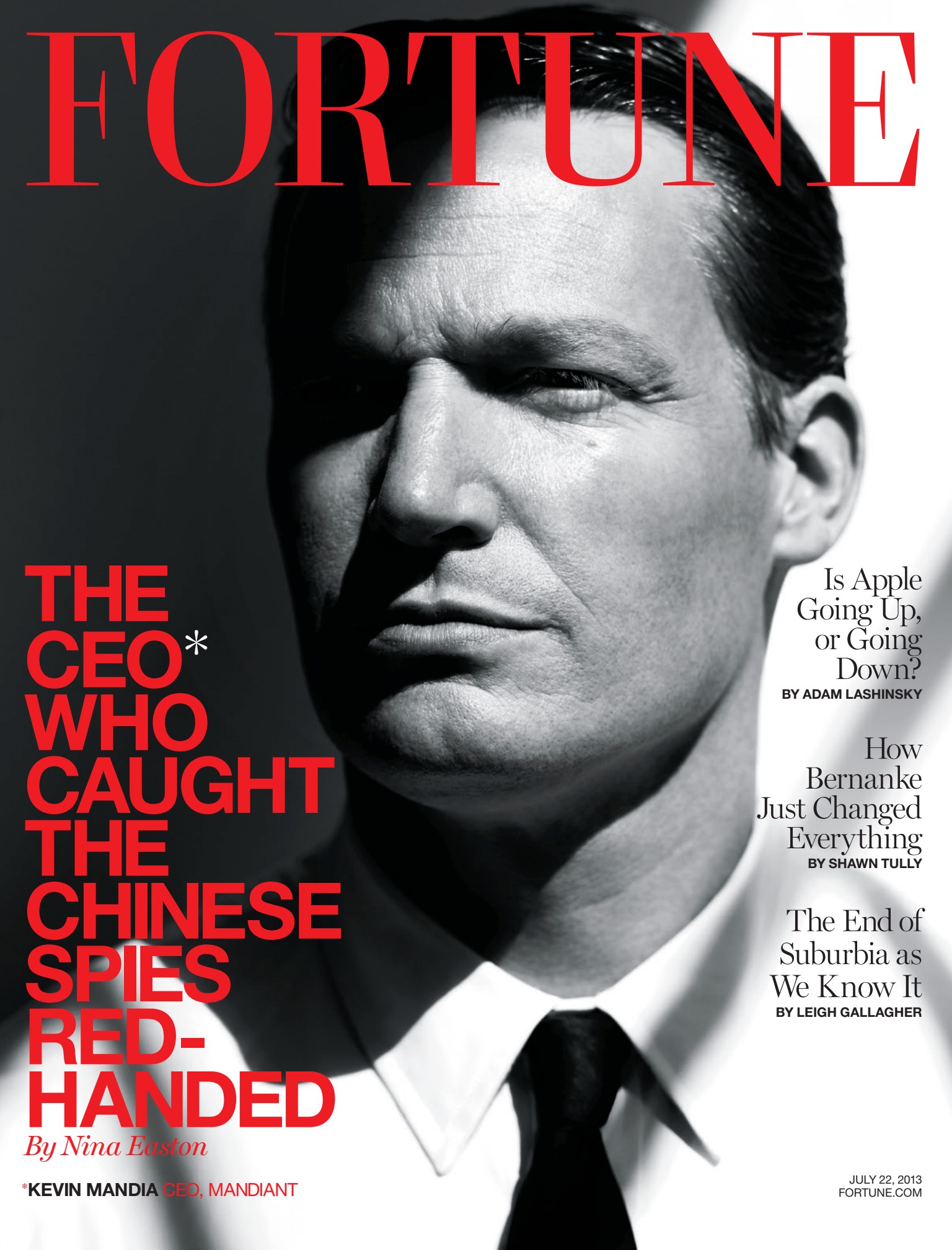
FORTUNE



THE CEO* WHO CAUGHT THE CHINESE SPIES RED-HANDED

By Nina Easton

*KEVIN MANDIA CEO, MANDIANT

Is Apple Going Up, or Going Down?

