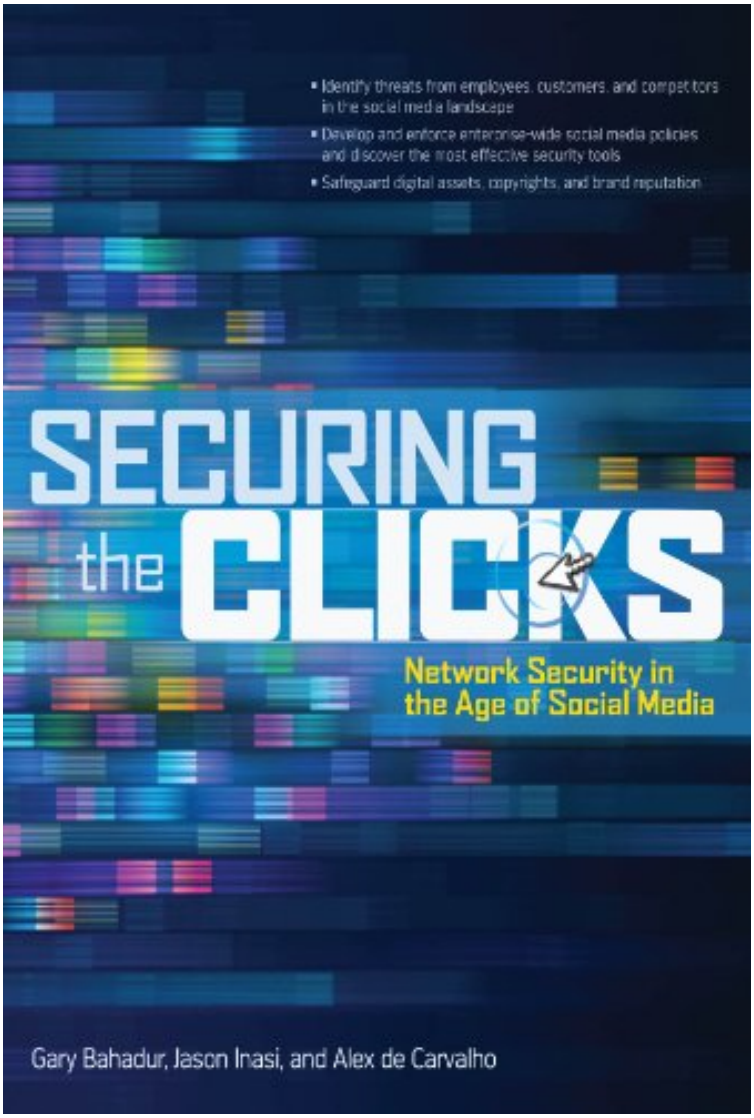
Securing the Clicks Network Security in the Age of Social Media

Gary Bahadur, Jason Inasi, Alex de Carvalho
**Download PDF | ePub | DOC | audiobook | ebooks*



#2009638 in eBooks 2011-10-22 2011-10-22File Name: B0060JOICQ | File size: 16.Mb

Gary Bahadur, Jason Inasi, Alex de Carvalho : Securing the Clicks Network Security in the Age of Social Media before purchasing it in order to gage whether or not it would be worth my time, and all praised Securing the Clicks Network Security in the Age of Social Media:

12 of 12 people found the following review helpful. Required reading for those looking to securely use social mediaBy Ben RothkeIn the book Digital Assassination: Protecting Your Reputation, Brand, or Business Against Online Attacks, it states that businesses that take days to respond to social media issues are way behind the curve. Social media operates in real-time, and responses need to be almost as quick.In a valuable new book on the topic, Securing the Clicks Network Security in the Age of Social Media, Gary Bahadur, Jason Inasi and Alex de Carvalho provide the

