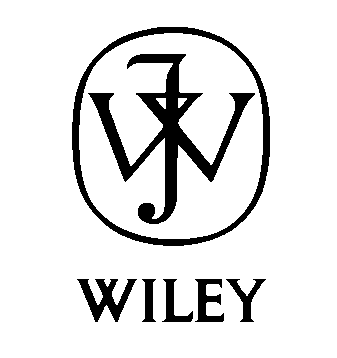
**WILEY PUBLISHING, INC.**

**Author’s Book Proposal Form**

**Today’s Date:** 2013-05-07

**Tentative Title:** Security Through Data Analysis

**Tentative Subtitle:** Harnessing The Power Of Feedback

**Author (s) Information:**

Name: Bob Rudis

Please list your full name, as you would like it to appear on the book.

Job Title: Director, Enterprise Information Security & IT Risk Management

Work Affiliation: Liberty Mutual Insurance

Business address: 225 Borthwick Ave, Portsmouth, NH, 03801

Business phone/fax: 603-245-3347

Home address: 15 Long Hall Drive, Berwick, ME, 03901

Home phone/fax: 207-619-3074

Email address: bob@rudis.net

Date of Birth: 10/15/1968

Preferred method of contact (voice or email): e-mail

Preferred place of contact (home or office): home

Primary author contact if more than one author:

Name: Jay Jacobs

Please list your full name, as you would like it to appear on the book.

Job Title: Sr. Data Analyst

Work Affiliation: Verizon

Business address: <work from home>

Business phone/fax:

Home address: 1023 Delaware Avenue, Mendota Heights, MN, 55118

Home phone/fax: 651-554-1616

Email address: jay@beechplane.com

Date of Birth: (we need this for Library of Congress registration) 02/01/1971

Preferred method of contact (voice or email): email

Preferred place of contact (home or office): home

Primary author contact if more than one author:

**Brief Author (s) Biography:**

**Bob Rudis** is a 20-year veteran of IT and Security and has consulted in and worked for many of the largest global enterprises, and currently directs Enterprise Information Risk Management for Liberty Mutual Insurance. He has written articles for Security Focus and FedTech Magazine, co-authored a paper for the SANS Reading Room, is a former blogger for The Apple Blog and a serial poster at his own blog (rud.is) on technology, data analysis & visualization and information security. His real-time Sandy tracker was featured on numerous blogs during the height of the crisis and was added to and featured on the R Graph Gallery (http://gallery.r-enthusiasts.com/graph/SuperStorm\_Sandy\_170).

Bob has been a regular contributor to the open source community throughout his career, including publishing of a application to track hurricanes (MegaTrack). During the Internet boom, Bob also built the first comprehensive Bible & associated study tools search engine and analytics tool (biblestudytools.net).

Bob has always been interested in data acquisition, analysis and visualizations, demonstrated through his passion for measuring & tracking our world. He has built numerous weather stations from scratch and worked to transfer the concepts of predictive modeling and analysis into other disciplines.

Bob has been a speaker at numerous security-related conferences, most recently at RSA where he and Jay Jacobs gave a well-received introduction to Data Analysis & Visualization. He is currently on the Board of Directors for the Society of Information Risk Analysis and has been named one of the Top 25 Influencers in Information Security by Tripwire Inc.

**Jay Jacobs** is the Sr. Data Analyst on Verizon’s RISK team where he collects, analyzes and visualizes information security data and he is a co-author of the Verizon Data Breach Investigations Report series, a study that researches and presents an extensive picture of cybercrime around the globe.

Jacobs is a co-founder of the Society of Information Risk Analysts and currently serves on the organization’s board of directors. He is also one of the primary authors of the OpenPERT project, an open-source Excel plug-in for risk analysis. He is a blogger (securityblog.verizonbusiness.com), and a co-host on the Risk Science podcast. Jay has written several articles for the ISSA Journal on cryptographic key management and risk analysis. Jay has been a speaker at numerous security-related conferences, most recently at RSA where he and Bob Rudis gave a well-received introduction to Data Analysis & Visualization.

What you do, who you do it for, what you’ve written, created, invented, or researched that makes you the best choice to write this book; also professional societies to which you belong and any related special awards or honors you’ve received.