BY ADAM LASHINSKY

How Bernanke Just Changed Everything

BY SHAWN TULLY

The End of Suburbia as We Know It

BY LEIGH GALLAGHER

JULY 22, 2013
FORTUNE.COM

The CEO Who Caught the Chinese Spies Red-Handed

by NINA EASTON

Kevin Mandia revealed that the People's Liberation Army has systematically hacked U.S. companies. Here is the exclusive inside look at why he did it—and how he's dealing with the explosive fallout.

INSIDE HARVARD BUSINESS SCHOOL'S McArthur Hall, executive MBA student and CEO Kevin Mandia held a 60-page report in his hands and weighed a risky decision: Should he go public with the document, a detailed exposé of Chinese theft of American trade secrets, based on seven years of work for nearly 150 corporate clients? The report's allegations—that a Chinese military unit was likely engaged in systematic hacking and surveillance of U.S. companies—not only would make Mandia and his young cyber-security firm a target for potential retaliation but would also test Washington's already strained relations with Beijing. The 42-year-old former Air Force intelligence officer had a high tolerance for risk,

STYLING BY JESSIE COHAN—ART DEPT; GROOMING BY JANE CHOI FOR LA MER AT STOCKLAND MARTEL. JACKET, SUIT, AND SHIRT BY CLUB MONACO; TIE BY ALEXANDER OLCH

Photographs by RICHARD PHIBBS

but as he pondered his options that February evening, he wasn't sure that disclosure was a smart move. "We'd have a gigantic bull's-eye on our back," he kept thinking.

As much of the world now knows, Mandia did go public with "APT1: Exposing One of China's Cyber Espionage Units." What hasn't been told until now is the story of Kevin Mandia: How he became one of America's top private cybersleuths, how he laid the groundwork for the report's release, and how he and his firm, Mandiant, are dealing with the subsequent political fallout. He spoke exclusively with *Fortune* amid an intensifying drumbeat of news around online spying, data mining, and espionage.

Mandia's report offered detailed evidence of what U.S. intelligence officials had been asserting for years—that the Chinese government is behind a vast heist of America's trade secrets. International intellectual-property theft, mostly by China, costs the U.S. as much as $300 billion and 1.2 million jobs a year, according to the Commission on the Theft of American Intellectual Property, an independent, bipartisan group. National Security Agency director Keith Alexander likens Chinese cyber-espionage to "the greatest transfer of wealth in history." State-sponsored hacking also undermines America's national security: In May the Pentagon asserted that China has hacked into the U.S. defense industrial base, stealing plans for sophisticated weaponry to modernize its military. American allegations (and China's equally aggressive denials) over cyber theft have now emerged as the central source of conflict between the world's two largest economies.

A bipartisan group says intellectual property theft costs the U.S. $300 billion and 1.2 million jobs a year.

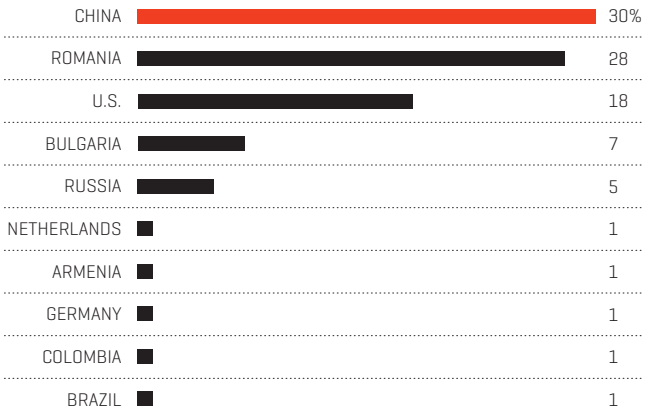
In the past U.S. officials have mostly raised objections behind closed doors, and the official Chinese response has been to deny, take offense, and point to U.S. hacking by the NSA and other agencies. (Later, reported allegations by onetime NSA contractor-turned-leaker Edward Snowden that the NSA has hacked Chinese computers would further complicate those talks.)

