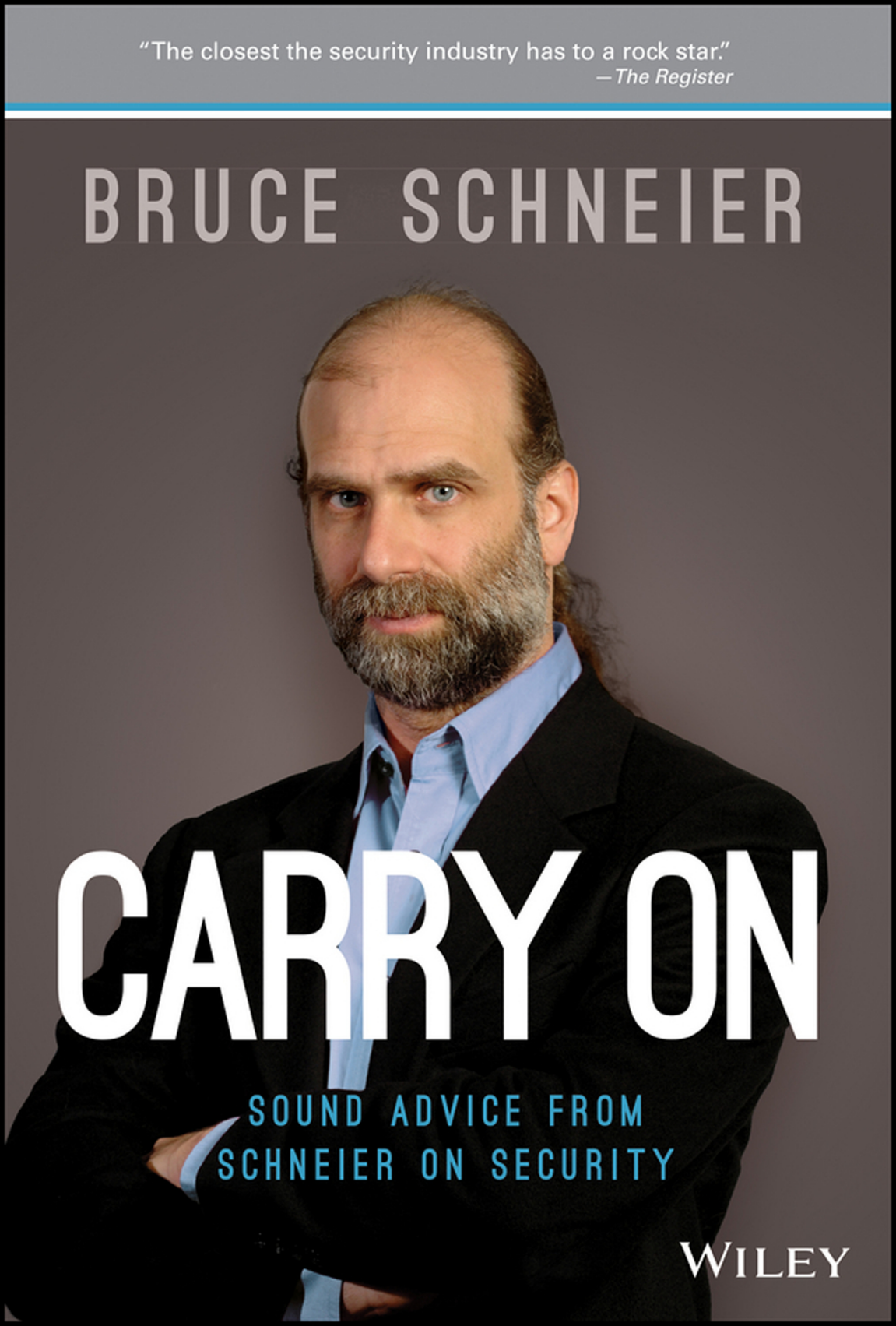
"The closest the security industry has to a rock star."
—*The Register*

BRUCE SCHNEIER



CARRY ON

SOUND ADVICE FROM SCHNEIER ON SECURITY

WILEY

Carry On

Carry On

Sound Advice from Schneier on Security

Bruce Schneier

WILEY

Carry On: Sound Advice from Schneier on Security

Published by
John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Copyright © 2014 by Bruce Schneier

Published by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-118-79081-6
ISBN: 978-1-118-79083-0 (ebk)
ISBN: 978-1-118-79082-3 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2013954201

