The Chief Information Security Officers Toolkit Security Program Metrics

The Chief Information Security Officer's Toolkit
IT Security Governance Guidebook with Security Program Metrics on CD-ROM
The Metrics Manifesto
The Chief Information Security Officer
Information Security Management Metrics
Measuring and Communicating Security's Value
Measures and Metrics in Corporate Security
The CISO Evolution
Security Metrics Management
Security Metrics Management
The Chief Security Officer’s Handbook
PRAGMATIC Security Metrics
FISMA and the Risk Management Framework
Security Metrics, A Beginner's Guide
Computer Security Handbook, Set
Information Security Risk Assessment Toolkit
IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data
Security Awareness For Dummies
Advances in Human Factors in Cybersecurity
The Security Culture Playbook
Information Security Management Metrics
The CSO Guide
Building a Security Measures and Metrics Program
Nominations of Erroll G. Southers and Daniel I. Gordon
Cybersecurity Operations and Fusion Centers
Financial Cybersecurity Risk Management
Complete Guide to Security and Privacy Metrics
Information security Department of Homeland Security needs to fully implement its security program : report to the Ranking Minority Member, Committee on Homeland Security and Governmental Affairs, U.S. Senate.

Core Software Security

Energy and Water Development Appropriations for 2012: Dept. of Energy FY 2012 justifications

The Chief Information Security Officers Toolkit Security Program Metrics pdf
The Chief Information Security Officers Toolkit Security Program Metrics pdf download
The Chief Information Security Officers Toolkit Security Program Metrics pdf free
The Chief Information Security Officers Toolkit Security Program Metrics References
The Chief Information Security Officers Toolkit Security Program Metrics Descriptions
The Chief Information Security Officers Toolkit Security Program Metrics Books
What is the The Chief Information Security Officers Toolkit Security Program Metrics?
What is a The Chief Information Security Officers Toolkit Security Program Metrics?
What are The Chief Information Security Officers Toolkit Security Program Metrics?
What is The Chief Information Security Officers Toolkit Security Program Metrics?

2022-01-26 Matthew K. Sharp Learn to effectively deliver business aligned cybersecurity outcomes In The CISO Evolution: Business Knowledge for Cybersecurity Executives, information security experts Matthew K. Sharp and Kyriakos “Rock” Lambros deliver an insightful and practical resource to help cybersecurity professionals develop the skills they need to effectively communicate with senior management and boards. They assert business aligned cybersecurity is crucial and demonstrate how business acumen is being put into action to deliver meaningful business outcomes. The authors use illustrative stories to show professionals how to establish an executive presence and avoid the most common pitfalls experienced by technology experts when speaking and presenting to executives. The book will show you how to: Inspire trust in senior business leaders by properly aligning and setting expectations around risk appetite and capital allocation Properly characterize the indispensable role of cybersecurity in your company’s overall strategic plan Acquire the necessary funding and resources for your company’s cybersecurity program and avoid the stress and anxiety that comes with underfunding Perfect for security and risk professionals, IT auditors, and risk managers looking for effective strategies to communicate cybersecurity concepts and ideas to business professionals without a background in technology. The CISO Evolution is also a must-read resource for business executives, managers, and leaders hoping to improve the quality of dialogue with their cybersecurity leaders.