In recent months, though, the Obama administration has gone on the offensive. Indeed, President Obama's State of the Union address in February, in which he denounced "foreign countries and companies [that] swipe our corporate secrets," signaled to Mandia that the White House was dropping quiet diplomacy on cyber theft and putting on boxing gloves. It was all the encouragement he needed: Six days after Obama's speech, Mandia's report, with confirmation from intelligence officials, landed on the front page of the *New York Times*. Outgoing National Security Adviser Tom Donilon, considered Beijing-friendly, subsequently decried the "targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale." And in June, President Obama aired his own complaints personally with new Chinese President Xi Jinping in California. (Xi gave no ground.)

The tone of Mandia's report is academic, almost clinical, but the details are dramatic: It offers evidence of a Shanghai-based Chinese military unit's raids on 147 Western corporations across 20 industries—stealing technology blueprints, proprietary manufacturing processes, test results, even executives' contact lists. Documentation includes photos of a 12-story Shanghai facility, headquarters of People's Liberation Army Unit 61398, squeezed between massage parlors and restaurants, which is home to hundreds, perhaps thousands, of hackers. APT1 (for Advanced Persistent Threat) consists of four large networks targeting *Fortune* 500 companies, "is likely government-sponsored and one of the most persistent of China's cyber threat actors"—and is one of several similar operations with

WHERE THE HACKERS ARE

A Verizon investigation pinpointed the origins of "external actors" responsible for online data breaches. These external actors could be engaged in organized crime, espionage, or even activism.



GRAPHIC SOURCE: VERIZON 2013 DATA BREACH INVESTIGATION REPORT

Mandia , 42, founded his company nine years ago after service in the Air Force.

Chinese military ties, the report asserts. Mandia is quick to note that although the report is based on work done for clients of his company, it doesn't name victims and isn't based on classified information, even though Mandia carries a top-secret clearance. He was careful to run it by top intel officials, who, tellingly, didn't object to its release.

The blowback from Beijing has been predictably fierce—especially toward Mandia and his company, based in northern Virginia. "Irresponsible and unprofessional," said the Chinese foreign ministry. It "reeks of a commercial stunt" to boost the company's profits, said Xinhua news agency. The Chinese embassy did not respond to repeated calls for comment.

For Mandia the report's release was anything but a stunt. Yes, the report turned out to be a marketing boon for his venture-backed company, which has $100 million a year in revenue. But the downside for the fledgling firm and its founder was also considerable. One investor worried that Mandia and his employees' emails would be hacked, and potentially embarrassing ones would be disclosed. Indeed, attacks on Mandiant computer systems have escalated, Mandia says, and he remains wary about the prospect of payback from China.

Yet Mandia's decision to publish his report really wasn't much of a choice at all: His worldview—moralistic, patriotic, and fiercely competitive—practically compelled him to release the report. "We were sick of the Chinese saying it wasn't them," he says, referring to his contacts in the intelligence and corporate security community. "We were also tired of references to unnamed hackers in China when we knew it was the military." At six feet tall with reddish-brown hair, Mandia in many ways fits the public's image of a swashbuckling crime fighter (ex-military, nationalistic, computer-savvy, Liam Neeson good looks), but our time together reveals a complex figure, a ramrod-straight personality who also possesses a flip sense of humor and a bit of a problem with authority: He quit the Air Force because it was too bureaucratic, and before he released the APT1 report to the public (it is available online) he warned only one of his five other board members. He admits he was partially "baited" into releasing his document by Chinese officials' demands for "solid proof" to back up disclosures by the *New York Times*, a Mandiant client, that its computers had been hacked.

Since the report's release, closed-door negotiations have ramped up to open charges and countercharges. "It was a game changer in terms of public awareness," said Alec Ross, until recently the State Department's senior adviser for innovation. "The economic consequences of cyber aggression have gotten to the point where you can't remain silent on it. This report makes it easier to lean on China. It reduces the level of credible deniability." The Mandiant report, says Sen. Kay Hagan, the North Carolina Demo-

crat who chairs the Senate's emerging-threats subcommittee, "left no doubt about the magnitude of the theft of technology."

MANDIA AND I ARE DRIVING BACK to his office in a nondescript black SUV. We're returning from a Senate hearing at which he testified. In these highly politicized times, Mandia's appeal and credibility cross party lines. He's explaining how APT1 was just the tip of the iceberg. "We could have made a stronger case if we had wanted to," he boasts. "But that would have been overly embarrassing for the Chinese. We didn't want to hit them with an uppercut, but we wanted to hook them."