**Definition of Topic and/or Product:**

Simply define and describe the topic as if you were talking to a non-technical person

This book will have a heavy “how-to” feel to it and mix in a healthy dose of concepts and contextualize data analysis into the information security field. It will teach data analysis by building on the skills and perspectives common among information security professionals. Unfortunately, most practitioners still rely on very basic tools and techniques to make sense of and learn within the information security domain. These professionals often look at the fields of statistics and the displays of modern visualizations as inherent gifts of specialists versus skills they are very capable of learning and using. The goal of this book is to show information security practitioners that they cannot only grasp data analysis concepts, but they can apply them in their daily workflows and use them to significantly improve how they make decisions and understand their environments.

and then tell us why the market needs this book

The current “data boom” has spawned a variety of texts, blog posts and talks on the subject of data analysis. Online classrooms, such as Coursera, even provide free virtual classrooms to explore these subjects. Yet, information technology and information security professionals have been slow to embrace these resources because the concepts presented are viewed as either out of reach (e.g. statistical analysis) or presented in a way that is viewed as not relevant to their world (many view the I.T. security world as unique). Working with perfect data sets on diamond production or car mileage (as two prominent examples) is viewed as playing with toys that have no relevance. Furthermore, these resources have been developed by and are presented by authors and instructors that have no familiarity with or credibility in the fields of information technology or information security.

The development of a foundational resource by respected members of the field would become a valuable resource that will be trusted and relied upon by the community of professionals tasked with understanding and improving their complex environments.

**Book Contents in Brief:**

Using a few sentences, summarize the book contents and accompanying media, if applicable) and then, using bullets, call out at least four of the important topics covered in the book-make sure to add a one-sentence tag line for case studies, source code, etc.

This book will present the core elements of analyzing I.T. system data and information security feedback by using real case studies and domain-specific data sets with a focus on practical “how-to” use versus theoretical concepts. This hands-on approach will be covered in context and will not be limited to just the analysis, but all the supporting skills needed to learn from our data. We will cover data analysis from start to finish: from the data collection and preparation through the data storage and management fundamentals then into the analysis and finally touch on data visualization and communication techniques.

**Book Contents in Not-So-Brief:**

Please attach a full Table of Contents in traditional outline form with at least two levels of subheadings or a Table of Contents with chapter titles and detailed content narrative for each chapter. Please be sure to include “active” words in your headings/subheading like: describing, understanding, implementing, and follow as closely as possible the enclosed document: Creating an Outline.

**Audience Profile:**

Primary audience: Information Technology and Information Security professionals

Secondary audience: Individuals looking for a practical take on the subjects of data analysis within an applied perspective.

**Ideal Reader:**

Fill in this sentence: “The ideal reader for this book would be a...”

The ideal reader for this book would be an IT/security professional who wants to learn how to understand her environment better and learn how to communicate attributes of it in compelling and engaging new ways.

What prior knowledge does this reader need (i.e. basic networking knowledge/ability to program in C)?

The book will be using terms and concepts from the fields of IT and information security, so knowledge of them would be helpful in understanding the material. Familiarity with tools such as Microsoft Excel will be beneficial in working through some of the examples. While R and Python source code will be presented, no former knowledge of them is expected or required.

**Competition:**

What other books are out there on your subject, if any, and what advantages in one or two sentences, does your book offer over each of them. Please list title, author, price, pages, publication date, publisher, and ISBN of those books.

**“Applied Security Visualization”, Raffael Marty**, $37.25 (amazon), 552 pages, August 2008, Addison-Wesley, 978-0321510105

Marty’s book was the first attempt by an active person in both the information security and data visualization field. But it has a failed premise that I.T. and information security has unique problems and therefor this book does not draw from any previous research and attempts to develop novel and unique solutions to problems that have solutions in other fields. It also focuses exclusively at a very technical level, alienating decision makers or more strategic thinkers in the industry. This book was also printed with low quality and in black and white, limiting the effectiveness the color used in the examples.

Our book will be much different in this that we will build off of the work of other fields and will integrate (and not contradict) established practices in data visualization into the field of I.T. and information security.

