KEVIN MITNICK IS THE MOST NOTORIOUS HACKER IN THE WORLD. SOME SAY HE IS ALSO THE MOST DANGEROUS. HERE, FOR THE FIRST TIME, IS THE INSIDE STORY OF HOW HE STAYED A STEP AHEAD OF THE FBI UNTIL FINALLY, INEXPLICABLY, HE MADE A SIMPLE MISTAKE THAT BROUGHT HIM DOWN

THE INVISIBLE DIGITAL MAN

BY JONATHAN LITTMAN

The master of ceremonies takes the microphone in the tastefully appointed ballroom to announce a special guest. "I'm pleased to tell you that we have Kevin Mitnick with us today," the MC tells the exclusive audience of 150. "Kevin is a legendary hacker gone straight."

Mitnick, a chunky man with thick, matted hair and wearing a dark suit, jubilantly lifts his arms overhead to cheers and laughter. "He's managing his own security company," continues the announcer. "You may have seen him on *60 Minutes*. He's got a great career going now that he's gone straight. We're all happy about that! So please welcome Kevin Mitnick!"

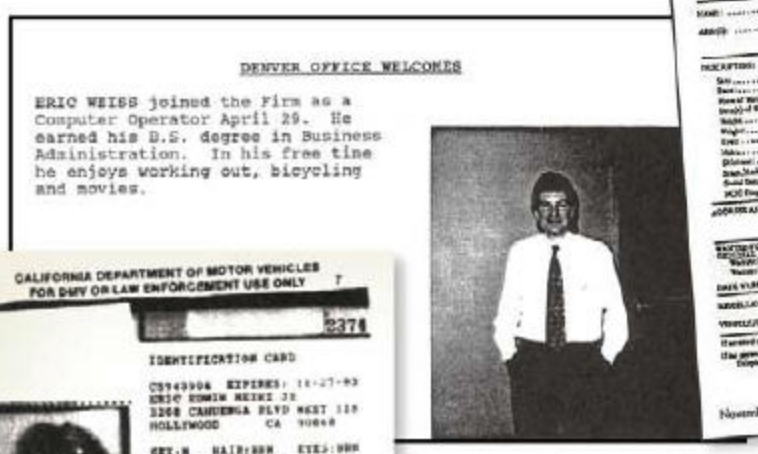
The applauding guests are executives and top managers of a major high-technology firm. Outside the windows are the velvety practice putting green and posh clubhouse of one of the world's most exclusive seaside golf resorts. The past couple of days the guests have been regaled with golf, fine dining, deluxe accommodations and the most expensive corporate speakers money can buy. But the attendees won't be teeing up this afternoon.

Kevin Mitnick is not typical corporate-lecture fare. He spent nearly five years in a federal penitentiary for his computer crimes and led the FBI on a wild two-year cross-country chase. Today he earns in the low six figures by advising executives on how to protect their companies from the current generation of ingenious but reckless geeks. Brilliant and self-taught, Mitnick possesses a deep, intuitive knowledge of the backbones of communication and commerce, everything from phone switches to cellular networks and computer operating systems. I first talked to Mitnick when he was a fugitive in the mid-1990s, and I wrote a book about his case, *The Fugitive Game: Online With Kevin Mitnick*. Now that the final terms of his probation have ended, Mitnick has decided to speak to PLAYBOY and for the first time reveal the most dramatic part of his tale: his life on the run from the FBI.

Kevin Mitnick loves to perform. He takes the podium at the golf resort and gleefully proceeds to demonstrate the crowd's electronic vulnerability. He invites a gray-haired woman up, raps out a few quick keystrokes on his giant laptop and in 30 seconds flashes her Social Security number and home address on a giant presentation screen. That was so much fun, Mitnick merrily asks whose driver's license the audience would like to see. He passes on George W. Bush and instead flashes his hands over the keys to broadcast the first president Bush's Texas license to the group. After that he requests another guinea pig.

PHOTOGRAPHY BY JAMES IMBROGNO


STAIRWAY



From top: Kevin Mitnick is led into court in North Carolina following his 1995 arrest. During his two years on the run, Mitnick stole the identity of Eric Weiss (chosen because his name resembles the given name of Mitnick's idol Harry Houdini) and found work at a Denver law firm. A faxed copy of a driver's license Mitnick obtained for Eric Heinz, the alias of an FBI informer who tried to entrap him. Supporters in 1999 protested that Mitnick had been held for nearly five years without trial. Security specialist Tsutomu Shimomura (bottom right) tracked the fugitive hacker to Raleigh. Today Mitnick (bottom left) is a highly paid consultant.