For all his bluster and passion, Mandia was nonetheless meticulous and strategic in timing the publication of the report. It came out over the Chinese New Year, when much of the country (including hackers) shuts down or slows down; that gave vulnerable companies time to shore up their defenses. He'd cooperated with the *New York Times*' story on the report, knowing the paper's authority and independent confirmation of the findings from its intelligence sources would bolster his credibility—and even help protect him. "If anything happens, I expect to be avenged properly," he deadpans during our car ride. I cannot tell whether he's joking. He's not. Since the report's release, Mandiant says it has seen escalated "spear phishing" attempts to crack into the company's computer system. Fake car-service receipts and emails from Mandia to his employees surfaced. "The Chinese have the ability to wreck my life—no question about it," Mandia says. "They could hack my email, change it, post it, do whatever they want."

To be sure, this isn't the typical approach of Chinese hackers, Mandia notes: Public shaming, à la the "hacktivist" group Anonymous, isn't China's style. Nor are the attacks emanating out of China aimed at wreaking havoc. (For a closer look at the origins of hacks from around the world, see the chart on page 4.) Systems and files aren't damaged. There's no attempt to crash a company or a public utility. "I've never seen them change the integrity of data or shut down machines," says Mandia. "We've never seen destructive activity."

Sometimes the hackers simply aim to send a message. After the *New York Times* ran an Oct. 25 story on the business dealings of the family of then–Prime Minister Wen Jiabao, Chinese officials warned there would be "consequences." A Mandiant team came in and spent months surreptitiously studying the *Times*' network and

"The Chinese have the ability to wreck my life—no question about it," Mandia says.

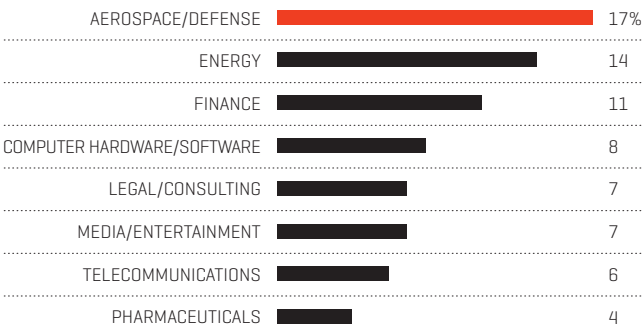
observed hackers passing through university networks, entering the *Times*' systems, and stealing employee passwords. While other corporations are reluctant to tell the world they've been violated, "I don't think there was ever a doubt that we were going to write about [the *Times* intrusion]," veteran chief Washington correspondent David Sanger tells *Fortune*. "The only question was timing. We had to wait until they were out of the system, and that took months." As soon as the hackers had been thoroughly blocked, the *Times* went public; in its Jan. 30 account of the intrusion, editor Jill Abramson said the hackers had not yet accessed sensitive files or emails connected to the Wen family investigation.

Weeks after the *Times* story about its own attack, Sanger and two other reporters would reveal, and confirm, the conclusions of the Mandiant report on other U.S. victims. "As we wrote, you could track individual hackers at specific IP locations and in some cases watch what was going on on their screens. The limitation was that they could only take you to the front door of unit 61398," the PLA's alleged cyber operation, says Sanger. "But to believe that the attacks were emanating from someplace else, you'd have to believe it was coming from noodle shops" surrounding the PLA unit.