2011 United States. Congress. Senate. Committee on Homeland Security and Governmental Affairs

2023-10-19 Kevin Lynn McLaughlin Cybersecurity Operations and Fusion Centers: A Comprehensive Guide to SOC and TIC Strategy by Dr. Kevin Lynn McLaughlin is a must-have resource for anyone involved in the establishment and operation of a Cybersecurity Operations and Fusion Center (SOFC). Think of a combination cybersecurity SOC and cybersecurity Threat Intelligence Center (TIC). In this book, Dr. McLaughlin, who is a well-respected cybersecurity expert, provides a comprehensive guide to the critical importance of having an SOFC and the various options available to organizations to either build one from scratch or purchase a ready-made solution. The author takes the reader through the crucial steps of designing an SOFC model, offering expert advice on selecting the right partner, allocating resources, and building a strong and effective team. The book also provides an in-depth exploration of the design and implementation of the SOFC infrastructure and toolset, including the use of virtual tools, the physical security of the SOFC, and the impact of COVID-19 on remote workforce operations. A bit of gamification is described in the book as a way to motivate and maintain teams of high-performing and well-trained cybersecurity professionals. The day-to-day operations of an SOFC are also thoroughly examined, including the monitoring and detection process, security operations (SecOps), and incident response and remediation. The book highlights the significance of effective reporting in driving improvements in an organization’s security posture. With its comprehensive analysis of all aspects of the SOFC, from team building to incident response, this book is an invaluable resource for anyone looking to establish and operate a successful SOFC. Whether you are a security analyst, senior analyst, or executive, this book will provide you with the necessary insights and strategies to ensure maximum performance and long-term success for your SOFC. By having this book as your guide, you can rest assured that you have the knowledge and skills necessary to protect an organization’s data, assets, and operations.

2012-12-31 Stephen D. Gantz FISMA and the Risk Management Framework: The New Practice of Federal Cyber Security deals with the Federal Information Security Management Act (FISMA), a law that provides the framework for securing information systems and managing risk associated with information resources in federal government agencies. Comprised of 17

chapters, the book explains the FISMA legislation and its provisions, strengths and limitations, as well as the expectations and obligations of federal agencies subject to FISMA. It also discusses the processes and activities necessary to implement effective information security management following the passage of FISMA, and it describes the National Institute of Standards and Technology's Risk Management Framework. The book looks at how information assurance, risk management, and information systems security is practiced in federal government agencies; the three primary documents that make up the security authorization package: system security plan, security assessment report, and plan of action and milestones; and federal information security-management requirements and initiatives not explicitly covered by FISMA. This book will be helpful to security officers, risk managers, system owners, IT managers, contractors, consultants, service providers, and others involved in securing, managing, or overseeing federal information systems, as well as the mission functions and business processes supported by those systems. Learn how to build a robust, near real-time risk management system and comply with FISMA Discover the changes to FISMA compliance and beyond Gain your systems the authorization they need

2022-05-03 Ira Winkler Make security a priority on your team Every organization needs a strong security program. One recent study estimated that a hacker attack occurs somewhere every 37 seconds. Since security programs are only as effective as a team’s willingness to follow their rules and protocols, it’s increasingly necessary to have not just a widely accessible gold standard of security, but also a practical plan for rolling it out and getting others on board with following it. Security Awareness For Dummies gives you the blueprint for implementing this sort of holistic and hyper-secure program in your organization. Written by one of the world’s most influential security professionals—and an Information Systems Security Association Hall of Famer—this pragmatic and easy-to-follow book provides a framework for creating new and highly effective awareness programs from scratch, as well as steps to take to improve on existing ones. It also covers how to measure and evaluate the success of your program and highlight its value to management. Customize and create your own program Make employees aware of the importance of security Develop metrics for success Follow industry-specific sample programs Cyberattacks aren’t going away anytime soon: get this smart, friendly guide on how to get a workgroup on board with their role in security and save your organization big money in the long run.

2018-06-23 Tareq Z. Ahram This book reports on the latest research and developments in the field of cybersecurity, particularly focusing on personal security and new methods for reducing human error and increasing cyber awareness, as well as innovative solutions for increasing the security of advanced Information Technology (IT) infrastructures. It covers a broad range of topics, including methods for human training; novel cyber-physical and process-control systems; social, economic, and behavioral aspects of cyberspace; issues concerning the cybersecurity index; security metrics for enterprises; and risk evaluation. Based on the AHFE 2018 International Conference on Human Factors in Cybersecurity, held on July 21–25, 2018, in Orlando, Florida, USA, the book not only presents innovative cybersecurity technologies, but also discusses emerging threats, current gaps in the available systems, and future challenges that can be successfully overcome with the help of human factors research.

