



The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk

By N.K. McCarthy, Matthew Todd, Jeff Klaben

[Download now](#)

[Read Online](#) 

The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk By N.K. McCarthy, Matthew Todd, Jeff Klaben

Uncertainty and risk, meet planning and action.

Reinforce your organization's security posture using the expert information contained in this tactical guide. *The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk* shows you how to build and manage successful response plans for the cyber incidents that have become inevitable for organizations of any size. Find out why these plans work. Learn the step-by-step process for developing and managing plans built to address the wide range of issues organizations face in times of crisis.

- Contains the essentials for developing both data breach and malware outbreak response plans—and best practices for maintaining those plans
- Features ready-to-implement CIRPs—derived from living incident response plans that have survived the rigors of repeated execution and numerous audits
- Clearly explains how to minimize the risk of post-event litigation, brand impact, fines and penalties—and how to protect shareholder value
- Supports corporate compliance with industry standards and requirements, including PCI, HIPAA, SOX, and CA SB-24

 [Download The Computer Incident Response Planning Handbook: ...pdf](#)

 [Read Online The Computer Incident Response Planning Handbook ...pdf](#)

The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk

By N.K. McCarthy, Matthew Todd, Jeff Klaben

The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk By N.K. McCarthy, Matthew Todd, Jeff Klaben

Uncertainty and risk, meet planning and action.

Reinforce your organization's security posture using the expert information contained in this tactical guide. *The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk* shows you how to build and manage successful response plans for the cyber incidents that have become inevitable for organizations of any size. Find out why these plans work. Learn the step-by-step process for developing and managing plans built to address the wide range of issues organizations face in times of crisis.

- Contains the essentials for developing both data breach and malware outbreak response plans—and best practices for maintaining those plans
- Features ready-to-implement CIRPs—derived from living incident response plans that have survived the rigors of repeated execution and numerous audits
- Clearly explains how to minimize the risk of post-event litigation, brand impact, fines and penalties—and how to protect shareholder value
- Supports corporate compliance with industry standards and requirements, including PCI, HIPAA, SOX, and CA SB-24

The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk By N.K. McCarthy, Matthew Todd, Jeff Klaben **Bibliography**

- Sales Rank: #471855 in eBooks
- Published on: 2012-08-07
- Released on: 2012-08-07
- Format: Kindle eBook



[Download The Computer Incident Response Planning Handbook: ...pdf](#)



[Read Online The Computer Incident Response Planning Handbook ...pdf](#)

Download and Read Free Online The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk By N.K. McCarthy, Matthew Todd, Jeff Klaben

Editorial Review

About the Author

N.K. McCarthy previously managed the Information Security Operations / Threat & Vulnerability Management for a Fortune 50 Corporation for several years. His international staff performed round-the-clock security event monitoring and response. His responsibilities included: security patch remediation, vulnerability scans, and remediation, penetration testing, system configuration monitoring and remediation, maintaining the various Computer Incident Response Plans (CIRP), and an active threat portfolio for key business functions, users, application platforms and persistent vulnerabilities.

With a career in over 20 plus years in IT, Mr. McCarthy has held a wide range of roles within IT including systems programming, IT consultant, technical management, and IT sales. He recently retired after 30 plus years as a Marine Corps reservist obtaining the rank of Lieutenant Colonel. His last reserve assignment of five years was with the U.S. Cyber Command. After 9/11, Lt. Col. McCarthy was mobilized and spent almost four years on active duty as an Information Warfare Officer working at the U.S. Strategic Command, the Pentagon, and the National Security Agency (NSA). Mr. McCarthy also has 17 years of experience as a volunteer reserve police officer. In this capacity he was able to attend U.S. DOJ (Law Enforcement Only) training in computer forensics and advanced Internet investigations. He was also certified by FEMA for its Incident Command System (ICS) and the National Incident Management System (NIMS). Mr. McCarthy is currently on the Board of Directors of the San Francisco Bay Area and Silicon Valley chapter of the FBI's Infragard program.

Mr. McCarthy has a B.S. degree in Computer Science, an M.B.A. and a CISSP. He is also the CEO of an SDVOB S-corporation with established and developing business in California and Nevada.

Dr. Matthew Todd is the Chief Security Officer and Vice President of Risk and Technical Operations for Financial Engines (NASDAQ: FNGN), a financial advisor with more than \$47 billion in assets under management. At Financial Engines, he is responsible for security, privacy, business continuity, audit, and risk management for the firm.

