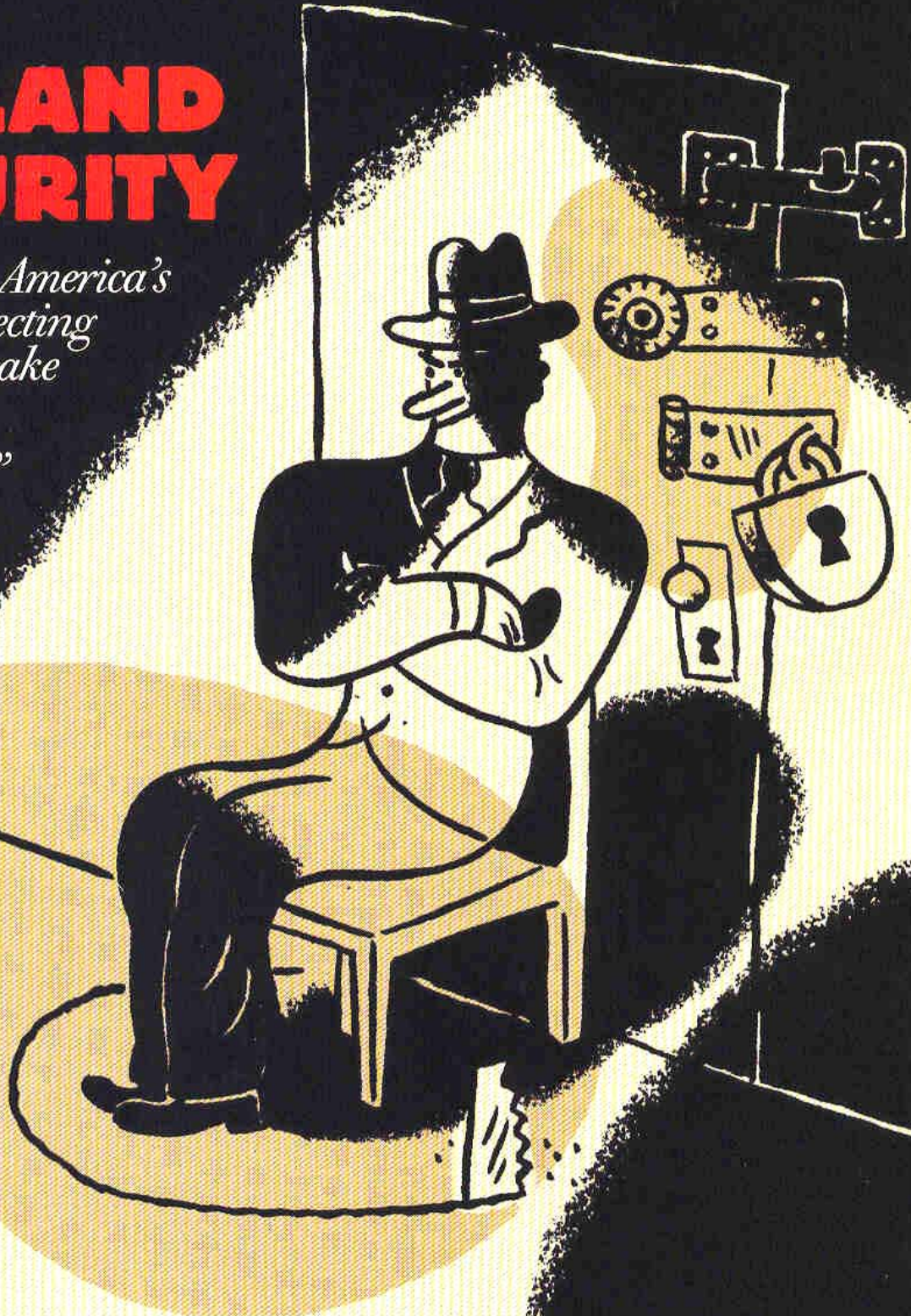# SPECIAL REPORT

HOMELAND INSECURITY

A top expert says America's approach to protecting itself will only make matters worse.

Forget "foolproof" technology—we need systems designed to fail smartly.

BY CHARLES C. MANN

Illustrations by Marc Rosenthal

HOMELAND INSECURITY

☛ *To stop the rampant theft of expensive cars, manufacturers in the 1990s began to make ignitions very difficult to hot-wire. This reduced the likelihood that cars would be stolen from parking lots—but apparently contributed to the sudden appearance of a new and more dangerous crime, carjacking.*

☛ *After a vote against management Vivendi Universal announced earlier this year that its electronic shareholder-voting system, which it had adopted to tabulate votes efficiently and securely, had been broken into by hackers. Because the new system eliminated the old paper ballots, recounting the votes— or even independently verifying that the attack had occurred—was impossible.*

☛ *To help merchants verify and protect the identity of their customers, marketing firms and financial institutions have created large computerized databases of personal information: Social Security numbers, credit-card numbers, telephone numbers, home addresses, and the like. With these databases being increasingly interconnected by means of the Internet, they have become irresistible targets for criminals. From 1995 to 2000 the incidence of identity theft tripled.*

As was often the case, Bruce Schneier was thinking about a really terrible idea. We were driving around the suburban-industrial wasteland south of San Francisco, on our way to a corporate presentation, while Schneier looked for something to eat not purveyed by a chain restaurant. This was important to Schneier, who in addition to being America's best-known ex-cryptographer is a food writer for an alternative newspaper in Minneapolis, where he lives. Initially he had been sure that in the crazy ethnic salad of Silicon Valley it would be impossible not to find someplace of culinary interest—a Libyan burger stop, a Hmong bagelry, a Szechuan taco stand. But as the rented car swept toward the vast, amoeboid office complex that was our destination, his faith slowly crumbled. Bowing to reality, he parked in front of a nondescript sandwich shop, disappointment evident on his face.

Schneier is a slight, busy man with a dark, full, closely cropped beard. Until a few years ago he was best known as a prominent creator of codes and ciphers; his book *Applied Cryptography* (1993) is a classic in the field. But despite his success he virtually abandoned cryptography in 1999 and co-founded a company named Counterpane Internet Security. Counterpane has spent considerable sums on advanced engineering, but at heart the company is dedicated to bringing one of the oldest forms of policing—the cop on the beat—to the digital realm. Aided by high-tech sensors, human guards at Counterpane patrol computer networks, helping corporations and governments to keep their secrets secret. In a world that is both ever more interconnected and full of malice, this is a task of considerable difficulty and great importance. It is also what Schneier long believed cryptography would do—which brings us back to his terrible idea.

"Pornography!" he exclaimed. If the rise of the Internet has shown anything, it is that huge numbers of middle-class, middle-management types like to look at dirty pictures on computer screens. A good way to steal the corporate or government secrets these middle managers are privy to, Schneier said, would be to set up a pornographic Web site. The Web site would be free, but visitors would have to register to download the naughty bits. Registration would involve creating a password—and here Schneier's deep-set blue eyes widened mischievously.

