[MOBI] Corporate Personnel Protection Developing And Executing An Effective Program Within A Business Corporation

Right here, we have countless ebook **corporate personnel protection developing and executing an effective program within a business corporation** and collections to check out. We additionally provide variant types and as a consequence type of the books to browse. The all right book, fiction, history, novel, scientific research, as skillfully as various new sorts of books are readily within reach here.

As this corporate personnel protection developing and executing an effective program within a business corporation, it ends up innate one of the favored book corporate personnel protection developing and executing an effective program within a business corporation collections that we have. This is why you remain in the best website to look the unbelievable ebook to have.

Designing Network Security - Merike Kaeo - 2004

Personnel Protection: Vehicle Operations and Safety - Jerome Miller - 2014-06-09
Personnel Protection: Vehicle Operations and Safety is a video presentation. Length: 20 minutes. Because a business executive typically spends a considerable amount of time travelling by vehicle, the greatest risk of injury or death to the executive is by vehicle accident or attack while in the vehicle. In Personnel Protection: Vehicle Operations and Safety, presenters Jerome Miller and Radford Jones discuss the basic security principles of executive driver safety and training. This 20-minute video presentation of narrated slides covers the challenges the executive driver may face, how and why to vary routes, schedules, and vehicles, and the characteristics of a qualified executive driver. This presentation is one of 11 modules in the Personnel Protection presentation series, which is designed for companies considering an executive security program or for companies with an executive security program already in place. Other topics in this series include: concepts of executive security; advance procedures; security personnel; the executive threat assessment profile; kidnapping issues and guidelines; security procedures for residence, worksite, and aircraft operations; and executive compensation issues, including IRS requirements. The Personnel Protection presentation series 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 20-minute, visual PowerPoint presentation with audio narration format is excellent for group learning Covers basic vehicle security principles, such as varying routes, schedules, and vehicles Addresses the challenges the executive driver may face due to the type of vehicle being used and travel conditions

Personnel Protection: Vehicle Operations and Safety - Jerome Miller - 2014-06-09
Personnel Protection: Vehicle Operations and Safety is a video presentation. Length: 20 minutes. Because a business executive typically spends a considerable amount of time travelling by vehicle, the greatest risk of injury or death to the executive is by vehicle accident or attack while in the vehicle. In Personnel Protection: Vehicle Operations and Safety, presenters Jerome Miller and Radford Jones discuss the basic security principles of executive driver safety and training. This 20-minute video presentation of narrated slides covers the challenges the executive driver may face, how and why to vary routes, schedules, and vehicles, and the characteristics of a qualified executive driver. This presentation is one of 11 modules in the Personnel Protection presentation series, which is designed for companies considering an executive security program or for companies with an executive security program already in place. Other topics in this series include: concepts of executive security; advance procedures; security personnel; the executive threat assessment profile; kidnapping issues and guidelines; security procedures for residence, worksite, and aircraft operations; and executive compensation issues, including IRS requirements. The Personnel Protection presentation series 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 20-minute, visual PowerPoint presentation with audio narration format is excellent for group learning Covers basic vehicle security principles, such as varying routes, schedules, and vehicles Addresses the challenges the executive driver may face due to the type of vehicle being used and travel conditions

HOW TO BE YOUR COMPANY'S SECURITY DIRECTOR - Keith Smith Shannon - 1999-01-01
The intent of this book is to give a working business professional a realistic review of security issues that a business may have to deal with on an everyday basis. Many texts have been written discussing these issues in great detail offering solutions. While the value of these presentations is very worthwhile for the security professional, most management professionals need a more simple and workable way to deal with security problems. This presentation endeavors to outline security remedies and options on a level most useful for the average business professional. In many businesses, security management is assigned to administrative personnel not familiar with protection topics. This book will give those individuals a working knowledge of security issues and practices. It can be used as an informed starting point with which to deal with a security situation completely, or at best, give some general know ledge of the field if security professionals have to be called. This basic information can save a company money, and the person assigned the task can feel some level of comfort in dealing with the topic. The author emphasizes that the best methods for dealing with security problems are the simplest. Management desires a list of options from the security professional and then the best course of action has to be factored into the business life of the firm. The author shows how the best absolute security remedy will often not be the best overall action for the company, and that a combination of steps may have to be taken in order to address the problem.

HOW TO BE YOUR COMPANY'S SECURITY DIRECTOR - Keith Smith Shannon - 1999-01-01
The intent of this book is to give a working business professional a realistic review of security issues that a business may have to deal with on an everyday basis. Many texts have been written discussing these issues in great detail offering solutions. While the value of these presentations is very worthwhile for the security professional, most management professionals need a more simple and workable way to deal with security problems. This presentation endeavors to outline security remedies and options on a level most useful for the average business professional. In many businesses, security management is assigned to administrative personnel not familiar with protection topics. This book will give those individuals a working knowledge of security issues and practices. It can be used as an informed starting point with which to deal with a security situation completely, or at best, give some general know ledge of the field if security professionals have to be called. This basic information can save a company money, and the person assigned the task can feel some level of comfort in dealing with the topic. The author emphasizes that the best methods for dealing with security problems are the simplest. Management desires a list of options from the security professional and then the best course of action has to be factored into the business life of the firm. The author shows how the best absolute security remedy will often not be the best overall action for the company, and that a combination of steps may have to be taken in order to address the problem.

Personnel Protection: Security Personnel - Jerome Miller - 2013-09-06
When it comes to the physical safety of executives, no other preventative measure is more necessary than the proper screening and training of the personnel charged with their protection. In Personnel Protection: Security Personnel presenters Jerome Miller and Radford Jones discuss the critically important task of selecting and training security personnel for executive protection duties. In this seven-minute video presentation of narrated slides, the topics covered include a comparison of contracted and proprietary personnel, the pros and cons of armed versus unarmed personnel, the characteristics of the ideal security person, and the training requirements for hired security personnel. This presentation is one of 11 modules in the Personnel Protection presentation series, which is designed for companies considering an executive security program or for companies with an executive security program already in place. Each presentation in the series is narrated by Jerome Miller, formerly a commander in the Detroit Police Department and senior manager of international and special security operations at Chrysler Corporation, and Radford Jones, formerly manager of global security and fire protection at Ford Motor Company after 20 years with the U.S. Secret Service. Other topics in this series include concepts of executive security; advance procedures; the executive threat assessment profile; kidnapping issues and guidelines; security procedures for residences; worksite, aircraft, and vehicle operations; and executive compensation issues, including IRS requirements. Personnel Protection: Security Personnel 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 seven-minute, visual PowerPoint presentation with audio narration format is excellent for group learning Describes the advantages and challenges of using contracted versus proprietary and armed versus unarmed security personnel Covers the components of an executive security personnel training program and necessary training documentation

Personnel Protection: Security Personnel - Jerome Miller - 2013-09-06
When it comes to the physical safety of executives, no other preventative measure is more necessary than the proper screening and training of the personnel charged with their protection. In Personnel Protection: Security Personnel presenters Jerome Miller and Radford Jones discuss the critically important task of selecting and training security personnel for executive protection duties. In this seven-minute video presentation of narrated slides, the topics covered include a comparison of contracted and proprietary personnel, the pros and cons of armed versus unarmed personnel, the characteristics of the ideal security person, and the training requirements for hired security personnel. This presentation is one of 11 modules in the Personnel Protection presentation series, which is designed for companies considering an executive security program or for companies with an executive security program already in place. Each presentation in the series is narrated by Jerome Miller, formerly a commander in the Detroit Police Department and senior manager of international and special security operations at Chrysler Corporation, and Radford Jones, formerly manager of global security and fire protection at Ford Motor Company after 20 years with the U.S. Secret Service. Other topics in this series include concepts of executive security; advance procedures; the executive threat assessment profile; kidnapping issues and guidelines; security procedures for residences; worksite, aircraft, and vehicle operations; and executive compensation issues, including IRS requirements. Personnel Protection: Security Personnel 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 seven-minute, visual PowerPoint presentation with audio narration format is excellent for group learning Describes the advantages and challenges of using contracted versus proprietary and armed versus unarmed security personnel Covers the components of an executive security personnel training program and necessary training documentation

