HACKING WORK

BREAKING STUPID RULES FOR SMART RESULTS

Bill Jensen and Josh Klein

PORTFOLIO PENGUIN

PORTFOLIO PENGUIN
Published by the Penguin Group
Penguin Group (USA) Inc., 375 Hudson Street,
New York, New York 10014, U.S.A.
Penguin Group (Canada), 90 Eglinton Avenue East, Suite 700,
Toronto, Ontario, Canada M4P 2Y3
(a division of Pearson Penguin Canada Inc.)
Penguin Books Ltd, 80 Strand, London WC2R 0RL, England
Penguin Ireland, 25 St. Stephen's Green, Dublin 2, Ireland
(a division of Penguin Books Ltd)
Penguin Books Australia Ltd, 250 Camberwell Road, Camberwell,
Victoria 3124, Australia
(a division of Pearson Australia Group Pty Ltd)
Penguin Books India Pvt Ltd, 11 Community Centre, Panchsheel Park,
New Delhi – 110 017, India
Penguin Group (NZ), 67 Apollo Drive, Rosedale, North Shore 0632,
New Zealand (a division of Pearson New Zealand Ltd)
Penguin Books (South Africa) (Pty) Ltd, 24 Sturdee Avenue,
Rosebank, Johannesburg 2196, South Africa

Penguin Books Ltd, Registered Offices:
80 Strand, London WC2R 0RL, England

First published in 2010 by Portfolio Penguin,
a member of Penguin Group (USA) Inc.

1 3 5 7 9 10 8 6 4 2

LIBRARY OF CONGRESS CATALOGING IN PUBLICATION DATA
Jensen, Bill, date.
Hacking work: breaking stupid rules for smart results / Bill Jensen and Josh Klein.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-59184-357-3
1. Organizational effectiveness. 2. Creative thinking. 3. Problem solving. I. Klein, Josh, date. II. Title.
HD58.9.J463 2010
650.1—dc22
2010017336

Printed in the United States of America
Set in Whitman
Designed by Pauline Neuwirth, Neuwirth & Associates. Inc.

Dedication

To the underground army of benevolent hackers
who are saving business from itself,
one bad act at a time.
—Bill and Josh

To my folks, for giving me the courage to love what I do and to do what I love. They taught me to hack the right way—with courage and respect—and I thank them for it.
— Josh

Contents

PREFACE

PSSSSSST . . .

For several years we have foraged in the back alleys of business, arranging clandestine meetings with the bad boys and girls of work. Empty cans of Red Bull, pizza crusts, and shredded nondisclosure agreements littered our meeting places.

"Psssssst. How do you *really* get everything done? What are your work-arounds? The ones that keep your company afloat, keep customers happy, teammates employed, and keep you doing your best? We want the world to know about the power of benevolent hacking."

Who are we, and why do that? We're just two guys who have dedicated our professional lives to finding work-arounds to corporate bullshit.

Bill's day job is making it easier to get stuff done. Over the course of two decades, he has asked over five hundred thousand people around the world what makes their work so hard and complicated. C-suite dwellers love his findings on simplicity. Bill advises executives and their troops on how to work smarter by making work simpler. He has consulted with many of the biggest companies in the world, local and federal governments, even the U.S. Navy SEALs.

But Bill's most important advice has always hit a brick wall. His

research has consistently found that the number one source of work complexity is built into every company's infrastructure—the tools and processes we are supposed to use to get our work done. They are designed to help the *company* succeed but are not built for the success of the *individuals* who do the work.

Business's failure to deal with this obvious problem is one of its biggest problems. Yet the reaction from most graybeards has been decidedly chilly: "Let's not go there."

"Arrrrgh! How do I get these people to listen?" Bill wondered. Addressing this problem would be game changing . . . a true competitive advantage for every company and the end of so much frustration and wasted effort for every individual.

The answer finally appeared over drinks at a TED (Technology, Entertainment, Design) conference. "Change the approach," said Josh, who had just presented how he had hacked the work ethic of crows by training the birds to bring him money. "If their executives won't listen, let's show employees how to hack around their problems."

From his early days of snarfing Wi-Fi passwords in Seattle to his recent consulting work with U.S. intelligence agencies, Josh has been hacking technologies and putting them back together to great effect. Some years ago, he noticed that this kind of systems thinking could be applied to people and organizations, not just to technology.

As he helped companies all over the world make the most of their technologies, Josh saw firsthand how unwilling people are to question what they take for granted—and how powerful it can be to do so. From megacorporations to start-ups, from investors to students, he found that while everyone talked about innovation, few were willing to pull the trigger that would kill an old business model or to embrace the changes that would create a new one.

Josh's constant questioning of the status quo helped him publish a novel by giving it away for free, got him invited to speak at the most hard-to-access conference in the world by telling them what they were doing wrong, and enabled him to double his salary by quitting his job.

Between Josh's tech savvy and Bill's business background, our back-alley conversations produced straight talk from thousands of people. From those on the front lines serving customers to the geeks in corporate server closets, the workforce told us what they're not telling their bosses.

This book is a tough love letter: There's an underground army of benevolent hackers out there who are saving business from itself, one bad act at a time. This is their story.

Ours: Two guys hacking the future, one day at a time. Finding better ways to get stuff done and having fun along the way.

BILL@HACKINGWORK.COM
JOSH@HACKINGWORK.COM

W00T!

We are exposing the cheat codes for work and sharing them with the world.

Once employees know how to hack their work, everything's up for grabs—how we work, when and where we work, how we define effectiveness and success . . .

Everything.

Benevolent hackers see the future and pull us toward it, in whatever ways work best.

W00t! Expression of joy and excitement '80s hackers used to disguise that they had gained root access—(the most fundamental level of control)—to someone's system. Root was replaced with w00t!

1

SAVING BUSINESS FROM ITSELF, ONE BAD ACT AT A TIME

If you think you are too small to be effective, you have never been in bed with a mosquito.

—Betty Reese, American pilot

Business is broken. We all know it, even if we're scared to admit it.

Most of us feel screwed, and many of us feel helpless to change it. We have become slaves to our infrastructure—to business's controlling tools, procedures, and mandates. Something's got to give. Something already has.

Richard Saunders is living proof. He works for one of the top banks in the world. One of those institutions that did its job so well in 2008 that it helped dig us into the worst financial hole we've been in since the Great Depression. Yeah, one of those firms.

Richard's job is to provide the bank's clients—law firms and courts holding over $50 million in escrow for their clients—the reports they need to keep track of all those assets. His team takes thousands of different statements and consolidates them all into simple, easy-to-read reports for clients. It's like drinking from a fire hose so others don't have to.

Then there's his work for the senior team. As the crisis unfolded, they wanted their own custom-made distillations—lots of them. The problem was that nothing in this growing data stream helped serve clients better, increased the value of service provided, or predicted catastrophes. They were just more detailed rearview mirrors the executives used to calm themselves with the illusion of greater control. Even worse: What the execs *really* wanted—useful, insightful analysis—couldn't be easily produced using the software provided by corporate IT.

Poor Richard. What to do? Work twenty-nine hours a day, ten days a week, to manually create these reports and the much-needed analysis? Get stressed out, skip family time—all to soothe the shattered nerves of his senior execs? No way. He hacked the system.

Knowing that the software was written in the programming language Visual Basic and connected to a simple database, he used Microsoft Access to link to the database's back end. Getting the database password was easy enough. "I just called the software vendor," Richard says, "softened him up, and he readily gave it to me. Once I had that, I was able to tap into the database and pull all the data I needed—and make massive changes on the fly."