People have trouble with passwords. The idea is to have a random string of letters, numbers, and symbols that is easy to remember. Alas, random strings are by their nature hard to remember, so people use bad but easy-to-remember pass-

words, such as "hello" and "password." (A survey last year of 1,200 British office workers found that almost half chose their own name, the name of a pet, or that of a family member as a password; others based their passwords on the names Darth Vader and Homer Simpson.) Moreover, computer users can't keep different passwords straight, so they use the same bad passwords for all their accounts.

Many of his corporate porn surfers, Schneier predicted, would use for the dirty Web site the same password they used at work. Not only that, many users would surf to the porn site on the fast Internet connection at the office. The operators of Schneier's nefarious site would thus learn that, say, "Joesmith," who accessed the Web site from Anybusiness.com, used the password "JoeS." By trying to log on at Anybusiness.com as "Joesmith," they could learn whether "JoeS" was also the password into Joesmith's corporate account. Often it would be.

"In six months you'd be able to break into Fortune 500 companies and government agencies all over the world," Schneier said, chewing his nondescript meal. "It would work! It would work—that's the awful thing."

During the 1990s Schneier was a field marshal in the disheveled army of computer geeks, mathematicians, civil-liberties activists, and libertarian wackos that—in a series of bitter lawsuits that came to be known as the Crypto Wars—asserted the right of the U.S. citizenry to use the cryptographic equivalent of kryptonite: ciphers so powerful they cannot be broken by any government, no matter how long and hard it tries. Like his fellows, he believed that "strong crypto," as these ciphers are known, would forever guarantee the privacy and security of information—something that in the Information Age would be vital to people's lives. "It is insufficient to protect ourselves with laws," he wrote in *Applied Cryptography*. "We need to protect ourselves with mathematics."

Schneier's side won the battle as the nineties came to a close. But by that time he had realized that he was fighting the wrong war. Crypto was not enough to guarantee privacy and security. Failures occurred all the time—which was what Schneier's terrible idea demonstrated. No matter what kind of technological safeguards an organization uses, its secrets will never be safe while its employees are sending their passwords, however unwittingly, to pornographers— or to anyone else outside the organization.

The Parable of the Dirty Web Site illustrates part of what became the thesis of Schneier's most recent book, *Secrets and Lies* (2000): The way people think about security, especially security on computer networks, is almost always wrong. All too often planners seek technological cure-alls, when such security measures at best limit risks to acceptable levels. In particular, the consequences of going wrong—and all these systems go wrong sometimes—are rarely considered. For these reasons Schneier believes that most of the security measures envisioned after September 11 will be ineffective, and that some will make Americans *less* safe.

It is now a year since the World Trade Center was destroyed. Legislators, the law-enforcement community, and the Bush Administration are embroiled in an essential debate over the measures necessary to prevent future attacks. To armor-plate the nation's security they increasingly look to the most powerful technology available: retina, iris, and fingerprint scanners; "smart" driver's licenses and visas that incorporate anti-counterfeiting chips; digital surveillance of public places with face-recognition software; huge centralized databases that use data-mining routines to sniff out hidden terrorists. Some of these measures have already been mandated by Congress, and others are in the pipeline. State and local agencies around the nation are adopting their own schemes. More mandates and more schemes will surely follow.

Schneier is hardly against technology—he's the sort of person who immediately cases public areas for outlets to recharge the batteries in his laptop, phone, and

other electronic prostheses. "But if you think technology can solve your security problems," he says, "then you don't understand the problems and you don't understand the technology." Indeed, he regards the national push for a high-tech salve for security anxieties as a reprise of his own early and erroneous beliefs about the transforming power of strong crypto. The new technologies have enormous capacities, but their advocates have not realized that the most critical aspect of a security measure is not how well it works but how well it fails.

THE CRYPTO WARS

If mathematicians from the 1970s were suddenly transported through time to the present, they would be happily surprised by developments such as the proofs to Kepler's conjecture (proposed in 1611, confirmed in 1998) and to Fermat's last theorem (1637, 1994). But they would be absolutely astonished by the RSA Conference, the world's biggest trade show for cryptographers. Sponsored by the cryptography firm RSA Security, the conferences are attended by as many as 10,000 cryptographers, computer scientists, network managers, and digital-security professionals. What would amaze past mathematicians is not just the number of conferences but that they exist at all.

Cryptology is a specialized branch of mathematics with some computer science thrown in. As recently as the 1970s there were no cryptology courses in university mathematics or computer-science departments; nor were there crypto textbooks, crypto journals, or crypto software. There was no private crypto industry, let alone venture-capitalized crypto start-ups giving away key rings at trade shows (*crypto key* rings—techno-humor). Cryptography, the practice of cryptology, was the province of a tiny cadre of obsessed amateurs, the National Security Agency, and the NSA's counterparts abroad. Now it is a multibillion-dollar field with applications in almost every commercial arena.

As one of the people who helped to bring this change about, Schneier is always invited to speak at RSA conferences. Every time, the room is too small, and overflow crowds, eager to hear their favorite guru, force the session into a larger venue, which is what happened when I saw him speak at an RSA conference in San Francisco's Moscone Center last year. There was applause from the hundreds of seated cryptophiles when Schneier mounted the stage, and more applause from the throng standing in the aisles and exits when he apologized for the lack of seating capacity. He was there to talk about the state of computer security, he said. It was as bad as ever, maybe getting worse.

In the past security officers were usually terse ex-military types who wore holsters and brush cuts. But as computers have become both attackers' chief targets and their chief weapons, a new generation of security professionals has emerged, drawn from the ranks of engineering and computer science. Many of the new guys look like people the old guard would have wanted to arrest, and Schneier is no exception. Although he is a co-founder of a successful company, he sometimes wears scuffed black shoes and pants with a wavering press line; he gathers his thinning hair into a straggly ponytail. Ties, for the most part, are not an issue. Schneier's style marks him as a true nerd—someone who knows the potential, both good and bad, of technology, which in our technocentric era is an asset.

Schneier was raised in Brooklyn. He got a B.S. in physics from the University of Rochester in 1985 and an M.S. in computer science from American University two years later. Until 1991 he worked for the Department of Defense, where he did things he won't discuss. Lots of kids are intrigued by codes and ciphers, but Schneier was surely one of the few to ask his father, a lawyer and a judge, to write secret messages for him to analyze. On his first visit to a voting booth, with his mother, he tried to figure out how she could cheat and vote twice. He didn't actually want her to vote twice—he just wanted, as he says, to "game the system."

The way people think about security, especially security on computer networks, is almost always wrong. All too often planners seek cures, magic bullets to make problems vanish. Most of the security measures envisioned after September 11 will be ineffective— and some will even make Americans less safe than they would be without them.

Unsurprisingly, someone so interested in figuring out the secrets of manipulating the system fell in love with the systems for manipulating secrets. Schneier's childhood years, as it happened, were a good time to become intrigued by cryptography—the best time in history, in fact. In 1976 two researchers at Stanford University invented an entirely new type of encryption, public-key encryption, which abruptly woke up the entire field.

