- Chapter 19. Social Engineering and Low-Tech Attacks (Karthik Raman, Susan Baumes, Kevin Beets and Carl Ness)
- Chapter 20. Spam, Phishing, and Trojans: Attacks Meant To Fool (Stephen Cobb)
- Chapter 21. Web-Based Vulnerabilities (Anup K. Ghosh, Kurt Baumgarten, Jennifer Hadley, and Steven Lovaas)
- Chapter 22. Physical Threats to the Information Infrastructure (Franklin Platt)

Part III. Prevention: Technical Defenses

- Chapter 23. Protecting the Information Infrastructure (Franklin Platt)
- Chapter 24. Operating System Security (William Stallings)
- Chapter 25. Local Area Networks (Gary C. Kessler and N. Todd Pritsky)
- Chapter 26. Gateway Security Devices (David Brussin and Justin Opatrny)

- Chapter 27. Intrusion Detection and Intrusion Prevention Devices (Rebecca Gurley Bace)
- Chapter 28. Identification and Authentication (Ravi Sandhu, Jennifer Hadley, Steven Lovaas, and Nicholas Takacs)
- Chapter 29. Biometric Authentication (David R. Lease, Robert Guess, Steven Lovaas, and Eric Salveggio)
- Chapter 30. E-Commerce and Web Server Safeguards (Robert Gezelter)
- Chapter 31. Web Monitoring and Content Filtering (Steven Lovaas)
- Chapter 32. Virtual Private Networks and Secure Remote Access (Justin Opatrny)
- Chapter 33. 802.11 Wireless LAN Security (Gary L. Tagg)
- Chapter 34. Securing VOIP (Christopher Dantos and John Mason)
- Chapter 35. Securing P2P, IM, SMS, and Collaboration Tools (Carl Ness)
- Chapter 36. Securing Stored Data (David J. Johnson, Nicholas Takacs, and Jennifer Hadley)
- Chapter 37. PKI and Certificate Authorities (Santosh Chokhani, A. Padgett Peterson, and Steven Lovaas)
- Chapter 38. Writing Secure Code (Lester E. Nichols, M. E. Kabay, and Timothy Braithwaite)
- Chapter 39. Software Development and Quality Assurance (John Mason, Jennifer Hadley, and Diane E. Levine)
- Chapter 40. Managing Software Patches and Vulnerabilities (Peter Mell and Karen Kent)
- Chapter 41. Antivirus Technology (Chey Cobb and Allysa Myers)
- Chapter 42. Protecting Digital Rights: Technical Approaches (Robert Guess, Jennifer Hadley, Steven Lovaas, and Diane E. Levine)

Part IV. Prevention: Human Factors

- Chapter 43. Ethical Decision Making and High Technology (James Landon Linderman)
- Chapter 44. Security Policy Guidelines (M. E. Kabay and Bridgitt Robertson)
- Chapter 45. Employment Practices and Policies (M. E. Kabay and Bridgitt Robertson)
- Chapter 46. Vulnerability Assessment (Rebecca Gurley Bace)
- Chapter 47. Operations Security and Production Controls (M. E. Kabay, Don Holden, and Myles Walsh)
- Chapter 48. E-Mail and Internet Use Policies (M. E. Kabay and Nicholas Takacs)
- Chapter 49. Implementing a Security Awareness Program (K Rudolph)
- Chapter 50. Using Social Psychology to Implement Security Policies (M. E. Kabay, Bridgitt Robertson, Mani Akella, and D. T. Lang)
- Chapter 51. Security Standards for Products (Paul Brusil and Noel Zakin)

Part V. Detecting Security Breaches

- Chapter 52. Application Controls (Myles Walsh)
- Chapter 53. Monitoring and Control Systems (Caleb S. Coggins and Diane E. Levine)

- Chapter 54. Security Audits, Standards and Inspections (Donald Glass, Chris Davis, John Mason, Richard O. Moore, David Gursky, James Thomas, Wendy Carr, and Diane Levine)
- Chapter 55. Cyber Investigation (Peter Stephenson)

Part VI. Response & Remediation

- Chapter 56. Computer Security Incident Response Teams (Michael Miora, M. E. Kabay, and Bernie Cowens)
- Chapter 57. Data Backups and Archives (M. E. Kabay and Don Holden)
- Chapter 58. Business Continuity Planning (Michael Miora)
- Chapter 59. Disaster Recovery (Michael Miora)
- Chapter 60. Insurance Relief (Robert A. Parisi, Jr., Chaim Haas, and Nancy Callahan)
- Chapter 61. Working with Law Enforcement (David A. Land)

Part VII. Management's Role In Security

- Chapter 62. Risk Assessment and Risk Management (Robert V. Jacobson)
- Chapter 63. Management Responsibilities and Liabilities (Carl Hallberg, M. E. Kabay, Bridgitt Robertson, and Arthur E. Hutt)
- Chapter 64. U.S. Legal and Regulatory Security Issues (Timothy Virtue)
- Chapter 65. The Role of the CISO (Karen F. Worstell)
- Chapter 66. Developing Security Policies (M. E. Kabay and Sean Kelley)
- Chapter 67. Developing Classification Policies for Data (Karthik Raman and Kevin Beets)
- Chapter 68. Outsourcing and Security (Kip Boyle, Michael Buglewicz, and Steven Lovaas)

Part VIII. Public Policy And Other Considerations

- Chapter 69. Privacy in Cyberspace: U.S. and European Perspectives (Marc Rotenberg)
- Chapter 70. Anonymity and Identity in Cyberspace (M. E. Kabay, Eric Salveggio and Robert Guess)
- Chapter 71. Medical Records Protection (Paul J. Brusil)
- Chapter 72. Legal and Policy Issues of Censorship and Content Filtering (Lee Tien, Seth Finkelstein, and Steven Lovaas)
- Chapter 73. Expert Witnesses and the Daubert Challenge (Chey Cobb)
- Chapter 74. Professional Certification and Training in Information Assurance (Christopher Christian, M. E. Kabay, Kevin Henry, and Sondra Schneider)
75. Undergraduate and Graduate Education in Information Assurance (Vic Maconachy, John Orlando, and Seymour Bosworth)
76. European Graduate Work in Information Assurance and the Bologna Declaration (Urs E. Gattiker)
77. The Failure of Information Assurance (Peter G. Neumann)