Would the bank's auditors and IT security guys freak out if they knew that Richard had hacked their system and had almost full access to all customer data? You bet. But since his hack, Richard has become incredibly productive and is the companywide authority on these types of accounts. He's now the go-to hero with all those senior execs because he's been able to give them a lot more than just data dumps—and he's preempted a ton of problems for clients along the way.

If they only knew the full story. Says Richard (not his real name, of course), "As a result of this hack, I keep senior management off our backs, so we're able to keep doing more for our clients with less."

He's not alone in believing that he has to change the rules for getting things done if he's going to increase his productivity and achieve

better results for the firm. Many in our workforce are coming to the same conclusion.

Evers Pearce, a university employee in Oxford who had his budget slashed to nothing, is another example. Instead of accepting this edict, he funded his projects with £37,000 by selling on eBay what he was supposed to be throwing away—furniture, engine parts, construction waste—and wrangled the income back into the finance system.

Elizabeth is a manager whose bosses would not approve her customer satisfaction project—even though the entire senior team deemed it crucial—because the payoff wouldn't be realized for at least four financial quarters. So she secretly videotaped customers voicing their complaints as well as their wish lists for enhancing the company's product lines and posted it on YouTube. Within days, there was enough public outcry that senior management reversed their decision and approved her project.

One new hire, Matt, so disagreed with his employer's assessment process that he Googled "performance assessment" and created a seventeen-question mash-up that matched *his* career goals—not just the company's goals for him. His manager and the HR department were shocked and pissed off, but he had spent months refining his performance tool. He'd done his homework, seeking advice from one of the gurus in the assessment field whom he'd contacted through LinkedIn. With the support of his co-workers, Matt stood his ground, and management ended up using his assessment in conjunction with their own.

What's even more telling about this challenge to the status quo is that it came in the midst of an economic crisis and a horrible job market. "My career path and my future can't be just about keeping *this* job," says Matt. "It's the mix of projects I work on, and how I improve my own performance at each successive job. I'm better at what I do—for my company and customers as well as for me—because I hacked their assessment process and helped create one that worked for *me*."

These are not isolated incidents.

Change is coming, and it's coming in every workplace, in every industry, from every generation across the globe.

We're outing the biggest open secret of the working world: Today's top performers are taking matters into their own hands. They are bypassing sacred structures and breaking all sorts of rules just to get their work done.

We're exposing the cheat codes for work and sharing them with the world.

Every day in every workplace, benevolent rule breakers like these are ensuring that business succeeds despite itself. They are reinventing how to approach productivity and how to consistently achieve *morebetterfaster* results.

They're hacking work, and you can, too.

Business's love of lingering bureaucracy, legacy technologies, and deeply embedded procedures is killing us. More and more of us are finding that our work tools and structures are completely out of sync with what we need to do our best. Most of our daily needs, dreams, desires, and goals are far ahead of our employers' technological, procedural, and social adoption curves.

The bad guys in this story are not economic turmoil or traumatic market shifts; nor are they your boss or even your company. The bad guys are the tools, processes, procedures, and structures we all use to get work done.

Business's infrastructure is not keeping up with us. That which was supposed to help us now dictates too much of what we *can't* get done. Our tools have become more bossy than our bosses.

What makes this story so urgent and timely isn't just what a pain in the ass all this is, or even that it's costing us our jobs—it's that it's so devastating at the same time there are quantum leaps everywhere *but* work. Even though business spent $1.5 trillion on info tech in 2010,[1] the tools we have outside of work are leapfrogging past what we use on the job.

When a twelve-year-old can gather information faster, process it better, reference more diverse professionals, and get volunteer guidance from better sources than you can at work, how can you pretend you're competitive? When you have more empowering tools in your mobile phone for your personal use than what your company provides or approves for your projects—how can you work within, or be saved from, devastating market forces?

You can't.

So what *can* you do? Start hacking.

Start taking the usual ways of doing things and work around them to produce improved results. Bend the rules for the good of all. That's what benevolent hackers do.

What was once shunned as bad is now the new good, because it challenges outdated tools and procedures that refuse to budge. We've uncovered what nobody wanted you to know: You no longer have to play the game the way your company insists you do. The illusion of corporate control is being shattered in the name of personal efficiency.

Once employees know how to hack their work, everything's up for grabs—how we work, when and where we work, how we define effectiveness and success . . . everything.

Want to work smarter, not harder? Start hacking.

Want to be a better manager, leader, or entrepreneur? Embrace the hackers around you and learn from them.

Want to leave a legacy and make a real difference? Start hacking.

Benevolent hackers are on a mission: to save business from itself, and you from business.

Come join our thriving underground army of heroes. You will hack work-arounds big and small, high-tech and no-tech, risky and safe, enduring and ephemeral. You will improve the productivity of your company, yourself, and everyone you touch.

2

YOU WERE BORN TO HACK

Dare to be naïve.

—R. Buckminster Fuller, architect and futurist

THERE IS NO THEM, ONLY US

Have you ever called the person in charge of a process and negotiated an exception to a deadline or a rule? How about emailing a company file to yourself at a personal address just so you could work on it at home? Have you ever bent the rules just to check off more to-dos? If the answer is yes, would you say you were more efficient and effective because of it?

Then you're a hacker.

You were born to hack. All children are.

That's because hacking is the act of understanding a system well enough to take it apart, play with its inner workings, and do something better with it. This desire to disassemble and improve is natural and built into all of us. Most children are fascinated with figuring out how innovation and creation work, and it all begins by taking things apart.

SMARTSTART

HACKING WORK DEFINED

Hacking work is forbidden innovation. It is the act of getting what you need to do your best by exploiting loopholes and creating work-arounds. It is taking the usual ways of doing things and bypassing them to produce improved results.

Hacking work is getting the system to work for you, not just the other way around . . . making it easier to do great work.

Benevolent hackers see the future and pull us toward it. Every day in every workplace, hackers are the heroes who ensure that business succeeds *despite* itself. Their innovations plug the holes in business's strategies, structures, tools, and processes with work-arounds. Their efforts change bureaucracies into meritocracies—with or without permission.

Bill began by disassembling his favorite toy, Mr. Machine, and too many of Mom's appliances to name. Later, he figured out how to hack systems of authority, like using the principal's office and budget to organize and fund Senior Cut Day in high school. Josh figured out the authority thing a little earlier. At age seven, he hacked the tooth fairy. His hacker's note explained that because of inflation, the price of teeth had just risen from a quarter to a dollar. His parents still have the tooth and note, documenting how he reworked the fairy's decision-making process.

Think back. Surely you have similar stories. It may have been reinventing your mom's favorite recipe, reprogramming the family's electronics, or redesigning the routines behind your allowance to yield the highest reward for the least effort. This is what children do. They hack to learn, to grow, to imagine completely new possibilities. It's a natural approach, and it works. Taking something apart and

reconstructing the pieces has long been shown to be one of the most effective ways to master any subject.

Unfortunately, most of us grew up. That is, we came to accept that hacking things was the wrong way to learn. The right way is to sit in neat little rows, keep quiet until called upon, raise our hand to speak, and always, always follow a planned, predictable process laid out by an authority figure.

Hacking, bad. Tsk, tsk. Learning by following the rules and paying attention to the boss at the head of the class, good. Gold star!