Public-key encryption is complicated in detail but simple in outline. All ciphers employ mathematical procedures called algorithms to transform messages from their original form into an unreadable jumble. (Cryptographers work with ciphers and not codes, which are spy-movie-style lists of prearranged substitutes for letters, words, or phrases—"meet at the theater" for "attack at nightfall.") Most ciphers use secret keys: mathematical values that plug into the algorithm. Breaking a cipher means figuring out the key. In a kind of mathematical sleight of hand, public-key encryption encodes messages with keys that can be published openly and decodes them with different keys that stay secret and are effectively impossible to break using today's technology. (A more complete explanation of public-key encryption is on *The Atlantic*'s Web site, www.theatlantic.com.)

The best-known public-key algorithm is the RSA algorithm, whose name comes from the initials of the three mathematicians who invented it. RSA keys are created by manipulating big prime numbers. If the private decoding RSA key is properly chosen, guessing it necessarily involves factoring a very large number into its constituent primes, something for which no mathematician has ever devised an adequate shortcut. Even if demented government agents spent a trillion dollars on custom factoring computers, Schneier has estimated, the sun would likely go nova before they cracked a message enciphered with a public key of sufficient length.

Schneier and other technophiles grasped early how important computer networks would become to daily life. They also understood that those networks were dreadfully insecure. Strong crypto, in their view, was an answer of almost magical efficacy. Even federal officials believed that strong crypto would Change Everything Forever—except they thought the change would be for the worse. Strong encryption "jeopardizes the public safety and national security of this country," Louis Freeh, then the director of the (famously computer-challenged) Federal Bureau of Investigation, told Congress in 1995. "Drug cartels, terrorists, and kidnappers will use telephones and other communications media with impunity knowing that their conversations are immune" from wiretaps.

The Crypto Wars erupted in 1991, when Washington attempted to limit the spread of strong crypto. Schneier testified before Congress against restrictions on encryption, campaigned for crypto freedom on the Internet, co-wrote an influential report on the technical snarls awaiting federal plans to control cryptographic protocols, and rallied 75,000 crypto fans to the cause in his free monthly e-mail newsletter, *Crypto-Gram* (www.counterpane.com/crypto-gram.html). Most important, he wrote *Applied Cryptography*, the first-ever comprehensive guide to the practice of cryptology.

Washington lost the wars in 1999, when an appellate court ruled that restrictions on cryptography were illegal, because crypto algorithms were a form of speech and thus covered by the First Amendment. After the ruling the FBI and the NSA more or less surrendered. In the sudden silence the dazed combatants surveyed the battleground. Crypto had become widely available, and it had indeed fallen into unsavory hands. But the results were different from what either side had expected.

As the crypto aficionados had envisioned, software companies inserted crypto into their products. On the "Tools" menu in Microsoft Outlook, for example, "encrypt" is an option. And encryption became big business, as part of the infrastructure for e-commerce—it is the little padlock that appears in the corner

WHY THE MAGINOT LINE FAILED

In fact, the Maginot Line, the chain of fortifications on France's border with Germany, was indicative neither of despair about defeating Germany nor of thought mired in the past. It was instead evidence of faith that technology could substitute for manpower. It was a forerunner of the strategic bomber, the guided missile, and the "smart bomb." The same faith led to France's building tanks with thicker armor and bigger guns than German tanks had, deploying immensely larger quantities of mobile big guns, and above all committing to maintain a continuous line—that is, advancing or retreating in such coordination as to prevent an enemy from establishing a salient from which it could cut off a French unit from supplies and reinforcements. (Today, military strategists call this "force protection.") But having machines do the work of men and putting emphasis on minimal loss of life carried a price in sloweddown reaction times and lessened initiative for battlefield commanders.

—*Ernest R. May,* Strange Victory: Hitler's Conquest of France *(2000)*

of Net surfers' browsers when they buy books at Amazon.com, signifying that credit-card numbers are being enciphered. But encryption is rarely used by the citizenry it was supposed to protect and empower. Cryptophiles, Schneier among them, had been so enraptured by the possibilities of uncrackable ciphers that they forgot they were living in a world in which people can't program VCRs. Inescapably, an encrypted message is harder to send than an unencrypted one, if only because of the effort involved in using all the extra software. So few people use encryption software that most companies have stopped selling it to individuals.

Among the few who do use crypto are human-rights activists living under dictatorships. But, just as the FBI feared, terrorists, child pornographers, and the Mafia use it too. Yet crypto has not protected any of them. As an example, Schneier points to the case of Nicodemo Scarfo, who the FBI believed was being groomed to take over a gambling operation in New Jersey. Agents surreptitiously searched his office in 1999 and discovered that he was that rarity, a gangster nerd. On his computer was the long-awaited nightmare for law enforcement: a crucial document scrambled by strong encryption software. Rather than sit by, the FBI installed a "keystroke logger" on Scarfo's machine. The logger recorded the decrypting key—or, more precisely, the passphrase Scarfo used to generate that key—as he typed it in, and gained access to his incriminating files. Scarfo pleaded guilty to charges of running an illegal gambling business on February 28 of this year.

Schneier was not surprised by this demonstration of the impotence of cryptography. Just after the Crypto Wars ended, he had begun writing a follow-up to *Applied Cryptography*. But this time Schneier, a fluent writer, was blocked—he couldn't make himself extol strong crypto as a security panacea. As Schneier put it in *Secrets and Lies*, the very different book he eventually did write, he had been portraying cryptography—in his speeches, in his congressional testimony, in *Applied Cryptography*—as "a kind of magic security dust that [people] could sprinkle over their software and make it secure." It was not. Nothing could be. Humiliatingly, Schneier discovered that, as a friend wrote him, "the world was full of bad security systems designed by people who read *Applied Cryptography*."

In retrospect he says, "Crypto solved the wrong problem." Ciphers scramble messages and documents, preventing them from being read while, say, they are transmitted on the Internet. But the strongest crypto is gossamer protection if malevolent people have access to the computers on the other end. Encrypting transactions on the Internet, the Purdue computer scientist Eugene Spafford has remarked, "is the equivalent of arranging an armored car to deliver credit-card information from someone living in a cardboard box to someone living on a park bench."

To effectively seize control of Scarfo's computer, FBI agents had to break into his office and physically alter his machine. Such black-bag jobs are ever less necessary, because the rise of networks and the Internet means that computers can be controlled remotely, without their operators' knowledge. Huge computer databases may be useful, but they also become tempting targets for criminals and terrorists. So do home computers, even if they are connected only intermittently to the Web. Hackers look for vulnerable machines, using software that scans thousands of Net connections at once. This vulnerability, Schneier came to think, is the real security issue.

THE WORM IN THE MACHINE

Buffer overflows (sometimes called *stack smashing*) are the most common form of security vulnerability in the last ten years. They're also the easiest to exploit; more attacks are the result of buffer overflows than any other problem ...

