



# The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk (Networking & Comm - OMG)

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 (Networking & Comm - OMG)** 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 (Networking & Comm - OMG)**

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

**The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk (Networking & Comm - OMG)** 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 (Networking & Comm - OMG)** By N.K. McCarthy, Matthew Todd, Jeff Klaben **Bibliography**

- Sales Rank: #680995 in Books
- Brand: Brand: McGraw-Hill Osborne Media
- Published on: 2012-08-07
- Released on: 2012-07-17
- Original language: English
- Number of items: 1
- Dimensions: 9.10" h x .50" w x 7.40" l, .90 pounds
- Binding: Paperback
- 240 pages

 [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 (Networking & Comm - OMG) 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:**

#### **Jeffrey Smith:**

As people who live in the actual modest era should be up-date about what going on or details even knowledge to make these people keep up with the era and that is always change and progress. Some of you maybe will update themselves by reading books. It is a good choice to suit your needs but the problems coming to a person is you don't know which you should start with. This The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk (Networking & Comm - OMG) is our recommendation to help you keep up with the world. Why, because this book serves what you want and wish in this era.

#### **John Lopez:**

The experience that you get from The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk (Networking & Comm - OMG) is a more deep you rooting the information that hide inside words the more you get interested in reading it. It doesn't mean that this book is hard to know but The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk (Networking & Comm - OMG) giving you thrill feeling of reading. The author conveys their point in certain way that can be understood through anyone who read the item because the author of this e-book is well-known enough. This book also makes your own personal vocabulary increase well. So it is easy to understand then can go with you, both in printed or e-book style are available. We propose you for having this specific The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk (Networking & Comm - OMG) instantly.

#### **Patrick Duenas:**

Reading a book to get new life style in this season; every people loves to go through a book. When you examine a book you can get a wide range of benefit. When you read books, you can improve your knowledge, since book has a lot of information onto it. The information that you will get depend on what sorts of book that you have read. If you need to get information about your analysis, you can read education books, but if you want to entertain yourself you can read a fiction books, these us novel, comics, and soon. The The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at

Risk (Networking & Comm - OMG) provide you with a new experience in looking at a book.

**Edward Doucet:**

This The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk (Networking & Comm - OMG) is new way for you who has curiosity to look for some information since it relief your hunger of information. Getting deeper you on it getting knowledge more you know or you who still having bit of digest in reading this The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk (Networking & Comm - OMG) can be the light food for you personally because the information inside this particular book is easy to get by simply anyone. These books build itself in the form that is reachable by anyone, yep I mean in the e-book application form. People who think that in guide form make them feel drowsy even dizzy this reserve is the answer. So there is no in reading a book especially this one. You can find actually looking for. It should be here for anyone. So , don't miss that! Just read this e-book style for your better life as well as knowledge.

**Download and Read Online The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk (Networking & Comm - OMG) By N.K. McCarthy, Matthew Todd, Jeff Klaben #SX62R4AUMBW**

## **Read The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk (Networking & Comm - OMG) By N.K. McCarthy, Matthew Todd, Jeff Klaben for online ebook**

The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk (Networking & Comm - OMG) 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 (Networking & Comm - OMG) 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 (Networking & Comm - OMG) By N.K. McCarthy, Matthew Todd, Jeff Klaben ebook PDF download**

**The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk (Networking & Comm - OMG) By N.K. McCarthy, Matthew Todd, Jeff Klaben Doc**

**The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk (Networking & Comm - OMG) By N.K. McCarthy, Matthew Todd, Jeff Klaben Mobipocket**

**The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk (Networking & Comm - OMG) By N.K. McCarthy, Matthew Todd, Jeff Klaben EPub**

**SX62R4AUMBW: The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk (Networking & Comm - OMG) By N.K. McCarthy, Matthew Todd, Jeff Klaben**