

## The Computer Incident Response Planning Handbook Executable Plans For Protecting Information At Risk

This comprehensive book instructs IT managers to adhere to federally mandated compliance requirements. FISMA Compliance Handbook Second Edition explains what the requirements are for FISMA compliance and why FISMA compliance is mandated by federal law. The evolution of Certification and Accreditation is discussed. This book walks the reader through the entire FISMA compliance process and includes guidance on how to manage a FISMA compliance project from start to finish. The book has chapters for all FISMA compliance deliverables and includes information on how to conduct a FISMA compliant security assessment. Various topics discussed in this book include the NIST Risk Management Framework, how to characterize the sensitivity level of your system, contingency plan, system security plan development, security awareness training, privacy impact assessments, security assessments and more. Readers will learn how to obtain an Authority to Operate for an information system and what actions to take in regards to vulnerabilities and audit findings. FISMA Compliance Handbook Second Edition, also includes all-new coverage of federal cloud computing compliance from author Laura Taylor, the federal government's technical lead for FedRAMP, the government program used to assess and authorize cloud products and services. Includes new information on cloud computing compliance from Laura Taylor, the federal government's technical lead for FedRAMP Includes coverage for both corporate and government IT managers Learn how to prepare for, perform, and document FISMA compliance projects This book is used by various colleges and universities in information security and MBA curriculums

Something's happening to Superman, Batman and Wonder Woman. First, a shared dream of a trapped alien consciousness ... and then all hell breaks loose as giant robots and then the mighty Konvikt attack! But why are Morgana Le Fay, Despero and the mysterious Enigma taking an interest in the three heroes?

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 Conferences Proceedings of 20th European Conference on Cyber Warfare and Security

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

## Download Ebook The Computer Incident Response Planning Handbook Executable Plans For Protecting Information At Risk

### Professional

"This Working Paper and its technical annexes identify and discuss four key pillars that are necessary to foster a secure electronic environment and the safety and soundness of financial systems worldwide. Hence, it is intended for those formulating policies in the area of electronic security and those working with financial services providers (such as executives and management). The detailed annexes of this monograph are relevant for chief information and security officers and others who are responsible for securing network systems." --Résumé de l'éditeur.

Considered the gold-standard reference on information security, the Information Security Management Handbook provides an authoritative compilation of the fundamental knowledge, skills, techniques, and tools required of today's IT security professional. Now in its sixth edition, this 3200 page, 4 volume stand-alone reference is organized under the CISSP Common Body of Knowledge domains and has been updated yearly. Each annual update, the latest is Volume 6, reflects the changes to the CBK in response to new laws and evolving technology.

You will be breached—the only question is whether you'll be ready A cyber breach could cost your organization millions of dollars—in 2019, the average cost of a cyber breach for companies was \$3.9M, a figure that is increasing 20-30% annually. But effective planning can lessen the impact and duration of an inevitable cyberattack. *Cyber Breach Response That Actually Works* provides a business-focused methodology that will allow you to address the aftermath of a cyber breach and reduce its impact to your enterprise. This book goes beyond step-by-step instructions for technical staff, focusing on big-picture planning and strategy that makes the most business impact. Inside, you'll learn what drives cyber incident response and how to build effective incident response capabilities. Expert author Andrew Gorecki delivers a vendor-agnostic approach based on his experience with Fortune 500 organizations. Understand the evolving threat landscape and learn how to address tactical and strategic challenges to build a comprehensive and cohesive cyber breach response program Discover how incident response fits within your overall information security program, including a look at risk management Build a capable incident response team and create an actionable incident response plan to prepare for cyberattacks and minimize their impact to your organization Effectively investigate small and large-scale incidents and recover faster by leveraging proven industry practices Navigate legal issues impacting incident response, including laws and regulations, criminal cases and civil litigation, and types of evidence and their admissibility in court In addition to its valuable breadth of discussion on incident response from a business strategy perspective, *Cyber Breach Response That Actually Works* offers information on key technology considerations to aid you in building an effective capability and accelerating investigations to ensure your organization can continue business operations during significant cyber events.