Trademarks: Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

Credits

Executive Editor
Carol Long

Project Editor
Tom Dinse

Senior Production Editor
Kathleen Wisor

Editorial Manager
Mary Beth Wakefield

Freelancer Editorial Manager
Rosemarie Graham

Associate Director of Marketing
David Mayhew

Marketing Manager
Ashley Zurcher

Business Manager
Amy Knies

Vice President and Executive Group Publisher
Richard Swadley

Associate Publisher
Jim Minatel

Project Coordinator, Cover
Katie Crocker

Proofreader
Nancy Carrasco

Indexer
Johnna VanHoose Dinse

Cover Image
Steve Woit

Cover Designer
Ryan Sneed

Contents

Introduction

I like writing essays. I like the length: 600 to 1,200 words is my personal sweet spot. I like the format: a tight argument designed to make a particular point. And I like the style: explaining complicated topics to a lay audience is something I do well. Books are long, both in actual words and in the time they take to write. But I can write an essay in a fit of inspiration in a morning, and get it published the next day if everything goes well.

Not that it always goes that well, of course. Some essays are harder to write than others, and some are *very* hard. I like to take a few days to consider an issue before I write about it, which means that mine is generally not the first essay on the Internet after a news event. Editors, of course, hate this. They want something that catches the current news cycle.

Still, writing is something I'm good at and something I do a lot of. Since 1992, I have written almost 500 essays, op-eds, and articles for a wide variety of publications. They're all on my website—`www.schneier.com`, if you don't already know—and a selection of them has been collected into two books. The first collection, *Schneier on Security*, covered essays from April 2002 to February 2008. This volume covers essays from March 2008 to June 2013.

Looking back at the entire body of work, I have some lessons, observations, and advice for others trying to get their own articles published. And while my writing is mostly about security, much of the advice is general.

- **Opinions are cheap.** Charles McCabe famously said, "Any clod can have the facts, but having opinions is an art." He's right, but it doesn't follow that any clod lacks an opinion. On the Internet, opinions are a dime a dozen. I rarely get paid for my essays. Oh, there were a few fun years where *Wired* paid me to write a regular column, but they eventually realized that it was cheaper to not bother paying me for them, since I was going to keep writing in any case. I'm not saying that it's impossible to get paid for writing opinions—of course it is—only that it's increasingly rare and difficult.
- **Persuading someone is hard—and rare.** My goal is to write persuasive essays, but I doubt they do a lot of actual persuading. More often, I'm writing to people who already agree with me, giving them new ways to think about the issue, or new words to use when doing their own persuading.

- **It's hard not to repeat yourself.** I write for many different audiences, often on very similar topics. And I often repeat myself. If I find a turn of phrase I like, I reuse it. If I have a perfect paragraph on a topic, I'm likely to use it again. I used to write restaurant reviews semiprofessionally, and would regularly complain about how few ways there are to say "this tastes good." It's not that bad in my security writing, but sometimes it feels as if it comes close.
- **Stories repeat.** Again and again, essays I wrote five or ten years ago suddenly become relevant after some news event. The essay I wrote about data mining in 2001 was important after the Boston Marathon bombing. The essay I wrote about fingerprint scanners in 1998 was important when Apple released an iPhone with a fingerprint scanner. The essay I wrote about Chinese cyberattacks in 2008 has been pertinent every couple of years since then. Drug testing in sports, TSA security, the value of privacy, ubiquitous surveillance, security against lone shooters: it all becomes relevant again after a news event. Sometimes I dust off an old essay, tack on a new introduction, and republish it. But most of the time I try for a new perspective. I don't like resaying old things, even if they are new again.
- **Editors rewrite.** Sometimes they only rewrite a little, but sometimes they rewrite a lot. Sometimes their rewrites are improvements, and sometimes they're just different. It's okay to push back on rewrites that don't improve your work. Once I refused to let a publication publish an essay of mine because they changed too much and wouldn't change things back. And there were a few times I wish that I'd yanked essays where the editors cut too much.
- **The headline isn't your problem.** As an essay writer, you don't get any say in your headline. If you're lucky, you'll get to see it before it's published, but you probably won't. The headline is how the publication entices readers to your essay. As such, it'll be more sensationalist than you want. Or it'll be simpler than you want. Or it'll be less descriptive than you want. Let it go—you can't change it.
- **Links rot.** It's frustrating, but they do. Links you include in essays you write today are likely to return "Page not found" errors a few years from now. For my last volume of essays, I included links at the end. I was going to do the same for this book, but link-checking showed that almost a tenth of them were already dead. These aren't ancient essays; the oldest are six years old and the newest are current.