2013-12-09 James Ransome "... an engaging book that will empower readers in both large and small software development and engineering organizations to build security into their products. ... Readers are armed with firm solutions for the fight against cyber threats." —Dr. Dena Haritos Tsamitis. Carnegie Mellon University "... a must read for security specialists, software developers and software engineers. ... should be part of every security professional’s library." —Dr. Larry Ponemon, Ponemon Institute "... the definitive how-to guide for software security professionals. Dr.

Ransome, Anmol Misra, and Brook Schoenfield deftly outline the procedures and policies needed to integrate real security into the software development process. ...A must-have for anyone on the front lines of the Cyber War ..." —Cedric Leighton, Colonel, USAF (Ret.), Cedric Leighton Associates "Dr. Ransome, Anmol Misra, and Brook Schoenfield give you a magic formula in this book - the methodology and process to build security into the entire software development life cycle so that the software is secured at the source! " —Eric S. Yuan, Zoom Video Communications There is much publicity regarding network security, but the real cyber Achilles' heel is insecure software. Millions of software vulnerabilities create a cyber house of cards, in which we conduct our digital lives. In response, security people build ever more elaborate cyber fortresses to protect this vulnerable software. Despite their efforts, cyber fortifications consistently fail to protect our digital treasures. Why? The security industry has failed to engage fully with the creative, innovative people who write software. Core Software Security expounds developer-centric software security, a holistic process to engage creativity for security. As long as software is developed by humans, it requires the human element to fix it. Developer-centric security is not only feasible but also cost effective and operationally relevant. The methodology builds security into software development, which lies at the heart of our cyber infrastructure. Whatever development method is employed, software must be secured at the source. Book Highlights: Supplies a practitioner's view of the SDL Considers Agile as a security enabler Covers the privacy elements in an SDL Outlines a holistic business-savvy SDL framework that includes people, process, and technology Highlights the key success factors, deliverables, and metrics for each phase of the SDL Examines cost efficiencies, optimized performance, and organizational structure of a developer-centric software security program and PSIRT Includes a chapter by noted security architect Brook Schoenfield who shares his insights and experiences in applying the book's SDL framework View the authors' website at http://www.androidinsecurity.com/

2009-03-30 W. Krag Brotby, CISM Spectacular security failures continue to dominate the headlines despite huge increases in security budgets and ever-more draconian regulations. The 20/20 hindsight of audits is no longer an effective solution to security weaknesses, and the necessity for real-time strategic metrics has never been more critical. Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement offers a radical new approach for developing and implementing security metrics essential for supporting business activities and managing information risk. This work provides anyone with security and risk management responsibilities insight into these critical security questions: How secure is my organization? How much security is enough? What are the most cost-effective security solutions? How secure is my organization? You can't manage what you can't measure This volume shows readers how to develop metrics that can be used across an organization to assure its information systems are functioning, secure, and supportive of the organization's business objectives. It provides a comprehensive overview of security metrics, discusses the current state of metrics in use today, and looks at promising new developments. Later chapters explore ways to develop effective strategic and management metrics for information security governance, risk management, program implementation and management, and incident management and response. The book ensures that every facet of security required by an organization is linked to business objectives, and provides metrics to measure it. Case studies effectively demonstrate specific ways that metrics can be implemented across an enterprise to maximize business benefit. With three decades of enterprise information security experience, author Krag Brotby presents a workable approach to developing and managing cost-effective enterprise information security.