Based on proven, rock-solid computer incident response plans The Computer Incident Response Planning Handbook is derived from real-world incident response plans that work and have survived audits and repeated execution during data breaches and due diligence. The book provides an overview of attack and breach types, strategies for assessing an organization, types of plans, and case examples. Tips for keeping data contained, reputations defended, and recognizing and handling the magnitude of any given threat are included. The Computer Incident Response Planning Handbook Contains ready-to-implement incident response plans with guidelines for ongoing due diligence, all based on actual, working, and tested CIRPs Prepares you to immediately build a CIRP for any organization, and keep that plan maintained Explains all the essentials involved in developing both data breach and malware outbreak CIRPs derived from tested incident response plans

## Download Ebook The Computer Incident Response Planning Handbook Executable Plans For Protecting Information At Risk

that have survived the rigors of repeated execution 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 like PCI, HIPAA, SOX, CA SB-1386 All plans derived from the book are technology-agnostic Provides supplementary reading to professionals studying for the CERT Certified Computer Security Incident Handler exam or the SANS/GIAC Certified Incident Handler exam (GCIH) In-depth coverage: The Latest Cyber Attacks and How They Are Business Killers; The Nebulous Standard of Cyber Due Diligence & The New Era of Information Risk; Introduction to Planning & Crisis; A Plan is Preparation Manifested; Getting More Out of Your Plans; Developing a Data Breach CIRP – Incident Preparation, Plan Execution, and Post-incident Planning; Developing a Malware Outbreak CIRP – Incident Preparation, Plan Execution, and Post-incident Planning; References

Learn how to identify vulnerabilities within computer networks and implement countermeasures that mitigate risks and damage with Whitman/Mattord's PRINCIPLES OF INCIDENT RESPONSE & DISASTER RECOVERY, 3rd Edition. This edition offers the knowledge you need to help organizations prepare for and avert system interruptions and natural disasters. Comprehensive coverage addresses information security and IT in contingency planning today. Updated content focuses on incident response and disaster recovery. You examine the complexities of organizational readiness from an IT and business perspective with emphasis on management practices and policy requirements. You review industry's best practices for minimizing downtime in emergencies and curbing losses during and after system service interruptions. This edition includes the latest NIST knowledge, expanded coverage of security information and event management (SIEM) and unified threat management, and more explanation of cloud-based systems and Web-accessible tools to prepare you for success. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version. The Effective Incident Response Team is the first complete guide to forming and managing a Computer Incident Response Team (CIRT). In this book, system and network administrators and managers will find comprehensive information on establishing a CIRT's focus and scope, complete with organizational and workflow strategies for maximizing available technical resources. The text is also a resource for working teams, and has many examples of day-to-day team operations, communications, forms, and legal references.

"The purpose of this publication is to assist Member States in developing comprehensive contingency plans for computer security incidents with the potential to impact nuclear security and/or nuclear safety. It provides an outline and recommendations for establishing a computer security incident response capability as part of a computer security programme, and considers the roles and responsibilities of the system owner, operator, competent authority, and national technical authority in responding to a computer security incident with possible nuclear security repercussions."--Publisher's description.

Powerful Earthquake Triggers Tsunami in Pacific. Hurricane Isaac Makes Landfall in the Gulf Coast. Wildfires Burn Hundreds of Houses and Businesses in Colorado. Tornado Touches Down in Missouri. These headlines not only have caught the attention of people around the world, they have had a significant effect on IT professionals as well. The new 2nd Edition of Business Continuity and Disaster Recovery for IT Professionals gives you the most up-to-date planning and risk management techniques for business continuity and disaster recovery (BCDR). With distributed networks, increasing demands for confidentiality, integrity and availability of data, and the widespread risks to the security of personal, confidential and sensitive data, no organization can afford to ignore the need for disaster planning. Author Susan Snedaker shares her expertise with you, including the most current options for disaster recovery and communication, BCDR for mobile devices, and the latest infrastructure considerations including cloud, virtualization, clustering, and more. Snedaker also provides you with new case studies in