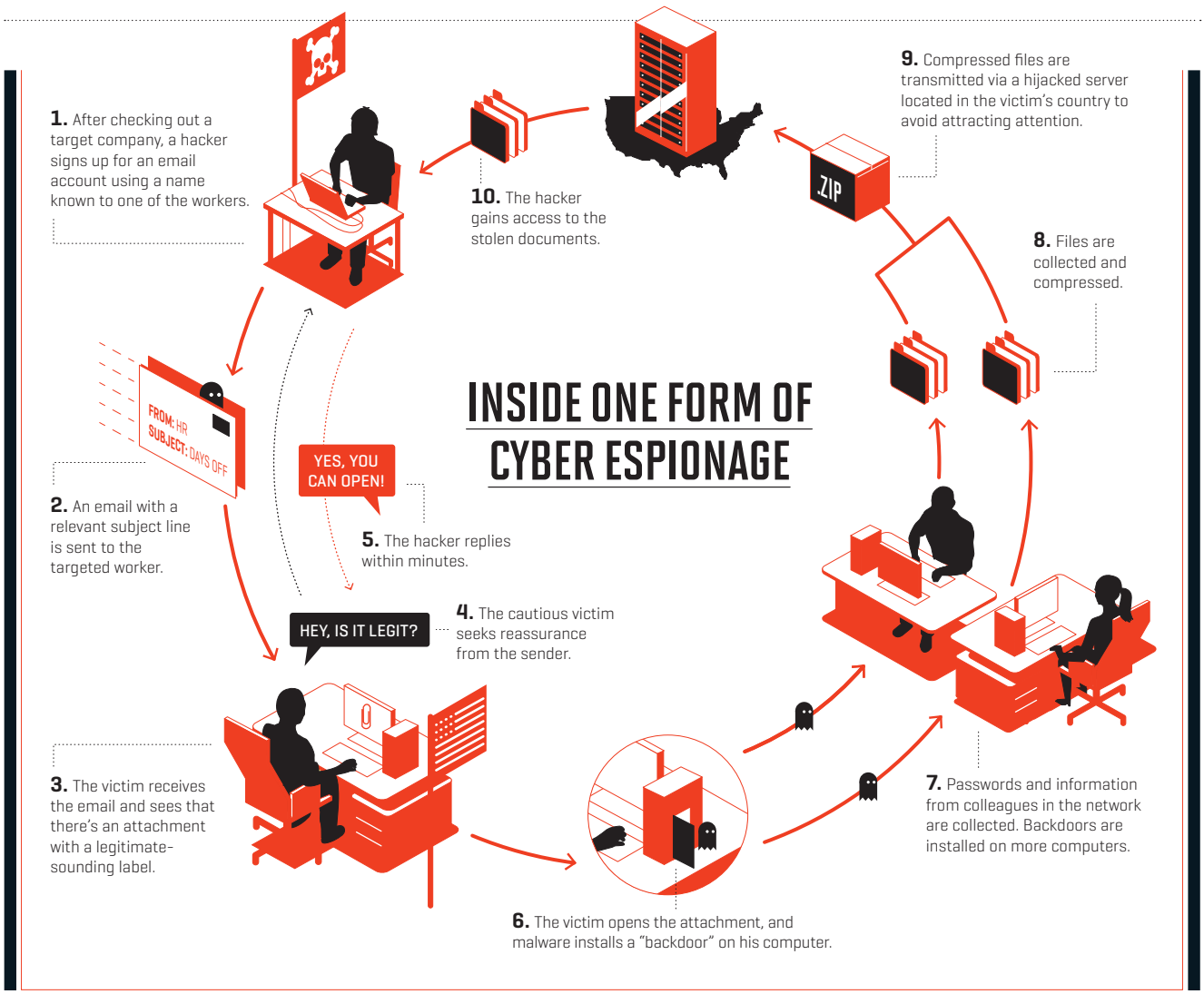
While the Pentagon, intelligence agencies, and related contractors have dozens of years of experience securing

WHO'S GETTING ATTACKED?

Mandiant data from 2012 rank the industries most likely to be attacked. [The data show all cyber incidents from all sources, not just intellectual-property hacks.]



SOURCE: MANDIANT



GRAPHIC: NICOLAS RAPP; SOURCE: MANDIANT

their systems, most of corporate America remains largely naked to attack. "Only 5% of corporate America gets an A on internal security," Mandia recently told a high-level class of cybersecurity experts. The CEO has built his own company on a stubborn belief that cyber intrusions cannot be prevented by firewalls—only stopped and contained after they happen. "You can have every technology on the book and still get an intrusion," he says.

Instead of peddling prevention, Mandia sends teams (mostly ex-intelligence officers and computer forensics experts) into corporate headquarters once an invasion has been detected. That's a business model that sets his nine-year-old company apart from the competition and has led to average annual revenue growth of 65%. Mandiant now boasts 319 employees across nine offices, including one in Dublin. This past spring Mandiant released a software product that acts as the ADT of cybersecurity: It monitors the network, sounds the alarm, and freezes the attackers. A Mandiant team can then converge on the problem, like local police responding to a break-in.