2007-01-22 Debra S. Herrmann While it has become increasingly apparent that individuals and organizations need a security metrics program, it has been exceedingly difficult to

define exactly what that means in a given situation. There are hundreds of metrics to choose from and an organization’s mission, industry, and size will affect the nature and scope of the task as well as the metrics and combinations of metrics appropriate to accomplish it. Finding the correct formula for a specific scenario calls for a clear concise guide with which to navigate this sea of information. Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI defines more than 900 ready to use metrics that measure compliance, resiliency, and return on investment. The author explains what needs to be measured, why and how to measure it, and how to tie security and privacy metrics to business goals and objectives. The book addresses measuring compliance with current legislation, regulations, and standards in the US, EC, and Canada including Sarbanes-Oxley, HIPAA, and the Data Protection Act-UK. The metrics covered are scaled by information sensitivity, asset criticality, and risk, and aligned to correspond with different lateral and hierarchical functions within an organization. They are flexible in terms of measurement boundaries and can be implemented individually or in combination to assess a single security control, system, network, region, or the entire enterprise at any point in the security engineering lifecycle. The text includes numerous examples and sample reports to illustrate these concepts and stresses a complete assessment by evaluating the interaction and interdependence between physical, personnel, IT, and operational security controls. Bringing a wealth of complex information into comprehensible focus, this book is ideal for corporate officers, security managers, internal and independent auditors, and system developers and integrators.

2013-06 George Campbell Building a Security Measures and Metrics Program discusses the need for and benefits of a corporate security measures and metrics program. This 40-minute video presentation of narrated slides makes the case for a security metrics program: metrics provide invaluable insight on program effectiveness, the means to influence business strategy and policy, and the ability to demonstrate the value of security services to business leaders. Presenter George Campbell, former chief security officer at Fidelity and 45-year security industry veteran, uses his experience with performance-centered security to expertly guide the audience through the development and management of a security metrics program. This presentation is a valuable resource for business leaders and risk mitigation professionals who want to quantify the effectiveness of the security team and its services. Building a Security Measures and Metrics Program is a part of Elsevier's Security Executive Council Risk Management Portfolio, a collection of real world solutions and "how-to" guidelines that equip executives, practitioners, and educators with proven information for successful security and risk management programs. The 40-minute, PowerPoint presentation with audio narration format is excellent for group learning Provides a basic understanding of the importance of performance measurement and the major elements of a security metrics program Includes examples of graphs, tables, and charts that can be used to display metric data

2022-03-08 Perry Carpenter Mitigate human risk and bake security into your organization’s culture from top to bottom with insights from leading experts in security awareness, behavior, and culture. The topic of security culture is mysterious and confusing to most leaders. But it doesn’t have to be. In The Security Culture Playbook, Perry Carpenter and Kai Roer, two veteran cybersecurity strategists deliver experience-driven, actionable insights into how to transform your organization’s security culture and reduce human risk at every level. This book exposes the gaps between how organizations have traditionally approached human risk and it provides security and business executives with the necessary information and tools needed to understand, measure, and improve facets of security culture across the organization. The book offers: An expose of what security culture really is and how it can be measured A careful exploration of the 7 dimensions that comprise security culture Practical tools for managing your security

culture program, such as the Security Culture Framework and the Security Culture Maturity Model Insights into building support within the executive team and Board of Directors for your culture management program Also including several revealing interviews from security culture thought leaders in a variety of industries, The Security Culture Playbook is an essential resource for cybersecurity professionals, risk and compliance managers, executives, board members, and other business leaders seeking to proactively manage and reduce risk.

2014-04-02 George Campbell The revised second edition of Measures and Metrics in Corporate Security is an indispensable guide to creating and managing a security metrics program. Authored by George Campbell, emeritus faculty of the Security Executive Council and former chief security officer of Fidelity Investments, this book shows how to improve security's bottom line and add value to the business. It provides a variety of organizational measurements, concepts, metrics, indicators and other criteria that may be employed to structure measures and metrics program models appropriate to the reader's specific operations and corporate sensitivities. There are several hundred examples of security metrics included in Measures and Metrics in Corporate Security, which are organized into categories of security services to allow readers to customize metrics to meet their operational needs. Measures and Metrics in Corporate Security is a part of Elsevier's Security Executive Council Risk Management Portfolio, a collection of real world solutions and "how-to" guidelines that equip executives, practitioners, and educators with proven information for successful security and risk management programs. Describes the basic components of a metrics program, as well as the business context for metrics Provides guidelines to help security managers leverage the volumes of data their security operations already create Identifies the metrics security executives have found tend to best serve security's unique (and often misunderstood) missions Includes 375 real examples of security metrics across 13 categories