- **Mistakes happen.** Don't be afraid to admit your mistakes. If you're going to write in anything resembling real time, your writing will sometimes contain errors—of fact, of logic, of conclusion, of opinion—of pretty much everything. When you do, admit them. Don't hedge. Don't mumble. Just admit them. You'll feel better, and your audience will respect you for it.
- **Opinions can change.** Don't be afraid to change your mind. If you're going to write over anything resembling a reasonable length of time, you're going to change your mind about some things. Maybe you'll discover new facts that cause you to reach different conclusions. Maybe you'll just think about things in a new light and reach different conclusions. That's fine. Just explain it. John Maynard Keynes said, "When the facts change, I change my mind. What do you do, sir?" Exactly.
- **You need to write in order to be read.** The world is full of people with great ideas who never make them available to the wider world. My first rule of writing is that you can't improve it until it's written down. So write that first draft; it's really the only way you'll see the weaker parts of your argument. (The world is also filled with people with terrible ideas who make them available to everyone—but that's a separate problem.)
- **Beta readers are important.** Cultivate a stable of them. The more people you have reading your essays before publication, the better your writing will be. Don't be afraid of criticism. Divorce your ego from your writing. That's the key for accepting criticism, and being able to process and use it; you can't let your ego interfere with hearing what your beta readers are telling you. The way I think of it is that people will criticize my work regardless, but if they criticize a draft, I have the opportunity to fix it before publication. Almost all of my essays have been improved by someone else's comments on an early draft, and some of my essays would have been terrible without those improvements.

When I write a book, it's easy to thank the people who read and commented on it. It's impossible to do the same with essays. So here, in this collection of essays, I would like to thank all the people who have read and commented on essay drafts: David M. Perry, Greg Guerin, Steve Bass, Bill Herdle, David Prentiss, Vicki Laidler, Stephen Leigh, Moshe Yudkowsky, Jon Callas, Doug Whiting, Stefan Lucks, and Jesse Walker. I apologize for any names I inadvertently omitted. I haven't kept a list, and I know I'm not remembering everybody.

So, welcome to my second collection of essays. I think there's something in here for everyone's tastes, as long as their tastes include security: technology and security, economics and security, psychology and security, politics and security. I'm still writing, and will probably publish a third volume of these in five or so years. Thanks for reading.

Bruce Schneier

The essays in this book previously appeared in various publications and may follow the usage conventions of the original publishers.

Carry On

1 The Business and Economics of Security

Consolidation: Plague or Progress

Originally published in Information Security, *March 2008*

This essay appeared as the second half of a point/counterpoint with Marcus Ranum.

We know what we don't like about buying consolidated product suites: one great product and a bunch of mediocre ones. And we know what we don't like about buying best-of-breed: multiple vendors, multiple interfaces, and multiple products that don't work well together. The security industry has gone back and forth between the two, as a new generation of IT security professionals rediscovers the downsides of each solution.

The real problem is that neither solution really works, and we continually fool ourselves into believing whatever we don't have is better than what we have at the time. And the real solution is to buy results, not products.

Honestly, no one wants to buy IT security. People want to buy whatever they want—connectivity, a Web presence, email, networked applications, whatever—and they want it to be secure. That they're forced to spend money on IT security is an artifact of the youth of the computer industry. And sooner or later the need to buy security will disappear.

It will disappear because IT vendors are starting to realize they have to provide security as part of whatever they're selling. It will disappear because organizations are starting to buy services instead of products, and demanding security as part of those services. It will disappear because the security industry will disappear as a consumer category, and will instead market to the IT industry.

The critical driver here is outsourcing. Outsourcing is the ultimate consolidator, because the customer no longer cares about the details. If I buy my network services from a large IT infrastructure company, I don't care if it secures things by installing the hot new intrusion prevention systems, by configuring

the routers and servers as to obviate the need for network-based security, or if it uses magic security dust given to it by elven kings. I just want a contract that specifies a level and quality of service, and my vendor can figure it out.