Cybersecurity has become a hot business, with traditional defense firms in particular bolstering their online offerings. In 2011, Mandia took a big step to expand Mandiant. He accepted $70 million in private equity from J.P. Morgan Chase's One Equity Partners unit and storied Silicon Valley firm Kleiner Perkins Caufield & Byers. The private equity guys, who bought out Mandia's early angel investors, think Mandiant's market is only going to grow. "If you're a major company spending $100 million or $500 million on IT, wouldn't you want to spend a couple million more to make sure that if you are breached you

Mandia, age 6, sporting a Captain America T-shirt under his jacket; at his Air Force commissioning in 1992; playing a friend's guitar in 2003. "I was playing 'Crazy Train,' which I normally play whenever I first pick up a Flying V guitar."

can contain it and fight it off?" asks One Equity's Jody Gessow, who also sits on Mandiant's board.

A call to Mandiant's main office—there is no sign, and the cubicles are decorated with football helmets bearing the "M" from the company logo—typically comes months after the break-in first occurs. The average in 2011 was one year; in 2012 that dropped to 113 days. Sometimes a firm's internal security systems might be tipped off when, for example, systems have slowed. But more often than not a senior executive has gotten that dreaded call—from the FBI. Chinese hackers in particular use frighteningly easy-to-deceive techniques to get into a company's system—an email that appears to be from your boss, an attachment from an organizer of a conference you just attended. The prominent computer security firm RSA was breached in 2012 when an employee opened a file named "2011 Recruitment Plan."

When he answers those calls from nervous executives, Mandia is hyper-aware that the club of the hacked is a lonely one. While the SEC mandates disclosure of material breaches, executives at victim companies aren't eager to air their break-ins. "The business leaders I've worked with are frustrated," he says. "You can't really come out and wave a flag saying, 'Hey, I was hacked, and you should lose confidence in my business.'" What Mandiant brings to the table is a seen-it-all knowledge of specific hackers—and their techniques—that the firm's champions say rivals the knowledge base of the NSA. Mandia himself has been investigating cybercrime since he was a second lieutenant in the Pentagon, "putting eyes on the network" to track what went in and out. That was in the early 1990s, when modems were still dial-up. He operated with top-secret security clearance and training out of the Air Force Office of Special Investigations, delving into everything from a military-base child-porn case to Chinese and Russian hackers. He was at the center of action when attacks migrated from Unix systems to Windows in 1998—"Webline commerce started to fly, and everyone was going online unarmed and unprepared," he recalls. The FBI tapped him to train the agency's computer security experts. And in 2001 he literally wrote the book on the subject (with the less-than-arresting title *Incident Response and Computer Forensics*).

No one would mistake Mandia for Sergey Brin or Larry Page or some of the other tech entrepreneurs he protects (Google is a client). Yes, he was the second kid in his ninth-grade class to buy a computer in 1980—a Radio Shack TRS-80—and he's been in front of screens ever since. But Mandia spent his teen years watching *Quincy M.E.*, a show about a medical examiner who used science and forensics to solve murders. He went to high school in Rochester, N.Y., but when his parents divorced in his senior year, he moved to Pittsburgh with his father, a human resources specialist. His mother, who did a bit of backup doo-wop singing as a teen, sold Mary Kay cosmetics. Her son inherited that musical gene, teaching himself to play guitar starting in the eighth grade. His tastes run from Pearl Jam to classical, and he fronted a series of bands, playing gigs with his buddies, that ended only recently when running a company overtook his life. These days he says he plays a "mean 'Edelweiss'" to lull his two young daughters to sleep. When he's not shuttling them around in the family minivan, he drives a Porsche Panamera Turbo.

He attended Lafayette College in Easton, Pa., on an Air Force ROTC scholarship, joined a fraternity, and played football. In 1993 he landed at the Pentagon and pursued computer security because "it was the least bad option" the Air Force was offering. Still, he was drawn to the science of solving crimes, *CSI*-style, so he signed up for a forensics degree at George Washington University. "There were a lot of lieutenants who thought Kevin was crazy for studying cadavers at night instead of staying in the ever-growing world of computers," says one friend. But the forensics training also transformed Mandia into a pioneering computer crime detective.