Building a Corporate Culture of Security - John Sullivant - 2016-02-24
Building a Corporate Culture of Security: Strategies for Strengthening Organizational Resiliency provides readers with the proven strategies, methods, and techniques they need to present ideas and a sound business case for improving or enhancing security resilience to senior management. Presented from the viewpoint of a leading expert in the field, the book offers proven and integrated strategies that convert threats, hazards, risks, and vulnerabilities into actionable security solutions, thus enhancing organizational resiliency in ways that executive management will accept. The book delivers a much-needed look into why some corporate security practices programs work and others don’t. Offering the tools necessary for anyone in the organization charged with security operations, Building a Corporate Culture of Security provides practical and useful guidance on handling security issues corporate executives hesitate to address until it’s too late. Provides a comprehensive understanding of the root causes of the most common security vulnerabilities that impact organizations and strategies for their early detection and prevention Offers techniques for security managers on how to establish and maintain effective communications with executives, especially when bringing security weakness--and solutions--to them Outlines a strategy for determining the value and contribution of protocols to the organization, how to detect gaps, duplications and omissions from those protocols, and how to improve their purpose and usefulness Explores strategies for building professional competencies; managing security operations, and assessing risks, threats, vulnerabilities, and consequences Shows how to establish a solid foundation for the layering of security and building a resilient protection-in-depth capability that benefits the entire organization Offers appendices with proven risk management and risk-based metric frameworks and architecture platforms

Building a Corporate Culture of Security - John Sullivant - 2016-02-24
Building a Corporate Culture of Security: Strategies for Strengthening Organizational Resiliency provides readers with the proven strategies, methods, and techniques they need to present ideas and a sound business case for improving or enhancing security resilience to senior management. Presented from the viewpoint of a leading expert in the field, the book offers proven and integrated strategies that convert threats, hazards, risks, and vulnerabilities into actionable security solutions, thus enhancing organizational resiliency in ways that executive management will accept. The book delivers a much-needed look into why some corporate security practices programs work and others don’t. Offering the tools necessary for anyone in the organization charged with security operations, Building a Corporate Culture of Security provides practical and useful guidance on handling security issues corporate executives hesitate to address until it’s too late. Provides a comprehensive understanding of the root causes of the most common security vulnerabilities that impact organizations and strategies for their early detection and prevention Offers techniques for security managers on how to establish and maintain effective communications with executives, especially when bringing security weakness--and solutions--to them Outlines a strategy for determining the value and contribution of protocols to the organization, how to detect gaps, duplications and omissions from those protocols, and how to improve their purpose and usefulness Explores strategies for building professional competencies; managing security operations, and assessing risks, threats, vulnerabilities, and consequences Shows how to establish a solid foundation for the layering of security and building a resilient protection-in-depth capability that benefits the entire organization Offers appendices with proven risk management and risk-based metric frameworks and architecture platforms

Risk and Security Management - Michael Blyth - 2008-07-23
Learn to measure risk and develop a plan to protect employees and company interests by applying the advice and tools in Risk and Security Management: Protecting People and Sites Worldwide. In a world concerned with global terrorism, instability of emerging markets, and hazardous commercial operations, this book shines as a relevant and timely text with a plan you can easily apply to your organization. Find a series of strategic to granular level policies, systems, and concepts which identify and address risk, enabling business to occur in a manner which best protects you and your company.

Risk and Security Management - Michael Blyth - 2008-07-23
Learn to measure risk and develop a plan to protect employees and company interests by applying the advice and tools in Risk and Security Management: Protecting People and Sites Worldwide. In a world concerned with global terrorism, instability of emerging markets, and hazardous commercial operations, this book shines as a relevant and timely text with a plan you can easily apply to your organization. Find a series of strategic to granular level policies, systems, and concepts which identify and address risk, enabling business to occur in a manner which best protects you and your company.

A Guide to Developing a Company Industrial Civil Defense Manual - United States. Office of Civil Defense - 1969

A Guide to Developing a Company Industrial Civil Defense Manual - United States. Office of Civil Defense - 1969

Handbook of Loss Prevention and Crime Prevention - Lawrence J. Fennelly - 2012
The Handbook of Loss Prevention and Crime Prevention, 5th Edition, is a trusted foundation for security professionals just entering the field and a reference for seasoned professionals. This book provides a comprehensive overview of current approaches to security and crime prevention, tools and technologies to put these approaches into action, and information on a wide range of specific areas within the field of physical security. These include school and campus security, cargo security, access control, the increasingly violent healthcare security environment, and prevention or mitigation of terrorism and natural disasters. * Covers every important topic in the field, including the latest on wireless security applications, data analysis and visualization, situational crime prevention, and global security standards and compliance issues * Required reading for the certification DHS selected for its infrastructure security professionals * Each chapter is contributed by a top security professional with subject-matter expertise

Handbook of Loss Prevention and Crime Prevention - Lawrence J. Fennelly - 2012
The Handbook of Loss Prevention and Crime Prevention, 5th Edition, is a trusted foundation for security professionals just entering the field and a reference for seasoned professionals. This book provides a comprehensive overview of current approaches to security and crime prevention, tools and technologies to put these approaches into action, and information on a wide range of specific areas within the field of physical security. These include school and campus security, cargo security, access control, the increasingly violent healthcare security environment, and prevention or mitigation of terrorism and natural disasters. * Covers every important topic in the field, including the latest on wireless security applications, data analysis and visualization, situational crime prevention, and global security standards and compliance issues * Required reading for the certification DHS selected for its infrastructure security professionals * Each chapter is contributed by a top security professional with subject-matter expertise

A Decade of Social Protection Development in Selected Asian Countries - OECD - 2017-05-11
Over the past ten years economic growth in Asia has contributed to a reduction of poverty as well as fertility rates, and greater prosperity has contributed to gains in life expectancy.

A Decade of Social Protection Development in Selected Asian Countries - OECD - 2017-05-11
Over the past ten years economic growth in Asia has contributed to a reduction of poverty as well as fertility rates, and greater prosperity has contributed to gains in life expectancy.

Designing Network Security - Merike Kaeo - 2004
bull; Gain a comprehensive view of network security issues and concepts, then master specific implementations based on your network needs bull; Learn how to use new and legacy Cisco Systems equipment to secure your networks bull; Understand how to design and build security services while also learning the legal and network accessibility impact of those services

bull; Gain a comprehensive view of network security issues and concepts, then master specific implementations based on your network needs bull; Learn how to use new and legacy Cisco Systems equipment to secure your networks bull; Understand how to design and build security services while also learning the legal and network accessibility impact of those services

Office and Office Building Security - Edward Luis - 1994-05-06
Office and Office Building Security, Second Edition, is the first book of its type to address issues of violence in the workplace to breaking and entering. As a working guide for administrators, property managers and security personnel, this book is devoted exclusively to total office security programs, detailing hundreds of professional secrets for the safety of employees and the complex. Office and Office Building Security, Second Edition, provides the background to create a safe and secure workplace, regardless of location, size and number of employees. Provides updated and current information on every office security issue or concern Trains the businessperson to be responsive to 'foreseeability' issues alluded to in the court system Examines issues of violence and crime, as well as the dynamics