Computers store everything, programs and data, in memory. If the computer asks a user for an 8-character password and receives a 200-character password, those extra characters may overwrite some other area in memory. (They're not supposed to— that's the bug.) If it is just the right area of memory, and we overwrite it with just the right characters, we can change a "deny connection" instruction to an "allow access" command or even get our own code executed.

The Morris worm is probably the most famous overflow-bug exploit. It exploited a buffer overflow in the UNIX fingerd program. It's supposed to be a benign program, returning the identity of a user to whomever asks. This program accepted as input a variable that is supposed to contain the identity of the user. Unfortunately, the fingerd program never limited the size of the input. Input larger than 512 bytes overflowed the buffer, and Morris wrote a specific large input that allowed his rogue program to [install and run] itself ... Over 6,000 servers crashed as a result; at the time [in 1988] that was about 10 percent of the Internet.

Skilled programming can prevent this kind of attack. The program can truncate the password at 8 characters, so those extra 192 characters never get written into memory anywhere ...The problem is that with any piece of modern, large, complex code, there are just too many places where buffer overflows are possible ... It's very difficult to guarantee that there are no overflow problems, even if you take the time to check. The larger and more complex the code is, the more likely the attack.

Windows 2000 has somewhere between 35 and 60 million lines of code, and no one outside the programming team has ever seen them.

— Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* (2000)

With this realization he closed Counterpane Systems, his five-person crypto-consulting company in Chicago, in 1999. He revamped it and reopened immediately in Silicon Valley with a new name, Counterpane Internet Security, and a new idea—one that relied on old-fashioned methods. Counterpane would still keep data secret. But the lessons of the Crypto Wars had given Schneier a different vision of how to do that—a vision that has considerable relevance for a nation attempting to prevent terrorist crimes.

Where Schneier had sought one overarching technical fix, hard experience had taught him the quest was illusory. Indeed, yielding to the American penchant for all-in-one high-tech solutions can make us *less* safe—especially when it leads to enormous databases full of confidential information. Secrecy is important, of course, but it is also a trap. The more secrets necessary to a security system, the more vulnerable it becomes.

To forestall attacks, security systems need to be small-scale, redundant, and compartmentalized. Rather than large, sweeping programs, they should be carefully crafted mosaics, each piece aimed at a specific weakness. The federal government and the airlines are spending millions of dollars, Schneier points out, on systems that screen every passenger to keep knives and weapons out of planes. But what matters most is keeping dangerous passengers out of airline cockpits, which can be accomplished by reinforcing the door. Similarly, it is seldom necessary to gather large amounts of additional information, because in modern societies people leave wide audit trails. The problem is sifting through the already existing mountain of data. Calls for heavy monitoring and record-keeping are thus usually a mistake. ("Broad surveillance is a mark of bad security," Schneier wrote in a recent *Crypto-Gram.*)

To halt attacks once they start, security measures must avoid being subject to single points of failure. Computer networks are particularly vulnerable: once hackers bypass the firewall, the whole system is often open for exploitation. Because every security measure in every system can be broken or gotten around, failure must be incorporated into the design. No single failure should compromise the normal functioning of the entire system or, worse, add to the gravity of the initial breach. Finally, and most important, decisions need to be made by people at close range—and the responsibility needs to be given explicitly to people, not computers.

Unfortunately, there is little evidence that these principles are playing any role in the debate in the Administration, Congress, and the media about how to protect the nation. Indeed, in the argument over policy and principle almost no one seems to be paying attention to the practicalities of security—a lapse that Schneier, like other security professionals, finds as incomprehensible as it is dangerous.

STEALING YOUR THUMB

A couple of months after September 11, I flew from Seattle to Los Angeles to meet Schneier. As I was checking in at Sea-Tac Airport, someone ran through the metal detector and disappeared onto the little subway that runs among the terminals. Although the authorities quickly identified the miscreant, a concession stand worker, they still had to empty all the terminals and re-screen everyone in the airport, including passengers who had already boarded planes. Masses of unhappy passengers stretched back hundreds of feet from the checkpoints. Planes by the dozen sat waiting at the gates. I called Schneier on a cell phone to report my delay. I had to shout over the noise of all the other people on their cell phones making similar calls. "What a mess," Schneier said. "The problem with airport security, you know, is that it fails badly."

For a moment I couldn't make sense of this gnomic utterance. Then I realized he meant that when something goes wrong with security, the system should

> The moral, Schneier came to believe, is that security measures are characterized less by their success than by their manner of failure. All security systems eventually miscarry in one way or another. But when this happens to the good ones, they stretch and sag before breaking, each component failure leaving the whole as unaffected as possible.

recover well. In Seattle a single slip-up shut down the entire airport, which delayed flights across the nation. Sea-Tac, Schneier told me on the phone, had no adequate way to contain the damage from a breakdown—such as a button installed near the x-ray machines to stop the subway, so that idiots who bolt from checkpoints cannot disappear into another terminal. The shutdown would inconvenience subway riders, but not as much as being forced to go through security again after a wait of several hours. An even better idea would be to place the x-ray machines at the departure gates, as some are in Europe, in order to scan each group of passengers closely and minimize inconvenience to the whole airport if a risk is detected—or if a machine or a guard fails.

Schneier was in Los Angeles for two reasons. He was to speak to ICANN, the Internet Corporation for Assigned Names and Numbers, which controls the "domain name system" of Internet addresses. It is Schneier's belief that attacks on the address database are the best means of taking down the Internet. He also wanted to review Ginza Sushi-Ko, perhaps the nation's most exclusive restaurant, for the food column he writes with his wife, Karen Cooper.

Minutes after my delayed arrival Schneier had with characteristic celerity packed himself and me into a taxi. The restaurant was in a shopping mall in Beverly Hills that was disguised to look like a collection of nineteenth-century Italian villas. By the time Schneier strode into the tiny lobby, he had picked up the thread of our airport discussion. Failing badly, he told me, was something he had been forced to spend time thinking about.

In his technophilic exuberance he had been seduced by the promise of public-key encryption. But ultimately Schneier observed that even strong crypto fails badly. When something bypasses it, as the keystroke logger did with Nicodemo Scarfo's encryption, it provides no protection at all. The moral, Schneier came to believe, is that security measures are characterized less by their manner of success than by their manner of failure. All security systems eventually miscarry. But when this happens to the good ones, they stretch and sag before breaking, each component failure leaving the whole as unaffected as possible. Engineers call such failure-tolerant systems "ductile." One way to capture much of what Schneier told me is to say that he believes that when possible, security schemes should be designed to maximize ductility, whereas they often maximize strength.

Since September 11 the government has been calling for a new security infrastructure—one that employs advanced technology to protect the citizenry and track down malefactors. Already the USA PATRIOT Act, which Congress passed in October, mandates the establishment of a "cross-agency, cross-platform electronic system … to confirm the identity" of visa applicants, along with a "highly secure network" for financial-crime data and "secure information sharing systems" to link other, previously separate databases. Pending legislation demands that the Attorney General employ "technology including, but not limited to, electronic fingerprinting, face recognition, and retinal scan technology." The proposed Department of Homeland Security is intended to oversee a "national research and development enterprise for homeland security comparable in emphasis and scope to that which has supported the national security community for more than fifty years"—a domestic version of the high-tech R&D juggernaut that produced stealth bombers, smart weapons, and anti-missile defense.