With trepidation, a man hands Mitnick his personal cell phone. In less than a minute, after pressing some keys on his laptop and the phone, he magically makes the man's calls appear to come from the White House.

While Mitnick dials a number on a ballroom phone, he issues a disclaimer: This is just a demonstration, the ex-convict insists. He has cloned Citibank's telebanking system to show how easily a customer could be fooled into handing over enough information to empty his or her bank account. "Welcome to Citibank automated service," oozes a woman's silky voice. "If you have a debit-card number, press one."

Mitnick jauntily presses one and jokes, "Anybody have a debit-card number they want to share?" Nervous laughter rocks the room.

For his next trick Mitnick hands a tall blonde a pinkie-size USB storage device to plug into her laptop. He warns that any unknown storage device—a gift or something found in a parking lot—could be a hacker's ploy.

On the giant presentation screen, the woman's laptop directory appears. "You don't mind me looking through your hard drive, do you?" Mitnick chuckles, getting laughs.

She's nearly shaking. "You can stop now," she says.

Mitnick wraps it up, and Frank Abagnale, the legendary reformed master imposter and con artist (played by Leonardo DiCaprio in *Catch Me If You Can*), takes the microphone and gives another of his highly sought-after performances. Mitnick sits with me in the back, enjoying the show. When Abagnale finishes his performance, Mitnick stops to say hello—one artist to another—and hands him a thin metal business card, bearing his name, with pieces that appear to break away. He asks Abagnale if he recognizes it.

Abagnale grins and says, "Yeah, it's a lock-pick set.'"

On July 4, 1994 *The New York Times* put Mitnick's story on the front page and branded him "cyberspace's most wanted." The Justice Department and some of the world's largest computer and cell phone companies considered Mitnick an electronic terrorist. "Here was somebody running amok through the Internet, exposing all the vulnerabilities from social engineering to technical intrusions," says David Schindler, the former federal prosecutor who oversaw the effort to catch Mitnick. "When you talk about this veritable tornado of fraud, the scope of what he was doing, the brazen nature of it, the broader implications, there was the sense that he was the wake-up call."

Mark Rasch, another former prosecutor, says Mitnick became a bogeyman. "If we were going to run nuclear power plants and do our billing and insurance online, we needed to feel it was safe, and Kevin shattered our illusion," says Rasch. "Not just Kevin Mitnick but all the Kevin Mitnicks out there."

Beyond the prosecutors, it's difficult to convince people who had intimate dealings with Mitnick to discuss the damage he inflicted. Motorola, Nokia, Sun and virtually every other victim refused to comment for this story. An FBI spokeswoman said the lead agent on the case didn't see "the benefit to the Bureau" of discussing Mitnick. Who can blame them? Mitnick cleverly acquired the cell phone numbers of the FBI white-collar crime squad tasked with capturing him and tracked their movements and their calls to other agencies. That brazenness is not something the FBI appreciates. Suspects don't generally investigate the Bureau.

But today the hacker appears to have left his colorful criminal past behind. Having done his time, Mitnick found his skills and notoriety could fuel a lucrative second act. His passport bears the stamps of 34 countries, and in the past few months he has lectured and hacked legally in Moscow, Bogotá, Barcelona and Johannesburg. Mitnick makes a nice living advising U.S. agencies (including the Social Security Administration and NASA) and corporations around the world on how to shore up their digital defenses.

Mitnick was a popular guy in prison. A Colombian drug kingpin offered him millions to electronically alter his records for an early release. Ed Bradley visited him in jail for the first of two *60 Minutes* interviews. Once out of prison, Mitnick was invited to testify before Congress and then in 2004 did the unthinkable for a devout antiauthoritarian: He helped police identify a student making bomb threats to his high school. Though the FBI plastered a promotional plug from Mitnick on the cover of its most recent computer-crime survey, some critics refuse to believe he has gone straight. "He doesn't acknowledge the malicious nature of his crimes," says Ira Winkler, an Internet security expert who formerly worked for the National Security Agency. "He has a Jekyll-and-Hyde personality."