IT is infrastructure. Infrastructure is always outsourced. And the details of how the infrastructure works are left to the companies that provide it.

This is the future of IT, and when that happens we're going to start to see a type of consolidation we haven't seen before. Instead of large security companies gobbling up small security companies, both large and small security companies will be gobbled up by non-security companies. It's already starting to happen. In 2006, IBM bought ISS. The same year BT bought my company, Counterpane, and last year it bought INS. These aren't large security companies buying small security companies; these are non-security companies buying large and small security companies.

If I were Symantec and McAfee, I would be preparing myself for a buyer.

This is good consolidation. Instead of having to choose between a single product suite that isn't very good or a best-of-breed set of products that don't work well together, we can ignore the issue completely. We can just find an infrastructure provider that will figure it out and make it work—who cares how?

Prediction: RSA Conference Will Shrink Like a Punctured Balloon

Originally published in Wired News*, April 17, 2008*

Last week was the RSA Conference, easily the largest information security conference in the world. More than 17,000 people descended on San Francisco's Moscone Center to hear some of the more than 250 talks, attend I-didn't-try-to-count parties, and try to evade over 350 exhibitors vying to sell them stuff.

Talk to the exhibitors, though, and the most common complaint is that the attendees aren't buying.

It's not the quality of the wares. The show floor is filled with new security products, new technologies, and new ideas. Many of these are products that will make the attendees' companies more secure in all sorts of different ways. The problem is that most of the people attending the RSA Conference can't understand what the products do or why they should buy them. So they don't.

I spoke with one person whose trip was paid for by a smallish security firm. He was one of the company's first customers, and the company was proud to parade him in front of the press. I asked him whether he walked through the show floor, looking at the company's competitors to see if there was any benefit to switching.

"I can't figure out what any of those companies do," he replied.

I believe him. The booths are filled with broad product claims, meaningless security platitudes and unintelligible marketing literature. You could walk into a booth, listen to a five-minute sales pitch by a marketing type, and still not know what the company does. Even seasoned security professionals are confused.

Commerce requires a meeting of the minds between buyer and seller, and it's just not happening. The sellers can't explain what they're selling to the buyers, and the buyers don't buy because they don't understand what the sellers are selling. There's a mismatch between the two; they're so far apart that they're barely speaking the same language.

This is a bad thing in the near term—some good companies will go bankrupt and some good security technologies won't get deployed—but it's a good thing in the long run. It demonstrates that the computer industry is maturing: IT is getting complicated and subtle, and users are starting to treat it like infrastructure.

For a while now I have predicted the death of the security industry. Not the death of information security as a vital requirement, of course, but the death of the end-user security industry that gathers at the RSA Conference. When something becomes infrastructure—power, water, cleaning service, tax preparation—customers care less about details and more about results. Technological innovations become something the infrastructure providers pay attention to, and they package it for their customers.

No one wants to buy security. They want to buy something truly useful—database management systems, Web 2.0 collaboration tools, a company-wide network—and they want it to be secure. They don't want to have to become IT security experts. They don't want to have to go to the RSA Conference. This is the future of IT security.

You can see it in the large IT outsourcing contracts that companies are signing—not security outsourcing contracts, but more general IT contracts that include security. You can see it in the current wave of industry consolidation: not large security companies buying small security companies, but non-security companies buying security companies. And you can see it in

the new popularity of software as a service: Customers want solutions; who cares about the details?

Imagine if the inventor of antilock brakes—or any automobile safety or security feature—had to sell them directly to the consumer. It would be an uphill battle convincing the average driver that he needed to buy them; maybe that technology would have succeeded and maybe it wouldn't. But that's not what happens. Antilock brakes, airbags and that annoying sensor that beeps when you're backing up too close to another object are sold to automobile companies, and those companies bundle them together into cars that are sold to consumers. This doesn't mean that automobile safety isn't important, and often these new features are touted by the car manufacturers.

The RSA Conference won't die, of course. Security is too important for that. There will still be new technologies, new products and new startups. But it will become inward-facing, slowly turning into an industry conference. It'll be security companies selling to the companies who sell to corporate and home users—and will no longer be a 17,000-person user conference.

How to Sell Security

Originally published in CIO*, May 26, 2008*

It's a truism in sales that it's easier to sell someone something he wants than a defense against something he wants to avoid. People are reluctant to buy insurance, or home security devices, or computer security anything. It's not they don't ever buy these things, but it's an uphill struggle.