He left the military in 1998 after growing impatient with the hierarchy and processes. "If you want to move with intent and speed, being a government employee is a

tough place to be," he says. In one interview, Mandia confided to me, with a laugh, "I love watching someone going 100 mph into a wall [by making a wrong choice]. I've done it myself." After the military, he worked in private industry but left to run into his own walls.

In 2004 he started a company, Red Cliff, which would morph into Mandiant. "Find evil and stop crime" was the motto hanging in the office. "This idea of fighting evil—it really is what makes him tick. There really isn't a profit motive," says childhood friend Doug DelaMater. Nine months later Mandia was diagnosed with testicular cancer. He was 32. "I went to treatment every morning, threw up, and went back to work," he says, matter-of-factly, as if he had been fighting a bout of migraines. He is cancer-free today.

Friends say Mandia has always shown such determination. While he was a lieutenant in the Air Force, he was so keen to best a captain who declared himself the easy winner in an upcoming 5K race that even after he missed the shuttle bus to the event, he ran to the starting line, took off, and won. "He always has to win," says Ryan Schedler, a college friend and early investor. "He can wear people out."

It is a trait that makes him a good entrepreneur but may frustrate employees or even investors who are looking for him to sell Mandiant to a strategic buyer or go public—two scenarios that might require Mandia to play up profits rather than his mission of taking down the bad guys. (He once laughed in the face of one prospective investor who asked him, "So, what's your exit strategy?") He recognizes that he needs to think a bit more like an executive, especially with deep-pocketed and well-connected competitors like Hewlett-Packard eyeing his business; that's why he signed up for the HBS executive program.

But he seems to have a love-hate relationship with corporate life. (His offbeat sense of humor colors his own managerial style. He's been known to call all the interns in the office "Ted.") "You won't learn anything from our investors about me except that I'm stubborn, I don't listen, I don't take instruction well, and I'm incorrigible," Mandia warns me. "If you do everything your board tells you, you will fail." He playfully mocks financiers who talk about "creating value," and then, catching himself, he insists: "I love my board members, by the way. It's just when you sit in those meetings, answering 'Did you think of this? Did you think of that?'—before long you get defensive."

Not surprisingly, Mandia's backers don't mind his barbs—they see in Mandia someone who can help them multiply their money. Board member Ted Schlein, who has pioneered Kleiner Perkins' investments in computer security firms, draws comparisons to Amazon CEO Jeff Bezos. "Bezos had a vision," Schlein says. "He was a missionary, not a mercenary, and he wasn't going to stop at anything in order to accomplish it. He didn't always listen, he didn't care if it was profitable, but he believed in the mission. I see a lot of similarities with Kevin."

"If you do everything your board tells you, you will fail," Mandia says.

ESPECIALLY SINCE THE RELEASE of his company's report, Washington policymakers are pounding their desks to "do something" to stop Chinese cyber espionage—something Mandia equates with Congress trying to legislate a cure for cancer. "You can't stop it, but you can reduce the time between detection and remediation," he says. Giving companies legal protection from punishments like regulatory action or shareholder suits so that they can freely share information about their own intrusions would help, he says.

A White House executive order, issued by President Obama in January and aimed at protecting critical infrastructure, promises more government information sharing with the private sector. The order also directed agencies to develop voluntary standards for private companies involved in critical infrastructure. Likewise, an information-sharing bill, which Mandia supports, passed the House in April with bipartisan support.

Nursing a martini at the Four Seasons in Georgetown, Mandia tells me he doesn't see the threat abating, in part because "every company wants to do business with China. Companies will do everything they can to secure their networks after they've broken in. But they're not going to point fingers at 'those SOBs' in China. They don't want to have a loud voice because they want to do trade. They want to have good relations." Indeed, critics say American companies voluntarily engage in "technology transfer" by giving local partners access to their IP in exchange for the ability to do business in China.

That leaves Mandia, who has settled comfortably into his life's mission—and his self-styled patriotic cause. "The worst thing about cyberspace is that we, the U.S., are playing goalie," he says. "We're not going to score points in cyberspace. We're the ones with everything to lose."