HOW TO BET ON
THE NEXT BITCOIN

FORTUNE

SILICON VALLEY'S NEXT BIG IDEA:
**PAYING YOU
NOT TO WORK**

JULY 1, 2017
FORTUNE.COM
ASIA PACIFIC
EDITION
NUMBER 9

IN THE TIME IT TOOK
YOU TO READ THIS,
A CYBERCRIMINAL
BREACHED YOUR NETWORK.

HACKED

HERE'S HOW
GOOGLE & OTHERS
ARE FIGHTING BACK.

12TH HOLE ROYAL BIRKDALE

TOM WATSON 1980

ARNOLD PALMER 1961

THE OPEN
146TH ROYAL BIRKDALE

THE OPEN CHAMPIONSHIP
ROYAL BIRKDALE GOLF CLUB
ENGLAND
JULY 20TH TO 23RD, 2017

PHIL MICKELSON 2013

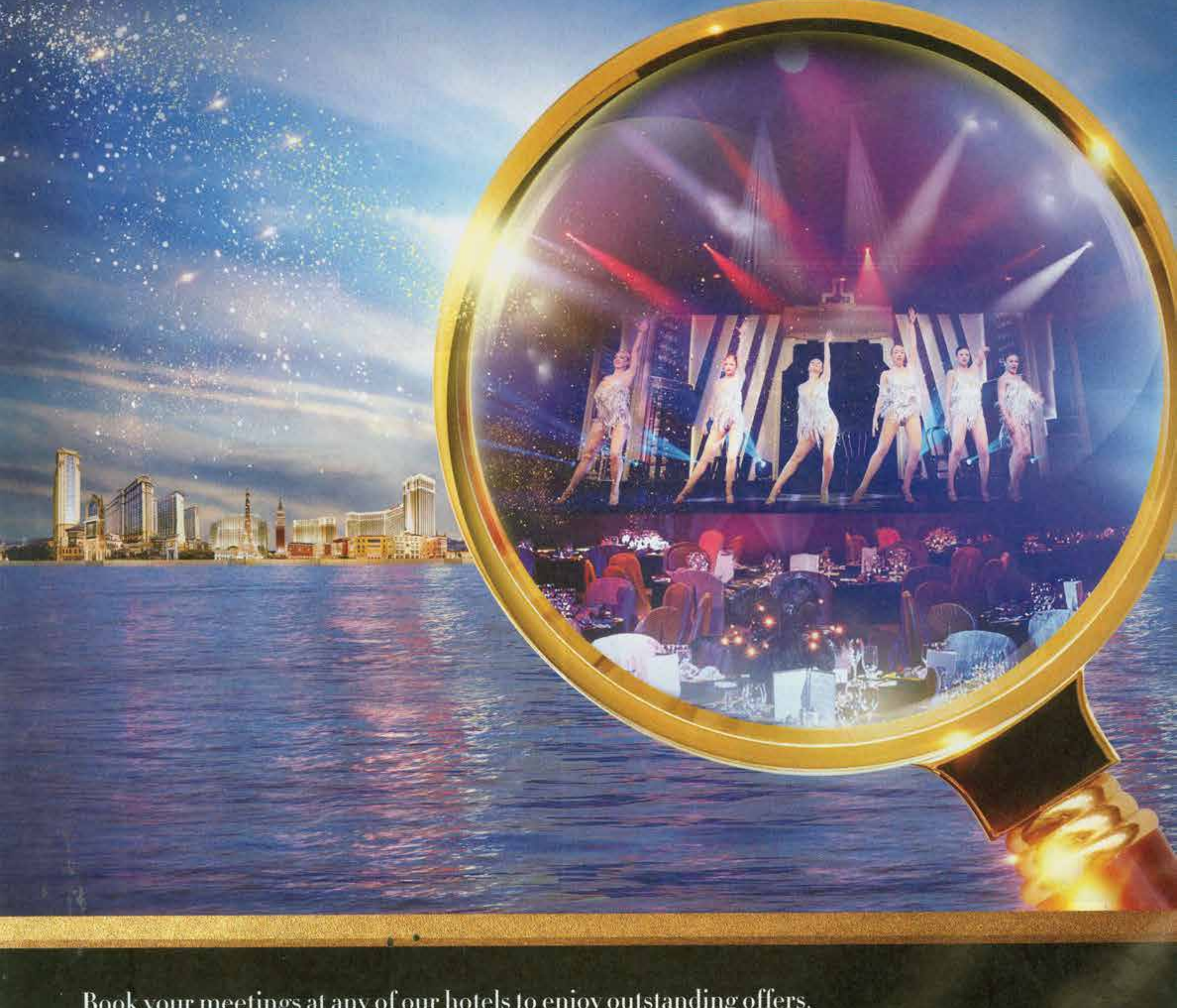
ROYAL BIRKDALE CLUBHOUSE

OYSTER PERPETUAL DAY-DATE 40

SMART MEETINGS

AT SANDS RESORTS MACAO

The widest spectrum of offerings
in one ultimate events and meetings destination



Book your meetings at any of our hotels to enjoy outstanding offers.

- 5% off master bill
- Complimentary room and upgrade
- 20% off audio visual equipment rentals
- 50% off ferry tickets
- 50% off entertainment to enhance your event

Contract your meeting by 31 December 2017 for arrivals until 22 December 2018

ST REGIS · FOUR SEASONS · THE VENETIAN MACAO · THE PARISIAN MACAO · 假日酒店 Holiday Inn · CONRAD · Sheraton Grand

SandsResortsMacao.com/SmartMeetings

*Terms and Conditions Apply

澳门金沙度假区

Sands

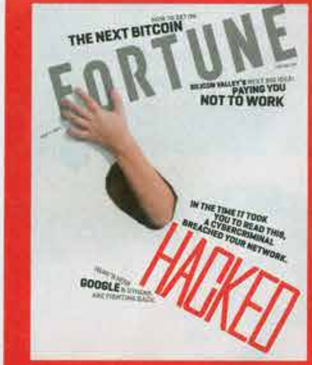
RESORTS MACAO

CONTENTS

JULY 1, 2017

FEATURES

32


HOW TO GET IN ON
THE NEXT BITCOIN
FORTUNE
SILICON VALLEY'S NEXT BIG IDEA:
PAYING YOU
NOT TO WORK
IN THE TIME IT TOOK YOU TO READ THIS, A CYBERCRIMINAL BREACHED YOUR NETWORK.
HACKED
GOOGLE
ARE FIGHTING BACK

▲ ON THE COVER: PHOTOGRAPH FROM EYEEM/GETTY IMAGES

VOLUME 176 /// NUMBER 1

CONTENTS

VOLUME 176 // NUMBER 1

18

DEPARTMENTS

BRIEFING

FOCUS

TECH

VENTURE

PASSIONS

FORUM

BACK PAGE

LAST BYTE

17

Fortune Asia [ISSN 0738-5587] is published monthly, with extra issues in March, June, September, and December, by Time Asia [Hong Kong] Limited. *Fortune* Asia may also publish occasional extra issues. Customer Service and Subscriptions: For 24/7 service, please use our website: fortune.com/customerserviceasia. You may also contact Customer Services Center at 852-3128-5688, or email to enquiries@timeasia.com or write to Time Asia [Hong Kong] Limited, 37/F Oxford House, Taikoo Place, 979 King's Road, Quarry Bay, Hong Kong. Subscribers: If the postal authorities alert us that your magazine is undeliverable, we have no further obligation unless we receive a corrected address within two years. Mailing List: We make a portion of our mailing list available to reputable firms. If you would prefer that we not include your name, please contact Customer Services Center. Member, Audit Bureau of Circulations. *Fortune* Asia is printed in Singapore. Singapore MCI [P] 061/11/2016. Malaysia KKDN permit no. PPS1162/05/2013 [022950].