The irony of the Mitnick saga may be that his extraordinary skills made him a target. In pushing back against the FBI and a mysterious Japanese security expert, Mitnick learned too much about how the government and those who do its bidding track outlaws. The trouble that led to his two years as a fugitive began in 1991. The 28-year-old Mitnick was trying to go straight, counting the days until the end of his probation stemming from a 1988 conviction for swiping code from Digital Equipment Corporation.

One day, out of the blue, he received a call from Eric Heinz, *(continued on page 133)*

DIGITAL MAN

(continued from page 66)

a Los Angeles rock musician eager to talk about hacking. Through a trick at the phone switch, Mitnick gleaned the man's phone number and traced him to his home in an Oakwood apartment complex. Why would this hipster be staying at a place for corporate stiffs? Within days Mitnick obtained a copy of the rental agreement and learned someone else paid the $1,300 rent each month.

"We met at Hamburger Hamlet and started talking about our capabilities," Mitnick recalls. Heinz let slip about a secret phone-company system that Mitnick and his longtime cohort, Lewis De Payne, had never heard of. Mitnick quickly located and mastered the system. It was a hacker's dream: an internal Pac Bell system to troubleshoot phone lines that could be used for remote wiretaps.

So Mitnick monitored Heinz's phone. "We pop onto the line and hear him talking to some man," says Mitnick. "Then we hear him say 'Ken.' I hear my name, Mitnick. I'm freaking out. My heart's beating like crazy. This is 100 percent confirmation. Ken McGuire, the other man on the line, is an FBI agent. They're talking about evidence to get a search warrant."

Heinz was actually Justin Petersen, a thief the FBI paid to entrap hackers. Mitnick began tracking the whereabouts of Petersen and McGuire, his FBI control. He entered the cell numbers of McGuire and other agents into his scanner and tracked their movements throughout southern California. He knew where they lived, as well as their cover names, driver's license numbers and home addresses. The FBI wasn't happy. The Bureau had to keep moving its undercover operative to new safe houses after Mitnick kept cracking them. In December 1992, a year after Mitnick first spoke to Petersen, the G-men knocked on his door. The jig was up. They planned to revoke his probation and send him back to jail, but Mitnick had already split. On Christmas Eve he checked into a budget hotel in Las Vegas. He planned to stay a month, enough time to establish a new identity and fly away. But Mitnick didn't know that, in early January, Tsutomu Shimomura, a brilliant computational physicist at the federally funded Supercomputer Center in San Diego, would remind his favorite *New York Times* reporter that Mitnick was about to go free, noting that his "conditional release is up sometime around now, isn't it?" The FBI wasn't the only entity interested in the hacker's whereabouts.

•

So how does a wanted man escape the watchful eye of the FBI? He walks into the Department of Motor Vehicles as one person and walks out as another. The character in *The Fugitive* couldn't have done better. Impersonating a cop, Mitnick phoned Oregon's DMV "looking for a suspect" and found the ideal target, a man who couldn't drive because of medical problems. Mitnick applied for a temporary license using this new identity. Then he picked up W-2 forms at Office Depot, invented a tax identification number for a phony employer and used these and other forged documents to apply for a copy of his new birth certificate. Soon he had an authentic driver's license, a Social Security card and a bank account under his new name. Mitnick headed to the library to select his next destination. With sunshine 300 days a year, glorious mountains, great skiing and plentiful jobs, Denver sounded like an adventure. Mitnick began to meticulously develop his cover. "People might start asking questions, and you can't give different answers to different people," he says. "I created a story for where I grew up, where I went to school and who my parents were."

As a boy Mitnick loved reading about spies, secret agents and magic. The identity he'd created was a fanciful concession to his first childhood hero. When his plane landed at Denver International Airport, tucked into his wallet was a new Social Security card and American Express checks made out in the name of Eric Weiss, an approximation of Ehrich Weiss, the given name of Harry Houdini.

•

Eric Weiss, a.k.a. Kevin Mitnick, was called in for an interview by the downtown Denver law firm of Holme, Roberts & Owen. The company checked his references, phoning Paul Michaels, president of Green Valley Systems. Michaels—actually Mitnick working from a pay phone in a nearby hotel—returned the call. "Eric is an excellent worker," Mitnick said, lowering his voice. "If he ever moves back to Las Vegas, I'd hire him in a minute."

