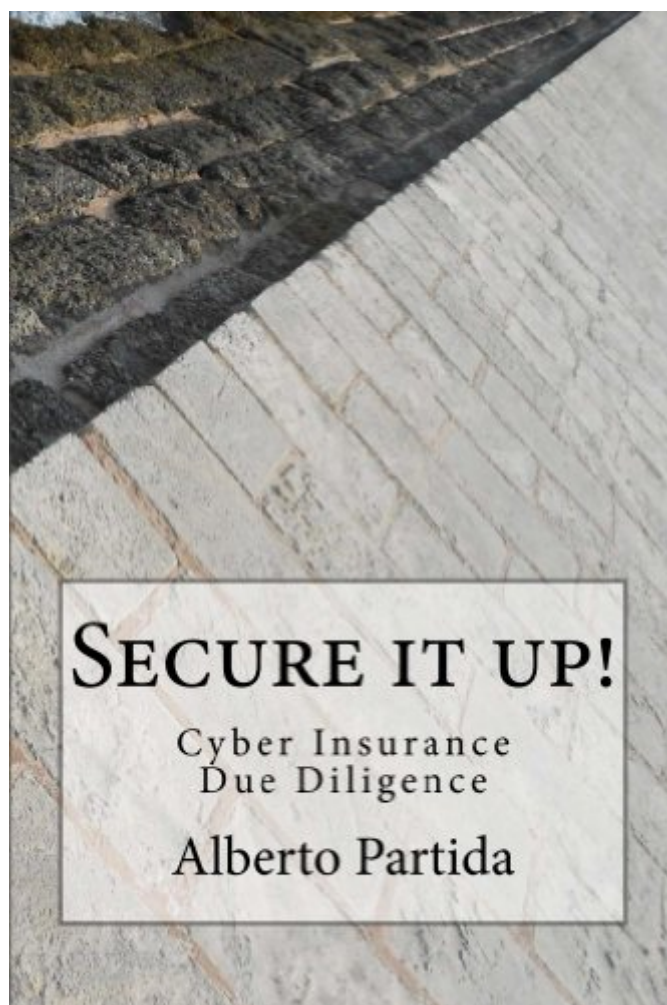


The book was found

Secure IT Up! Cyber Insurance Due Diligence



Synopsis

Alberto Partida's first book, "itsecuriteers", published in 2010, revealed HOW to create an Information Security team that enables business objectives. "Secure IT Up!", his second book, provides qualitative and quantitative insights that justify WHY the adoption of Information Security measures brings benefits to organisations and facilitates cyber-insurance due diligence processes. In the world we live in, risk management and information risk management are complex fields under continuous development. If you need to justify why applying security to your organisation will provide value to your customers or you are involved in cyber-insurance due diligence engagements, "Secure it up!" helps you with a statistically sound quantitative study and a set of reputable literature references. "The recommendations in this book are simple but effective: managers will find them of practical relevance and easy to communicate. They are based on sound empirical research which makes them go beyond consultancy speak." Jean-Noel Ezingear, Dean and Professor of Processes and Systems Management at Kingston University, London. "Alberto Partida combines a comprehensive analysis of existing literature and the results of surveys of subject matter experts to make his argument for combining Enterprise Risk Management (ERM) with information security practices." Richard Stiennon, Chief Research Analyst at IT-Harvest, Author of "Surviving Cyberwar", "Cyber Defense: Countering Targeted Attacks", Blogger at forbes.com, Michigan. Alberto is an information security analyst. He blogs at securityandrisk.blogspot.com and tweets as @itsecuriteer.

Book Information

File Size: 2961 KB

Print Length: 314 pages

Publisher: @itsecuriteer; 1 edition (December 18, 2012)

Publication Date: December 18, 2012

Sold by: Æ Æ Digital Services LLC

Language: English

ASIN: B00AQ6YXA6

Text-to-Speech: Enabled

X-Ray: Not Enabled

Word Wise: Enabled

Lending: Not Enabled

Enhanced Typesetting: Not Enabled

Best Sellers Rank: #1,852,065 Paid in Kindle Store (See Top 100 Paid in Kindle Store) #32 in Kindle Store > Kindle eBooks > Business & Money > Industries > Insurance > Liability #84 in Kindle Store > Kindle eBooks > Business & Money > Insurance > Liability #2378 in Kindle Store > Kindle eBooks > Computers & Technology > Security & Encryption

Customer Reviews

Great book covering the most important topics of the security, and an easy way to understand all you need about security in the companies.