## Download Ebook The Computer Incident Response Planning Handbook Executable Plans For Protecting Information At Risk

several business areas, along with a review of high availability and information security in healthcare IT. Don't be caught off guard—Business Continuity and Disaster Recovery for IT Professionals, 2nd Edition, is required reading for anyone in the IT field charged with keeping information secure and systems up and running. Complete coverage of the 3 categories of disaster: natural hazards, human-caused hazards, and accidental / technical hazards Extensive disaster planning and readiness checklists for IT infrastructure, enterprise applications, servers and desktops Clear guidance on developing alternate work and computing sites and emergency facilities Actionable advice on emergency readiness and response Up-to-date information on the legal implications of data loss following a security breach or disaster

Fourth Edition (Traditional Chinese Translation) Sheds New Light on Open Source Intelligence Collection and Analysis. Author Michael Bazzell has been well known and respected in government circles for his ability to locate personal information about any target through Open Source Intelligence (OSINT). In this book, he shares his methods in great detail. Each step of his process is explained throughout sixteen chapters of specialized websites, application programming interfaces, and software solutions. Based on his live and online video training at IntelTechniques.com, over 250 resources are identified with narrative tutorials and screen captures. This book will serve as a reference guide for anyone that is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials as they go. The search techniques offered will inspire analysts to "think outside the box" when scouring the internet for personal information. Much of the content of this book has never been discussed in any publication. Always thinking like a hacker, the author has identified new ways to use various technologies for an unintended purpose. This book will improve anyone's online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network Content Cell Phone Owner Information Twitter GPS & Account Data Hidden Photo GPS & Metadata Deleted Websites & Posts Website Owner Information Alias Social Network Profiles Additional User Accounts Sensitive Documents & Photos Live Streaming Social Content IP Addresses of Users Newspaper Archives & Scans Social Content by Location Private Email Addresses Hidden Personal Videos Duplicate Copies of Photos Personal Radio Communications Compromised Email Information Wireless Routers by Location Hidden Mapping Applications Complete Facebook Data Free Investigative Software Alternative Search Engines Mobile App Network Data Unlisted Addresses Unlisted Phone Numbers Useful Browser Extensions Public Government Records Document Metadata Rental Vehicle Contracts Online Criminal Activity

Guidance Software's EnCase product is the premier computer forensics tool on the market, used in law enforcement labs for digital evidence collection; in commercial settings for incident response and information assurance; and by the FBI and Department of Defense to detect domestic and international threats This guide prepares readers for both the CBT and practical phases of the exam that validates mastery of EnCase Written by two law enforcement professionals who are computer forensics specialists and EnCase trainers Includes the EnCase Legal Journal, essential for forensics investigators who need to be sure they are operating within the law and able to give expert testimony The CD includes tools to help readers prepare for Phase II of the certification, which requires candidates to examine computer evidence, as well as a searchable PDF of the text

This book shows what IT in organizations need to accomplish to implement The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets and The National Strategy to Secure Cyberspace which were developed by the Department of Homeland Security after the terrorist attacks of September 2001. The September 11, 2001, attacks illustrated the immense vulnerability to terrorist threats. Since then there have been considerable efforts to develop plans and methods to protect critical

## Download Ebook The Computer Incident Response Planning Handbook Executable Plans For Protecting Information At Risk

infrastructures and key assets. The government at all levels, private sector organizations, as well as concerned citizens have begun to establish partnerships and to develop action plans. But there are many questions yet to be answered about what organizations should actually do to protect their assets and their people while participating in national efforts to improve security. This book provides practical steps that IT managers in all organizations and sectors can take to move security from the planning process into practice. \*A one-minute manager approach to issues provides background and explanations in all areas \*Step-by-step instructions on how to accomplish objectives guide readers through processes \*Easy to implement advice allows readers to take quick action

An incident management and response guide for IT or security professionals wanting to establish or improve their incident response and overall security capabilities. Included are templates for response tools, policies, and plans. This look into how to plan, prepare, and respond also includes links to valuable resources needed for planning, training, and overall management of a Computer Security Incident Response Team.