Iris, retina, and fingerprint scanners; hand-geometry assayers; remote video-network surveillance; face-recognition software; smart cards with custom identification chips; decompressive baggage checkers that vacuum-extract minute chemical samples from inside suitcases; tiny radio implants beneath the skin that continually broadcast people's identification codes; pulsed fast-neutron analysis of shipping containers ("so precise," according to one manufacturer, "it can determine within inches the location of the concealed target"); a vast national network of

interconnected databases—the list goes on and on. In the first five months after the terrorist attacks the Pentagon liaison office that works with technology companies received more than 12,000 proposals for high-tech security measures. Credit-card companies expertly manage credit risks with advanced information-sorting algorithms, Larry Ellison, the head of Oracle, the world's biggest database firm, told *The New York Times* in April; "We should be managing security risks in exactly the same way." To "win the war on terrorism," a former deputy undersecretary of commerce, David J. Rothkopf, explained in the May/June issue of *Foreign Policy*, the nation will need "regiments of geeks"—"pocket-protector brigades" who "will provide the software, systems, and analytical resources" to "close the gaps Mohammed Atta and his associates revealed."

Such ideas have provoked the ire of civil-liberties groups, which fear that governments, corporations, and the police will misuse the new technology. Schneier's concerns are more basic. In his view, these measures can be useful, but their large-scale application will have little effect against terrorism. Worse, their use may make Americans less safe, because many of these tools fail badly—they're "brittle," in engineering jargon. Meanwhile, simple, effective, ductile measures are being overlooked or even rejected.

The distinction between ductile and brittle security dates back, Schneier has argued, to the nineteenth-century linguist and cryptographer Auguste Kerckhoffs, who set down what is now known as Kerckhoffs's principle. In good crypto systems, Kerckhoffs wrote, "the system should not depend on secrecy, and it should be able to fall into the enemy's hands without disadvantage." In other words, it should permit people to keep messages secret even if outsiders find out exactly how the encryption algorithm works.

At first blush this idea seems ludicrous. But contemporary cryptography follows Kerckhoffs's principle closely. The algorithms—the scrambling methods—are openly revealed; the only secret is the key. Indeed, Schneier says, Kerckhoffs's principle applies beyond codes and ciphers to security systems in general: every secret creates a potential failure point. Secrecy, in other words, is a prime cause of brittleness—and therefore something likely to make a system prone to catastrophic collapse. Conversely, openness provides ductility.

From this can be drawn several corollaries. One is that plans to add new layers of secrecy to security systems should automatically be viewed with suspicion. Another is that security systems that utterly depend on keeping secrets tend not to work very well. Alas, airport security is among these. Procedures for screening passengers, for examining luggage, for allowing people on the tarmac, for entering the cockpit, for running the autopilot software—all must be concealed, and all seriously compromise the system if they become known. As a result, Schneier wrote in the May issue of *Crypto-Gram*, brittleness "is an inherent property of airline security."

Few of the new airport-security proposals address this problem. Instead, Schneier told me in Los Angeles, they address problems that don't exist. "The idea that to stop bombings cars have to park three hundred feet away from the terminal, but meanwhile they can drop off passengers right up front like they always have ..." He laughed. "The only ideas I've heard that make any sense are reinforcing the cockpit door and getting the passengers to fight back." Both measures test well against Kerckhoffs's principle: knowing ahead of time that law-abiding passengers may forcefully resist a hijacking en masse, for example, doesn't help hijackers to fend off their assault. Both are small-scale, compartmentalized measures that make the system more ductile, because no matter how hijackers get aboard, beefed-up doors and resistant passengers will make it harder for them to fly into a nuclear plant. And neither measure has any adverse effect on civil liberties.

The government has been calling for a new security infrastructure: iris, retina, and fingerprint scanners; hand-geometry assayers; face-recognition software; smart cards with custom identification chips. Their use may on the whole make Americans less safe, because many of these tools fail badly— they're "brittle," in engineering jargon.

Tsutomu Matsumoto, a Japanese cryptographer, recently decided to look at biometric fingerprint devices. These are security systems that attempt to identify people based on their fingerprint. For years the companies selling these devices have claimed that they are very secure, and that it is almost impossible to fool them into accepting a fake finger as genuine. Matsumoto, along with his students at the Yokohama National University, showed that they can be reliably fooled with a little ingenuity and $10 worth of household supplies.

Matsumoto uses gelatin, the stuff that Gummi Bears are made out of. First he takes a live finger and makes a plastic mold. (He uses a free-molding plastic used to make plastic molds, and is sold at hobby shops.) Then he pours liquid gelatin into the mold and lets it harden. (The gelatin comes in solid sheets, and is used to make jellied meats, soups, and candies, and is sold in grocery stores.) This gelatin fake finger fools fingerprint detectors about 80% of the time …

There's both a specific and a general moral to take away from this result. Matsumoto is not a professional fake-finger scientist; he's a mathematician. He didn't use expensive equipment or a specialized laboratory. He used $10 of ingredients you could buy, and whipped up his gummy fingers in the equivalent of a home kitchen. And he defeated eleven different commercial fingerprint readers, with both optical and capacitive sensors, and some with "live finger detection" features … If he could do this, then any semi-professional can almost certainly do much more.

—*Bruce Schneier*, Crypto-Gram,
May 15, 2002

Evaluations of a security proposal's merits, in Schneier's view, should not be much different from the ordinary cost-benefit calculations we make in daily life. The first question to ask of any new security proposal is, What problem does it solve? The second: What problems does it cause, especially when it fails?

Failure comes in many kinds, but two of the more important are simple failure (the security measure is ineffective) and what might be called subtractive failure (the security measure makes people less secure than before). An example of simple failure is face-recognition technology. In basic terms, face-recognition devices photograph people; break down their features into "facial building elements"; convert these into numbers that, like fingerprints, uniquely identify individuals; and compare the results with those stored in a database. If someone's facial score matches that of a criminal in the database, the person is detained. Since September 11 face-recognition technology has been placed in an increasing number of public spaces: airports, beaches, nightlife districts. Even visitors to the Statue of Liberty now have their faces scanned.

Face-recognition software could be useful. If an airline employee has to type in an identifying number to enter a secure area, for example, it can help to confirm that someone claiming to be that specific employee is indeed that person. But it cannot pick random terrorists out of the mob in an airline terminal. That much-larger-scale task requires comparing many sets of features with the many other sets of features in a database of people on a "watch list." Identix, of Minnesota, one of the largest face-recognition-technology companies, contends that in independent tests its FaceIt software has a success rate of 99.32 percent—that is, when the software matches a passenger's face with a face on a list of terrorists, it is mistaken only 0.68 percent of the time. Assume for the moment that this claim is credible; assume, too, that good pictures of suspected terrorists are readily available. About 25 million passengers used Boston's Logan Airport in 2001. Had face-recognition software been used on 25 million faces, it would have wrongly picked out just 0.68 percent of them—but that would have been enough, given the large number of passengers, to flag as many as 170,000 innocent people as terrorists. With almost 500 false alarms a day, the face-recognition system would quickly become something to ignore.