GREAT HACKERS NEVER GROW UP

The best hackers among us never stayed within the lines of their coloring books. They never allowed childlike wonder to be squeezed out of them. From kindergarten through university and now in the workplace, these hackers can't figure out why anyone would give up digging their fingers into everything just to learn how things work and how they could be changed. That's core to any hacker's drive: unleashing the untapped potential in everything; reworking the status quo so it works better.

In our workplace, that means removing barriers that slow us down and frustrate us, giving us more power to do what needs to be done. Benevolent hackers are the personification of all that is good in our workforce. Against all odds, they *will* find a way to do their best.

Among the most successful hackers, the alpha geeks, this is a natural proclivity that just can't be denied. They are a passionate lot, and what they do at work and play is just a side effect of that passion.

That's how Josh was once given a brand-new Mac by a friend.

"What's wrong with it?" he asked.

"Nothing," was the matter-of-fact reply.

And that was the problem. The operating system was reliable

enough that there was nothing to fix, and the hardware was sturdy and well constructed, so there was no need to take it apart. Where's the fun in that? To an alpha, that's a dead end. To this day, Josh's friend still runs Windows. Lots to fix there!

Whether you're an alpha geek, an occasional dabbler, or a corporate minion who desperately needs to get out of bureaucratic purgatory, the motivation to hack always falls within the same categories:

Curiosity: "I wonder what would happen if . . ."
Imagination: "Gee, wouldn't it be cool if . . . ?"
Drive: "I will not accept 'no.' There has got to be a better way!"

This is what makes hacking work so powerful and necessary. Our bosses are too busy trying to figure out how to get their companies out of death spirals to rethink their work designs. Enter you: full of childlike wonder and enthusiasm, and—most important—with the on-the-ground experience needed to solve problems that are plaguing us all. You're just the kind of hero business needs, especially if it's too stuck in its ways to know it.

That's an important principle to remember as you think about hacking work. Hacking doesn't have to begin with a solution in mind. You don't necessarily have to have the right answer, nor does business necessarily have the wrong one. Hacking begins with "What if . . . ?" and "I wonder why . . ."

Hacking works because it's not really about your boss or bureaucracy or that stupid procedure. It's you standing on a chair with a blanket for a cape, leaping off with the confidence that you're about to fly into the world of unlimited possibilities!

EVERYBODY EVERYWHERE HACKS

Let's begin our relationship with complete honesty: You are no virgin when it comes to this stuff. You've been hacking for years.

And you're not the only one who hacks. So does he, she, us, them, the young and the old, the über-elite and the clueless, the slackers and the fast trackers. . . . Everybody everywhere hacks.

New technologies have so radically changed the social, cultural, and economic landscape of human connections that, increasingly,

SMARTSTART

WHY HACK: WIIFM?

What's in it for me if I hack or if I embrace the hackers within my firm?

Individuals Win:

- Easier to do great work
- Greater control over your own destiny
- Truly working smarter, not harder . . . tailoring a lot more to your individual needs
- Better qualified in your own job. . . less dependence on your company's survival
- Better sex, longer life, more meaningful relationships
- More fun

The Company Wins:

- Easier for every individual to do great work: which translates into . . .
- Unleashes everyone's capacity, creativity, innovations: which translates into . . .
- *Morebetterfastercheaper:* which translates into . . .
- Creates new and sustainable competitive advantages
- Reinvents your relationship with your workforce: much more symbiotic win/win
- Did we mention *morebetterfastercheaper*?

everyone participates as hackers: Are you looking for a picture of a mermaid on roller skates to use in a presentation? Use Flickr! Want the best deal on a new product? Use RetailMeNot, BuyWithMe, Ebates, or Stingier! Want to run for president of the United States without owing your soul to special-interest groups? Bypass how it's usually done and go directly to the masses for millions of $25 donations! Want to max out your 64 GB iPod Touch? Find what you need on ThePirateBay or Spotify or use your (or your kid's) university's free file-sharing system!

It's finally OK to admit it. Whether it's how you used a social connection or how you scored those tickets or that latest discount or freebie: You are a hacker. There are no non-hackers, only those who prefer to be perceived that way.

The global economy is moving so fast that most of its established systems can't keep up. That, combined with new technologies, creates opportunities to be exploited by everyone everywhere: Hacking any system that is too slow, too bureaucratic, too unresponsive, or too costly is now part of the global economic engine.

It began with hard-core geeks who wanted to learn whatever could be learned. Their guiding principle: Information wants to be free.

All knowledge is good. The only rule was, "Don't be a dick." If that meant sharing a codec so that any DVD can be watched anywhere or sharing backdoors into a car's computer system to improve its suspension—so be it. And if the masses benefit by making this information easily available . . . well, that's just being a good global citizen, right?

Now this practice has been mainstreamed. It's no longer just geeks who hack corporate systems. It's the founder of a three-person business in a small town you've never heard of halfway around the world, who believes she can take market share from the industry leader. She Googles "Google hacks" and instantly gets an extensive list of one-line queries she can use to study her competitors' client contacts, patent filings, contract documents, purchase orders, and more.

If mission-critical information like this is as easy to find as asking

Google, why should businesses be surprised that you—one of their star performers—would be cocky and brazen enough to hack your own workplace?

They shouldn't be. As a matter of fact, they put hacking in play and set the example for you years ago.

Employers have been hacking *your* systems since birth—every time they wanted to sell you something. Viral marketing was used to influence your mom to buy a specific diaper or detergent. Later, those same companies used your social network and the data they collected about you online to make you believe that their jeans or beer or mobile phone or sneakers were so cool that you just *had* to buy them. Then they created phone trees that use lots of your time instead of their customer service rep's, because that's more cost-effective for them. Even debt collectors are tapping into your Facebook page to monitor any purchases and finances you discuss with friends.

The list is endless—you have been hacked by somebody's employer your whole life! All in the name of their bottom line and market share.

It's time to hack back. After all, if it's good for them, it's good for you—turnabout is fair play.

SIDETRIP

A SHORT HISTORY OF HACKING'S JOURNEY FROM GOOD TO BAD TO GOOD

Hacking began as a very good thing. It borrowed its name from **1960s** MIT students—members of a model train group who modified trains, tracks, and switches to make them perform better. They later hacked MIT's mainframe computer to improve its performance, which is how the term *hacking* became associated with techies and their exploits.

(continued)

1970s: Phone "phreakers" discovered that a cheap whistle produced a 2,600 Hz sound that allowed free calls over AT&T's long-distance switching systems. Among the perpetrators who built "blue boxes" for free calls: college kids Steve Wozniak and Steve Jobs, future founders of Apple Computer.

1980s: The 1983 movie *WarGames* showed that anyone could break into any computer. Hackers become mainstream bad guys. Many gleaned an additional message from the film: Hacking gets you girls. Hacking takes off. In 1986, West German and KGB operatives try to break into U.S. government systems through University of California computers. And between 1988 and 1995, there was a major crackdown on the explosion of malicious hacks.

1990s: Hacks and hacking tools explode as the Internet makes everything available to everybody. Malicious hacks—"spoofing," "phishing," and worse—continue through the present day, but there's also a resurgence of good hacks. Many renew hacking's original mission: to improve overall performance.

2000s: By the end of the decade, hacking has both regained its luster as a good thing (White Hat Hackers) and attracted more bad people (Black Hatters—from script kiddies to the Russian mafia). There are also Gray Hatters, who expose vulnerabilities in systems in order to improve them, with no malicious intent. This book is an example of a Gray Hat hack.