ROADMAP TO INFORMATION SECURITY: FOR IT AND INFOSEC MANAGERS provides a solid overview of information security and its relationship to the information needs of an organization. Content is tailored to the unique needs of information systems professionals who find themselves brought in to the intricacies of information security responsibilities. The book is written for a wide variety of audiences looking to step up to emerging security challenges, ranging from students to experienced professionals. This book is designed to guide the information technology manager in dealing with the challenges associated with the security aspects of their role, providing concise guidance on assessing and improving an organization's security. The content helps IT managers to handle an assignment to an information security role in ways that conform to expectations and requirements, while supporting the goals of the manager in building and maintaining a solid information security program. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Cyber forensic knowledge requirements have expanded and evolved just as fast as the nature of digital information has—requiring cyber forensics professionals to understand far more than just hard drive intrusion analysis. The Certified Cyber Forensics Professional (CCFP<sup>SM</sup>) designation ensures that certification holders possess the necessary breadth, depth of knowledge, and analytical skills needed to address modern cyber forensics challenges. Official (ISC)<sup>2</sup><sup>®</sup> Guide to the CCFP<sup>®</sup> CBK<sup>®</sup> supplies an authoritative review of the key concepts and requirements of the Certified Cyber Forensics Professional (CCFP<sup>®</sup>) Common Body of Knowledge (CBK<sup>®</sup>). Encompassing all of the knowledge elements needed to demonstrate competency in cyber forensics, it covers the six domains: Legal and Ethical Principles, Investigations, Forensic Science, Digital Forensics, Application Forensics, and Hybrid and Emerging Technologies. Compiled by leading digital forensics experts from around the world, the book provides the practical understanding in forensics techniques and procedures, standards of practice, and legal and ethical principles required to ensure accurate, complete, and reliable digital evidence that is admissible in a court of law. This official guide supplies a global perspective of key topics within the cyber forensics field, including chain of custody, evidence analysis, network forensics, and

## Download Ebook The Computer Incident Response Planning Handbook Executable Plans For Protecting Information At Risk

cloud forensics. It also explains how to apply forensics techniques to other information security disciplines, such as e-discovery, malware analysis, or incident response. Utilize this book as your fundamental study tool for achieving the CCFP certification the first time around. Beyond that, it will serve as a reliable resource for cyber forensics knowledge throughout your career.

Here's easy-to-understand book that introduces you to fundamental network security concepts, principles, and terms, while providing you with practical techniques that you can apply on the job. It helps you identify the best type of intrusion detection system for your environment, develop organizational guidelines for passwords, set general computer security policies, and perform a security review and risk assessment .

The business to business trade publication for information and physical Security professionals.

Create, maintain, and manage a continual cybersecurity incident response program using the practical steps presented in this book. Don't allow your cybersecurity incident responses (IR) to fall short of the mark due to lack of planning, preparation, leadership, and management support. Surviving an incident, or a breach, requires the best response possible. This book provides practical guidance for the containment, eradication, and recovery from cybersecurity events and incidents. The book takes the approach that incident response should be a continual program. Leaders must understand the organizational environment, the strengths and weaknesses of the program and team, and how to strategically respond. Successful behaviors and actions required for each phase of incident response are explored in the book. Straight from NIST 800-61, these actions include: Planning and practicing Detection Containment Eradication Post-incident actions What You'll Learn Know the sub-categories of the NIST Cybersecurity Framework Understand the components of incident response Go beyond the incident response plan Turn the plan into a program that needs vision, leadership, and culture to make it successful Be effective in your role on the incident response team Who This Book Is For Cybersecurity leaders, executives, consultants, and entry-level professionals responsible for executing the incident response plan when something goes wrong

Computer Incident Response and Forensics Team Management provides security professionals with a complete handbook of computer incident response from the perspective of forensics team management. This unique approach teaches readers the concepts and principles they need to conduct a successful incident response investigation, ensuring that proven policies and procedures are established and followed by all team members. Leighton R. Johnson III describes the processes within an incident response event and shows the crucial importance of skillful forensics team management, including when and where the transition to forensics investigation should occur during an incident response event. The book also provides discussions of key incident response components. Provides readers with a complete handbook on computer incident response from the perspective of forensics team management Identify the key steps to completing a successful computer incident response investigation Defines the qualities necessary to become a successful forensics investigation team member, as well as the interpersonal relationship skills necessary for successful incident response and forensics investigation teams