***“*Security Metrics: Replacing Fear, Uncertainty, and Doubt*”, Andrew Jaquith,*** *$35 (amazon), 336 pages, April, 2007, Addison-Wesley Professional, 978-0321349989*

.

**“Security Data Visualization: Graphical Techniques for Network Analysis”, Greg Conti,** $25 (amazon), 384 pages, September, 2012, New Riders, 978-0321834737

(Amazon Reviewer) To those in the information assurance or network security fields, Security Data Visualization by Greg Conti is a must read title due to the fact that it represents the first significant text to analyze its namesake of its title. For those unfamiliar with the utility of visualization systems, the text provides excellent examples on the graphical presentation of information to aid analysis, and how human intuition can be far more effective than standard machine processing. After establishing the basics early on, the book dives into security applications very quickly. By the end of Chapter 2, Conti has already shown enough so that the reader can see how to find a security vulnerability in the file structure of Microsoft Word documents via visualization techniques. As the book progresses so do the applications covered, which include network traffic visualization, visualization of firewall logs, and a handful of other topics. The work presented is extremely eye-opening, as it really has not gotten much attention outside of research and conferences. Security-minded readers unacquainted with this niche field will find the book impossible to put down. This book will take a modern approach and introduce additional concepts (also, Conti’s book is only available in electronic or used print format).

**“Information Dashboard Design”, Stephen Few,** $60, 224 pages, January, 2006 (another edition is coming I’ve heard), O’Reilly, 978-0596100162

Stephen Few is a well-known name in the data visualization world and this book helped put him there. We will learn from work like this and translate this into the language of I.T. and information security. Few often presents the academic side of data visualization. We would place any of Edward Tufte’s books and Stephen Few’s other books in with this book, but the book on information dashboard design is more relevant to our book since we will have material covering dashboard design theory as it applies to our target demographic.

**Your Previous Books:**

Please list title, price, pages, publication date, publisher, ISBN, and units sold to date.

**What Makes This Book Unique:**

In terms of what’s already out there/important timing/changes in technology, etc.

The market of I.T. and information security is largely an untapped demographic for data analysis and is on the verge of an explosion of interest in data analysis. This demographic is somewhat reticent when it comes to learning from other disciplines. As such, this book will be unique in that it will bridge the existing world of data analysis and visualization to information security and I.T. It will present the pertinent aspects of data analysis to I.T. and info security professionals in their language and in the context of their daily work.

**Book Hooks:**

List the 4 most important reasons why you think this book will sell lots of copies and why will it stand out on the shelf.

* Data analysis is a very in-demand topic and this book presents a comprehensive hands-on approach covering the topics from start to finish.
* Information technology and security professionals are searching for resources like this book to help them to understand the mounting data collections so they can be more successful in their jobs.
* The book will have a solid balance between theory and practice by intertwining the theory with practical real-world examples and it will be very usable as an a reference.
* The examples will be both compelling and reproducible and some will be immediately accessible with little more than the ability to work in Excel. This is very different from many of the book’s peers.

**Education Ancillaries:**

*Is your book used in colleges or universities? If so, what higher education ancillaries will you be able to provide with this revised edition? Typically, those would include a course syllabus or end-of-chapter questions and/or a test bank.*

This book would fit very well into information technology track and information security track university programs, especially since it presents concepts that are severely lacking in those programs. Working the analysis examples into a form where additional questions could be posed would be very straightforward and the development of a syllabus and test bank would be equally as straightforward.

**Conferences/Publications:**

Are there specific conferences, events, journals, or magazines that would be a perfect match for your book?

RSA Conference (both in the U.S. and international conferences)

Microsoft’s TechEd

Interop

Secure360

Blackhat/Defcon

CSO Magazine

Infosec Magazine

ISSA Journal

**Time Sensitive:**

Is this book’s publication planned for the release or upgrade of a certain product, approval of a standard or technology? If so, please explain.

The goal would be to have the book available for the 2014 RSA Conference, which will occur in late February, 2014.