WallpaperSTORE*

Design lovers say, 'Yes', when you order online at WallpaperSTORE*

WHEN GUANGZHOU MEETS FORTUNE

An innovative city with ambition

The five-year plan states that Guangzhou will give impetus to the development of emerging strategic industries like new-generation information technology, biology and health, new materials, high-end equipment, and new-energy vehicles.

Artificial intelligence, virtual reality, new energy, bio-medicine — a wide array of as many as 1,300 new technologies and innovations were showcased at the China Innovation and Entrepreneurship Fair held in Guangzhou May 26-27.

The fair, which has been undertaken by Guangzhou for three years, aimed to set up a complete transaction chain for technology, capital, talents and information, while focusing on technological innovations, industrialization and services.

The fair is both an important part of the city's innovation-driven development strategy and its ambition to build itself into an international hub of science and technological innovation. The central government has also assigned Guangdong province with Guangzhou as its capital city a pivotal role to play in the nation's implementation of innovation-driven development strategy.

By the end of 2016, Guangzhou had 4,739 high-tech companies, among which 2,820 were newly set up, an increase that ranked second in China to Beijing. The output value of the city's high-tech industries amounted to almost $131 billion, accounting for 46 percent of the city's total of large and medium-sized industrial enterprises.

Guangzhou is also a popular city for start-ups, with over 200 incubators covering an area of 8.6 million square meters and housing more than 10,000 enterprises and projects. The city has also built 14 national-level and 23 provincial-level international technological cooperation bases.

To create a favorable environment for innovation, entrepreneurship, investment and financing, the government will set up, in 2017, a $727 million fund to facilitate the industrialization of technological innovations, aiming to channel $3 billion of social capital. The government will also implement a plan to increase its budget to as much as $1.57 billion and aim to channel $8.59 billion of social capital for research and development.

By 2020, according to the city's newly promulgated 13th Five-year Plan for Innovations in Science and Technology, Guangzhou will build itself into a national demonstration city of independent innovation as well as a national innovation center, giving full play to its leading role in the city's surrounding Pearl River Delta region.

The five-year plan states that Guangzhou will give impetus to the development of emerging strategic industries like new-generation information technology, biology and health, new materials, high-end equipment, and new-energy vehicles. In addition, the city will also accelerate the development of industries of the future, covering artificial intelligence and robotics, precision medicine, wearable devices, cloud computing, big data and additive manufacturing.

Guangzhou annually hosts a large number of conferences and activities themed on technological innovation, entrepreneurship and high-caliber talents in science and technology, such as the Convention of Exchange of Overseas Talents in China, the Guangzhou International Award for Urban Innovation, and the China Investment Conference, as well as the newly concluded China Innovation and Entrepreneurship Fair.

This year, to beef up its efforts in this sector, Guangzhou will launch an award for scientific and technological innovation on the sidelines of the 2017 *Fortune Global Forum*.

THE WORLD IN 9 PAGES

BRIEFING

JULY 1, 2017

Sweaty Betty
3,700+ TESTED RECIPES WHEREVER YOU ROAM
DOWNLOAD THE WHOLE FOODS MARKET APP FOR iOS & ANDROID
WFM.COM/APPS
WHOLE FOODS MARKET
RECYCLE THIS BAG
Marlboro NEW JERSEY

○ Amazon will get a nationwide distribution network and more if it can get Whole Foods to the checkout line.

○ DOLLY FAIBYSHEV—THE NEW YORK TIMES/REDUX

The Deal That Made an Industry Shudder

It's not just grocery chains that should worry about Amazon's Whole Foods acquisition; it could impact every company that touches the food we eat. BY BETH KOWITT

CLOSER LOOK **FOR YEARS, AMAZON** has been the specter looming over retail, as once-dominant department stores and specialty chains fell on harder and harder times. But up until now, the e-commerce titan has managed to irrevocably alter the industry without making much of a dent in retail's biggest moneymaker of all—the $800 billion grocery business.