The need for information security management has never been greater. With constantly changing technology, external intrusions, and internal thefts of data, information security officers face threats at every turn. The Information Security Management Handbook on CD-ROM, 2006 Edition is now available. Containing the complete contents of the Information Security Management Handbook, this is a resource that is portable, linked and searchable by keyword. In addition to an electronic version of the most comprehensive resource for information security management, this CD-ROM contains an extra volume's worth of information that is not found anywhere else, including chapters from other

## Download Ebook The Computer Incident Response Planning Handbook Executable Plans For Protecting Information At Risk

security and networking books that have never appeared in the print editions. Exportable text and hard copies are available at the click of a mouse. The Handbook's numerous authors present the ten domains of the Information Security Common Body of Knowledge (CBK) ®. The CD-ROM serves as an everyday reference for information security practitioners and an important tool for any one preparing for the Certified Information System Security Professional (CISSP) ® examination. New content to this Edition: Sensitive/Critical Data Access Controls Role-Based Access Control Smartcards A Guide to Evaluating Tokens Identity Management-Benefits and Challenges An Examination of Firewall Architectures The Five "W's" and Designing a Secure Identity Based Self-Defending Network Maintaining Network Security-Availability via Intelligent Agents PBX Firewalls: Closing the Back Door Voice over WLAN Spam Wars: How to Deal with Junk E-Mail Auditing the Telephony System: Defenses against Communications Security Breaches and Toll Fraud The "Controls" Matrix Information Security Governance Any good attacker will tell you that expensive security monitoring and prevention tools aren't enough to keep you secure. This practical book demonstrates a data-centric approach to distilling complex security monitoring, incident response, and threat analysis ideas into their most basic elements. You'll learn how to develop your own threat intelligence and incident detection strategy, rather than depend on security tools alone. Written by members of Cisco's Computer Security Incident Response Team, this book shows IT and information security professionals how to create an InfoSec playbook by developing strategy, technique, and architecture. Learn incident response fundamentals—and the importance of getting back to basics Understand threats you face and what you should be protecting Collect, mine, organize, and analyze as many relevant data sources as possible Build your own playbook of repeatable methods for security monitoring and response Learn how to put your plan into action and keep it running smoothly Select the right monitoring and detection tools for your environment Develop queries to help you sort through data and create valuable reports Know what actions to take during the incident response phase

Discover the latest trends, developments and technology in information security today with Whitman/Mattord's market-leading PRINCIPLES OF INFORMATION SECURITY, 7th Edition. Designed specifically to meet the needs of those studying information systems, this edition's balanced focus addresses all aspects of information security, rather than simply offering a technical control perspective. This overview explores important terms and examines what is needed to manage an effective information security program. A new module details incident response and detection strategies. In addition, current, relevant updates highlight the latest practices in security operations as well as legislative issues, information management toolsets and digital forensics. Coverage of the most recent policies and guidelines that correspond to federal and international standards further prepare you for success both in information systems and as a business decision-maker. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

A practical guide to deploying digital forensic techniques in response to cyber security incidents About This Book Learn incident response fundamentals and create an effective incident response framework Master forensics investigation utilizing digital investigative techniques Contains real-life scenarios that effectively use threat intelligence and modeling techniques Who This Book Is For This book is targeted at Information Security professionals, forensics practitioners, and students with knowledge and experience in the use of software applications and basic command-line experience. It will also help professionals who are new to the incident response/digital forensics role within their organization. What You Will Learn Create and deploy incident response capabilities within your organization Build a solid foundation for acquiring and handling suitable evidence for later analysis Analyze collected evidence and determine the root cause of a security incident

## Download Ebook The Computer Incident Response Planning Handbook Executable Plans For Protecting Information At Risk

Learn to integrate digital forensic techniques and procedures into the overall incident response process Integrate threat intelligence in digital evidence analysis Prepare written documentation for use internally or with external parties such as regulators or law enforcement agencies In Detail Digital Forensics and Incident Response will guide you through the entire spectrum of tasks associated with incident response, starting with preparatory activities associated with creating an incident response plan and creating a digital forensics capability within your own organization. You will then begin a detailed examination of digital forensic techniques including acquiring evidence, examining volatile memory, hard drive assessment, and network-based evidence. You will also explore the role that threat intelligence plays in the incident response process. Finally, a detailed section on preparing reports will help you prepare a written report for use either internally or in a courtroom. By the end of the book, you will have mastered forensic techniques and incident response and you will have a solid foundation on which to increase your ability to investigate such incidents in your organization. Style and approach The book covers practical scenarios and examples in an enterprise setting to give you an understanding of how digital forensics integrates with the overall response to cyber security incidents. You will also learn the proper use of tools and techniques to investigate common cyber security incidents such as malware infestation, memory analysis, disk analysis, and network analysis.