3

WHAT'S NEW, WHAT'S NOT, WHAT'S THE MOST COMMON HACK?

> Discovery consists of seeing what everybody has seen and thinking what nobody has thought.
>
> —Heraclitus, Greek philosopher

HACKING WORK IS NOT NEW

Hacking work has been a hallmark of success since the very first bureaucracy—from Archimedes to Galileo to the Founding Fathers, breaking and reinventing the rules is the foundation for innovation.

Agriculture was most likely a work hack: Instead of always roaming over the next hill every time the clan needed grain, someone cleverly figured out that they could grow it closer to camp. Gronk, their leader, neither asked for nor approved this change. And his head of manufacturing—Club and Spear Guy—most certainly felt threatened. The clan's operations would have to change to meet the needs of its new farmers. Still, some hacker found a more efficient way to feed everyone and human history was forever changed.

Commerce, arts, sports, education, war, agriculture, medicine, and government have all been pushed forward by hackers. Thousands

of years after Gronk, farmers were having a tough time plowing their soil, so John Deere hacked a work-around by forging the first steel plow out of a saw blade. During World War I, French, German, and American ace fighter pilots stormed into factories and hacked the production of planes, working backward from the needs of the pilot. Their hacks pushed the aviation industry out of its infancy. The history of hacking *is* the history of innovation.

The art of hacking has now crept into most every aspect of society.

There are life hacks, for those who want work-arounds for living a simpler life. There are instruction manual hacks—if it weren't for the *Harry Potter* series, the *Dummies* books would rank among the world's best sellers.

Do-it-yourselfers are reworking nearly every product to meet their own needs. For example, "I look at Ikea more as a hardware store or as a component store than as a place that sells items," says Randall Kramer, a Chicago-based furniture designer. "I see many of the things they sell as a building block. It's not that they've dropped the ball—it's like they left it for you to individualize or customize it."[1] Even the lowly calculator has a dedicated base of hackers who build their own versions of Whac-A-Mole, Tetris, or new operating systems into their devices. "It's all about taking a limited device and doing the impossible with it," says hobbyist Brandon Wilson.[2]

WHAT IS NEW: THE OPENNESS AND AUDACITY TO EMBRACE SMALL BAD ACTS AS THE NEW GOOD

Originally, we thought this book would be about Gen Y, the Millennials. We know that this generation of hackers already has back-of-the-hand knowledge with many tools to do things their parents and managers never tried or imagined, and as soon as they hit critical mass in the workforce—*wham* . . . watch out!

We still see them as a force to be reckoned with (see chapter 8),

but the deeper we dug, the more obvious it became that hacking work is not just a Young Turk thing. It's a massive, ongoing, leaderless underground response to feeling screwed.

We met with every generation currently working, in almost every industry, and found a pervasive and universal problem: The design of work isn't meeting the needs of the people who do the work. And nobody's happy about that!

What's changing—and why now is the time to release your inner hacker—is a growing openness about challenging the tools and procedures we're handed. Boomers and X'ers are seeing Millennials hack what's broken and then share what they changed with their friends. That open sharing of hacks among teammates wasn't happening until very recently.

As Microsoft founder Bill Gates said at a recent TED conference: "There are some very important problems that don't get worked on naturally. . . . The market does not drive the scientists, the communicators, the thinkers, the governments, to do the right things. And only by paying attention to these things, and having brilliant people who care and draw other people in, can we make as much progress as we need to."

The new openness around hacking work makes it possible to draw in brilliant people like you to fix what market forces aren't fixing.

The market doesn't care that corporate IT is more of a barrier to you than an enabler. (That includes many of Gates's own products.) The market doesn't care that HR is still living in the 1950s, shoving one-way assessment tools down your throat. The market doesn't care that your manager sucks or that she's in your way or that she can't build a team. The market simply doesn't work on problems at your level.

And that's why hacking is so powerful. That's why it works. That's why it's coming out of the closet now. Hacking fixes many of business's chronic problems that wouldn't have been fixed otherwise.

That idea is spreading. A recent conference on educational reform

was titled "Hacking Education," and a session at the 2010 Davos World Economic Forum was titled "Hacking Management." Hacking as a positive force for change has come of age.

TODAY'S MOST COMMON HACK

Need more of a nudge to draw outside the lines and start breaking some rules? Just consider how many corporate rules were made to be broken because they needlessly make your life harder. For example, Andy's company uses Microsoft's SharePoint servers, and his bosses insist that all presentations be delivered in PowerPoint. Trouble was, when Andy needed to collaborate with others on PowerPoint slides, it took forever to upload to SharePoint and then another chunk of forever to download from it. Every presentation began with the same collective groan: "Pain in the ass!"

While home from college one weekend, Andy's son showed him how to use Google Documents. What a difference! Now Andy's teammates do all their work collaboratively, from work or home or while on the road—easily, quickly—and save it to PowerPoint only at the last minute, just in time to upload to the SharePoint server. "We do this all the time to make presentations to bosses whose brains would explode if you don't use PowerPoint," says Andy. "No one's ever the wiser."

Once they got comfortable bypassing corporate IT, his team went even further. They now use Google's social media, Buzz, for most of their team updates and on-the-fly meetings.

Andy's story tracks perfectly with one of the most common hacks we found: jumping IT's firewall and working around their restrictions and tools in open computing environments, then bringing the work back over the firewall and presenting it to bosses as if the corporate tools had actually been used.

All this is necessary because the tools that so many of us are given to use are corporate centered—designed to help the company

succeed, but not necessarily designed for our needs. However, the universe of tools available to us in the outside world, like Gmail and Google Docs and iPhone apps, are user centered—easily customized for each individual's needs. (We'll dive into this problem in a lot more detail in chapter 7.)

SMARTSTART

THREE KEY TAKEAWAYS

1. **Hacking work is not new.**
2. **What is new** is the audacity to openly embrace hacking as an **amazing innovation engine** to solve business's most chronic problems. But no matter how benevolent the end result, what makes a hacker a hacker is bypassing, reworking, and bending the rules that keep you from doing your best. Standard operating procedures be damned.
3. **Hacking work is not just for techies:** You don't need to be a techno-geek to do a great hack. While many hacks do require technological work-arounds, some of the best solutions involve simple changes in relationships and sharing information differently, using tools you already have.

SMALL, LOW-TECH WORK-AROUNDS: BIG RESULTS

Lots of valuable hacks involve only tiny changes. They can be low-tech and low-risk and still create big results. Sean's story is a perfect example. His hacks are neither extraordinary nor revolutionary and mostly involved changes in relationships. But his work-arounds saved his sanity, his soul, and many jobs.

Sean works for a major telecom company, creating computer training for their billing systems, project management, and knowledge-sharing tools. Eight years ago, his team knew they would function best within HR, but the gods of corporate structures knew better, so they got stuck reporting to the CIO.

During an org chart shuffle, a new CIO showed up with plans to reduce spending. Danger, danger: Layoff alert! If Sean had been a typical midmanager, many of his team members would have been on their way out the door. Fortunately for them, Sean is a hacker.

He convinced the CIO that a great way to reduce his budget would be to off-load Sean's team onto HR, and he then dangled a carrot in front of the head of HR. With his team reporting to her, she could increase her ability to impact the company's bottom line.

Hacking Round 1: Two relationship work-arounds, resulting in multiple jobs saved.