2009-03-30 CISM, W. Krag Brotby Spectacular security failures continue to dominate the headlines despite huge increases in security budgets and ever-more draconian regulations. The 20/20 hindsight of audits is no longer an effective solution to security weaknesses, and the necessity for real-time strategic metrics has never been more critical. Information Security Management Metr

2018-12-13 Paul Rohmeyer Understand critical cybersecurity and risk perspectives, insights, and tools for the leaders of complex financial systems and markets. This book offers guidance for decision makers and helps establish a framework for communication between cyber leaders and front-line professionals. Information is provided to help in the analysis of cyber challenges and choosing between risk treatment options. Financial cybersecurity is a complex, systemic risk challenge that includes technological and operational elements. The interconnectedness of financial systems and markets creates dynamic, high-risk environments where organizational security is greatly impacted by the level of security effectiveness of partners, counterparties, and other external organizations. The result is a high-risk environment with a growing need for cooperation between enterprises that are otherwise direct competitors. There is a new normal of continuous attack pressures that produce unprecedented enterprise threats that must be met with an array of countermeasures. Financial Cybersecurity Risk Management explores a range of cybersecurity topics impacting financial enterprises. This includes the threat and vulnerability landscape confronting the financial sector, risk assessment practices and methodologies, and cybersecurity data analytics. Governance perspectives, including executive and board considerations, are analyzed as are the appropriate control measures and executive risk reporting. What You'll Learn Analyze the threat and vulnerability landscape confronting the financial sector Implement effective technology risk assessment practices and methodologies Craft strategies to treat observed risks in financial systemsImprove the

effectiveness of enterprise cybersecurity capabilities Evaluate critical aspects of cybersecurity governance, including executive and board oversight Identify significant cybersecurity operational challenges Consider the impact of the cybersecurity mission across the enterpriseLeverage cybersecurity regulatory and industry standards to help manage financial services risksUse cybersecurity scenarios to measure systemic risks in financial systems environmentsApply key experiences from actual cybersecurity events to develop more robust cybersecurity architectures Who This Book Is For Decision makers, cyber leaders, and front-line professionals, including: chief risk officers, operational risk officers, chief information security officers, chief security officers, chief information officers, enterprise risk managers, cybersecurity operations directors, technology and cybersecurity risk analysts, cybersecurity architects and engineers, and compliance officers

2016-11-22 Scott Ellis This guide provides a complete road-map for building, maintaining, and augmenting an information security program based on IT security best practices and standards. It provides all of the basic information needed to perform as a high-functioning information security manager or CISO / CSO. It looks at the role of the CISO, and includes the following: The CISO Skillsets, Building a Security Program from Scratch, Security Organization Models, Communications and Executive Buy-in, and Executive Reporting. It introduces the 80/20 rule for CISO's. If you are responsible for running the information security program, this guide is for you. It talks about performing risk assessments (NIST, HIPAA, PCI DSS), developing a plan of action and tactical and strategic security plans. It talks about developing security policies and procedures. It introduces the concept of security prioritization, data classification, and data protection. The overall goal is to provide you with a template that illustrates everything needed to build, maintain, or augment a security program successfully.