Written from the perspective of prevention, Disaster & Recovery Planning: A Guide for Facility Managers focuses on identifying the issues that create hazards, and defines the strategies that all companies can use to address disaster response and recovery. Although written for facility managers, this book also targets other professionals that are responsible for designing, installing, and maintaining programs and systems within an organization. These include safety compliance officers, risk managers, consultants, engineers, maintenance executives and human resources managers. This volume can also guide top management in heightening awareness to issues of prevention, and it can assist them in meeting their responsibilities for ensuring the safety of their employees, tenant/occupants, or companies.

Learn how to build a Security Incident Response team with guidance from a leading SIRT from Cisco Gain insight into the best practices of one of the foremost incident response teams Master your plan for building a SIRT (Security Incidence Response Team) with detailed guidelines and expert advice for incident handling and response Review legal issues from a variety of national perspectives, and consider practical aspects of coordination with other organizations Network Security Incident Response provides practical guidelines for building an SIRT team as well offering advice on responding to actual incidents. For many companies, incident response is new territory. Some companies do not have an incidence response team at all. Some would like to have one but need guidance to start and others would like to improve existing practices. Today, there are only a handful of organizations that do have mature and experienced teams. For that reason this book is structured to provide help in both creating and running an effective Security Incident Response Team. Organizations who are evaluating whether to invest in a SIRT or who are just getting started building one will find the information in this book to be invaluable in helping them understand the nature of the threats, justifying resources, and building effective IR (Incidence Response) teams. Established IR teams will also benefit from the best practices highlighted in building IR teams as well as information on the current state of incident response handling, incident coordination, and legal issues. Written by a leading SIRT (Security Incident Response Team) from Cisco, the expertise and guidance provided in this book will serve as the blueprint for successful incidence response planning for most any organization.

Readers discover a managerially-focused overview of information security with a thorough treatment of how to most effectively administer it with MANAGEMENT OF INFORMATION SECURITY, 5E. Information throughout helps readers become information security management practitioners able to secure systems and networks in a world where continuously emerging threats, ever-present attacks, and the success of

## Download Ebook The Computer Incident Response Planning Handbook Executable Plans For Protecting Information At Risk

criminals illustrate the weaknesses in current information technologies. Current and future professional managers complete this book with the exceptional blend of skills and experiences to develop and manage the more secure computing environments that today's organizations need. This edition offers a tightened focus on key executive and managerial aspects of information security while still emphasizing the important foundational material to reinforce key concepts. Updated content reflects the most recent developments in the field, including NIST, ISO, and security governance. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

This is a print on demand edition of a hard to find publication. This guide provides instructions, recommendations, and considerations for federal information system contingency planning. Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods. This guide addresses specific contingency planning recommendations for three platform types and provides strategies and techniques common to all systems: Client/server systems; Telecomm. systems; and Mainframe systems. Charts and tables.

The definitive guide to incident response--updated for the first time in a decade! Thoroughly revised to cover the latest and most effective tools and techniques, Incident Response & Computer Forensics, Third Edition arms you with the information you need to get your organization out of trouble when data breaches occur. This practical resource covers the entire lifecycle of incident response, including preparation, data collection, data analysis, and remediation. Real-world case studies reveal the methods behind--and remediation strategies for--today's most insidious attacks. Architect an infrastructure that allows for methodical investigation and remediation Develop leads, identify indicators of compromise, and determine incident scope Collect and preserve live data Perform forensic duplication Analyze data from networks, enterprise services, and applications Investigate Windows and Mac OS X systems Perform malware triage Write detailed incident response reports Create and implement comprehensive remediation plans

[Copyright: 0ec926cee01a40f0893132bbf62015c7](#)