A while later, Sean's team was told to stop working on one of their ongoing projects—it was in direct conflict with what the CIO had hired an outside consulting firm to do. Sean asked if they could finish a simple prototype at zero cost and use it to gather feedback to be passed on to the consultants. A year later, the CIO's officially sanctioned project was canceled, having produced not a single result, and Sean's "prototype" was already widely adopted throughout the company. Six years after that, Sean's team's work is still in use.

Hacking Round 2: A process work-around. Prototyping the program was just a ruse. Sean knew that once users had access to his team's program, it would take off. Just as in the outside marketplace, where people are clamoring for solutions *now*, a hacker's ability to gain rapid adoption of his ideas can outmuscle and outlast lesser solutions from corporate.

Then came the economic meltdown. All of Sean's spending was suspended until further notice. In his own words: "With a large team, a pile of commitments to internal customers, and no money for anything but salaries, I kept thinking: What are we going to do

now? After lots of agonizing, it hit me. A better question is: What are we *not* going to do? For the first time in years, I'm free to say no to the mind-numbing, soul-sucking projects that we foolishly agreed to do when we thought saying yes to everything was the best way to survive. My team is now focusing on the projects most likely to succeed and delivering real value for the organization. The bad economy has actually set up our next adventure!"

Sean didn't commit heresy. He didn't set out to free the proletariat or consciously break the rules or piss people off. He just couldn't accept the status quo and had to find work-arounds. That's all that hacking is: getting what you need to do your best by creating work-arounds that produce better results.

But, boy, did he succeed! During the past eight years, he saved his teammates' jobs as well as his own, and together they saved a business from itself by outperforming a CIO and his high-priced consultants. That last result cannot be overstated. Even if his boss won't happily admit it, in this one case Sean served the entire company better than the CIO did. Great hacking is not about saving yourself at the expense of the company. It's about saving yourself *and* the company!

Finally, faced with dire financial restraints, Sean donned a blanket for a cape, stood on a chair, and leapt off into a world where it's possible to say no to a lot more stupid work!

Extraordinary results from ordinary work-arounds. That's the power that's in your hands right now.

WORKING AROUND POWER STRUCTURES

Hacking work is happening in all kinds of workplaces. LeeAnne Del Rio is a teacher trying to change the educational system. In her own words: "There are lots of us out there supporting the efforts of LISTA [Leaders Imagining Solutions Through Action] to wean students off the quiz-for-the-right-answer approach and teach them to trust their brilliance to figure out a lot more on their own. Our goal

FASTHACKS

WORK-AROUNDS FROM THE FIELD

Changing the Rules from Raveena, a corporate trainer who confides to her trainees that because of budget constraints, much of what she provides "sucks." So she sends her trainees to free online sources outside of the company. Then, after testing them on what they learned, she validates their certificates in required courses they never attended. Result: They consistently learn more this way.

Jumping the Firewall from a team at one of the world's largest credit card companies that secretly hosts some of its information on outside servers. (Don't worry, there's no secure customer data outside the firewall—only internal information the team members need to do their jobs.) Nobody listened to their complaints that IT's restrictions hurt their ability to meet their deadlines and accountabilities. So several years ago, they hacked a work-around. Since then, their senior execs hold them up as examples of what can be done with decreased

is big changes. But in the meantime, I have to keep my job and pay my bills."

As a part-time sociology instructor at a community college, LeeAnne often found that she was left out of the departmental loop. Even though part-timers make up 75% of the teachers at most colleges in California, they don't get invited to faculty meetings, take part in board meetings, or become involved in departmental decision making. Denied the opportunity to make a real difference within the system, LeeAnne took matters into her own hands.

"With no authority or permission to do so, I started a Web page and online community for sociology and psychology instructors to share resources and syllabi, communicate ideas, and chat. Everyone

resources and budgets. If they only knew what had to be done to deliver those results.

Expense Report Makeover from Danny, who was tired of carrying pockets full of receipts while traveling for business. What made it worse was the six to eight hours a month he had to spend doing his expense reports according to his employer's policies. This receipt had to be handed in a certain way, that form had to be filled out in a certain way. He said, "This is crazy. You're reducing my billable client time by eight hours a month. Here . . . I run my financial life on Mint.com. I already did this work once, for myself. Here's a one-page printout that has everything you need." Now, rather than save receipts he just orders up duplicate sets to match his expenses from SalesReceiptStore.com, a service that prints and mails receipt copies for expense reports. Then he attaches them to the one-pager from Mint.com and submits them to accounting. He's been reimbursed correctly and quickly ever since. Net/net: He gets reimbursed *and* he eliminated two hours of stupid-work per week.

in those meetings that I was excluded from started coming to me. Now I'm a consultant to the college, helping them accomplish the same kind of community building and sharing with all faculty—both full- and part-time."

Even in the most bureaucratic and hierarchical situations, there's always a work-around that will help you accomplish your goals.

YOU NEED TO HACK

While the learn-by-hacking gene is in all of us since birth, what forces it out in our workplace is business's failure to meet more of our needs and its insistence on focusing mainly on its needs.

When company leaders talk about "productivity" and "efficiency," they're using *organizational* definitions: the fewest people accomplishing the highest output in the least amount of time at the lowest cost.

When hackers use those terms, they're referring to *personal* definitions: how I juggle all the daily demands in my life—my commitments to me, my family, my boss, my teammates, my customers, my company, my community, my dreams—with the least amount of effort, time, and hassle in ways that deliver the most value and allow me to be true to myself.

You deserve to have the tools, structures, and processes that *you* need to do your best, not just the ones the company needs to do its best. You *should and must* maintain your own view of personal productivity: the least amount of effort from you with the most value returned back to you, which keeps you doing your best. That's the only way to ensure your success as well as your contribution's largest impact.

If you're getting all that and more from your current job—great! No need to hack. But if you haven't been given the tools and processes you need, it's time to go get them or rework them. What you need to succeed is readily available, even if your boss didn't give it to you.

It's time to free your inner hacker. We'll show you how.

SIDETRIP

WHAT COLOR IS YOUR HAT?

White Hat Hackers are ethical hackers. They're most often insiders who work around their own systems to improve them. Good guys.

Gray Hat Hackers expose vulnerabilities in systems to help make the systems better. Good guys (as long as the owners of the systems are open to tough love).

Black Hat Hackers attack systems for profit and fun at the expense of others or to advance an agenda. Indisputable bad guys.

SIDETRIP

YES, THERE IS A DARK SIDE

This book is focused on benevolent hacks, but we cannot ignore that Black Hatters are doing evil things and giving some hacks a bad name.

These acts range from mildly bad (law firm Pillsbury Winthrop Shaw Pittman had salary cuts disclosed on blogs before some of the associates affected were told by their managers) to horribly bad (in 2008, hacker Albert Gonzalez and two Russian counterparts were charged for breaching over 130 million credit card records). In 2009, Iraqi insurgents hacked U.S. military drones using $26 software, and in 2010, Israeli soldier GI Schmo revealed his unit's secret upcoming raid to the world, including the enemy, on Facebook.

The most recent security threat report by Sophos says that unprotected data remains a top concern and that digital espionage and cybercrime are increasing. It lists examples such as Great Britain's biggest bank robbery ever, executed by hackers, and the theft of a single laptop that put 109,000 pension holders at risk. Also, one in four businesses report that malware and phishing have snuck in through their employees' use of social networking sites.

Yes, hacking has a dark side requiring constant vigilance. Acknowledge its presence, respect its power for doing harm, but never let those evildoers stop you from benevolent hacks. Make sure the White Hatters win!