The hardest thing during the crazy charade was to keep from laughing. Mitnick carefully laid the groundwork for this elaborate fiction: letterhead for the imaginary Vegas company and $30 for a mail drop and an answering service. Mitnick got a second interview and the job as a computer operator. His capabilities soon endeared him to his boss: "She started calling me the law-firm hacker."

Mitnick would often stay until midnight, researching his defense with the firm's abundant law books and enjoying the comfortable furniture. He left few electronic fingerprints. He felt safe. Forty-three floors up, he hooked his scanner to his laptop and began intercepting the electronic serial numbers of cellular callers. He skipped from one account to another so customers would be unlikely to notice the extra phone

charges. His cell and laptop became his mobile hacking launchpad.

Mitnick targeted Neill Clift, an Englishman famous for collecting software bugs on Digital Equipment Corporation computers. In spring 1993 Mitnick, posing as Derrell Piper, a noted security expert at DEC, began sending Clift e-mails. He claimed he was compiling a log of all the DEC vulnerabilities and needed Clift's assistance. To assure Clift he wasn't what he actually was, a notorious hacker, Mitnick raised the subject himself. "I didn't want him to start thinking, Could this be Mitnick? So I thought, Well, bring him up." As they began exchanging messages, Mitnick casually told Clift, "I heard this Mitnick guy was after you."

The tactic put Clift at ease, and he fell for the ploy, e-mailing the major vulnerabilities of DEC computers to the last person on earth the company would want to have them. "I'm still missing one more report," the hacker e-mailed Clift. "Please send me the $getjpi bug report.... I forgot to include it in my request yesterday. It's been a very busy week." The thrill of conning Clift sent Mitnick soaring. Encouraged, he began contemplating a hack that would ultimately rock the security foundations of telecommunications giants around the globe.

•

Where did Mitnick's compulsion begin? "My father divorced my mother when I was three," Mitnick explains in a matter-of-fact tone. "She married four times—she had lots of boyfriends." Mitnick was shuttled through a series of apartments in the San Fernando Valley, and one stepfather beat him so badly that Mitnick was removed from the home. As a chubby teenager, he became infatuated with ham radio and became known for his on-air screeds. But the real precursor to his hacking came from another technology: At 16, Mitnick fell into heavy phone phreaking. "You'd call a number, enter a secret five-digit code and call anywhere in the world for free," he says. "I loved the illusion, the magic."

Mitnick hacked the switch that controlled many of the phones at the NSA, eavesdropped on a call and then decided that might not be wise. He wrote a program to swipe his teacher's password and leapfrogged from a high school computer into the University of Southern California's network to play computer games. On another occasion an adversary picked up his home phone one day to hear a recorded voice asking him to deposit a dime—Mitnick had turned it into a pay phone. Once, for kicks, Mitnick intercepted directory assistance in Rhode Island. Callers got mind-spinning listings. "That number is 555, 2 one-half 37," Mitnick says he deadpanned, loving it when befuddled callers would ask, "How do you dial a half?"

Bored with school, Mitnick passed his GED and broke into one of Pac Bell's key buildings, only to be chased on the 405 freeway by investigators from the district attorney's office. "They pulled me out of the car, handcuffed me really tight," he says. He remembers being told, "We're going to teach you to stop fucking around with Pac Bell." Charged with grand theft, burglary and computer fraud, Mitnick received probation and a mandatory psychological exam. "Kevin feels indignant that authority figures often unjustly have the upper hand," the psychiatrist reported to the juvenile-court judge. "Kevin's preoccupation, if not obsession, is derived in part from the sense of power he gains, power which offers a sense of security and power which enables him to get even if he chooses."

Mitnick's early exploits were among the first to inspire theories of computer addiction. Tripped up in 1988 because he had nowhere to stash his digital loot but USC's computers, Mitnick was found to be a "very great danger to the community" by a federal judge, who sentenced him to a year in jail. DARK SIDE HACKER SEEN AS ELECTRONIC TERRORIST was the headline in the *Los Angeles Times*. "The final digits of his unlisted home phone were 007," wrote the *Times*, "reportedly billed to the name James Bond."