That changed on June 16 when Amazon announced its intention to acquire Whole Foods, the upscale supermarket chain that played ▷▷

▷▷ a pivotal role in taking organic and natural foods mainstream. Whole Foods itself may have been under duress, pressured by an activist investor and softening sales, but the healthy-food movement and the meticulously curated store experience that it pioneered is alive and well. "Amazon is placing its bet on the future of the food industry," says Errol Schweizer, a former Whole Foods executive who is now an industry adviser, "and they see Whole Foods as the leadership."

Most Amazon watchers are focused on the some 450 stores the e-commerce behemoth scoops up in the deal. These brick-and-mortar locations instantly give it a national physical presence, as well as a network of mini distribution centers for fresh produce—by far the most challenging part of the grocery delivery business because of spoilage and the fragility of fruits and vegetables. (Upon news of the bid, grocery stocks took a nosedive accordingly.)

But Amazon isn't just trying to change how we buy groceries. Remember the company's original disruption: bookselling. Jeff Bezos not only shifted how and where books were sold; he also changed how they were made, by forcing publishers, authors, and everybody else along the book supply chain to cut their costs. The same thing could very well happen in food, and the outcome for food manufacturers could be as dire it was for book publishers. "I would be terrified if I were a consumer packaged-goods company right now," says Benzi Ronen, CEO and founder of food hub management software startup Farmigo. Indeed, packaged-goods producers' businesses are already under stress, with manufactured-food volumes at large companies declining 4% this year, as consumers seek out less-processed fare. And on the long-shot chance that Walmart, playing defense, swoops in with a bigger bid, the same pressures will still be in play.

"I WOULD BE TERRIFIED IF I WERE A CONSUMER PACKAGED-GOODS COMPANY RIGHT NOW."
—BENZI RONEN

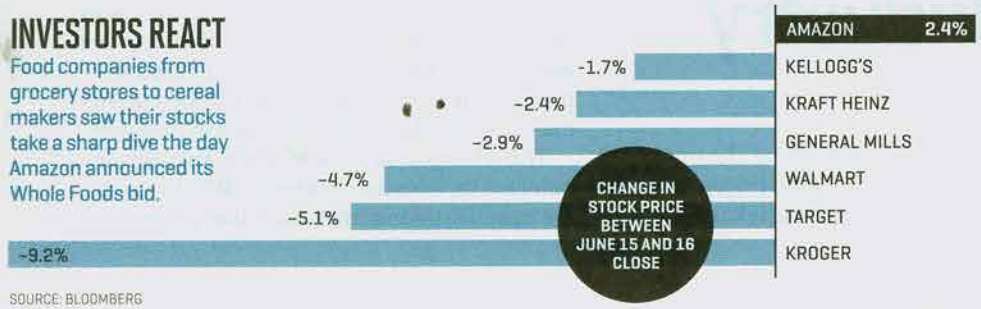
The overlooked asset Amazon gets in the deal is Whole Foods' 365 house brand—one of the most coveted in the organic and natural space, private label and otherwise. This is not your mother's generic box of cornflakes, with its bad design and perceived quality issues. A Piper Jaffray survey last spring found that 365 is customers' favorite organic-food brand, ahead of premium names like Kellogg's-owned Kashi and General Mills' Annie's. The 365 brand is virtually unavailable online, but that will change if Amazon is smart about it. "The opportunity to use the 365 brand as a mainstay of their online offering is really profound," says Bernstein analyst Alexia Howard. "It puts a huge amount of pressure on branded food sales."