GET HACKING

Stupid rules shift the costs of work from the company onto you without delivering equal or better value back to you.

This means you pay the price for someone else's bureaucracy or, worse, for their bad decisions.

Breaking stupid rules means getting smarter results: for you, your team, and your company.

Here's how. . . .

4

BREAKING STUPID RULES FOR SMART RESULTS

Get rid of everything that isn't useful, beautiful, or joyful.

—Anonymous, via viral email

GETTING STARTED

All Nina needed was a new printer. Why wouldn't her company get it for her, and why should you care? Because her plight is exactly why we must all hack our work. At its core, her story is our story.

Nina is a teleworker who manages projects for a health care organization from her home. In the spring of 2009, her company refused to replace her color printer, even though it was on its last legs after seven years. They insisted on a black-and-white model because that could translate to a savings of about $300 per year in toner costs. Multiply that by thousands of printers throughout the company, and at first glance, that mandate makes perfect sense—cost controls are necessary in all businesses.

But nobody listened to why Nina insisted on color: The way IT set up her project management system, everyone she communicates with

gets assigned a different color within their electronic exchanges. So for her paper-based files and project maps (which are required by her company to qualify for ongoing project manager certification), Nina bought her own rainbow assortment of colored highlighters and now has to manually highlight each person's contributions and changes with a different color.

Nowhere does the company's balance sheet record that it created $300 in savings by off-loading all that extra work onto Nina. Nowhere does Nina's salary or bonus or job description reflect this extra pain-in-the-ass, non-value-added work. Nowhere do corporate productivity numbers record that the company actually *decreased* Nina's personal productivity and minimized her ability to do her best work by saving itself a few hundred bucks.

This kind of destructive cost shift is more the norm than the exception. Each and every one of us has our own Nina story—where there is no tracking of all the hard and soft costs that corporate-centered processes create for and off-load onto us.

If it's not a printer, it's a regimented procedure or form or software that means more work for us but fewer costs and more control for the company.

Now that you know you were born to hack, and before we jump into the how-tos, never forget *why* you're hacking. Cost controls are just as necessary for you as they are for your company, and hacking is a way of exercising your own controls. If, like Nina, you've had enough of all those destructive cost shifts, here's how to get started.

WHAT'S BUGGING YOU?

The first step is the easiest. You tried to get something done and how you were forced to do it ticked you off. You grumbled to yourself, "Stupid procedure," or, "Stupid meeting, stupid form," stupid this or that. Start there, with whatever's bugging you, not because it bugs you—that's not reason enough—but because you know this problem. You

SMARTSTART

SELECTING WHAT TO HACK

1. **Select the Three Things That Drive You the Most Crazy.** You know the enemy: stupid rules, lack of common sense, and "Because I say so." Which three pain-in-the-ass tools, rules, and processes are the biggest drain on your personal productivity?
2. **Learn a Little More About Each One.** What *don't* you know about how that form or process or tool works? Why do others insist you do things that way? Who or what would be affected if you hacked a work-around?
3. **For Your First Hack, Keep It Simple.** Select your first hack for how easy it is to create your work-around. Most people should attempt more difficult hacks only with the help of a team or with some hacking experience.
4. **Start with the End in Mind: Define Success.** How will your hack change . . . your workload? your stress or frustration? your productivity? how you spend your time? What will you do with the extra time, energy, and passion now available because of your hack?

live it every day. It's one of the ways you're *supposed* to do things that bears no resemblance to common sense. You're about to change that.

NEXT: LOOK TO YOUR LEFT, LOOK TO YOUR RIGHT

If hacking includes understanding a system well enough to take it apart and do something better with it—what's a system? Big subject, but all you need to know for hacking is one little thing: connections.

If you're going to hack a task, a process, or a tool, you need to be curious about how that thing is connected to other things. For example, if you were a Yale University student writing a paper about an idea that would eventually become FedEx, you'd look at how UPS got packages from Boston to Billings and from Berlin to Beijing. You'd study the connections between each task throughout the entire system—everything that happens between "I'd like to send a package" to "It just arrived"—and then find a way to hack it. FedEx founder and CEO Fred Smith did just that. His original innovation was to hack the system of shipping packages. He took it apart and put it back together in ways that saved money and greatly sped up how packages got from point A to point B.

Most readers of this book won't need to study entire systems as Smith did. Your most important job will be to look to your immediate left and right—to see the connections between whatever it is you've got to handle, how it was handed to you, and how you'll hand it off to others.

So if you're hacking an expense form that seems useless, first make sure you understand all the elements of the form that was handed to you and what happens to the numbers within the form after you turn it in. Same with hacking into anything related to IT: You already know the limitations of the tool you're stuck with; learn as much as you can about what it does well so your new solution doesn't lose any of that. Then think about how your boss and teammates will be affected by a new approach.

One potential danger: Better understanding of these things can sometimes lead to Stockholm syndrome, where someone who is forced to do things against his will ends up sympathizing with the perpetrator. Criminologist Nils Bejerot named this behavior when bank employees who were held hostage for six days defended their captors after they were freed, insisting that their kidnappers' cause was just. Your equivalent would be: "Oh, poor corporation. It must be tough having to secure all its IT tools from employees who would

download porn all day or share secrets with competitors or . . . horror of horrors . . . not use PowerPoint. I guess I'll use their outdated legacy systems and work twice as hard as I need to because *their* work will be harder if I don't."

Don't be a victim twice: As you seek to understand the system surrounding your hack, never forget that you are the one currently being held hostage! And that wasn't a nice thing to do to you.

Look to your left. Look to your right. Understand what's connected to whatever's bugging you. Done? OK, let's start hacking. . . .

THE TWO WAYS TO HACK

So many ways to take back control. So little time.

Let us help you focus your energies: There are only two broad categories for work hacks. Drawing upon tech-lingo, we call them Hard Hacks and Soft Hacks.

Hard Hacks mostly change things.

Soft Hacks mostly change working relationships.

Hard Hacks are any changes you make to non-living systems. They are the actions that enable you to bypass a work procedure that was designed for you to follow. Hard Hacks work around corporate-sponsored tools, to-dos, forms, and processes and create ways of doing things that work for *you* and your teammates.

Here's an example of a Hard Hack you could do easily with just your smartphone or laptop if you're on a wireless network. Hiroki, a mid-manager at an automobile-manufacturing firm, was tired of having to do meetings after the meeting with his boss to decide what should have been decided in the first meeting. Corporate culture included an unending series of "buy-in" meetings before anyone could actually do anything. And that meant everything took ten times longer than was necessary. (So this hack is focused on a procedure and will use technology as the work-around.)

Hiroki and his teammates started using instant messaging (IM)

to secretly pass notes back and forth to one another during team meetings. They were able to quickly come to consensus among themselves on whatever issue was before them while their boss blabbered on and on. Then at the end of the meeting, Hiroki proposed what he knew the team had already decided. Everyone agreed—no need for the meeting after the meeting or for the meeting after that to communicate what had been decided.

What's newly exciting about Hard Hacks is that even if your hack requires much higher levels of tech know-how and tools than Hiroki's work-around, you no longer have to be a geek to do them. You can Google "how to do . . ." for almost anything and you'll be blown away by the variety and depth of solutions out there. Tons of people are posting videos, offering detailed instructions, and participating in discussion groups about all sorts of work-arounds. So if what you want to do is hack something where the technology is beyond you, have no fear! There's somebody out there who's already written instructions for non-techies.