Office and Office Building Security - Edward Luis - 1994-05-06
Office and Office Building Security, Second Edition, is the first book of its type to address issues of violence in the workplace to breaking and entering. As a working guide for administrators, property managers and security personnel, this book is devoted exclusively to total office security programs, detailing hundreds of professional secrets for the safety of employees and the complex. Office and Office Building Security, Second Edition, provides the background to create a safe and secure workplace, regardless of location, size and number of employees. Provides updated and current information on every office security issue or concern Trains the businessperson to be responsive to 'foreseeability' issues alluded to in the court system Examines issues of violence and crime, as well as the dynamics

Building an Effective Security Program - Chris Williams - 2020-09-21
Building an Effective Security Program provides readers with a comprehensive approach to securing the IT systems in use at their organizations. This book provides information on how to structure and operate an effective cybersecurity program that includes people, processes, technologies, security awareness, and training. This program will establish and maintain effective security protections for the confidentiality, availability, and integrity of organization information. In this book, the authors take a pragmatic approach to building organization cyberdefenses that are effective while also remaining affordable. This book is intended for business leaders, IT professionals, cybersecurity personnel, educators, and students interested in deploying real-world cyberdefenses against today’s persistent and sometimes devastating cyberattacks. It includes detailed explanation of the following IT security topics: IT Security Mindset—Think like an IT security professional, and consider how your IT environment can be defended against potential cyberattacks. Risk Management—Identify the assets, vulnerabilities and threats that drive IT risk, along with the controls that can be used to mitigate such risk. Effective Cyberdefense—Consider the components of an effective organization cyberdefense to successfully protect computers, devices, networks, accounts, applications and data. Cyber Operations—Operate cyberdefense capabilities and controls so that assets are protected, and intruders can be detected and repelled before significant damage can be done. IT Security Awareness and Training—Promote effective cybersecurity practices at work, on travel, and at home, among your organization’s business leaders, IT professionals, and staff. Resilient IT Security—Implement, operate, monitor, assess, and improve your cybersecurity program on an ongoing basis to defend against the cyber threats of today and the future.

Building an Effective Security Program - Chris Williams - 2020-09-21
Building an Effective Security Program provides readers with a comprehensive approach to securing the IT systems in use at their organizations. This book provides information on how to structure and operate an effective cybersecurity program that includes people, processes, technologies, security awareness, and training. This program will establish and maintain effective security protections for the confidentiality, availability, and integrity of organization information. In this book, the authors take a pragmatic approach to building organization cyberdefenses that are effective while also remaining affordable. This book is intended for business leaders, IT professionals, cybersecurity personnel, educators, and students interested in deploying real-world cyberdefenses against today’s persistent and sometimes devastating cyberattacks. It includes detailed explanation of the following IT security topics: IT Security Mindset—Think like an IT security professional, and consider how your IT environment can be defended against potential cyberattacks. Risk Management—Identify the assets, vulnerabilities and threats that drive IT risk, along with the controls that can be used to mitigate such risk. Effective Cyberdefense—Consider the components of an effective organization cyberdefense to successfully protect computers, devices, networks, accounts, applications and data. Cyber Operations—Operate cyberdefense capabilities and controls so that assets are protected, and intruders can be detected and repelled before significant damage can be done. IT Security Awareness and Training—Promote effective cybersecurity practices at work, on travel, and at home, among your organization’s business leaders, IT professionals, and staff. Resilient IT Security—Implement, operate, monitor, assess, and improve your cybersecurity program on an ongoing basis to defend against the cyber threats of today and the future.

Developing sound business practices at the Department of Homeland Security - United States - 2004

Developing sound business practices at the Department of Homeland Security - United States - 2004

Conflict, Security and Development - Paul Jackson - 2014-11-07
This textbook draws on academic theory, field research and policy developments to provide an overview of the connections between security and development, before, during and after conflict. This 2nd edition is revised and updated to take account of changes that have occurred in both policy and academic arenas which are relevant to students and practitioners in this area. In an interdependent world it is often argued that the challenges of underdevelopment and insecurity have global implications. This textbook charts an accessible course through these complex debates, providing a comprehensive introduction for those encountering these issues for the first time. The main aims of the revised edition are: • to set out how thinking on conflict, security and development has changed over time and continues to evolve; • to explore the consequences of these changes, particularly for the theory and practice of development and security promotion; • to introduce a range of case studies from across the globe, in order to explore the implications of a combined approach to security and development. The authors are experienced in both the theory and the practice of this field, and illustrate the links between conflict, security and development with practical examples, drawing on key case studies from the past twenty years. Each chapter is informed by student pedagogy and the book will be essential reading for all students of development studies, war and conflict studies, and human security and is recommended for students of international security and IR in general.

Conflict, Security and Development - Paul Jackson - 2014-11-07
This textbook draws on academic theory, field research and policy developments to provide an overview of the connections between security and development, before, during and after conflict. This 2nd edition is revised and updated to take account of changes that have occurred in both policy and academic arenas which are relevant to students and practitioners in this area. In an interdependent world it is often argued that the challenges of underdevelopment and insecurity have global implications. This textbook charts an accessible course through these complex debates, providing a comprehensive introduction for those encountering these issues for the first time. The main aims of the revised edition are: • to set out how thinking on conflict, security and development has changed over time and continues to evolve; • to explore the consequences of these changes, particularly for the theory and practice of development and security promotion; • to introduce a range of case studies from across the globe, in order to explore the implications of a combined approach to security and development. The authors are experienced in both the theory and the practice of this field, and illustrate the links between conflict, security and development with practical examples, drawing on key case studies from the past twenty years. Each chapter is informed by student pedagogy and the book will be essential reading for all students of development studies, war and conflict studies, and human security and is recommended for students of international security and IR in general.

How to Develop and Implement a Security Master Plan - Timothy Giles - 2008-12-17
Engage Stakeholders with a Long-Term Solution The goal: Convince executive management to "buy in" to your security program, support it, and provide the largest possible amount of funding. The solution: Develop a meticulously detailed long-term plan that sells decision-makers on the dire need for your program, and then maps out its direction and required budget. Assess and Outline Security Risks to Map Out Mitigation Strategies This practical guide details how to construct a customized, comprehensive five-year corporate security plan that synchronizes with the strategies of any business or institution. The author explains how to develop a plan and implementation strategy that aligns with an organization’s particular philosophies, strategies, goals, programs, and processes. Readers learn how to outline risks and then formulate appropriate mitigation strategies. This guide provides tested, real-world solutions on how to: Conduct an effective, efficient assessment of the site and security personnel, meticulously addressing the particular needs of many different environments Make decisions about security philosophies, strategies, contract relationships, technology, and equipment replacement Interview executive and security management to determine their concerns, educate them, and ensure that they buy in to your plan Use all gathered data to construct and finalize the Security Master Plan and then implement it into the management of the business Apply Insights from an Expert with Global Experience at the Highest Level Author Tim Giles worked at IBM for 31 years serving as Director of Security for the company’s operations in the United States and Canada, as well as Latin America and Asia-Pacific. His immeasurable experience and insight provide readers with an extraordinarily comprehensive understanding that they can use to design and execute a highly effective, tailored security program.

How to Develop and Implement a Security Master Plan - Timothy Giles - 2008-12-17
Engage Stakeholders with a Long-Term Solution The goal: Convince executive management to "buy in" to your security program, support it, and provide the largest possible amount of funding. The solution: Develop a meticulously detailed long-term plan that sells decision-makers on the dire need for your program, and then maps out its direction and required budget. Assess and Outline Security Risks to Map Out Mitigation Strategies This practical guide details how to construct a customized, comprehensive five-year corporate security plan that synchronizes with the strategies of any business or institution. The author explains how to develop a plan and implementation strategy that aligns with an organization’s particular philosophies, strategies, goals, programs, and processes. Readers learn how to outline risks and then formulate appropriate mitigation strategies. This guide provides tested, real-world solutions on how to: Conduct an effective, efficient assessment of the site and security personnel, meticulously addressing the particular needs of many different environments Make decisions about security philosophies, strategies, contract relationships, technology, and equipment replacement Interview executive and security management to determine their concerns, educate them, and ensure that they buy in to your plan Use all gathered data to construct and finalize the Security Master Plan and then implement it into the management of the business Apply Insights from an Expert with Global Experience at the Highest Level Author Tim Giles worked at IBM for 31 years serving as Director of Security for the company’s operations in the United States and Canada, as well as Latin America and Asia-Pacific. His immeasurable experience and insight provide readers with an extraordinarily comprehensive understanding that they can use to design and execute a highly effective, tailored security program.