Mitnick's exploits had the ring of myth. Reporters wrote that he had caused millions of dollars of damage by breaking into DEC's computers, compromised the security of the NSA and trashed a judge's credit report. The most incredible story recalled the 1983 hit movie *WarGames*, in which the young Matthew Broderick nearly starts World War III. According to the *Los Angeles Times* story, "Steven Rhoades, a fellow hacker and friend,...said he and Mitnick broke into a North American Aerospace Defense Command computer in Colorado Springs, Colorado." Fearful the hacker could wreak global havoc with a single phone call, the judge subjected the 25-year-old to eight months of solitary confinement. "It was tough psychologically," Mitnick says. "They'd concocted all these rumors about me. I was scared, locked in that little room for 23 out of 24 hours, four blank walls to stare at. It was like being locked in a coffin."

Mitnick believes he became a scapegoat for society's unease with the spread of technology. His handle for a time was Condor, taken from his favorite film, *Three Days of the Condor*, the Sydney Pollack thriller starring Robert Redford as a technically savvy agent hunted by a corrupt CIA. Mitnick knows the appeal of myth. "I knew they would exaggerate my crimes to

"Originally, it was just to mask my feelings for Tonto."

make me the example. Based on what happened in the past, being held in solitary confinement and NORAD and all that bullshit, I knew I was a pawn in the game."

•

Six years after his confinement, leading a double life at the Denver law firm, Mitnick attempted one of his greatest hacks, the full details of which have never been published before. The treasure: Motorola's most valuable source code. Why? Why do men climb mountains? Mitnick hoped the code would enable him to create an untraceable cell phone. Invisibility was his goal. Pride also figured in it. Mitnick thought getting the Motorola code would be a notch in his belt, a trophy; also the Motorola MicroTAC Ultralite was niftier than his Novatel model. "It looked like the *Star Trek* communicator," he says. "That's why I went after it."

Possibly the most jaw-dropping aspect of the hack was its spontaneity. Aided by the cell phone in his hand, Mitnick improvised a preposterous con job. One snowy February day he left work a little early and began the 20-minute walk to his apartment. "People are more cooperative at the end of the day," he says. "They want to get out of the office." He dialed Motorola headquarters in Schaumburg, Illinois as he walked, eventually reaching the voice mail of a vice president, Paula D. (the names of all Motorola employees have been changed). She was on vacation, which was perfect. That meant she wouldn't unravel his fraud. Her outgoing message said to call her assistant for help while she was gone.

"Hey, Ann, how are you?" Mitnick said on his next call. "Listen, did Paula leave on her vacation yet?"

Mitnick identified himself as Rick from research. "She told me she'd send me a copy of the source code for the MicroTAC. She said I should call you if she didn't have time, and you would help me out."

Mitnick was working what he calls his "authority principle."

"What version are you looking for?" Ann asked.

Thrown for a loop, Mitnick took in his surroundings. Downtown Denver, the snow pouring down in thick flakes, cars honking. He should have called from an office. But he felt invincible.

"How about the latest and greatest?"

"Sure," chirped Ann.

She began typing as she searched. Five minutes passed. Mitnick grew concerned.

She came back on. "Version 9366. That's the latest."

"Fantastic," Mitnick said.

"Rick," she said, "there are hundreds of files. What do you want me to do?"

He shifted his tone. He had to train his retriever.

"Do you know how to use Tar and GZip?" he asked.

She didn't. Mitnick explained that the commands would compress the files into one. Would she like to learn?

"Sure."

Just like that, Mitnick became her tutor. He taught her to compress the files, cementing his authority, bringing "reciprocity" into play. He asked if she knew how to use the file-transfer program; she did.

As he neared his apartment, Mitnick wondered where to send the loot. He couldn't give her a normal host name; she'd realize it wasn't Motorola. Then it came to him: Give her the arcane numerical code for an Internet address outside Motorola.

But he hit a snag: Ann couldn't connect to the address. "I think this could be a security issue," she told him.

She put him on hold, presumably to get help. The minutes ticked by. Mitnick worried.

"Rick," she said sharply as she came back on, "you're asking me to transfer the source code outside Motorola."

Mitnick thought he was cooked—until she said her security administrator had told her she needed "to use a special proxy server." Incredibly, the Motorola manager held her hand through the final technical steps. Mitnick had reached the entrance of his brick apartment building. "I about tripped and fell." He stared at his phone in disbelief. In 20 minutes, on a lark, he had phoned Motorola and obtained one of its most valuable assets.