**Manuscript Specifications:**

Wiley will provide you with a Word writing template already styled for manuscript preparation and instructions for submitting your electronic manuscript and art, as well as manuscript guidelines, which you can access at:

http://www.wiley.com/WileyCDA/Section/id-103181.html

**1. Estimated Final Pages:**

This number includes all blank pages, the table of contents, preface, foreword, index, appendices, bibliography, plus the actual book chapters. Typically, one book page holds 400 words with each figure counting as 200 words. Please use multiples of 24 for your estimated page count as we use printing signatures for calculation of page count. Please know that a 300-page book, means all the blanks, as well as title page, index (which we do) etc. Front matter and back matter takes up about 30 pieces of paper, so to speak.

360 pages

**2. Estimated Number of Illustrations:**

One illustration is counted as ½ page (200 words worth of space) in the final page count of the book. Source code samples are not considered as illustrations or figures.

40

**3.** **Web site**

Is there content, i.e. sample programs, downloadable code that would be of value to the reader as an enhancement to the book if it were developed by you, the author and promoted as a link to a site you would host? The web site should be a value-add to the book. The files should be created with the book in mind, and the book should bear in mind the Web site and cross-reference it whenever appropriate. (ALL WROX books have Wiley hosted web sites at wrox.com)

The book will absolutely need a companion web site and github repository. These resources will be maintained to keep the content fresh and working (there have been many book as recent as late 2011 that have entire chapters that no longer ‘work’; we do not want this to happen with our book).

**4. What art program do you typically use?** Adobe Photoshop & Adobe Illustrator or open-source competitors, Inkscape and Gimp.

**5. What word processing program do you typically use?** Microsoft Word

**6. State of the Project/ Schedule:**

What’s already done, what do you need to do, and when can you get the full manuscript to us? Typically our authors submit full manuscripts within four months (though depending on the topic or urgency to be first-to-market, it may be even shorter) from date of the signed contract. Please fill out, to the best of your abilities, a tentative chapter-by-chapter submission schedule with this proposal.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Today’s Date:** | 2013-05-07 |  |  |  |  |
| **Author(s):** | Jay Jacobs | Bob Rudis |  |  |  |
| **Book Title:** | Security Through Data Analysis: Harnessing The Power Of Feedback |  |  |  |  |
| **Ms Page/Word Count:** |  |  |  |  |  |
| **Ms Due Date:** |  |  |  |  |  |
| **Chapter #** (only sample numbering here-you may have more or less chapters and you may have Parts; label Parts as Part I, Part II, etc.) | **Chapter Title** (assignment of writing to individual author if there is more than one author) | **Approximate number of pages per chapter** | **Estimated figure count for each chapter** | **Date** you will submit to Wiley the complete chapter ready for editing & development by Wiley | **Author for who is writing the chapter** |
| Preface/Introduction |  |  |  | 10/14/2013 |  |
| 1 | Unleashing The Securing Power Of Data | 24 | 2 | 6/3/2013 | Jay/Bob |
| 2 | Finding Your Inner Security Data Scientist | 24 | 2 | 6/24/2013 | Jay/Bob |
| 3 | Learning The “Hello World” Of Security Data Analysis | 32 | 2 | 6/3/2013 | Bob/Jay |
| 4 | Tuning The Right Frequency: Security Analysis By The Numbers | 24 | 2 | 7/22/2013 | Jay/Bob |
| 5 | Knowing When 35 == 37: Finding The True Messages In Security Data | 28 | 2 | 8/12/2013 | Jay/Bob |
| 6 | Breaking Up With Your Relational Database | 28 | 2 | 6/24/2013 | Bob/Jay |
| 7 | Visualizing Your Security Data | 32 | 12 | 7/22/2013 | Bob/Jay |
| 8 | Mapping Security Data | 24 | 10 | 8/12/2013 | Bob/Jay |
| 9 | Making The Machine Learn For You | 32 | 2 | 9/2/2013 | Jay/Bob |
| 10 | Making The Machine Read For You | 32 | 2 | 9/2/2013 | Bob/Jay |
| 11 | Predicting The Future With Security Data | 28 | 2 | 9/30/2013 | Jay/Bob |
| 12 | Keeping It Simple | 24 | 0 | 9/30/2013 | Bob/Jay |
| References/Bibliography |  |  |  | 10/14/2013 | Both |
| Index (Wiley provides) |  |  |  |  |  |

Please submit this form to preese@wiley.com