reader with a comprehensive overview on how not to be a victim of social media based security problems.Social media is now mainstream in corporate America, and even though it is hot, the security and privacy issues around it are even hotter. In the past, many firms simply said no to social media at the corporate level. But as Natalie Petouhoff of Weber Shandwick has observed, that will no longer work, as "social media isn't a choice anymore; it's a business transformation tool".The main security and privacy issue around social media is that users will share huge amounts of highly confidential personal and business information with people they perceive to be legitimate. Besides that, issues such as malware, vulnerabilities (cross site scripting, cross site request forgery, etc.), corporate espionage, phishing, spear phishing and more; are just a few of the many security risks around social media that need to be taken into consideration.In the book, the authors detail a framework for analyzing the corporate threats that arise from social media. The book uses the H.U.M.O.R methodology (Human resources, Utilization of resources and assets, Monetary considerations, Operations management, Reputation management) a matrix that outlines a systematic approach for developing the necessary security plans, policies and processes to mitigate social media risks.At 325 pages, the books 5 parts and 18 chapters provide the reader with a comprehensive overview of all of the critical areas around social media secure, that can be used to safeguard its assets and digital rights, in addition to defending their reputation from social network-based attacks. The book covers all of the core topic areas, from assessing social media security, to monitoring in the social media landscape, threat assessments, reputation management: strategy and collaboration and more; the authors provide the reader with an enlightening overview of all of the core areas.In chapter 1, the authors astutely note that no company today is immune to the many threats posted by a single individual, let alone a socially engaged and networked population. No firm should engage in social media before they fully understand the security and privacy risks that are being introduced. This book not only effectually does that; it also provides an all-inclusive framework around social media security.As to the notion of the inherent security risks around social media, this was recently proven when Chris Hadnagy (author of Social Engineering: The Art of Human Hacking, reviewed here) and James O'Gorman detailed in their Social Engineering Capture the Flag results from Defcon 19 observed that information leakage via social media is a difficult problem to solve due to how it is used and the frequency it is used in today's society. Having access to social media from computers and cell phones means that people can update their accounts instantaneously, from anywhere. The ease of which an employee can share data can contribute heavily to information leakage.Chapter 4 on threat assessments provides an exhaustive list of the different types of attackers and threat vectors that need to be considered when using social media. The attacks in the social media space are often different from typical IT attackers. As to threat vectors, there are a number of different vectors, both internal and external that can impact an organization. The chapter lists those vectors and details them.Chapter 9 - monetary considerations - strategy and collaboration - is a fascinating chapter in that it notes that in many firms, IT security budgets have not yet clearly defined the line item for social media security. In addition, trying to retrofit the IT security budget by assuming that tools already purchased for data loss prevention will also cover social media security concerns will likely be inadequate.Chapter 11 deals with reputation management - which has the goal to build and protect a positive Internet-based reputation, and not let it get subterfuged via social media. This is a significant issue as the risk to a firm's reputation is significant and growing with the increased use of social networks.One very helpful feature of the book that effectively brings home the message is numerous real-world case studies in every chapter. One fascinating example in chapter 13 is about the Cooks Source infringement controversy and the nature of how not to respond to a social media issue.The book also lists numerous amounts of tools. Chapter 13 has a comprehensive list of monitoring tools and the appendix has a list of nearly 100 tools for activity tracking, analytics, geolocation, plagiarism checking and more. These lists are extremely helpful, and the reader can start using many of these tools to get an initial pulse on the level of security around how their firm uses social media.Chapter 14 provides excellent guidance on how to execute social media security on a limited budget. The authors suggest the use of free or inexpensive software and other resources that can be used to help a company monitor the impact of their social media infrastructure. The chapter also details how social media security can be executed on a bugger budget, via the use of more sophisticated tools that can be used to secure manage the data flows within an organization.It will not be long until Facebook has its 1 billionth user. Given that a New York court recently referred to a user's reasonable expectation of privacy on sites like Facebook and MySpace as wishful thinking, the importance of Securing the Clicks Network Security in the Age of Social Media can't be overemphasized.For those firms that are looking to securely use social media, and not get abused by it, this book should be required reading.3 of 3 people found the following review helpful. The Primer on Risk Management in the age of Social Media.By DanielIf you are a director in Information Security, IT, HR, Marketing, PR, Legal, or Communications, this book is a must have.What is Information Security in the 21st century? Is it policies, firewalls, intrusion detection systems, log management, identity management, threat management, vulnerability management, and anti-virus? In short, yes, and so much more. The 21st century is the age of the social network where human beings participate in a highly evolved, always on, privacy is an afterthought social paradigm. If we are going to protect against the risks of the 21st century, we will need to better understand this new social paradigm, how the bad guys are exploiting it, and the tools at our disposal. That's where Securing the Clicks: Network Security in the Age of Social Media comes in.The book discusses several cutting-edge topics including