Mitnick rushed into his apartment and hooked his cell to his laptop. He checked his network stash, and there it was. "I couldn't stop there," Mitnick says. Emboldened by his success, he now wanted full access to the Motorola cellular-development network. To connect remotely he would need a user name, password and SecurID—a credit-card-size electronic token that generates a second password. Experts considered the security routine extremely tough to crack.

A blizzard raged outside Motorola's Schaumburg offices. Late one Friday night, Mitnick called its computer room, saying he was working on a weekend project and couldn't get into the office with all the snow and damn if he hadn't left his SecurID in his desk drawer. Mitnick asked the operator if he could hop over to his office and read off the random password. It didn't fly. Mitnick hadn't expected it to. "Since you can't get my SecurID," Mitnick asked, "do you have one available in the IT department?"

"Yeah."

"Could we use that one?"

The operator phoned his boss, letting Mitnick listen in. "I have Rick on the phone. He's with the cellular subscriber group. He's working on a special project. Yeah, I know him."

Mitnick smiled to himself. The operator was vouching for him.

The boss wanted to talk with Mitnick.

"I really appreciate this," Mitnick said. "I understand it's outside anyone's scope."

Mitnick dropped a few names culled from a password file Ann had unwittingly sent him.

"This is unusual," the boss said, "but we can help you out."

Mitnick was in. But he wanted more. He could get only so far with these passwords, and they didn't allow him access to the code that ran Motorola's phones. So he hacked into a NeXT computer used by a few engineers who worked in the cellular subscriber group. He cracked their passwords, then phoned them at home. The first staffer was suspicious; Mitnick backed out. Then Earl R. answered.

There had been a computer crash, Mitnick told him. They were busy restoring the files. When would he need access?

Mitnick's "scarcity principle" in operation: Take something away, then give it back.

"Monday," Earl said.

"We're shooting for Thursday."

The man freaked. He had deadlines.

"Listen, if you don't tell anyone, I'll restore your files quicker," Mitnick offered. "I'll just need some information."

Mitnick verified Earl's account information, including his user name. Then he suggested picking a password.

"Never mind," Mitnick said. "Let's set it to your old one."

"Who are you again?"

Mitnick calmly repeated his alias. "You're concerned about security," he said. "Hold on a moment. I'll get your application for your secure ID." He put the phone down and waited, ruffling some papers.

"I found your form. I'll tell you the password you wrote down [which Mitnick had just hacked]. Is that okay?"

"Sure."

"Mary."

Placated, Earl handed over his new password, and Mitnick thanked him and hung up. He logged in as Earl R., slipping behind Motorola's final layer of security. He found a program to extract the MicroTAC source code and began the download. *Poof!* It was one hell of a hack. Indeed, in a report to the FBI, Motorola investigators stated that during the intrusions on February 19 and 20, the caller bypassed four separate levels of security.

•

Motorola was far from being the only corporate victim. By chance, Nokia had just come out with the first digital phone, and Mitnick had to have its code. He began cracking overseas computers. The Nokia investigators called it "hackering," and hackering in the U.K. led to a charge of hackering in Finland. On February 2 the FBI told the firm its source code had been found on a USC computer (where Mitnick had stored it); Nokia files had also been found in Colorado Springs. Finland's National Bureau of Investigation opened a case of international espionage, flying a detective to Los Angeles.

Mitnick meanwhile had made human connections. While hanging out on the Internet Relay Chat, an online channel where hackers trade real-time insults and attack scripts, Mitnick "met" JSZ. When Mitnick phoned him, JSZ took the call in the computer lab of an Israeli university where he was studying computer science. "He was mysterious," says Mitnick. "I didn't even know his full name." JSZ had gained full access to the networks of IBM, Sun and others. Mitnick didn't press for details. "I was a fugitive," he says. "I didn't want to make him nervous."

•

In early 1994 prosecutor David Schindler convened a meeting at the FBI office in Los Angeles with the embarrassed and alarmed representatives of major cell phone manufacturers who had been hit in a spate of hacker attacks. There were no introductions. "I had to dole out aliases," Schindler recalls. "This guy was from company A, this guy was from company B. It was a quid pro quo. They wouldn't do it any other way." They all had the same goal: to stop the intruder or intruders from gaining access to R&D they feared might cost them hundreds of millions of dollars in the marketplace if it fell into the hands of competitors or foreign governments.