International Security, Peace, Development and Environment - Volume II - Ursula Oswald Spring - 2009-08-30
International Security, Peace, Development, and Environment is a component of Encyclopedia of Institutional and Infrastructural Resources in the global Encyclopedia of Life Support Systems (EOLSS), which is an integrated compendium of twenty one Encyclopedias. The Theme on International Security, Peace, Development, and Environment deals, in seven parts and two volumes , with a myriad of issues of great relevance to our world such as: human, social, gender and environmental security; the transition in earth history from the holocene to the anthropocene potentially causing disasters and increasing resource scarcity; limits to growth, use of natural resources, sustainable livelihood and productive system through technology; rise of conflicts due to scarce and polluted resources and the concentration of humans in limited spaces of big cities; the gender violence; peace education and peace teaching as mechanisms to strengthen citizenship and to improve the understanding of cultural diversity; mechanisms to strengthen the resistance against monopolist interests in the present global world and whistle blowing as a phenomenon to protect social peace and civil resistance. The presentation culminates with a discussion on the means of active nonviolence to reinforce democratic behavior and to reduce tensions and violent outcomes in a complex world. These two volumes are aimed at the following five major target audiences: University and College students Educators, Professional practitioners, Research personnel and Policy analysts, managers, and decision makers and NGOs.

International Security, Peace, Development and Environment - Volume II - Ursula Oswald Spring - 2009-08-30
International Security, Peace, Development, and Environment is a component of Encyclopedia of Institutional and Infrastructural Resources in the global Encyclopedia of Life Support Systems (EOLSS), which is an integrated compendium of twenty one Encyclopedias. The Theme on International Security, Peace, Development, and Environment deals, in seven parts and two volumes , with a myriad of issues of great relevance to our world such as: human, social, gender and environmental security; the transition in earth history from the holocene to the anthropocene potentially causing disasters and increasing resource scarcity; limits to growth, use of natural resources, sustainable livelihood and productive system through technology; rise of conflicts due to scarce and polluted resources and the concentration of humans in limited spaces of big cities; the gender violence; peace education and peace teaching as mechanisms to strengthen citizenship and to improve the understanding of cultural diversity; mechanisms to strengthen the resistance against monopolist interests in the present global world and whistle blowing as a phenomenon to protect social peace and civil resistance. The presentation culminates with a discussion on the means of active nonviolence to reinforce democratic behavior and to reduce tensions and violent outcomes in a complex world. These two volumes are aimed at the following five major target audiences: University and College students Educators, Professional practitioners, Research personnel and Policy analysts, managers, and decision makers and NGOs.

Building and Implementing a Security Certification and Accreditation Program - Patrick D. Howard - 2005-12-15
Building and Implementing a Security Certification and Accreditation Program: Official (ISC)2 Guide to the CAP CBK demonstrates the practicality and effectiveness of certification and accreditation (C&A) as a risk management methodology for IT systems in both public and private organizations. It provides security professiona

Building and Implementing a Security Certification and Accreditation Program - Patrick D. Howard - 2005-12-15
Building and Implementing a Security Certification and Accreditation Program: Official (ISC)2 Guide to the CAP CBK demonstrates the practicality and effectiveness of certification and accreditation (C&A) as a risk management methodology for IT systems in both public and private organizations. It provides security professiona

International Development and Security Act - United States. Congress. House. Committee on Foreign Affairs - 1961
Considers H.R. 7372, to authorize FY62 foreign aid programs and to reorganize those programs.

International Development and Security Act - United States. Congress. House. Committee on Foreign Affairs - 1961
Considers H.R. 7372, to authorize FY62 foreign aid programs and to reorganize those programs.

Guide to developing an effective security plan for the highway transportation of hazardous materials - - 2003

Guide to developing an effective security plan for the highway transportation of hazardous materials - - 2003

The International Development and Security Act - United States. Congress. House. Committee on Foreign Affairs - 1961

The International Development and Security Act - United States. Congress. House. Committee on Foreign Affairs - 1961

Digital Business Security Development: Management Technologies - Kerr, Don - 2010-07-31
"This book provides comprehensive coverage of issues associated with maintaining business protection in digital environments, containing base level knowledge for managers who are not specialists in the field as well as advanced undergraduate and postgraduate students undertaking research and further study"--Provided by publisher.

Digital Business Security Development: Management Technologies - Kerr, Don - 2010-07-31
"This book provides comprehensive coverage of issues associated with maintaining business protection in digital environments, containing base level knowledge for managers who are not specialists in the field as well as advanced undergraduate and postgraduate students undertaking research and further study"--Provided by publisher.

Security, Development, and Violence in Afghanistan - Althea-Maria Rivas - 2020-04-20
Security, Development, and Violence in Afghanistan provides a unique insight into the lived realities of the international intervention in Afghanistan and highlights the diversity, relationships, and interdependence of various groups including both external actors and Afghan communities. Analysis of the international intervention in Afghanistan following the post 9/11 invasion in 2001, one of the largest and most expensive in history, tends to focus on the perspective of organisational dynamics and

of privacy protection, especially in the context of transborder data flows.
to explore the micro-level interactions between different actors, showing how communities, local leaders, aid workers, UN officials, military and others navigated shifting security, development, and conflict dynamics. Starting with a contextual introduction to the intervention and the key debates surrounding it, this book goes on to explore the stories of security, development, and violence as constructed through official policy discourse, and then through the lived experiences of interveners and local actors. The book weaves a compelling narrative which links local and global issues and focuses on the everyday practices, relationships and acts of resistance which take place in two provinces of Afghanistan. Finally, the author highlights what this book's findings mean both for what we know about Afghanistan and for how we understand international interventions and the everyday dynamics between actors who live and work in spaces of conflict. Security, Development, and Violence in Afghanistan: Everyday Stories of Intervention will be of considerable interest to scholars and professionals with an interest in Afghanistan, aid work, humanitarian intervention, development studies, and peace and conflict studies.

Security, Development, and Violence in Afghanistan - Althea-Maria Rivas - 2020-04-20
Security, Development, and Violence in Afghanistan provides a unique insight into the lived realities of the international intervention in Afghanistan and highlights the diversity, relationships, and interdependence of various groups including both external actors and Afghan communities. Analysis of the international intervention in Afghanistan following the post 9/11 invasion in 2001, one of the largest and most expensive in history, tends to focus on the perspective of organisational dynamics and policies or external actors. Drawing on the author's five years of experience living, researching and working in Afghanistan, this book uses ethnographic methodologies to explore the micro-level interactions between different actors, showing how communities, local leaders, aid workers, UN officials, military and others navigated shifting security, development, and conflict dynamics. Starting with a contextual introduction to the intervention and the key debates surrounding it, this book goes on to explore the stories of security, development, and violence as constructed through official policy discourse, and then through the lived experiences of interveners and local actors. The book weaves a compelling narrative which links local and global issues and focuses on the everyday practices, relationships and acts of resistance which take place in two provinces of Afghanistan. Finally, the author highlights what this book's findings mean both for what we know about Afghanistan and for how we understand international interventions and the everyday dynamics between actors who live and work in spaces of conflict. Security, Development, and Violence in Afghanistan: Everyday Stories of Intervention will be of considerable interest to scholars and professionals with an interest in Afghanistan, aid work, humanitarian intervention, development studies, and peace and conflict studies.