Some additional examples of Hard Hacks:

- Corporate firewalls make it hard to move information easily among teammates? No problem: Use Gmail, Google Docs, and open source Web tools as go-betweens.
- Corporate IT supports CrackBerrys, but not your iPhone or Nokia or Droid? No problem: Hack a work-around. All the instructions you need can be found on the Internet. For example, here's one forum's post for getting Lotus Notes onto your iPhone: "I use CompanionLink to sync my Notes account to a Google account, which is then pushed to my iPhone."
- Corporate IT makes it hard to get at data you need to do your job? No problem: An alpha geek will happily help you install a program that will dump a customer database into a spreadsheet.

Let's rewind through chapters 1 and 3 to see who used Hard Hacks: Richard Saunders's hack of his bank's IT system to meet the needs of his senior execs; the trainer whose material "sucked" because she was underfunded and sent her trainees elsewhere; the university employee who sold corporate trash on eBay to fund his projects; the manager who used YouTube to get her bosses to change their minds; the team who secretly hosted internal information on outside servers. These are all examples of Hard Hacks.

As you can see, there are many types of Hard Hacks, and they vary from relatively safe to daring. But what they all have in common is that the hack creates changes in a non-living system.

Soft Hacks are anything that changes your relationship or work agreement with another person or group—changing how they agree to operate because you intervened.

Many Soft Hacks will feel quite natural. Even though technically they are work-arounds, Soft Hacks are the obvious things that any smart person would do to build and maximize relationships, get work done, and achieve good results.

Soft Hacks are both a little easier and trickier than Hard Hacks. They can be easier because you can often sit down with the other party and say, "Hey, can we work this out?" You can't do that with a form or a tool or a mandated process or procedure. On the other hand, Soft Hacks can be trickier because you may be messing with that person's turf. And since they revolve around people, Soft Hacks are almost always more complicated.

Soft Hacks are generally broken down into two types: **Negotiating the Deal** and **Changing the Relationship**. The former involves setting the rules up front, before actual work begins; and the latter affects relationship norms that are already in place between you and the other parties.

Courtney employed a couple of **Negotiating the Deal** hacks when her family situation suddenly changed. She had to convince her manager to let her work remotely.

The first thing she did was to offer her manager something in return—she packaged her off-site request as a way to speed up delivery dates on two of his three top-priority projects. That took about a month of preplanning and behind-the-scenes secondary negotiations with teammates and vendors before she was ready to lay out everything for her manager. It also included some reordering of the sequence of tasks to be completed. Lots of people had to agree to help her make the changes she needed to make.

She didn't get everything she wanted; eventually, Courtney and her manager settled on a compromise—three days per week working remotely and two on-site. But she got further than anyone else in her position ever had.

Other examples of Negotiating the Deal hacks:

- Seeking different measures for your projects.
- Negotiating up front on salary and benefits. We discovered that in addition to using age-old techniques, many hackers are doing their own due diligence with new tools to play hardball with their employers. For example, BrightScope.com provides detailed comparative rankings for the 401(k) plans of hundreds of companies. Hackers who found that their potential employer was not in the top quartile used data from BrightScope to forge a better deal in other areas, like base compensation and benefits.
- Getting an extremely tailored training and development program. Same as above; we found that many hackers went to initial interviews armed with rankings of where their firm fell in terms of training and development and used that data to get a better overall deal than they could have otherwise.

What makes each of these a hack rather than a normal relationship give-and-take is that each is a clear exception to the company's normal procedures. For example, because of her supervisory role,

Courtney's job description never offered the possibility of working remotely. She had to create the exception to the rule. And while hacks on tightly controlled areas like compensation appear to be relatively minimal, they are definitely becoming more common. It is doable, even in a down economy! Hackers everywhere are discovering that if they do enough due diligence, almost any standardized "nonnegotiable" practice can be hacked.

Your Negotiating the Deal hack assumes that you are just as special as the most senior executive at your firm. You know that behind-closed-doors deals are made for them all the time; companies make all kinds of exceptions for the people who matter. In today's not-fair-to-all workplaces, Negotiating the Deal hacks are the only way to ensure that *you* matter as much as anyone else and that you get as good a deal as anyone else.

Could this create lots of complexity for companies—lots of people like you negotiating individual and tailored deals? Absolutely. Should you care? Not one bit! Did they care when their corporate-centered designs had you working twice as hard as necessary, forced work/life stresses onto you and your family, or forced you to take on twice as much work when they laid off your teammates? Their priority is to avoid tailored deals to create assembly-line efficiencies in all their people processes. Is that *your* priority? Didn't think so.

Most Boomers we interviewed saw Negotiating the Deal hacks as having to give up something in order to get what they wanted, just as Courtney did: "If you let me work remotely, I'll increase such-and-such for you." Their approach seemed to be "You get more flies with honey than with vinegar." Millennials, however, were more in-your-face: "Why should I even have to ask for these things? It's what I need to do my job!" Many in this generation will assume that almost everything is up for negotiation. That could mean lots more acceptance of this kind of hack or that you'll have lots of competition for the few tailored deals that are done.

Some think that negotiation must be hardball back-and-forth,

with both parties digging in to get their way. But negotiating can be as simple as asking to get a copy of a document emailed to you instead of faxed or requesting that you are called instead of emailed. Or it can be agreeing that in order to succeed, you will need certain questions answered before beginning each project—and if your boss doesn't have the answers, it's OK for you to ask her boss. Negotiating the Deal is setting precedents for how *you* need to work so that you can succeed and excel more often.

And that's the point. Too many times, the deal you're handed ensures the company's success, but not yours. Hacking back ensures that you get to do your best.

The other kind of Soft Hack involves **Changing the Relationship**:

- Organizing anything to improve morale, from safe approaches like sponsoring a company softball team to more daring approaches like confronting a toxic boss with your own bottom-up survey.
- Bypassing the formal 360° feedback or performance systems to get a good person promoted or a bad person disciplined.
- For those with great bosses, this hack is for you, too: Many hackers said that they partnered with their manager, who helped keep their hacks "under the radar" and provided "air cover" protection if those in power ever found out.
- Reaching out to your own social network instead of to the people assigned to you by the company.

All Soft Hacks involve social engineering, which is just a clever way of saying that everybody has needs, wants, and desires that can be leveraged with positive or negative reinforcement. If any of that makes you queasy or feels like manipulation, get over it! Remember, your company is hacking you right now. What do you think rewards and recognition are all about? Yup, social engineering.

A classic example comes from Josh's time at Microsoft. He was

a blue badge worker—a contractor. The red badgers were full-time employees, which included a crucial reward: stock options. Every midmorning, those red badgers would cluster over coffee to discuss that day's stock price. They'd chortle about how much richer they'd soon be, lording it over the blue badgers. The social pressure worked. Those blue contract workers were constantly putting in more effort, hoping they, too, could become one of those well-rewarded red badgers. And Microsoft benefited from all that extra effort, while only rarely elevating blue badgers to red status.

Sound familiar? Even if it's not as competitive or obvious, most companies have some version of red vs. blue social engineering.

We're just showing you how to hack back—how to level this portion of the playing field.

More important, know that it's called social *engineering* for a reason. Most of us manage the give-and-take of our relationships in a knee-jerk way as situations arise. Hacks that change your relationships are about being more proactive in thinking through how those relationships can help you do your best.

One final, crucial note about all Soft Hacks: If you rework any relationship to improve your output, you've got to deliver the goods! Hackers thrive in meritocracies, which means having the capabilities to back up your work-arounds with real value. Otherwise you'll be using others for your own gain. In hacker's lingo, that's "being a dick." Don't be a dick.