2019-06-20 Michael Allen The Chief Security Officer’s Handbook: Leading Your Team into the Future offers practical advice on how to embrace the future, align with your organizations mission, and develop a program that meets the needs of the enterprise. The book discusses real-life examples of what to do to align with other critical departments, how to avoid spending time and resources on unnecessary and outdated methods, and tomorrow’s security program. Today’s security executives need to help their industry, their organization and the next generation of security leaders to pioneer, optimize and transform every aspect of our programs, technologies and methods. The book is ideal for current chief security officers, aspiring security executives, and those interested in better understanding the critical need to modernize corporate security. Offers suggestions on the do's and don’ts of professional development Provides tangible examples on how the CSO works collaboratively with internal peers Instructs CSO's on how to align with the business while remaining agile Illustrates the various paths to becoming a CSO Demonstrates ways to move your program into one that embraces enterprise security risk management, convergence and automation

2016-11-30 Gerald L. Kovacich Security Metrics Management, Measuring the Effectiveness and Efficiency of a Security Program, Second Edition details the application of quantitative, statistical, and/or mathematical analyses to measure security functional trends and workload, tracking what each function is doing in terms of level of effort (LOE), costs, and productivity. This fully updated guide is the go-to reference for managing an asset protection program and related security functions through the use of metrics. It supports the security professional’s position on budget matters, helping to justify the cost-effectiveness of security-related decisions to senior management and other key decision-makers. The book is designed to provide easy-to-follow guidance, allowing security professionals to confidently measure the costs of their assets protection program - their security program - as well as its successes and failures. It includes a discussion of how to use the metrics to brief

management, build budgets, and provide trend analyses to develop a more efficient and effective asset protection program. Examines the latest techniques in both generating and evaluating security metrics, with guidance for creating a new metrics program or improving an existing one Features an easy-to-read, comprehensive implementation plan for establishing an asset protection program Outlines detailed strategies for creating metrics that measure the effectiveness and efficiency of an asset protection program Offers increased emphasis through metrics to justify security professionals as integral assets to the corporation Provides a detailed example of a corporation briefing for security directors to provide to executive management

2006 Gerald L. Kovacich Provides guidance on measuring the costs, successes and failures of asset protection and security programs.

2011 Barry L. Kouns Discover the skills you need to be a successful CISO in todays changing world! The role of the Chief Information Security Officer has evolved enormously in recent years in response to security threats and a challenging business environment. Instead of being primarily a master technician, todays CISO has to be a trusted advisor to senior management. Read this pocket guide and Learn how the role of a CISO has changed. Todays CISO must be integrated into all aspects of the business and have a full understanding of its strategy and objectives. Understand the importance of a risk management methodology. A good risk management methodology must take into account the special information security needs of the company as well as legal and regulatory requirements. Learn how to establish a successful ISMS. The guide explains how to design and implement an ISMS that is appropriate for the organization. It

2010-08-22 Lance Hayden Implement an Effective Security Metrics Project or Program IT Security Metrics provides a comprehensive approach to measuring risks, threats, operational activities, and the effectiveness of data protection in your organization. The book explains how to choose and design effective measurement strategies and addresses the data requirements of those strategies. The Security Process Management Framework is introduced and analytical strategies for security metrics data are discussed. You'll learn how to take a security metrics program and adapt it to a variety of organizational contexts to achieve continuous security improvement over time. Real-world examples of security measurement projects are included in this definitive guide. Define security metrics as a manageable amount of usable data Design effective security metrics Understand quantitative and qualitative data, data sources, and collection and normalization methods Implement a programmable approach to security using the Security Process Management Framework Analyze security metrics data using quantitative and qualitative methods Design a security measurement project for operational analysis of security metrics Measure security operations, compliance, cost and value, and people, organizations, and culture Manage groups of security measurement projects using the Security Improvement Program Apply organizational learning methods to security metrics