International Development and Security - United States. Congress. Senate. Committee on Foreign Relations - 1961
Classified material has been deleted.

International Development and Security - United States. Congress. Senate. Committee on Foreign Relations - 1961
Classified material has been deleted.

Security Software Development - Douglas A. Ashbaugh, CISSP - 2008-10-23
Threats to application security continue to evolve just as quickly as the systems that protect against cyber-threats. In many instances, traditional firewalls and other conventional controls can no longer get the job done. The latest line of defense is to build security features into software as it is being developed. Drawing from the author's extensive experience as a developer, Secure Software Development: Assessing and Managing Security Risks illustrates how software application security can be best, and most cost-effectively, achieved when developers monitor and regulate risks early on, integrating assessment and management into the development life cycle. This book identifies the two primary reasons for inadequate security safeguards: Development teams are not sufficiently trained to identify risks; and developers falsely believe that pre-existing perimeter security controls are adequate to protect newer software. Examining current trends, as well as problems that have plagued software security for more than a decade, this useful guide: Outlines and compares various techniques to assess, identify, and manage security risks and vulnerabilities, with step-by-step instruction on how to execute each approach Explains the fundamental terms related to the security process Elaborates on the pros and cons of each method, phase by phase, to help readers select the one that best suits their needs Despite decades of extraordinary growth in software development, many open-source, government, regulatory, and industry organizations have been slow to adopt new application safety controls, hesitant to take on the added expense. This book improves understanding of the security environment and the need for safety measures. It shows readers how to analyze relevant threats to their applications and then implement time- and money-saving techniques to safeguard them.

Security Software Development - Douglas A. Ashbaugh, CISSP - 2008-10-23
Threats to application security continue to evolve just as quickly as the systems that protect against cyber-threats. In many instances, traditional firewalls and other conventional controls can no longer get the job done. The latest line of defense is to build security features into software as it is being developed. Drawing from the author's extensive experience as a developer, Secure Software Development: Assessing and Managing Security Risks illustrates how software application security can be best, and most cost-effectively, achieved when developers monitor and regulate risks early on, integrating assessment and management into the development life cycle. This book identifies the two primary reasons for inadequate security safeguards: Development teams are not sufficiently trained to identify risks; and developers falsely believe that pre-existing perimeter security controls are adequate to protect newer software. Examining current trends, as well as problems that have plagued software security for more than a decade, this useful guide: Outlines and compares various techniques to assess, identify, and manage security risks and vulnerabilities, with step-by-step instruction on how to execute each approach Explains the fundamental terms related to the security process Elaborates on the pros and cons of each method, phase by phase, to help readers select the one that best suits their needs Despite decades of extraordinary growth in software development, many open-source, government, regulatory, and industry organizations have been slow to adopt new application safety controls, hesitant to take on the added expense. This book improves understanding of the security environment and the need for safety measures. It shows readers how to analyze relevant threats to their applications and then implement time- and money-saving techniques to safeguard them.

Interstate Commerce Commission Reports - United States. Interstate Commerce Commission - 1960

Interstate Commerce Commission Reports - United States. Interstate Commerce Commission - 1960

Building an Effective Security Program for Distributed Energy Resources and Systems - Mariana Hentea - 2021-04-06
Building an Effective Security Program for Distributed Energy Resources and Systems Build a critical and effective security program for DERs Building an Effective Security Program for Distributed Energy Resources and Systems requires a unified approach to establishing a critical security program for DER systems and Smart Grid applications. The methodology provided integrates systems security engineering principles, techniques, standards, and best practices. This publication introduces engineers on the design, implementation, and maintenance of a security program for distributed energy resources (DERs), smart grid, and industrial control systems. It provides security professionals with understanding the specific requirements of industrial control systems and real-time constrained applications for power systems. This book: Describes the cybersecurity needs for DERs and power grid as critical infrastructure Introduces the information security principles to assess and manage the security and privacy risks of the emerging Smart Grid technologies Outlines the functions of the security program as well as the scope and differences between traditional IT system security requirements and those required for industrial control systems such as SCADA systems Offers a full array of resources— cybersecurity concepts, frameworks, and emerging trends Security Professionals and Engineers can use Building an Effective Security Program for Distributed Energy Resources and Systems as a reliable resource that is dedicated to the essential topic of security for distributed energy resources and power grids. They will find standards, guidelines, and recommendations from standards organizations, such as ISO, IEC, NIST, IEEE, ENISA, ISA, ISACA, and ISF, conveniently included for reference within chapters.

Building an Effective Security Program for Distributed Energy Resources and Systems - Mariana Hentea - 2021-04-06
Building an Effective Security Program for Distributed Energy Resources and Systems Build a critical and effective security program for DERs Building an Effective Security Program for Distributed Energy Resources and Systems requires a unified approach to establishing a critical security program for DER systems and Smart Grid applications. The methodology provided integrates systems security engineering principles, techniques, standards, and best practices. This publication introduces engineers on the design, implementation, and maintenance of a security program for distributed energy resources (DERs), smart grid, and industrial control systems. It provides security professionals with understanding the specific requirements of industrial control systems and real-time constrained applications for power systems. This book: Describes the cybersecurity needs for DERs and power grid as critical infrastructure Introduces the information security principles to assess and manage the security and privacy risks of the emerging Smart Grid technologies Outlines the functions of the security program as well as the scope and differences between traditional IT system security requirements and those required for industrial control systems such as SCADA systems Offers a full array of resources— cybersecurity concepts, frameworks, and emerging trends Security Professionals and Engineers can use Building an Effective Security Program for Distributed Energy Resources and Systems as a reliable resource that is dedicated to the essential topic of security for distributed energy resources and power grids. They will find standards, guidelines, and recommendations from standards organizations, such as ISO, IEC, NIST, IEEE, ENISA, ISA, ISACA, and ISF, conveniently included for reference within chapters.

Globalization, Development and Human Security - Anthony McGrew - 2007
World poverty and development are more salient than ever on the global political agenda. The campaigns of the global justice movement, the growing securitization of development in the aftermath of 9-11, the intensification of global inequality, and the perceived threats of global pandemics, migrations and failed states have contributed to a sense of renewed urgency. The contributors to this volume, including Bjorn Hettne, Fantu Cheru, Jeffrey Haynes and Bonny Ibhawah, share a common intellectual aspiration to re-unite the study of development with the study of international relations or global politics as it is more broadly conceived today. Although globalization has transformed the context of development, it has yet to significantly transform for the better the prospects for real development or human security amongst the worlds most vulnerable communities. Whether globalization, development and human security are inescapably trapped within a vicious circle or a virtuous cycle is the central concern of this book. The volume will be importance to student of development studies, international relations and politics, globalization and economics.

Globalization, Development and Human Security - Anthony McGrew - 2007
World poverty and development are more salient than ever on the global political agenda. The campaigns of the global justice movement, the growing securitization of development in the aftermath of 9-11, the intensification of global inequality, and the perceived threats of global pandemics, migrations and failed states have contributed to a sense of renewed urgency. The contributors to this volume, including Bjorn Hettne, Fantu Cheru, Jeffrey Haynes and Bonny Ibhawah, share a common intellectual aspiration to re-unite the study of development with the study of international relations or global politics as it is more broadly conceived today. Although globalization has transformed the context of development, it has yet to significantly transform for the better the prospects for real development or human security amongst the worlds most vulnerable communities. Whether globalization, development and human security are inescapably trapped within a vicious circle or a virtuous cycle is the central concern of this book. The volume will be importance to student of development studies, international relations and politics, globalization and economics.

Conflict, Security and Development - Danielle Beswick - 2013-06-17
This textbook draws on academic theory, field research and policy developments to provide an overview of the connections between security and development, before, during and after conflict.