POP QUIZ AND A FEW QUICK TIPS

Remember Matt, the new hire in chapter 1 who created his own performance assessment tool and got his company to agree to use it? Quiz time: Did Matt employ a Hard Hack or a Soft Hack?

Trick question! He used both. Redesigning his company's performance assessment tool was a Hard Hack—he changed a non-living thing. But he got it implemented through Soft Hacks. First he used

LinkedIn, a social networking tool, to find someone to help him improve his hack. Then, prepared with a negotiation strategy as well as the backing of some of his teammates, he went to HR and his boss and won a new negotiated deal.

The most effective hacks often combine hard and soft approaches. Examples from what you've read already in chapter 3: Sean's negotiations with the CIO to off-load his team onto HR and then working around the CIO with his team's prototype; LeeAnne Del Rio's use of a Web site to change relationships between part-time and full-time teachers. These are examples of Hard Hacks combined with Soft Hacks.

Why does this work so well? Most often because you're making it easier for them—all they have to do is say OK to a fix that solves their own problem.

Hacking Quick Tip 1: Use Hard and Soft Hacks in Combination. Even if you're hacking a non-living thing, you are also changing somebody's world. Somebody owns that form or process. If you can, work with those who will be impacted. Or, as Matt did, seek the support of others so you don't go it alone. The biggest enemy to a successful hack is catching others by surprise. Many of the most effective hackers said that their immediate supervisor was in on their hack. The more people you can loop into your hack and empower by your hack, the better.

Hacking Quick Tip 2: Hard Hacks Are Often Bold Acts. Hard Hacks have the potential to create the biggest shifts in power in the shortest period of time. This is because many of them can be scaled—replicated by lots of others—and because they're often easier to keep underground for a longer period of time. This makes Hard Hacks the most effective, but also the most risky. Bosses don't expect anyone to question their system, so redesigning your work tools can be like telling the emperor he needs new clothes.

Hacking Quick Tip 3: Pick Battles You Can Win. After trying unsuccessfully for months to get a color printer, Nina finally decided

to take another tack. Having proven herself to be a vital resource to the company, she used a Negotiating the Deal hack to reprioritize her workload, more than making up for the silly extra duties of highlighting printouts.

You now have the basics for getting started. In chapter 5, we'll go deeper into breaking stupid rules for smart results—how to build your own hacker's toolkit and the five hacks you definitely should try.

FASTHACKS

WORK-AROUNDS FROM THE FIELD

How Techies Negotiate for Time Off from Jessica: "I recently worked for a company that was stingy with time-off allocations but demanded a lot of overtime. What made my situation worse was that while I was putting in all that overtime, my supervisor worked just enough to get by and always took off as soon as our boss left for the day.

"I knew that all our work involved the same network. Since I was in charge of the network, I wrote a script to send me an email every time my supervisor logged in and out. I wrote the same script to track my log-in and log-out times. I imported all the data into a spreadsheet and could soon accurately compare my sixty-plus-hour workweeks with my supervisor's forty-plus-hour weeks.

"Later that year, I met with both my supervisor and our boss and told them I was going to take an extra week over Christmas holiday to visit my in-laws overseas. After the yelling had ended, I handed them my spreadsheet comparing my supervisor's work hours and mine. Instead of the additional week I had requested, they gave me ten additional days off.

(continued)

"Upon my return, I was treated with much greater respect, and my employment with them lasted until I chose to end it."

Even Apples Need Hacking from Lucas: "I emailed [CEO] Steve Jobs instead of following the standard chain of command at Apple to address coding issues with a customer interface. We had been having this problem for several months, and we were getting nowhere. Needless to say, the problem was miraculously addressed the next day."

Postscript

REPORTS FROM EARLY CONVERSATIONS

Nine months before *Hacking Work* hit bookstores, *Harvard Business Review* saw an early draft and named this book one of the top ten breakthrough ideas for 2010.

That meant even more opportunities to talk to people about what's behind benevolent hacking, and more opportunities to listen and learn. Here is what we took away from those conversations.

1. There's lots more hacking going on than we uncovered!
Benevolent hacking is the duct tape of the work world. It's the universal solution to every poorly designed and corporate-centered procedure, tool, rule, and process. If hackers stopped hacking, almost all business would grind to a halt. And if all hackers came out of the closet and shared what they are up to . . . wow, what a force to be reckoned with.

2. Most senior execs: "Yeah, but . . ."
"Yeah, our infrastructure is totally corporate centered. Yeah, that sucks for the workforce. But we gotta have our controls. What you're

proposing is anarchy." Guys, we're just reporting what is already happening right under your nose. It's up to you to choose whether you view benevolent hackers as rogue rule breakers who must be contained or as a major competitive advantage to be leveraged. You already know what we think your competitors are doing.

3. Some midmanagers: "Yeah, but . . ."

"Yeah, hacking work could free me from tons of stupid-work and give me control of my life. But I've got 2.2 kids, a mortgage, and expensive habits I don't want to kick. I can't take the risk." Understood. Working around stupid-work isn't for everyone, and it can be a scary idea to grapple with. If you're not ready to take the plunge, we encourage you to hold onto this book until you are—we're hopeful that someday it will help you realize your passions.

4. Always remember: It's about change, not technology.

To alpha geeks, *Hacking Work* is like their world on training wheels. We get that. We didn't emphasize specific technologies for two reasons. First, detailed assessments of technologies, along with their how-to's, are better served and spread virally, through online forums. But more important—technology is just a powerful enabler. *Hacking Work* is about personal choice: Now that you know you can save business and succeed and work smarter by breaking stupid rules, will you?

Acknowledgments

THANK YOU!

Two guys hacking the future, one day at a time. These are the people who kept us grounded in reality as we pursued that lofty goal.

From Bill: Thank you Desi, Taylor, Stephen, and Ian for keeping Bill laughing, somewhat sane, and very loved and grounded throughout this project. Couldn't have done this without you!

From both Bill and Josh: To the work-in-progress counselors and readers: Someone had to tell us when we were on the wrong track and when our babblings were incoherent. Among a cast of hundreds, these folks deserve special mention for performing that service: Rick Bradley, Julian Chapman, Johan D'Haeseleer, Chris Ernst, Susan Flowers, Joe Fratoni, Phyllis Frazer, Sylvain Gauthier, David Horth, Lindsay Hurst, Dave Jardin, Cecil Johnson, Kim Jones, Mark Koskiniemi, Scott Leavitt, Mark Leyba, Lorraine Mahoney, Bruce Morton, Jim Phelan, Anna Pringle, Emma Reynolds, Sharrann Simmons, Janice Swift, Andy Szpekman, Graham Westwood. Thanks folks!

To our book teammates: We owe Dave Moldawer, Will Wiesser, Amanda Pritzker, Emily Angell, Mollie Glick, and the entire Portfolio team a huge thank-you. Will and Dave are the sages at Portfolio who "got" our vision and kept us honest to it. Amanda made sure this book got the marketing buzz it deserved. And Emily's attention to detail kept all our eyes on the prize. Mollie started it all: She's our book agent and so much more. Mollie took our original proposal and reshaped it so it actually made sense. Our thanks to all of you!

To our book interviewees and anonymous contributors: We didn't really author this book; you did. *Hacking Work* is your story. Thank you for sharing it with us so we could share it with the world. (And we'll keep our promise to keep you anonymous if that's how you wish to stay!)