Amazon has tried to develop its own private label in food for years. In 2016 it rolled out its Happy Belly coffee, Mama Bear baby food, and Wickedly Prime snacks. These brands are available only to Amazon Prime members, who pay $99 a year for free two-day shipping, among a litany of other benefits. In a sign of how powerful its private label can be, analytics company 1010data found that for a 12-month period ending last year, 94% of all batteries sold online went through Amazon sites, and Amazon's own brand made up about a third of all online battery sales. Its Amazon Elements baby wipes, introduced in 2014, have managed to capture 16% of online market share, despite being available only to Prime members.

Amazon and Whole Foods might seem like they are on opposite ends of the retail spectrum—a relatively small, high-end grocer vs. the massive e-commerce Everything Store—but they overlap in the power of their brands. That's a rarity for a purveyor of food. Under the old model of food retailing, "the brand you trusted was the manufacturer," Ronen says. "Today you go onto Amazon and filter everything by what's Prime." Similarly, Whole Foods acts as a curator for shoppers by banning ingredients like saccharin and bleached flour from the products it sells. Together, the two trusted brands should create an even more powerful one. That could fundamentally alter the way grocery aisles look—and even make the aisles themselves obsolete. ■

INVESTORS REACT

Food companies from grocery stores to cereal makers saw their stocks take a sharp dive the day Amazon announced its Whole Foods bid.