Conflict, Security and Development - Danielle Beswick - 2013-06-17
This textbook draws on academic theory, field research and policy developments to provide an overview of the connections between security and development, before, during and after conflict.

Cyber Law and Cyber Security in Developing and Emerging Economies - Zeinab Karake-Shalhoub - 2010-01-01
This timely and important book illuminates the impact of cyber law on the growth and development of emerging and developing economies. Using a strong theoretical framework firmly grounded in resource-based and technology diffusion literature, the authors convey a subtle understanding of the ways public and private sector entities in developing and emerging countries adopt cyber space processes. This book reveals that the diffusion of cyber activities in developing and emerging economies is relatively low, with the main stumbling blocks resting in regulatory, cultural, and social factors. The authors argue that cyber crimes constitute a prime obstacle to the diffusion of e-commence and e-governments in developing economies, and governments have an important role in developing control mechanisms in the form of laws. However, setting appropriate policies and complementary services, particularly those affecting the telecommunications sector and other infrastructure, human capital and the investment environment, severely constrains Internet access. Using both strategic and operational perspectives, the authors discuss the concrete experience of constructing and implementing cyber laws and cyber security measures in developing and emerging countries, and analyse their content and appropriateness. Professionals, academics, students, and policymakers working in the area of cyber space, e-commerce and economic development, and United Nations entities working closely with the Millennium Development Goals, will find this book an invaluable reference.

Cyber Law and Cyber Security in Developing and Emerging Economies - Zeinab Karake-Shalhoub - 2010-01-01
This timely and important book illuminates the impact of cyber law on the growth and development of emerging and developing economies. Using a strong theoretical framework firmly grounded in resource-based and technology diffusion literature, the authors convey a subtle understanding of the ways public and private sector entities in developing and emerging countries adopt cyber space processes. This book reveals that the diffusion of cyber activities in developing and emerging economies is relatively low, with the main stumbling blocks resting in regulatory, cultural, and social factors. The authors argue that cyber crimes constitute a prime obstacle to the diffusion of e-commence and e-governments in developing economies, and governments have an important role in developing control mechanisms in the form of laws. However, setting appropriate policies and complementary services, particularly those affecting the telecommunications sector and other infrastructure, human capital and the investment environment, severely constrains Internet access. Using both strategic and operational perspectives, the authors discuss the concrete experience of constructing and implementing cyber laws and cyber security measures in developing and emerging countries, and analyse their content and appropriateness. Professionals, academics, students, and policymakers working in the area of cyber space, e-commerce and economic development, and United Nations entities working closely with the Millennium Development Goals, will find this book an invaluable reference.

Building a Practical Information Security Program - Jason Andress - 2016-11-01
Building a Practical Information Security Program provides users with a strategic view on how to build an information security program that aligns with business objectives. The information provided enables both executive management and IT managers not only to validate existing security programs, but also to build new business-driven security programs. In addition, the subject matter supports aspiring security engineers to forge a career path to successfully manage a security program, thereby adding value and reducing risk to the business. Readers learn how to translate technical challenges into business requirements, understand when to "go big or go home," explore in-depth defense strategies, and review tactics on when to absorb risks. This book explains how to properly plan and implement an infosec program based on business strategy and results. Provides a roadmap on how to build a security program that will protect companies from intrusion Shows how to focus the security program on its essential mission and move past FUD (fear, uncertainty, and doubt) to provide business value Teaches how to build consensus with an effective business-focused program

Building a Practical Information Security Program - Jason Andress - 2016-11-01
Building a Practical Information Security Program provides users with a strategic view on how to build an information security program that aligns with business objectives. The information provided enables both executive management and IT managers not only to validate existing security programs, but also to build new business-driven security programs. In addition, the subject matter supports aspiring security engineers to forge a career path to successfully manage a security program, thereby adding value and reducing risk to the business. Readers learn how to translate technical challenges into business requirements, understand when to "go big or go home," explore in-depth defense strategies, and review tactics on when to absorb risks. This book explains how to properly plan and implement an infosec program based on business strategy and results. Provides a roadmap on how to build a security program that will protect companies from intrusion Shows how to focus the security program on its essential mission and move past FUD (fear, uncertainty, and doubt) to provide business value Teaches how to build consensus with an effective business-focused program

Personal Passenger Safety in Railway Stations - Great Britain. Parliament. House of Commons. Transport Committee - 2006-05-25
Personal passenger safety in railway Stations : Oral and written evidence, oral evidence taken on Wednesday 19 April 2006

Personal Passenger Safety in Railway Stations - Great Britain. Parliament. House of Commons. Transport Committee - 2006-05-25
Personal passenger safety in railway Stations : Oral and written evidence, oral evidence taken on Wednesday 19 April 2006

Business Guide to Privacy and Data Protection Legislation - Charles Franklin - 1996-03-26
The Business Guide to Privacy and Data Protection Legislation presents a collection of reports from over 16 countries. Each report provides an introductory overview of current developments in the privacy field in each country, followed by a description of the laws in this area. One of the unique features of this new, second edition is that it combines within one volume the most authoritative translations of the privacy and data protection laws in each country. Another feature is its broad coverage. Originally covering seven countries, including France, Sweden, Denmark, Germany, the Guide has been expanded to include new reports where data protection laws have been passed more recently. These include reports on Switzerland, Belgium, Japan, Canada, the United States, The Netherlands, United Kingdom, Denmark, Iceland, Finland, France, Germany, etc. The Guide contains key resource material for those seeking to navigate their way through the sometimes complex environment

Business Guide to Privacy and Data Protection Legislation - Charles Franklin - 1996-03-26
The Business Guide to Privacy and Data Protection Legislation presents a collection of reports from over 16 countries. Each report provides an introductory overview of current developments in the privacy field in each country, followed by a description of the laws in this area. One of the unique features of this new, second edition is that it combines within one volume the most authoritative translations of the privacy and data protection laws in each country. Another feature is its broad coverage. Originally covering seven countries, including France, Sweden, Denmark, Germany, the Guide has been expanded to include new reports where data protection laws have been passed more recently. These include reports on Switzerland, Belgium, Japan, Canada, the United States, The Netherlands, United Kingdom, Denmark, Iceland, Finland, France, Germany, etc. The Guide contains key resource material for those seeking to navigate their way through the sometimes complex environment of privacy protection, especially in the context of transborder data flows.

Mobile Application Development, Usability, and Security - Mukherjea, Sougata - 2016-10-19
The development of mobile technology has experienced exponential growth in recent years. Mobile devices are ubiquitous in modern society, impacting both our personal and professional lives. Mobile Application Development, Usability, and Security provides a thorough overview on the different facets of mobile technology management and its integration into modern society. Highlighting issues related to analytics, cloud computing, and different types of application development, this book is a pivotal reference source for professionals, researchers, upper-level students, and practitioners actively involved in the area of mobile computing.

Mobile Application Development, Usability, and Security - Mukherjea, Sougata - 2016-10-19
The development of mobile technology has experienced exponential growth in recent years. Mobile devices are ubiquitous in modern society, impacting both our personal and professional lives. Mobile Application Development, Usability, and Security provides a thorough overview on the different facets of mobile technology management and its integration into modern society. Highlighting issues related to analytics, cloud computing, and different types of application development, this book is a pivotal reference source for professionals, researchers, upper-level students, and practitioners actively involved in the area of mobile computing.