Everyone suspected Mitnick. "It would be a pretty big coincidence if all of a sudden multiple hackers within days or weeks were looking for the same thing," Schindler says. Assuming Mitnick was behind the attacks, Schindler pondered his motives. "What's the purpose of gathering all this code? Is somebody sponsoring him? Is he selling it? From a threat assessment, what can he do with it?"

The intrusions only highlighted the FBI's limitations in fighting cybercrime. Mitnick boasted an electronic dossier on his pursuers: cell numbers, Social Security numbers, addresses, aliases. In contrast, the FBI knew relatively little about Mitnick. Then something unexpected threw the hacker off course. He was fired. The Denver law firm suspected he was consulting during office hours. Mitnick retired Eric Weiss and started the laborious process of stepping into a new identity he had been grooming for more than a year, Brian Merrill. A month later Mitnick took a train to Seattle, arriving late and checking into a downtown hotel.

On July 4 Mitnick's pager buzzed just after dawn, flashing 3—an emergency—and 000—the code for Mom. Mitnick phoned the Sahara in Las Vegas and asked the operator to page someone. Mitnick's mom, a waitress in Vegas, knew

her pseudonyms, so when she heard "Paging Betty Sue Miller," she knew her fugitive son was on the line.

Mom told him to find a copy of *The New York Times*. Mitnick stared in disbelief at his face on the front page—a scruffy booking photo taken a few years earlier. Under the headline CYBERSPACE'S MOST WANTED: HACKER ELUDES FBI PURSUIT, the story by *Times* tech reporter John Markoff began, "Combining technical wizardry with the ages-old guile of a grifter, Kevin Mitnick is a computer programmer run amok. And law enforcement officials cannot seem to catch up with him."

•

All along Mitnick had been keeping tabs on Ken McGuire, the FBI agent tasked with bringing him to justice. But he couldn't imagine the bigger threat that would come when he hacked a man whose role and motivations were less clear. It happened by accident. Mitnick decided to attack a fellow hacker who was under federal indictment. The hacker was selling a mobile hacker kit, software and accessories to transform the OKI 900 cell phone into a laptop-powered portable handheld scanner and wiretapping system.

Mitnick wasn't in the habit of paying for his software. He dropped in for an uninvited visit to the man's network and grabbed everything: personal e-mail, files, programs. Poring through his electronic spoils with JSZ, Mitnick hoped to discover that the hacker had reverse-engineered the OKI, taking it apart and putting it back together to unlock its secrets. Sure enough, he had, but the biggest surprise was that the eavesdropping kit was developed with the help of Tsutomu Shimomura. JSZ knew Shimomura by reputation only and told Mitnick he was arrogant, though in the dicey netherworld of hacking he was considered one of the cowboys wearing a white hat. So why would Shimomura help a hacker design a custom fix for counter-surveillance and eavesdropping? Mitnick and JSZ decided they needed to find out what Shimomura was up to.

On Christmas Day JSZ struck the computer of a friend of Shimomura's in Silicon Valley. First came the automatic spoof—a 16-second burst of packets that flooded the trusted server. The attack unlocked a signature footprint that acted like certified mail, acknowledging the receipt of a packet. The attack program fired packets at Shimomura's machine, packets that appeared to be coming from the trusted machine. Next came the fake acknowledgement—a veritable handshake. Duped, Shimomura's workstation thought it should trust this server. The attack program ordered Shimomura's machine to trust the entire Internet—a security expert's worst nightmare.

Mitnick was back in Denver. After narrowly escaping arrest by the Secret Service in Seattle, he had fled to southern California. This was a stopover on his way to North Carolina. JSZ e-mailed him. "I usually don't celebrate Christmas," the Israeli hacker told him, "but I got you a present: I got into Shimomura's system." Mitnick ran to his computer. The Israeli had set up a back door, and just like that, Mitnick too was in—with full control. He shoveled as much of Shimomura's e-mail, data and security programs as he could into an online stash.