In addition to his work at Financial Engines, Dr. Todd is the president of the San Francisco Bay Area InfraGard chapter, representing more than 1000 volunteer InfraGard members. He has been a local mentor for the SANS Institute, is a CISM and CIPP, and holds the GSEC certification. He has more than 20 years of experience in the technology space and has been actively involved in information security for the last 15 years. He obtained his Ph.D. from Northwestern University and was a fellow of both the National Science Foundation (U.S.) and the Danish National Science Foundation.

Jeff Klaben is an Adjunct Professor with Santa Clara University's College of Engineering, where he currently teaches Information Assurance and Computer Forensics. He is also a principal with Neohapsis, helping Fortune 500 organizations and leading security technology providers overcome global challenges in technology risk management, competitive strategy, product engineering, compliance, and trusted collaboration to achieve break-through innovation. Previously, Jeff served as Group Director of Technology Risk Management at SanDisk, Chief Information Security Officer for Life Technologies, Engineering Group Director with Cadence Design Systems, and Senior Manager of Enterprise Architecture, IT Security, and Compliance at Applied Materials. He also led product management, professional services delivery, and start-up incubation at Accenture.

Jeff is a frequent speaker at industry conferences, and for the past decade, has served on the board of directors of the San Francisco Bay Area InfraGard, a 501(c)(3) nonprofit and public/private partnership dedicated to information sharing for critical infrastructure protection. He assisted the White House as town hall moderator for the rollout of the National Strategy to Secure Cyberspace and was recognized by the U.S. Department of Justice with awards for Dedicated Service and Exceptional Service in the Public Interest. He also received the Belotti Award for Outstanding Business Policy in High Technology Firms from Santa Clara University's Leavey School of Business. Jeff earned an M.B.A. from Santa Clara University, a B.S. in Information Systems from Wright State University, and the credentials of Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and Certified Information Systems Auditor (CISA).

Users Review

From reader reviews:

Harry Nelson:

Are you kind of busy person, only have 10 or perhaps 15 minute in your moment to upgrading your mind skill or thinking skill possibly analytical thinking? Then you are experiencing problem with the book as compared to can satisfy your short time to read it because this time you only find guide that need more time to be study. The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk can be your answer because it can be read by anyone who have those short free time problems.

Lonnie Hammer:

Don't be worry in case you are afraid that this book can filled the space in your house, you will get it in e-book approach, more simple and reachable. This kind of The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk can give you a lot of pals because by you investigating this one book you have matter that they don't and make you more like an interesting person. This kind of book can be one of a step for you to get success. This guide offer you information that probably your friend doesn't recognize, by knowing more than different make you to be great men and women. So , why hesitate? We need to have The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk.

James Chavez:

As we know that book is important thing to add our information for everything. By a publication we can know everything we wish. A book is a range of written, printed, illustrated or perhaps blank sheet. Every year had been exactly added. This reserve The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk was filled regarding science. Spend your spare time to add your knowledge about your technology competence. Some people has distinct feel when they reading the book. If you know how big advantage of a book, you can really feel enjoy to read a guide. In the modern era like at this point, many ways to get book you wanted.

Joseph Bateman:

That e-book can make you to feel relax. This particular book The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk was multi-colored and of course has pictures on there. As we know that book The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk has many kinds or type. Start from kids until youngsters. For example Naruto or Investigator Conan you can read and believe you are the character on there. Therefore , not at all of book tend to be make you bored, any it can make you feel happy, fun and loosen up. Try to choose the best book in your case and try to like reading which.

**Download and Read Online The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk By N.K. McCarthy, Matthew Todd, Jeff Klaben
#XJI1DVUT83E**

Read The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk By N.K. McCarthy, Matthew Todd, Jeff Klaben for online ebook

The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk By N.K. McCarthy, Matthew Todd, Jeff Klaben Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk By N.K. McCarthy, Matthew Todd, Jeff Klaben books to read online.

Online The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk By N.K. McCarthy, Matthew Todd, Jeff Klaben ebook PDF download

The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk By N.K. McCarthy, Matthew Todd, Jeff Klaben Doc

The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk By N.K. McCarthy, Matthew Todd, Jeff Klaben MobiPocket

The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk By N.K. McCarthy, Matthew Todd, Jeff Klaben EPub