Building the Infrastructure for Cloud Security - Raghuram Yeluri - 2014-03-29
For cloud users and providers alike, security is an everyday concern, yet there are very few books covering cloud security as a main subject. This book will help address this information gap from an Information Technology solution and usage-centric view of cloud infrastructure security. The book highlights the fundamental technology components necessary to build and enable trusted clouds. Here also is an explanation of the security and compliance challenges organizations face as they migrate mission-critical applications to the cloud, and how trusted clouds, that have their integrity rooted in hardware, can address these challenges. This book provides: Use cases and solution reference architectures to enable infrastructure integrity and the creation of trusted pools leveraging Intel Trusted Execution Technology (TXT). Trusted geo-location management in the cloud, enabling workload and data location compliance and boundary control usages in the cloud. OpenStack-based reference architecture of tenant-controlled virtual machine and workload protection in the cloud. A reference design to enable secure hybrid clouds for a cloud bursting use case, providing infrastructure visibility and control to organizations. "A valuable guide to the next generation of cloud security and hardware based root of trust. More than an explanation of the what and how, is the explanation of why. And why you can't afford to ignore it!" —Vince Lubsey, Vice President, Product Development, Virtustream Inc. " Raghu provides a valuable reference for the new 'inside out' approach, where trust in hardware, software, and privileged users is never assumed—but instead measured, attested, and limited according to least privilege principles." —John Skinner, Vice President, HyTrust Inc. "Traditional parameter based defenses are in sufficient in the cloud. Raghu's book addresses this problem head-on by highlighting unique usage models to enable trusted infrastructure in this open environment. A must read if you are exposed in cloud." —Nikhil Sharma, Sr. Director of Cloud Solutions, Office of CTO, EMC Corporation

Building the Infrastructure for Cloud Security - Raghuram Yeluri - 2014-03-29
For cloud users and providers alike, security is an everyday concern, yet there are very few books covering cloud security as a main subject. This book will help address this information gap from an Information Technology solution and usage-centric view of cloud infrastructure security. The book highlights the fundamental technology components necessary to build and enable trusted clouds. Here also is an explanation of the security and compliance challenges organizations face as they migrate mission-critical applications to the cloud, and how trusted clouds, that have their integrity rooted in hardware, can address these challenges. This book provides: Use cases and solution reference architectures to enable infrastructure integrity and the creation of trusted pools leveraging Intel Trusted Execution Technology (TXT). Trusted geo-location management in the cloud, enabling workload and data location compliance and boundary control usages in the cloud. OpenStack-based reference architecture of tenant-controlled virtual machine and workload protection in the cloud. A reference design to enable secure hybrid clouds for a cloud bursting use case, providing infrastructure visibility and control to organizations. "A valuable guide to the next generation of cloud security and hardware based root of trust. More than an explanation of the what and how, is the explanation of why. And why you can't afford to ignore it!" —Vince Lubsey, Vice President, Product Development, Virtustream Inc. " Raghu provides a valuable reference for the new 'inside out' approach, where trust in hardware, software, and privileged users is never assumed—but instead measured, attested, and limited according to least privilege principles." —John Skinner, Vice President, HyTrust Inc. "Traditional parameter based defenses are in sufficient in the cloud. Raghu's book addresses this problem head-on by highlighting unique usage models to enable trusted infrastructure in this open environment. A must read if you are exposed in cloud." —Nikhil Sharma, Sr. Director of Cloud Solutions, Office of CTO, EMC Corporation

Security in Virtual Worlds, 3D Webs, and Immersive Environments: Models for Development, Interaction, and Management - Rea, Alan - 2010-11-30
Although one finds much discussion and research on the features and functionality of Rich Internet Applications (RIAs), the 3D Web, Immersive Environments (e.g. MMORPGs) and Virtual Worlds in both scholarly and popular publications, very little is written about the issues and techniques one must consider when creating, deploying, interacting within, and managing them securely. Security in Virtual Worlds, 3D Webs, and Immersive Environments: Models for Development, Interaction, and Management brings together the issues that managers, practitioners, and researchers must consider when planning, implementing, working within, and managing these promising virtual technologies for secure processes and initiatives. This publication discusses the uses and potential of these virtual technologies and examines secure policy formation and practices that can be applied specifically to each.

Security in Virtual Worlds, 3D Webs, and Immersive Environments: Models for Development, Interaction, and Management - Rea, Alan - 2010-11-30
Although one finds much discussion and research on the features and functionality of Rich Internet Applications (RIAs), the 3D Web, Immersive Environments (e.g. MMORPGs) and Virtual Worlds in both scholarly and popular publications, very little is written about the issues and techniques one must consider when creating, deploying, interacting within, and managing them securely. Security in Virtual Worlds, 3D Webs, and Immersive Environments: Models for Development, Interaction, and Management brings together the issues that managers, practitioners, and researchers must consider when planning, implementing, working within, and managing these promising virtual technologies for secure processes and initiatives. This publication discusses the uses and potential of these virtual technologies and examines secure policy formation and practices that can be applied specifically to each.

Web Services Security Development and Architecture: Theoretical and Practical Issues - Guti�rrez, Carlos A. - 2010-01-31
"This book's main objective is to present some of the key approaches, research lines, and challenges that exist in the field of security in SOA systems"--Provided by publisher.

Web Services Security Development and Architecture: Theoretical and Practical Issues - Guti�rrez, Carlos A. - 2010-01-31
"This book's main objective is to present some of the key approaches, research lines, and challenges that exist in the field of security in SOA systems"--Provided by publisher.

Building in Security at Agile Speed - James Ransome - 2021-04-21
Today's high-speed and rapidly changing development environments demand equally high-speed security practices. Still, achieving security remains a human endeavor, a core part of designing, generating and verifying software. Dr. James Ransome and Brook S.E. Schoenfield have built upon their previous works to explain that security starts with people; ultimately, humans generate software security. People collectively act through a particular and distinct set of methodologies, processes, and technologies that the authors have brought together into a newly designed, holistic, generic software development lifecycle facilitating software security at Agile, DevOps speed. —Eric. S. Yuan, Founder and CEO, Zoom Video Communications, Inc. It is essential that we embrace a mantra that ensures security is baked in throughout any development process. Ransome and Schoenfield leverage their abundance of experience and knowledge to clearly define why and how we need to build this new model around an understanding that the human element is the ultimate key to success. —Jennifer Sunshine Steffens, CEO of IOActive Both practical and strategic, Building in Security at Agile Speed is an invaluable resource for change leaders committed to building secure software solutions in a world characterized by increasing threats and uncertainty. Ransome and Schoenfield brilliantly demonstrate why creating robust software is a result of not only technical, but deeply human elements of agile ways of working. —Jorgen Hesselberg, author of Unlocking Agility and Cofounder of Comparative Agility The proliferation of open source components and distributed software services makes the principles detailed in Building in Security at Agile Speed more relevant than ever. Incorporating the principles and detailed guidance in this book into your SDLC is a must for all software developers and IT organizations. —George K Tsantes, CEO of Cyberphos, former partner at Accenture and Principal at EY Detailing the people, processes, and technical aspects of software security, Building in Security at Agile Speed emphasizes that the people element remains critical because software is developed, managed, and exploited by humans. This book presents a step-by-step process for software security that is relevant to today's technical, operational, business, and development environments with a focus on what humans can do to control and manage the process in the form of best practices and metrics.

Building in Security at Agile Speed - James Ransome - 2021-04-21
Today's high-speed and rapidly changing development environments demand equally high-speed security practices. Still, achieving security remains a human endeavor, a core part of designing, generating and verifying software. Dr. James Ransome and Brook S.E. Schoenfield have built upon their previous works to explain that security starts with people; ultimately, humans generate software security. People collectively act through a particular and distinct set of methodologies, processes, and technologies that the authors have brought together into a newly designed, holistic, generic software development lifecycle facilitating software security at Agile, DevOps speed. —Eric. S. Yuan, Founder and CEO, Zoom Video Communications, Inc. It is essential that we embrace a mantra that ensures security is baked in throughout any development process. Ransome and Schoenfield leverage their abundance of experience and knowledge to clearly define why and how we need to build this new model around an understanding that the human element is the ultimate key to success. —Jennifer Sunshine Steffens, CEO of IOActive Both practical and strategic, Building in Security at Agile Speed is an invaluable resource for change leaders committed to building secure software solutions in a world characterized by increasing threats and uncertainty. Ransome and Schoenfield brilliantly demonstrate why creating robust software is a result of not only technical, but deeply human elements of agile ways of working. —Jorgen Hesselberg, author of Unlocking Agility and Cofounder of Comparative Agility The proliferation of open source components and distributed software services makes the principles detailed in Building in Security at Agile Speed more relevant than ever. Incorporating the principles and detailed guidance in this book into your SDLC is a must for all software developers and IT organizations. —George K Tsantes, CEO of Cyberphos, former partner at Accenture and Principal at EY Detailing the people, processes, and technical aspects of software security, Building in Security at Agile Speed emphasizes that the people element remains critical because software is developed, managed, and exploited by humans. This book presents a step-by-step process for software security that is relevant to today's technical, operational, business, and development environments with a focus on what humans can do to control and manage the process in the form of best practices and metrics.