online reputation management, protecting intellectual property rights, preserving brand image, cyberstalking, and much more.The authors, Gary Bahadur, Jason Inasi, and Alex de Carvalho have done an excellent job laying out the risks introduced by social media, the context surrounding these risks, and then lay out a practical framework for implementing a risk management program. There are two points that I really appreciate, how clearly and succinctly the authors lay out the risk management program and how the program is laid out in a way that leverages all of the corporate processes a corporate employee must work with.The book is broken up into five parts:- Part I discusses how to assess your current risk as it pertains to Social Media. You'll understand what your company, and your competitors, are doing in the Social Media space. The authors also introduce the H.U.M.O.R. matrix, which you'll use as a practical and succinct risk management framework.- Part II focuses on Social Media threats. You'll learn how to identify and categorize threats in relation to their impact to your organization. The authors also provide you a look at how the bad guys are exploiting Social Media for their own gain.- Part III provides the meat and potatoes, how to implement controls in your organization to protect against Social Media risks. The authors walk you through a series of operational policies and procedures that should be implemented to ensure that your organization is protected.- Part IV addresses monitoring and reporting. In short, now that you've put all of these controls in place, how do you ensure that they are operating effectively and as intended? This part helps you put a management framework in place to ensure that you continually monitor the effectiveness of your controls.- Part V takes a look into the future of social media and what new risks may yet be introduced.As an Information Security practitioner and attorney, I found that this book had an immediate impact on my ability to help manage the risks of the 21st century. I found this book to be practical, succinct, and contextually relevant to a person working within a corporate environment. I would highly recommend this book to anyone who wants to learn more about the risks introduced by social media and how to manage those risks.I would also recommend you peruse the books website at [...].0 of 0 people found the following review helpful. Social repuation managementBy M. FernandesThis book is a great starting point for organizations looking to develop a strategy and to manage their online reputation. Securing the Clicks does a good job of identifying a baseline, plus it provides advanced tips for adopting best practices and policies geared towards managing a sound social presence, across all internal and external vectors. Organizations no longer have the luxury of ignoring their online presence in this new age of digital reputation and intellectual property protection. The book identifies great starting points for policy definition around acceptable usage and how to engage stakeholders across organization to make each approach a success. The book demonstrates how to assess, monitor, measure and implement controls with policies and technology tools. The H.U.M.O.R matrix allows the reader to use the publication as a reference book allowing practitioners to search for and apply the knowledge in their organizations.As practitioners in the field looking to help clients define comprehensive security, this book helps identify and address the gap of social presence protection, intellectual property leakage protection and online reputation management. The content is useful to consultants, legal, human resources, corporate policy makers and information technology practitioners.

Defend against corporate espionage launched from social networks Protect your organization from devastating social media attacks with instruction from a team of information security experts. Securing the Clicks: Network Security in the Age of Social Media explains the latest threats along with detailed fixes, best practices, and "from the headlines" case studies. Find out how to analyze risk, implement robust security protocols, and enforce social media usage policies. Regulatory compliance, online reputation management, and incident response are also covered in this comprehensive volume. Assess your global social media presence and identify vulnerabilities Establish solid security policies at every level of your organization Allocate resources for planning, administration, and corrective action Monitor usage by employees, clients, competitors, and the public Block cyberstalking. phishing, malware, and identity theft exploits Guard intellectual property rights, trademarks, copyrights, and logos Preserve your brand image using online reputation management tools Gary Bahadur is the founder and CEO of KRAA Security [www.kraasecurity.com/social-media-security], which protects organizations from threats through a combination of prevention services. He was the cofounder and CIO of Foundstone, Inc. Jason Inasi is CEO and cofounder of The Factory Interactive {www.thefactoryi.com], a digital design and marketing agency, and president of Inasi Group, an international, multidisciplinary, technology advisory firm. Alex de Carvalho is vice president of business development and community at VoxMed, cofounder of The Startup Forum, director of social media at Medimix International, and adjunct professor of social media at the University of Miami.