From the Forward I wrote for Alberto's latest book: Secure IT Up! Just as organizations are waking up to the fact that information security plays an important role in business success there is a revolution on the near horizon. A revolution in the very risks that pose an existential threat to the enterprise. This came about as the natural consequence of the information revolution that began in the '90s. Every organization has realized tremendous gains in efficiency, customer acquisition, and new capabilities, all brought about by the rise of the Internet, the Web, and the global reach they provide to anyone with a computer or cell phone. Yet, their appreciation of risk has not grown, in part due to the fact that their business and their IT infrastructure grew up in a time which, in hindsight, was relatively risk free. Most organizations have applied security controls that are sufficient to keep operations functioning. The threats of a few short years ago, viruses, worms and adware, are addressed by a regime of firewalls, anti-virus software, and patch management, all necessary but not sufficient to protect critical assets. The first time I presented on risk management to an audience of IT auditors and security practitioners I was brought up short by my first slide which is the mandatory slide on asset classification that is the basis of all formal risk management regimes. The problem with asset based risk management, in terms of IT security, is that every asset in an enterprise is mission critical just by its very existence. You will never encounter an IT administrator who would volunteer his particular server or application as "low value". Thus, the asset identification exercise leaves us where we began: the role of IT risk management is to protect all of the IT assets. It is only through integration with the business risk management program that information security can be given relevance, which is the premise of this book. Alberto Partida combines a comprehensive analysis of existing literature and the results of surveys of subject matter experts to make his argument for combining Enterprise Risk Management (ERM) with information security practices. Of the three benefits his survey work derives - stakeholder value, new business opportunities, and improved compliance - I would like to expand on the second. Demonstrated

security expertise is becoming a critical factor in branding and trust building. In short, security sells. On the customer facing side a website that uses SSL, has a strong privacy statement, and is not prone to defacement or exploitation by hackers is required to attract users. On the operational side the absence of major breaches at a time when just about every industry sector has experienced its Hurricane Katrina moment, is a positive business statement that helps to establish trust with partners, customers, and stakeholders. The revolution that is fast approaching is a shift from asset-based risk management to threat-based. Thanks to the sophistication of successful campaigns like the joint Israeli-US attacks on Iran's uranium refining capabilities through the combined use of Flame-Duqu-Stuxnet enterprises are beginning to realize that even the most efficient application of traditional tools does nothing to stop the determined attacker. Attacks on business, government, and earth resource companies from nation state actors have demonstrated what a determined campaign can accomplish. It is in this new threat environment that threat-based risk management is coming into its own. The approach acknowledges that attackers will find a way in even if they have to resort to bribery, extortion, and physical breaches. What is required is to turn around the traditional approach of identifying critical assets to protect, and instead, focus on identifying the threat actors and cataloging their capabilities and intent; just as a data center located on the Gulf of Mexico may experience a risk profile change from concerns about redundancy and power costs to building up dikes when it is subjected to a storm surge. But changing to a threat-based risk management regime requires the existence of a risk management approach that already incorporates the business risks with information security, which is why this book is so timely.

[Download to continue reading...](#)

Secure IT Up! Cyber Insurance Due Diligence AUTO INSURANCE: A Business Guide On How To Save Money On Car Insurance (Home insurance, car insurance, health insurance) INSURANCE: The Ultimate How-To Guide on Deciding What Insurance Is Right for You (Insurance, Insurance policies, AIG story, Risk Management, Coverage, Life insurance, Book 1) Equity Crowdfunding for Investors: A Guide to Risks, Returns, Regulations, Funding Portals, Due Diligence, and Deal Terms (Wiley Finance) Private Equity Operational Due Diligence, + Website: Tools to Evaluate Liquidity, Valuation, and Documentation Private Equity Operational Due Diligence: Tools to Evaluate Liquidity, Valuation, and Documentation (Wiley Finance) IT Due Diligence Checklist: Fourth Edition Checklists for Due Diligence The Due Diligence Handbook For Commercial Real Estate: A Proven System To Save Time, Money, Headaches And Create Value When Buying Commercial Real Estate Car insurance book: A Complete Guide to Car insurance (Auto insurance book, Understanding your car insurance) Secure Web Application Deployment using OWASP Standards: An expert way of Secure

Web Application deployment Cyber Insurance Basics: an Installment in the Building Blocks Series of Insurance Content The Devil's Due and Other Stories: The Devil's Due, The Portal, Disfigured, Empathy, and Epitaph (International Thriller Writers Presents: Thriller, Vol. 1) Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace Cyber-Safe Kids, Cyber-Savvy Teens: Helping Young People Learn To Use the Internet Safely and Responsibly Life Insurance Made Easy: A Quick Guide - Whole Life Insurance Policy and Term Life Insurance Coverage Questions Answered Cyber Liability & Insurance: Managing the Risks of Intangible Assets (Commercial Lines) Cyber Insurance 2015: Guide for Small and Medium Sized Businesses Cyber Liability & Insurance (Commercial Lines) Money. Wealth. Life Insurance.: How the Wealthy Use Life Insurance as a Tax-Free Personal Bank to Supercharge Their Savings

[Contact Us](#)

[DMCA](#)

[Privacy](#)

[FAQ & Help](#)