Development and Security in Southeast Asia - Carolina G. Hernandez - 2019-07-15
This title was first published in 2003. This three-volume set examines the relationship between government and civil society in their efforts to define and pursue security. Including the results of an extensive research program, each volume is organized around one of the three principal themes - environment, people and globalization, supplying compelling evidence of the tension between economic change and human well-being. Challenging the conventional wisdom about the beneficial results of economically induced change, this first volume suggests that too often the mismanagement of development jeopardizes the security of individuals, families, communities, and possibly the state, by harming the very environment which is required to sustain both people and their economic existence. Bringing together an international group of scholars from a variety of disciplines, this volume is particularly relevant for academic and general research communities in the areas of social, economic, political and security matters of Southeast Asia.

Development and Security in Southeast Asia - Carolina G. Hernandez - 2019-07-15
This title was first published in 2003. This three-volume set examines the relationship between government and civil society in their efforts to define and pursue security. Including the results of an extensive research program, each volume is organized around one of the three principal themes - environment, people and globalization, supplying compelling evidence of the tension between economic change and human well-being. Challenging the conventional wisdom about the beneficial results of economically induced change, this first volume suggests that too often the mismanagement of development jeopardizes the security of individuals, families, communities, and possibly the state, by harming the very environment which is required to sustain both people and their economic existence. Bringing together an international group of scholars from a variety of disciplines, this volume is particularly relevant for academic and general research communities in the areas of social, economic, political and security matters of Southeast Asia.

Profits, Security, and Human Rights in Developing Countries - James Rochlin - 2015-06-19
The extractive sector is a particular area of expertise for Canada and more than half of Canada's mining assets abroad are located in Latin America, specifically in Brazil, Peru, Chile, and Colombia. The Canada-Colombia accord was the first free-trade agreement in the world to include annual Human Rights Impact Assessments (HRIA), and also includes a labour side accord where abuse complaints can be formally registered. Using Colombia as a case study, James Rochlin and his international and multidisciplinary line up of Canadian and Colombian scholars, and activists working in the area of human rights, and the judiciary explore: What is the best way to identify and operationalize for mutual benefit the concentric space between the interests of extractive corporations in profit and security, on the one hand, and the interests of the host communities in the promotion of human rights and human security, on the other? What can the four emblematic and diverse cases in Colombia (Meta, Sergovia, Marmato, and Bolivar/La Guajira) tell us about how to fine tune and improve a newly implemented governmental HRIA to render it an increasingly useful global instrument to promote simultaneously corporate security and human security for host communities? What is the most efficient and effective way to design and implement Corporate Social Responsibility Programs in a manner that promotes simultaneously corporate security and community human security? Written in a clear and accessible style, Profits, Security, and Human Rights presents practical lessons on how to promote both corporate security and human security in communities where the extractive sector operates in the Global South.

Profits, Security, and Human Rights in Developing Countries - James Rochlin - 2015-06-19
The extractive sector is a particular area of expertise for Canada and more than half of Canada's mining assets abroad are located in Latin America, specifically in Brazil, Peru, Chile, and Colombia. The Canada-Colombia accord was the first free-trade agreement in the world to include annual Human Rights Impact Assessments (HRIA), and also includes a labour side accord where abuse complaints can be formally registered. Using Colombia as a case study, James Rochlin and his international and multidisciplinary line up of Canadian and Colombian scholars, and activists working in the area of human rights, and the judiciary explore: What is the best way to identify and operationalize for mutual benefit the concentric space between the interests of extractive corporations in profit and security, on the one hand, and the interests of the host communities in the promotion of human rights and human security, on the other? What can the four emblematic and diverse cases in Colombia (Meta, Sergovia, Marmato, and Bolivar/La Guajira) tell us about how to fine tune and improve a newly implemented governmental HRIA to render it an increasingly useful global instrument to promote simultaneously corporate security and human security for host communities? What is the most efficient and effective way to design and implement Corporate Social Responsibility Programs in a manner that promotes simultaneously corporate security and community human security? Written in a clear and accessible style, Profits, Security, and Human Rights presents practical lessons on how to promote both corporate security and human security in communities where the extractive sector operates in the Global South.

How to Cheat at Designing Security for a Windows Server 2003 Network - Chris Ruston - 2005-12-15
Windows 2003 Server is unquestionably the dominant enterprise level operating system in the industry, with 95% of all companies running it. And for the last tow years, over 50% of all product upgrades have been security related. Securing Windows Server, according to bill gates, is the company's #1 priority. While considering the security needs of your organiztion, you need to balance the human and the technical in order to create the best security design for your organization. Securing a Windows Server 2003 enterprise network is hardly a small undertaking, but it becomes quite manageable if you approach it in an organized and systematic way. This includes configuring software, services, and protocols to meet an organization's security needs. * The Perfect Guide if "System Administrator is NOT your primary job function * Avoid "time drains" configuring the many different security standards built into Windows 2003 * Secure VPN and Extranet Communications

How to Cheat at Designing Security for a Windows Server 2003 Network - Chris Ruston - 2005-12-15
Windows 2003 Server is unquestionably the dominant enterprise level operating system in the industry, with 95% of all companies running it. And for the last tow years, over 50% of all product upgrades have been security related. Securing Windows Server, according to bill gates, is the company's #1 priority. While considering the security needs of your organiztion, you need to balance the human and the technical in order to create the best security design for your organization. Securing a Windows Server 2003 enterprise network is hardly a small undertaking, but it becomes quite manageable if you approach it in an organized and systematic way. This includes configuring software, services, and protocols to meet an organization's security needs. * The Perfect Guide if "System Administrator is NOT your primary job function * Avoid "time drains" configuring the many different security standards built into Windows 2003 * Secure VPN and Extranet Communications

This book constitutes the proceedings of the 6th Euro Symposium on Systems Analysis and Design, SIGSAND/PLAIS 2013, held in Gdańsk, Poland, in September 2013. The objective of this symposium is to promote and develop high-quality research on all issues related to systems analysis and design (SAND). It provides a forum for SAND researchers and practitioners in Europe and beyond to interact, collaborate, and develop their field. The 8 papers were carefully reviewed and selected with an acceptance rate of 40% and reflect the current trends in systems analysis and design. The contributions are organized into topical sections on information systems development, information systems security and information systems learning.

Information Systems: Development, Learning, Security - Stanisław Wrycza - 2013-09-16

This book constitutes the proceedings of the 6th Euro Symposium on Systems Analysis and Design, SIGSAND/PLAIS 2013, held in Gdańsk, Poland, in September 2013. The objective of this symposium is to promote and develop high-quality research on all issues related to systems analysis and design (SAND). It provides a forum for SAND researchers and practitioners in Europe and beyond to interact, collaborate, and develop their field. The 8 papers were carefully reviewed and selected with an acceptance rate of 40% and reflect the current trends in systems analysis and design. The contributions are organized into topical sections on information systems development, information systems security and information systems learning.