The potential for subtractive failure, different and more troublesome, is raised by recent calls to deploy biometric identification tools across the nation. Biometrics—"the only way to prevent identity fraud," according to the former senator Alan K. Simpson, of Wyoming—identifies people by precisely measuring their physical characteristics and matching them up against a database. The photographs on driver's licenses are an early example, but engineers have developed many high-tech alternatives, some of them already mentioned: fingerprint readers, voiceprint recorders, retina or iris scanners, face-recognition devices, hand-geometry assayers, even signature-geometry analyzers, which register pen pressure and writing speed as well as the appearance of a signature.

Appealingly, biometrics lets people be their own ID cards—no more passwords to forget! Unhappily, biometric measures are often implemented poorly. This past spring three reporters at *c't*, a German digital-culture magazine, tested a face-recognition system, an iris scanner, and nine fingerprint readers. All proved easy to outsmart. Even at the highest security setting, Cognitec's FaceVACS-Logon could be fooled by showing the sensor a short digital movie of someone known to the system—the president of a company, say—on a laptop screen. To beat Panasonic's Authenticam iris scanner, the German journalists photographed an authorized user, took the photo and created a detailed, life-size image of his eyes, cut out the pupils, and held the

image up before their faces like a mask. The scanner read the iris, detected the presence of a human pupil—and accepted the imposture. Many of the fingerprint readers could be tricked simply by breathing on them, reactivating the last user's fingerprint. Beating the more sophisticated Identix Bio-Touch fingerprint reader required a trip to a hobby shop. The journalists used graphite powder to dust the latent fingerprint—the kind left on glass—of a previous, authorized user; picked up the image on adhesive tape; and pressed the tape on the reader. The Identix reader, too, was fooled. Not all biometric devices are so poorly put together, of course. But all of them fail badly.

Consider the legislation introduced in May by Congressmen Jim Moran and Tom Davis, both of Virginia, that would mandate biometric data chips in driver's licenses—a sweeping, nationwide data-collection program, in essence. (Senator Dick Durbin, of Illinois, is proposing measures to force states to use a "single identifying designation unique to the individual on all driver's licenses"; President George W. Bush has already signed into law a requirement for biometric student visas.) Although Moran and Davis tied their proposal to the need for tighter security after last year's attacks, they also contended that the nation could combat fraud by using smart licenses with bank, credit, and Social Security cards, and for voter registration and airport identification. Maybe so, Schneier says. "But think about screw-ups, because the system *will* screw up."

Smart cards that store non-biometric data have been routinely cracked in the past, often with inexpensive oscilloscope-like devices that detect and interpret the timing and power fluctuations as the chip operates. An even cheaper method, announced in May by two Cambridge security researchers, requires only a bright light, a standard microscope, and duct tape. Biometric ID cards are equally vulnerable. Indeed, as a recent National Research Council study points out, the extra security supposedly provided by biometric ID cards will raise the economic incentive to counterfeit or steal them, with potentially disastrous consequences to the victims. "Okay, somebody steals your thumbprint," Schneier says. "Because we've centralized all the functions, the thief can tap your credit, open your medical records, start your car, any number of things. Now what do you do? With a credit card, the bank can issue you a new card with a new number. But this is your *thumb*—you can't get a new one."

The consequences of identity fraud might be offset if biometric licenses and visas helped to prevent terrorism. Yet smart cards would not have stopped the terrorists who attacked the World Trade Center and the Pentagon. According to the FBI, all the hijackers seem to have been who they said they were; their intentions, not their identities, were the issue. Each entered the country with a valid visa, and each had a photo ID in his real name (some obtained their IDs fraudulently, but the fakes correctly identified them). "What problem is being solved here?" Schneier asks.

Good security is built in overlapping, cross-checking layers, to slow down attacks; it reacts limberly to the unexpected. Its most important components are almost always human. "Governments have been relying on intelligent, trained guards for centuries," Schneier says. "They spot people doing bad things and then use laws to arrest them. All in all, I have to say, it's not a bad system."

THE HUMAN TOUCH

One of the first times I met with Schneier was at the Cato Institute, a libertarian think tank in Washington, D.C., that had asked him to speak about security. Afterward I wondered how the Cato people had reacted to the speech. Libertarians love cryptography, because they believe that it will let people keep their secrets forever, no matter what a government wants. To them, Schneier was a kind of hero, someone who fought the good fight. As a cryptog-

rapher, he had tremendous street cred: he had developed some of the world's coolest ciphers, including the first rigorous encryption algorithm ever published in a best-selling novel (*Cryptonomicon*, by Neal Stephenson) and the encryption for the "virtual box tops" on Kellogg's cereals (children type a code from the box top into a Web site to win prizes), and had been one of the finalists in the competition to write algorithms for the federal government's new encryption standard, which it adopted last year. Now, in the nicest possible way, he had just told the libertarians the bad news: he still loved cryptography for the intellectual challenge, but it was not all that relevant to protecting the privacy and security of real people.

In security terms, he explained, cryptography is classed as a protective counter-measure. No such measure can foil every attack, and all attacks must still be both detected and responded to. This is particularly true for digital security, and Schneier spent most of his speech evoking the staggering insecurity of networked computers. Countless numbers are broken into every year, including machines in people's homes. Taking over computers is simple with the right tools, because software is so often misconfigured or flawed. In the first five months of this year, for example, Microsoft released five "critical" security patches for Internet Explorer, each intended to rectify lapses in the original code.

Computer crime statistics are notoriously sketchy, but the best of a bad lot come from an annual survey of corporations and other institutions by the FBI and the Computer Security Institute, a research and training organization in San Francisco. In the most recent survey, released in April, 90 percent of the respondents had detected one or more computer-security breaches within the previous twelve months—a figure that Schneier calls "almost certainly an underestimate." His own experience suggests that a typical corporate network suffers a serious security breach four to six times a year—more often if the network is especially large or its operator is politically controversial.

Luckily for the victims, this digital mayhem is mostly wreaked not by the master hackers depicted in Hollywood techno-thrillers but by "script kiddies"— youths who know just enough about computers to download and run automated break-in programs. Twenty-four hours a day, seven days a week, script kiddies poke and prod at computer networks, searching for any of the thousands of known security vulnerabilities that administrators have not yet patched. A typical corporate network, Schneier says, is hit by such doorknob-rattling several times an hour. The great majority of these attacks achieve nothing, but eventually any existing security holes will be found and exploited. "It's very hard to communicate how bad the situation is," Schneier says, "because it doesn't correspond to our normal intuition of the world. To a first approximation, bank vaults are secure. Most of them don't get broken into, because it takes real skill. Computers are the opposite. Most of them get broken into all the time, and it takes practically no skill." Indeed, as automated cracking software improves, it takes ever less knowledge to mount ever more sophisticated attacks.