2012-10-26 Mark Talabis In order to protect company's information assets such as sensitive customer records, health care records, etc., the security practitioner first needs to find out: what needs protected, what risks those assets are exposed to, what controls are in place to offset those risks, and where to focus attention for risk treatment. This is the true value and purpose of information security risk assessments. Effective risk assessments are meant to provide a defendable analysis of residual risk associated with your key assets so that risk treatment options can be explored. Information Security Risk Assessment Toolkit gives you the tools and skills to get a quick, reliable, and thorough risk assessment for key stakeholders. Based on authors' experiences of real-world assessments, reports, and presentations Focuses on implementing a process, rather than theory, that allows you to derive a quick and valuable assessment Includes a companion web site with

spreadsheets you can utilize to create and maintain the risk assessment

2022-05-10 Richard Seiersen Security professionals are trained skeptics. They poke and prod at other people’s digital creations, expecting them to fail in unexpected ways. Shouldn’t that same skeptical power be turned inward? Shouldn’t practitioners ask: “How do I know that my enterprise security capabilities work? Are they scaling, accelerating, or slowing as the business exposes more value to more people and through more channels at higher velocities?” This is the start of the modern measurement mindset—the mindset that seeks to confront security with data. The Metrics Manifesto: Confronting Security with Data delivers an examination of security metrics with R, the popular open-source programming language and software development environment for statistical computing. This insightful and up-to-date guide offers readers a practical focus on applied measurement that can prove or disprove the efficacy of information security measures taken by a firm. The book’s detailed chapters combine topics like security, predictive analytics, and R programming to present an authoritative and innovative approach to security metrics. The author and security professional examines historical and modern methods of measurement with a particular emphasis on Bayesian Data Analysis to shed light on measuring security operations. Readers will learn how processing data with R can help measure security improvements and changes as well as help technology security teams identify and fix gaps in security. The book also includes downloadable code for people who are new to the R programming language. Perfect for security engineers, risk engineers, IT security managers, CISOs, and data scientists comfortable with a bit of code, The Metrics Manifesto offers readers an invaluable collection of information to help professionals prove the efficacy of security measures within their company.

2011-10-06 Caroline Wong Security Smarts for the Self-Guided IT Professional “An extraordinarily thorough and sophisticated explanation of why you need to measure the effectiveness of your security program and how to do it. A must-have for any quality security program!” —Dave Cullinane, CISSP, CISO & VP, Global Fraud, Risk & Security, eBay Learn how to communicate the value of an information security program, enable investment planning and decision making, and drive necessary change to improve the security of your organization. Security Metrics: A Beginner's Guide explains, step by step, how to develop and implement a successful security metrics program. This practical resource covers project management, communication, analytics tools, identifying targets, defining objectives, obtaining stakeholder buy-in, metrics automation, data quality, and resourcing. You'll also get details on cloud-based security metrics and process improvement. Templates, checklists, and examples give you the hands-on help you need to get started right away. Security Metrics: A Beginner's Guide features: Lingo--Common security terms defined so that you're in the know on the job IMHO--Frank and relevant opinions based on the author's years of industry experience Budget Note--Tips for getting security technologies and processes into your organization's budget In Actual Practice--Exceptions to the rules of security explained in real-world contexts Your Plan--Customizable checklists you can use on the job now Into Action--Tips on how, why, and when to apply new skills and techniques at work Caroline Wong, CISSP, was formerly the Chief of Staff for the Global Information Security Team at eBay, where she built the security metrics program from the ground up. She has been a featured speaker at RSA, ITWeb Summit, Metricon, the Executive Women's Forum, ISC2, and the Information Security Forum.

2015-03-28 George Campbell In corporate security today, while the topic of information technology (IT) security metrics has been extensively covered, there are too few knowledgeable contributions to the significantly larger field of global enterprise protection. Measuring and Communicating Security’s Value addresses this dearth of information by offering a collection of lessons

learned and proven approaches to enterprise security management. Authored by George Campbell, emeritus faculty of the Security Executive Council and former chief security officer of Fidelity Investments, this book can be used in conjunction with Measures and Metrics in Corporate Security, the foundational text for security metrics. This book builds on that foundation and covers the why, what, and how of a security metrics program, risk reporting, insider risk, building influence, business alignment, and much more. Emphasizes the importance of measuring and delivering actionable results Includes real world, practical examples that may be considered, applied, and tested across the full scope of the enterprise security mission Organized to build on a principal theme of having metrics that demonstrate the security department’s value to the corporation

2005-10-01 Fred Cohen This is CISO Security Program Metrics. It provides tools for the CISO to help get their job done effectively, efficiently, and properly. It consolidates material from hundreds of documents, standards, policies, books, and years of experience to provide a straight forward approach to top-down review of the information protection function of the enterprise.