SOURCE: BLOOMBERG

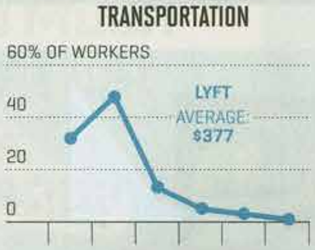
ANALYTICS

SEEING TRENDS IN THE DATA

THE WAY WE WORK NOW

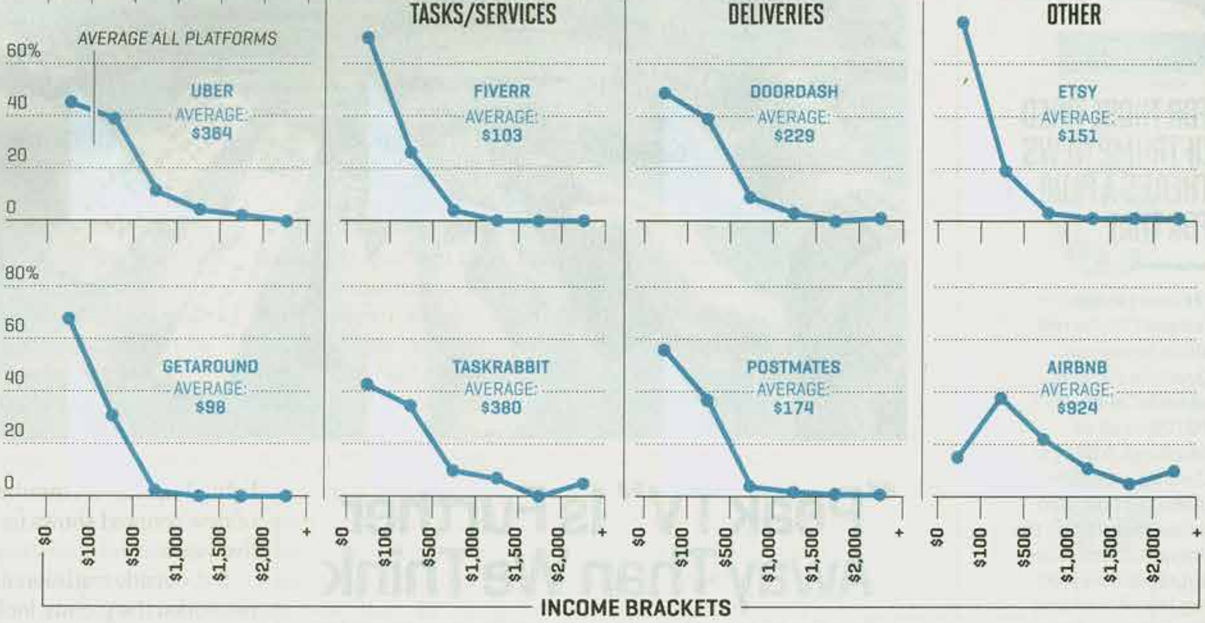
MAKING ENDS MEET IN THE SHARING ECONOMY

Most sharing-economy workers make under $500 a month from such jobs, according to data collected by consumer-lending startup Earnest. That paltry sum reflects how many people are just dabbling [as opposed to working full-time], but it also highlights how tricky it can be to earn a living at companies that don't actually "hire" most workers. It's perhaps telling that Airbnb paid out the most per month. Returns on capital [rather than labor] are pretty good these days.



BREAKDOWN OF WORKERS' MONTHLY INCOME

SOURCE: EARNEST

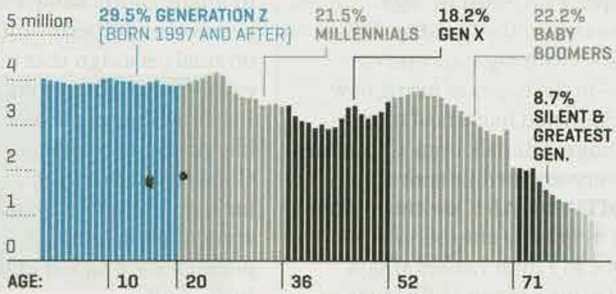


THE NEW KIDS

MILLENNIALS, MOVE OVER. GEN Z IS COMING

ENJOY IT WHILE YOU CAN, millennials. For years, businesses have relentlessly pursued the coveted demographic, creating products and campaigns just for them. But Gen Z is even larger [nearly 30% of the current U.S. population], and before long, they'll be spending like it.

U.S. POPULATION BY AGE



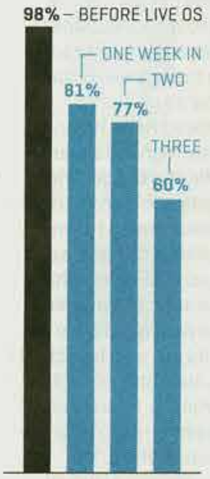
SOURCES: CENSUS BUREAU; PEW RESEARCH CENTER

STANDING DESKS

YOU'LL GET USED TO IT

SITTING IS KILLING US, or so scientists keep saying. Enter the standing desk, now de rigueur at tech companies and hipper *Fortune* 500 firms. But it takes a while to ease into, reports furniture maker Herman Miller, which measured usage of its Live OS desk technology. After a week, users spent 81% of their desk-time sitting. But after three weeks, they stood for more than a third of the time.

TIME SEATED AT DESK



SOURCE: HERMAN MILLER

MEDIA

FOR THOSE TIRED OF TRUMP NEWS, THERE'S A PLUG-IN FOR THAT

FEELING TRUMP fatigue? You're not alone. News app Quartz is allowing users to "snooze" POTUS-related headlines. A Google Chrome extension lets users filter out web pages mentioning the President. And news aggregator Nuzzel has introduced a no-Trump option for its newsletters and app. The company, which uses people's social media connections to pick stories relevant to them, says social shares on Trump-related news hit an all-time high in January. "We started getting complaints from users about seeing too many political stories," says Nuzzel CEO Jonathan Abrams. The premium service, which also cuts out ads, launched in June and costs $10 a month. Silence is golden—and naturally comes at a price.
—JENNIFER ALSEVER

"Peak TV" Is Further Away Than We Think

The boom in scripted shows on major networks may be tapering, but that doesn't mean the drama's over. BY TOM HUDDLESTON JR.

ENTERTAINMENT

HOW MUCH TV IS TOO MUCH TV? A record 454 scripted original series aired on television in 2016, up from 420 in 2015 and a 71% increase from five years earlier, according to FX Networks' tally. How high can that number go? 500 shows? 600? The peak, experts say, must be nigh.