Given the pervasive insecurity of networked computers, it is striking that nearly every proposal for "homeland security" entails the creation of large national databases. The Moran-Davis proposal, like other biometric schemes, envisions storing smart-card information in one such database; the USA PATRIOT Act effectively creates another; the proposed Department of Homeland Security would "fuse and analyze" information from more than a hundred agencies, and would "merge under one roof" scores or hundreds of previously separate databases. (A representative of the new department told me no one had a real idea of the number. "It's a lot," he said.) Better coordination of data could have obvious utility, as was made clear by recent headlines about the failure of the FBI and the CIA to communicate. But carefully linking selected fields of data is different

"Okay, somebody steals your thumb-print," Schneier says. "Because we've centralized all the functions, the thief can tap your credit, open your medical records, start your car, any number of things. Now what do you do? With a credit card, the bank can issue you a new card with a new number. But this is your *thumb*—you can't get a new one."

from creating huge national repositories of information about the citizenry, as is being proposed. Larry Ellison, the CEO of Oracle, has dismissed cautions about such databases as whiny cavils that don't take into account the existence of murderous adversaries. But murderous adversaries are exactly why we should ensure that new security measures actually make American life safer.

Any new database must be protected, which automatically entails a new layer of secrecy. As Kerckhoffs's principle suggests, the new secrecy introduces a new failure point. Government information is now scattered through scores of databases; however inadvertently, it has been compartmentalized—a basic security practice. (Following this practice, tourists divide their money between their wallets and hidden pouches; pickpockets are less likely to steal it all.) Many new proposals would change that. An example is Attorney General John Ashcroft's plan, announced in June, to fingerprint and photograph foreign visitors "who fall into categories of elevated national security concern" when they enter the United States ("approximately 100,000" will be tracked this way in the first year). The fingerprints and photographs will be compared with those of "known or suspected terrorists" and "wanted criminals." Alas, no such database of terrorist fingerprints and photographs exists. Most terrorists are outside the country, and thus hard to fingerprint, and latent fingerprints rarely survive bomb blasts. The databases of "wanted criminals" in Ashcroft's plan seem to be those maintained by the FBI and the Immigration and Naturalization Service. But using them for this purpose would presumably involve merging computer networks in these two agencies with the visa procedure in the State Department—a security nightmare, because no one entity will fully control access to the system.

Equivalents of the big, centralized databases under discussion already exist in the private sector: corporate warehouses of customer information, especially credit-card numbers. The record there is not reassuring. "Millions upon millions of credit-card numbers have been stolen from computer networks," Schneier says. So many, in fact, that Schneier believes that everyone reading this article "has, in his or her wallet right now, a credit card with a number that has been stolen," even if no criminal has yet used it. Number thieves, many of whom operate out of the former Soviet Union, sell them in bulk: $1,000 for 5,000 credit-card numbers, or twenty cents apiece. In a way, the sheer volume of theft is fortunate: so many numbers are floating around that the odds are small that any one will be heavily used by bad guys.

Large-scale federal databases would undergo similar assaults. The prospect is worrying, given the government's long-standing reputation for poor information security. Since September 11 at least forty government networks have been publicly cracked by typographically challenged vandals with names like "CriminalS," "S4t4n1c S0uls," "cr1m3 0rg4n1z4d0," and "Discordian Dodgers." Summing up the problem, a House subcommittee last November awarded federal agencies a collective computer-security grade of F. According to representatives of Oracle, the federal government has been talking with the company about employing its software for the new central databases. But judging from the past, involving the private sector will not greatly improve security. In March, CERT/CC, a computer-security watchdog based at Carnegie Mellon University, warned of thirty-eight

vulnerabilities in Oracle's database software. Meanwhile, a centerpiece of the company's international advertising is the claim that its software is "unbreakable." Other software vendors fare no better: CERT/CC issues a constant stream of vulnerability warnings about every major software firm.

Schneier, like most security experts I spoke to, does not oppose consolidating and modernizing federal databases per se. To avoid creating vast new opportunities for adversaries, the overhaul should be incremental and small-scale. Even so, it would need to be planned with extreme care—something that shows little sign of happening.

O ne key to the success of digital revamping will be a little-mentioned, even prosaic feature: training the users not to circumvent secure systems. The federal government already has several computer networks—INTELINK, SIPRNET, and NIPRNET among them—that are fully encrypted, accessible only from secure rooms and buildings, and never connected to the Internet. Yet despite their lack of Net access the secure networks have been infected by e-mail perils such as the Melissa and I Love You viruses, probably because some official checked e-mail on a laptop, got infected, and then plugged the same laptop into the classified network. Because secure networks are unavoidably harder to work with, people are frequently tempted to bypass them—one reason that researchers at weapons labs sometimes transfer their files to insecure but more convenient machines.

Schneier has long argued that the best way to improve the very bad situation in computer security is to change software licenses. If software is blatantly unsafe, owners have no such recourse, because it is licensed rather than bought, and the licenses forbid litigation. It is unclear whether the licenses can legally do this (courts currently disagree), but as a practical matter it is next to impossible to win a lawsuit against a software firm. If some big software companies lose product-liability suits, Schneier believes, their confreres will begin to take security seriously.

Computer networks are difficult to keep secure in part because they have so many functions, each of which must be accounted for. For that reason Schneier and other experts tend to favor narrowly focused security measures—more of them physical than digital—that target a few precisely identified problems. For air travel, along with reinforcing cockpit doors and teaching passengers to fight back, examples include armed uniformed—*not* plainclothes—guards on select flights; "dead-man" switches that in the event of a pilot's incapacitation force planes to land by autopilot at the nearest airport; positive bag matching (ensuring that luggage does not get on a plane unless its owner also boards); and separate decompression facilities that detonate any altitude bombs in cargo before takeoff. None of these is completely effective; bag matching, for instance, would not stop suicide bombers. But all are well tested, known to at least impede hijackers, not intrusive to passengers, and unlikely to make planes less secure if they fail.

It is impossible to guard all potential targets, because anything and everything can be subject to attack. Palestinian suicide bombers have shown this by murdering at random the occupants of pool halls and hotel meeting rooms. Horrible as these incidents are, they do not risk the lives of thousands of people, as would attacks on critical parts of the national infrastructure: nuclear-power plants, hydroelectric dams, reservoirs, gas and chemical facilities. Here a classic defense is available: tall fences and armed guards. Yet this past spring the Bush Administration cut by 93 percent the funds requested by the Energy Department to bolster security for nuclear weapons and waste; it denied completely the funds requested by the Army Corps of Engineers for guarding 200 reservoirs,

dams, and canals, leaving fourteen large public-works projects with no budget for protection. A recommendation by the American Association of Port Authorities that the nation spend a total of $700 million to inspect and control ship cargo (today less than two percent of container traffic is inspected) has so far resulted in grants of just $92 million. In all three proposals most of the money would have been spent on guards and fences.

