



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](#)

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:

Alex Jose:

Do you certainly one of people who can't read pleasurable if the sentence chained inside straightway, hold on guys this particular aren't like that. This The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk book is readable through you who hate the straight word style. You will find the data here are arrange for enjoyable examining experience without leaving possibly decrease the knowledge that want to give to you. The writer associated with The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk content conveys prospect easily to understand by a lot of people. The printed and e-book are not different in the written content but it just different by means of it. So , do you still thinking The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk is not loveable to be your top list reading book?

Michael Rahn:

Information is provisions for anyone to get better life, information currently can get by anyone at everywhere. The information can be a know-how or any news even a concern. What people must be consider any time those information which is inside former life are challenging be find than now's taking seriously which one is suitable to believe or which one often the resource are convinced. If you have the unstable resource then you understand it as your main information it will have huge disadvantage for you. All of those possibilities will not happen within you if you take The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk as your daily resource information.

Jodi Dunn:

Playing with family inside a park, coming to see the coastal world or hanging out with buddies is thing that usually you could have done when you have spare time, after that why you don't try matter that really opposite from that. A single activity that make you not experience tired but still relaxing, trilling like on roller coaster you already been ride on and with addition details. Even you love The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk, you can enjoy both. It is great combination right, you still would like to miss it? What kind of hangout type is it? Oh can occur its mind hangout people. What? Still don't buy it, oh come on its named reading friends.

Gary Collis:

This The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk is great reserve for you because the content which is full of information for you who also always deal with world and also have to make decision every minute. That book reveal it info accurately using great manage word or we can say no rambling sentences inside. So if you are read the idea hurriedly you can have whole information in it. Doesn't mean it only gives you straight forward sentences but tricky core information with lovely delivering sentences. Having The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk in your hand like keeping the world in your arm, details in it is not ridiculous one particular. We can say that no reserve that offer you world with ten or fifteen small right but this guide already do that. So , this is good reading book. Hello Mr. and Mrs. active do you still doubt that?

**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
#T9ZQ3PRAVHW**

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