The reason is psychological. And it's the same dynamic when it's a security vendor trying to sell its products or services, a CIO trying to convince senior management to invest in security or a security officer trying to implement a security policy with her company's employees.

It's also true that the better you understand your buyer, the better you can sell.

Why People Are Willing to Take Risks

First, a bit about Prospect Theory, the underlying theory behind the newly popular field of behavioral economics. Prospect Theory was developed by Daniel Kahneman and Amos Tversky in 1979 (Kahneman went on to win a Nobel Prize for this and other similar work) to explain how people make

trade-offs that involve risk. Before this work, economists had a model of "economic man," a rational being who makes trade-offs based on some logical calculation. Kahneman and Tversky showed that real people are far more subtle and ornery.

Here's an experiment that illustrates Prospect Theory. Take a roomful of subjects and divide them into two groups. Ask one group to choose between these two alternatives: a sure gain of $500 and 50 percent chance of gaining $1,000. Ask the other group to choose between these two alternatives: a sure loss of $500 and a 50 percent chance of losing $1,000.

These two trade-offs are very similar, and traditional economics predicts that whether you're contemplating a gain or a loss doesn't make a difference: People make trade-offs based on a straightforward calculation of the relative outcome. Some people prefer sure things and others prefer to take chances. Whether the outcome is a gain or a loss doesn't affect the mathematics and therefore shouldn't affect the results. This is traditional economics, and it's called Utility Theory.

But Kahneman's and Tversky's experiments contradicted Utility Theory. When faced with a gain, about 85 percent of people chose the sure smaller gain over the risky larger gain. But when faced with a loss, about 70 percent chose the risky larger loss over the sure smaller loss.

This experiment, repeated again and again by many researchers, across ages, genders, cultures and even species, rocked economics, yielded the same result. Directly contradicting the traditional idea of "economic man," Prospect Theory recognizes that people have subjective values for gains and losses. We have evolved a cognitive bias: a pair of heuristics. One, a sure gain is better than a chance at a greater gain, or "A bird in the hand is worth two in the bush." And two, a sure loss is worse than a chance at a greater loss, or "Run away and live to fight another day." Of course, these are not rigid rules. Only a fool would take a sure $100 over a 50 percent chance at $1,000,000. But all things being equal, we tend to be risk-averse when it comes to gains and risk-seeking when it comes to losses.

This cognitive bias is so powerful that it can lead to logically inconsistent results. Google the "Asian Disease Experiment" for an almost surreal example. Describing the same policy choice in different ways—either as "200 lives saved out of 600" or "400 lives lost out of 600"—yields wildly different risk reactions.

Evolutionarily, the bias makes sense. It's a better survival strategy to accept small gains rather than risk them for larger ones, and to risk larger losses rather than accept smaller losses. Lions, for example, chase young or wounded

wildebeests because the investment needed to kill them is lower. Mature and healthy prey would probably be more nutritious, but there's a risk of missing lunch entirely if it gets away. And a small meal will tide the lion over until another day. Getting through today is more important than the possibility of having food tomorrow. Similarly, it is better to risk a larger loss than to accept a smaller loss. Because animals tend to live on the razor's edge between starvation and reproduction, any loss of food—whether small or large—can be equally bad. Because both can result in death, and the best option is to risk everything for the chance at no loss at all.

How to Sell Security

How does Prospect Theory explain the difficulty of selling the prevention of a security breach? It's a choice between a small sure loss—the cost of the security product—and a large risky loss: for example, the results of an attack on one's network. Of course there's a lot more to the sale. The buyer has to be convinced that the product works, and he has to understand the threats against him and the risk that something bad will happen. But all things being equal, buyers would rather take the chance that the attack won't happen than suffer the sure loss that comes from purchasing the security product.

Security sellers know this, even if they don't understand why, and are continually trying to frame their products in positive results. That's why you see slogans with the basic message, "We take care of security so you can focus on your business," or carefully crafted ROI models that demonstrate how profitable a security purchase can be. But these never seem to work. Security is fundamentally a negative sell.

One solution is to stoke fear. Fear is a primal emotion, far older than our ability to calculate trade-offs. And when people are truly scared, they're willing to do almost anything to make that feeling go away; lots of other psychological research supports that. Any burglar alarm salesman will tell you that people buy only after they've been robbed, or after one of their neighbors has been robbed. And the fears stoked by 9/11, and the politics surrounding 9/11, have fueled an entire industry devoted to counterterrorism. When emotion takes over like that, people are much less likely to think rationally.