The most important element of any security measure, Schneier argues, is people, not technology—and the people need to be at the scene. Recall the German journalists who fooled the fingerprint readers and iris scanners. None of their tricks would have worked if a reasonably attentive guard had been watching. Conversely, legitimate employees with bandaged fingers or scratched corneas will never make it through security unless a guard at the scene is authorized to overrule the machinery. Giving guards increased authority provides more opportunities for abuse, Schneier says, so the guards must be supervised carefully. But a system with more people who have more responsibility "is more robust," he observed in the June *Crypto-Gram*, "and the best way to make things work. (The U.S. Marine Corps understands this principle; it's the heart of their chain of command rules.)"

"The trick is to remember that technology can't save you," Schneier says. "We know this in our own lives. We realize that there's no magic anti-burglary dust we can sprinkle on our cars to prevent them from being stolen. We know that car alarms don't offer much protection. The Club at best makes burglars steal the car next to you. For real safety we park on nice streets where people notice if somebody smashes the window. Or we park in garages, where somebody watches the car. In both cases people are the essential security element. You always build the system around people."

LOOKING FOR TROUBLE

After meeting Schneier at the Cato Institute, I drove with him to the Washington command post of Counterpane Internet Security. It was the first time in many months that he had visited either of his company's two operating centers (the other is in Silicon Valley). His absence had been due not to inattentiveness but to his determination to avoid the classic high-tech mistake of involving the alpha geek in day-to-day management. Besides, he lives in Minneapolis, and the company headquarters are in Cupertino, California. (Why Minneapolis? I asked. "My wife lives there," he said. "It seemed polite.") With his partner, Tom Rowley, supervising day-to-day operations, Schneier constantly travels in Counterpane's behalf, explaining how the company manages computer security for hundreds of large and medium-sized companies. It does this mainly by installing human beings.

The command post was nondescript even by the bland architectural standards of exurban office complexes. Gaining access was like a pop quiz in security: How would the operations center recognize and admit its boss, who was there only once or twice a year? In this country requests for identification are commonly answered with a driver's license. A few years ago Schneier devoted considerable effort to persuading the State of Illinois to issue him a driver's license that showed no picture, signature, or Social Security number. But Schneier's license serves as identification just as well as a license showing a picture and a signature—which is to say, not all that well. With or without a picture, with or without a biometric chip, licenses cannot be more than state-issued cards with people's names on them: good enough for social purposes, but never enough to assure identification when it is important. Authentication, Schneier says, involves something a person knows (a password or a PIN, say), has (a physical token, such as a driver's license or an ID bracelet), or is (biometric data). Security systems should

"The trick is to remember that technology can't save you," Schneier says. "We know this in our own lives. For real safety we park on nice streets where people notice if somebody smashes the window. Or we park in garages, where somebody watches the car. In both cases people are the essential security element. You always build the system around people."

use at least two of these; the Counterpane center employs all three. At the front door Schneier typed in a PIN and waved an iButton on his key chain at a sensor (iButtons, made by Dallas Semiconductor, are programmable chips embedded in stainless-steel discs about the size and shape of a camera battery). We entered a waiting room, where Schneier completed the identification trinity by placing his palm on a hand-geometry reader.

Beyond the waiting room, after a purposely long corridor studded with cameras, was a conference room with many electrical outlets, some of which Schneier commandeered for his cell phone, laptop, BlackBerry, and battery packs. One side of the room was a dark glass wall. Schneier flicked a switch, shifting the light and theatrically revealing the scene behind the glass. It was a Luddite nightmare: an auditorium-like space full of desks, each with two computer monitors; all the desks faced a wall of high-resolution screens. One displayed streams of data from the "sentry" machines that Counterpane installs in its clients' networks. Another displayed images from the video cameras scattered around both this command post and the one in Silicon Valley.

On a visual level the gadgetry overwhelmed the people sitting at the desks and watching over the data. Nonetheless, the people were the most important part of the operation. Networks record so much data about their usage that overwhelmed managers frequently turn off most of the logging programs and ignore the others. Among Counterpane's primary functions is to help companies make sense of the data they already have. "We turn the logs back on and monitor them," Schneier says. Counterpane researchers developed software to measure activity on client networks, but no software by itself can determine whether an unusual signal is a meaningless blip or an indication of trouble. That was the job of the people at the desks.

Highly trained and well paid, these people brought to the task a quality not yet found in any technology: human judgment, which is at the heart of most good security. Human beings do make mistakes, of course. But they can recover from failure in ways that machines and software cannot. The well-trained mind is ductile. It can understand surprises and overcome them. It fails well.

When I asked Schneier why Counterpane had such Darth Vaderish command centers, he laughed and said it helped to reassure potential clients that the company had mastered the technology. I asked if clients ever inquired how Counterpane trains the guards and analysts in the command centers. "Not often," he said, although that training is in fact the center of the whole system. Mixing long stretches of inactivity with short bursts of frenzy, the work rhythm of the Counterpane guards would have been familiar to police officers and firefighters everywhere. As I watched the guards, they were slurping soft drinks, listening to techno-death metal, and waiting for something to go wrong. They were in a protected space, looking out at a dangerous world. Sentries around Neolithic campfires did the same thing. Nothing better has been discovered since. Thinking otherwise, in Schneier's view, is a really terrible idea. △

FURTHER READING

For clear primers on modern cryptography and on network security, it is hard to do better than Bruce Schneier's *Applied Cryptography* (1993) and *Secrets and Lies* (2000), respectively; these books (especially the latter) render technological arcana comprehensible to even the willfully Luddite.

The consensus classic in the field of cryptology remains ***The Codebreakers: The Story of Secret Writing*** (1967), by David Kahn. Kahn spent four years working on a book that sought, in his words, "to cover the entire history of cryptology." (That is in fact a modest description of a 1,200-page book that begins with a chapter called "The First 3,000 Years" and closes, twenty-five chapters later, with "Messages From Outer Space.") All subsequent chroniclers of cryptography unavoidably stand on Kahn's shoulders. But *The Codebreakers* nearly died aborning: reportedly, the Pentagon tried to suppress its publication; only after Kahn agreed to delete three passages was the book finally published. Kahn issued a new edition of the book in 1996, bringing his history nearly up to the century's end. Two of the most relevant books on the subject of homeland security, both published in 1998, were also the most prescient. ***Terrorism and America: A Commonsense Strategy for a Democratic Society***, by Philip B. Heymann, and ***America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack***, by Richard A. Falkenrath, Robert D. Newman, and Bradley A. Thayer, warned of the imminent danger of a major terrorist attack on American soil.

Although the proposed Department of Homeland Security was hastily thrown together, the idea for such an entity had circulated within the government for years. Some of the proposals can be found in the excellent compilation of disparate reports that the U.S. Senate Committee on Foreign Relations put together last fall, when it was preparing for hearings on the subject of national security. The compilation is called ***Strategies for Homeland Defense*** and is available on the Internet at purl.access.gpo.gov/GPO/LPS15541.