Culling through his spoils, Mitnick found e-mails between Shimomura and Markoff, the *Times* reporter, stretching back several years. They're close, they're buddies, Mitnick thought as he examined the long digital trail. He couldn't believe what he was reading. Shimomura had been in direct contact with the FBI for years. An FBI agent had even asked Shimomura what prizes should be given for a successful sanctioned hack into the Bureau's D.C. headquarters. And there was more: a secret channel. Markoff had an e-mail account on the computers at the federally subsidized San Diego Supercomputer Center. Shimomura was not only sending e-mails to the *Times*, inquiring into the activities and whereabouts of "Kevin" and "KDM," he was communicating with the reporter in a sector Shimomura assumed would be perfectly secure: his own seemingly impenetrable government computer network. It was quite a twist for Mitnick. The hacker was accustomed to outsmarting his pursuers with his electronic tricks. Now he wondered if a trap was being laid for him by someone other than the FBI.

A month later the attack on Shimomura made the front page of the *Times*. Markoff warned that the technique used to access Shimomura's computer "leaves many of the 20 million government, business, university and home computers on the global Internet vulnerable." The story caught fire. The U.S. Marshals' office issued a press release requesting the public's assistance in capturing Mitnick, reciting his alleged crimes, including the fanciful idea that he had compromised NORAD. Markoff profiled Shimomura in a dramatic article. "It was as if the thieves, to prove their prowess, had burglarized the locksmith," he wrote, "which is why Tsutomu Shimomura, the keeper of the keys in this case, is taking the break-in as a personal affront and why he considers solving the crime a matter of honor."

As the saying goes, the rest is legend. Shimomura met with representatives from the companies that had been victimized. A federal prosecutor in San Francisco gave Shimomura, a private citizen, extraordinary access to phone traps and traces, and from there it was a straightforward matter for the security expert to bring his quarry to the ground. On February 12, 1995 Shimomura flew to Raleigh, North Carolina, where Markoff joined him hours later. Shimomura started tooling around in a car with a Sprint cellular technician and a scanner, tracking Mitnick's cell phone

calls. "I remember being furious when I learned a reporter was there," says David Schindler, the former federal prosecutor. "That gave me a window into the extent to which there was this parallel plan, that this was something more than the capture of Kevin Mitnick." After two years on the run Mitnick had gotten sloppy and hadn't even bothered to mask his calls. He'd only just arrived in Raleigh, and he knew how slowly the FBI normally moves. When agents knocked on his apartment door shortly after midnight, it was some time before he cracked it open.

In his story the next day, Markoff quoted Kent Walker, the San Francisco prosecutor, as saying, "Mitnick was clearly the most wanted computer hacker in the world. He allegedly had access to trade secrets worth billions of dollars. He was a very big threat."

Shimomura and Markoff promptly wrote the book *Takedown* and sold the movie rights. (The resulting film never played in U.S. theaters.) The security man and the reporter split more than $1.5 million.

Four years passed before Mitnick and his lawyers were allowed to view the digital evidence. JSZ, who has never been identified, told Mitnick he had taken a job on Wall Street. Shimomura was heralded as a hero by the government and the media. Damage claims ran into the hundreds of millions of dollars, boosted by an FBI agent who told corporations to claim the entire development cost of their stolen software. After Mitnick had spent years in jail without being tried, a "Free Mitnick" campaign began in the digital underground, and hackers defaced the *New York Times* website, demanding his release.

Mitnick eventually pleaded guilty to phone fraud and violating his probation; he served five years before being released in January 2000. Almost immediately Congress requested his testimony in a televised hearing. As the Associated Press put it, "The government that imprisoned the world's most infamous computer hacker for nearly five years sought his advice Thursday about how to keep its own networks safe from intruders." Mitnick was a hit, and the hacker began receiving speaking requests. After a fight in federal court, he earned the right to lecture and eventually consult for government agencies and corporations. Remember Frank Abagnale, whom Mitnick spoke with after they shared billing at the golf retreat? In the mid-1970s the government released Abagnale from prison early because it wanted him to train law enforcement agencies and companies to stop fraud. You can't help but wonder if things would have turned out differently had Mitnick been given that opportunity. It almost happened. I found an extraordinary footnote buried in the thousands of pages in the hacker's criminal file. When Mitnick was facing his first serious jail time as a teenager for breaking into USC's computers, a tall, monklike security expert named Donn Parker had petitioned the court to use the young hacker's "intelligence and experience" to prepare a Justice Department report on preventing intrusions.

The judge thought it was a terrible idea.