2012-07-18 Seymour Bosworth The classic and authoritative reference in the field of computer security, now completely updated and revised With the continued presence of large-scale computers; the proliferation of desktop, laptop, and handheld computers; and the vast international networks that interconnect them, the nature and extent of threats to computer security have grown enormously. Now in its fifth edition, Computer Security Handbook continues to provide authoritative guidance to identify and to eliminate these threats where possible, as well as to lessen any losses attributable to them. With seventy-seven chapters contributed by a panel of renowned industry professionals, the new edition has increased coverage in both breadth and depth of all ten domains of the Common Body of Knowledge defined by the International Information Systems Security Certification Consortium (ISC). Of the seventy-seven chapters in the fifth edition, twenty-five chapters are completely new, including: 1. Hardware Elements of Security 2. Fundamentals of Cryptography and Steganography 3. Mathematical models of information security 4. Insider threats 5. Social engineering and low-tech attacks 6. Spam, phishing, and Trojans: attacks meant to fool 7. Biometric authentication 8. VPNs and secure remote access 9. Securing Peer2Peer, IM, SMS, and collaboration tools 10. U.S. legal and regulatory security issues, such as GLBA and SOX Whether you are in charge of many computers or just one important one, there are immediate steps you can take to safeguard your computer system and its contents. Computer Security Handbook, Fifth Edition equips you to protect the information and networks that are vital to your organization.

2016-04-19 W. Krag Brotby Other books on information security metrics discuss number theory and statistics in academic terms. Light on mathematics and heavy on utility, PRAGMATIC Security Metrics: Applying Metametrics to Information Security breaks the mold. This is the ultimate how-to-do-it guide for security metrics. Packed with time-saving tips, the book offers easy-to-follow guidance for those struggling with security metrics. Step by step, it clearly explains how to specify, develop, use, and maintain an information security measurement system (a comprehensive suite of metrics) to help: Security professionals systematically improve information security, demonstrate the value they are adding, and gain management support for the things that need to be done Management address previously unsolvable problems rationally, making critical decisions such as resource allocation and prioritization of security relative to other business activities Stakeholders, both within and outside the organization, be assured that information security is being competently managed The PRAGMATIC approach lets you hone in on your problem areas and identify the few metrics that will generate real business value. The book: Helps you figure out exactly

what needs to be measured, how to measure it, and most importantly, why it needs to be measured Scores and ranks more than 150 candidate security metrics to demonstrate the value of the PRAGMATIC method Highlights security metrics that are widely used and recommended, yet turn out to be rather poor in practice Describes innovative and flexible measurement approaches such as capability maturity metrics with continuous scales Explains how to minimize both measurement and security risks using complementary metrics for greater assurance in critical areas such as governance and compliance In addition to its obvious utility in the information security realm, the PRAGMATIC approach, introduced for the first time in this book, has broader application across diverse fields of management including finance, human resources, engineering, and production—in fact any area that suffers a surplus of data but a deficit of useful information. Visit Security Metametrics. Security Metametrics supports the global community of professionals adopting the innovative techniques laid out in PRAGMATIC Security Metrics. If you, too, are struggling to make much sense of security metrics, or searching for better metrics to manage and improve information security, Security Metametrics is the place.

http://securitymetametrics.com/

2011 United States. Congress. House. Committee on Appropriations. Subcommittee on Energy and Water Development

2006-11-14 Fred Cohen The IT Security Governance Guidebook with Security Program Metrics on CD-ROM provides clear and concise explanations of key issues in information protection, describing the basic structure of information protection and enterprise protection programs. Including graphics to support the information in the text, this book includes both an overview of m