Though effective, fear mongering is not very ethical. The better solution is not to sell security directly, but to include it as part of a more general product or service. Your car comes with safety and security features built in; they're not sold separately. Same with your house. And it should be the same with computers and networks. Vendors need to build security into the products

and services that customers actually want. CIOs should include security as an integral part of everything they budget for. Security shouldn't be a separate policy for employees to follow but part of overall IT policy.

Security is inherently about avoiding a negative, so you can never ignore the cognitive bias embedded so deeply in the human brain. But if you understand it, you have a better chance of overcoming it.

Why Do We Accept Signatures by Fax?

Originally published in Wired News*, May 29, 2008*

Aren't fax signatures the weirdest thing? It's trivial to cut and paste—with real scissors and glue—anyone's signature onto a document so that it'll look real when faxed. There is so little security in fax signatures that it's mind-boggling that anyone accepts them.

Yet people do, all the time. I've signed book contracts, credit card authorizations, nondisclosure agreements and all sorts of financial documents—all by fax. I even have a scanned file of my signature on my computer, so I can virtually cut and paste it into documents and fax them directly from my computer without ever having to print them out. What in the world is going on here?

And, more importantly, why are fax signatures still being used after years of experience? Why aren't there many stories of signatures forged through the use of fax machines?

The answer comes from looking at fax signatures not as an isolated security measure, but in the context of the larger system. Fax signatures work because signed faxes exist within a broader communications context.

In a 2003 paper, *Economics*, *Psychology*, *and Sociology of Security*, professor Andrew Odlyzko looks at fax signatures and concludes:

> *Although fax signatures have become widespread, their usage is restricted. They are not used for final contracts of substantial value, such as home purchases. That means that the insecurity of fax communications is not easy to exploit for large gain. Additional protection against abuse of fax insecurity is provided by the context in which faxes are used. There are records of phone calls that carry the faxes, paper trails inside enterprises and so on. Furthermore, unexpected large financial transfers trigger scrutiny. As a result, successful frauds are not easy to carry out by purely technical means.*

He's right. Thinking back, there really aren't ways in which a criminal could use a forged document sent by fax to defraud me. I suppose an unscrupulous consulting client could forge my signature on a non-disclosure agreement and then sue me, but that hardly seems worth the effort. And if my broker received a fax document from me authorizing a money transfer to a Nigerian bank account, he would certainly call me before completing it.

Credit card signatures aren't verified in person, either—and I can already buy things over the phone with a credit card—so there are no new risks there, and Visa knows how to monitor transactions for fraud. Lots of companies accept purchase orders via fax, even for large amounts of stuff, but there's a physical audit trail, and the goods are shipped to a physical address—probably one the seller has shipped to before. Signatures are kind of a business lubricant: mostly, they help move things along smoothly.

Except when they don't.

On October 30, 2004, Tristian Wilson was released from a Memphis jail on the authority of a forged fax message. It wasn't even a particularly good forgery. It wasn't on the standard letterhead of the West Memphis Police Department. The name of the policeman who signed the fax was misspelled. And the time stamp on the top of the fax clearly showed that it was sent from a local McDonald's.

The success of this hack has nothing to do with the fact that it was sent over by fax. It worked because the jail had lousy verification procedures. They didn't notice any discrepancies in the fax. They didn't notice the phone number from which the fax was sent. They didn't call and verify that it was official. The jail was accustomed to getting release orders via fax, and just acted on this one without thinking. Would it have been any different had the forged release form been sent by mail or courier?

Yes, fax signatures always exist in context, but sometimes they are the linchpin within that context. If you can mimic enough of the context, or if those on the receiving end become complacent, you can get away with mischief.

Arguably, this is part of the security process. Signatures themselves are poorly defined. Sometimes a document is valid even if not signed: A person with both hands in a cast can still buy a house. Sometimes a document is invalid even if signed: The signer might be drunk, or have a gun pointed at his head. Or he might be a minor. Sometimes a valid signature isn't enough; in the United States there is an entire infrastructure of "notary publics" who officially witness signed documents. When I started filing my tax returns electronically, I had to sign a document stating that I wouldn't be signing my income tax documents. And banks don't even bother verifying signatures on