For years, networks have chased the "prestige TV" model—higher-quality shows with big stars and cinematic production values—in the hopes of luring new audiences. But critical acclaim and buckets of money haven't guaranteed big ratings. After all, even TV addicts struggle to find time for every worthwhile series.

Indeed, networks like MTV and A&E are cutting back on scripted programming in favor of cheaper nonfiction and reality shows. FX CEO John Landgraf says the saturation point could come as soon as this year or 2018. Meanwhile the five broadcast networks greenlighted the lowest number of new scripted shows in five years.

But outside traditional networks, the picture looks different. Together, Netflix and Amazon are spending more than $10.5 billion on original content this year alone. And the number of scripted original streaming shows more than doubled last year, to 92.

Netflix's recent decision to finally cancel some expensive, underperforming originals is a sign that it's getting more discerning. But now, digital players like Apple, Facebook, Google, and Snap are jumping into the original-content pool, pushing peak TV ever higher and further off.

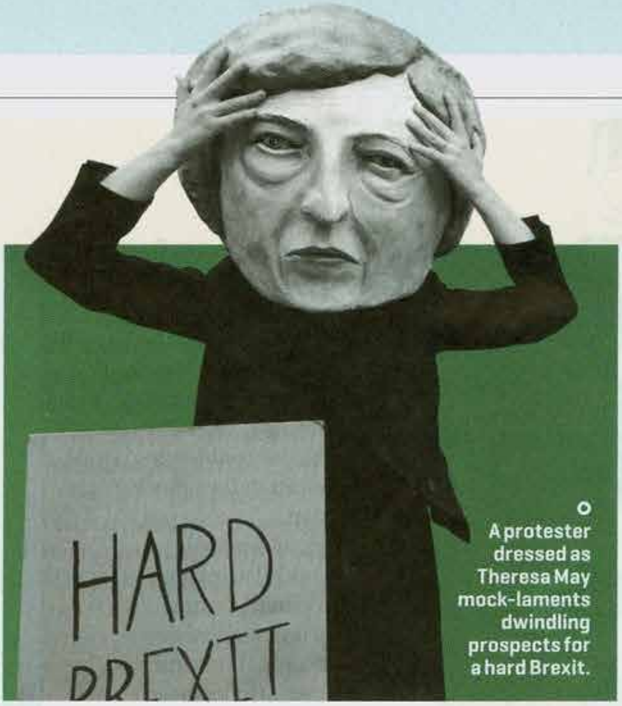
Couch potatoes, rejoice.

TV: ADRIAN HANCU—GETTY IMAGES/ISTOCKPHOTO; TV REMOTES: NOMADSOUL1—GETTY IMAGES/ISTOCKPHOTO; TRUMP: ANDREW HARRER-POOL/GETTY IMAGES; HAND: ISTOCKPHOTO/GETTY IMAGES

So Much for That Brexit Mandate

Theresa May's botched election has left her government in chaos. For U.K. businesses, though, it offers hope for closer EU ties.

BY GEOFFREY SMITH



A protester dressed as Theresa May mock-laments dwindling prospects for a hard Brexit.

EUROPE

WHEN U.K. Prime Minister Theresa May called a snap election in April, polls showed that she would win a big mandate for her high-risk Brexit strategy—which entailed leaving the EU's Single Market and its customs union in two years flat, even, if need be, without negotiating any future trading arrangements.

But her electoral gamble backfired spectacularly after voters went to the polls in June. Her Conservatives lost their slim majority in Parliament and are now hanging on to power only with the support of the fundamentalist Protestant Northern Irish Democratic Unionist Party (DUP). Her authority in tatters, May is now under pressure from all sides. The Tories' right wing wants a "hard" EU exit regardless. Business, hoping to avoid getting slammed by Brexit's full impact in 2019, is making a fresh push for a lengthy transition (enraging the Tory hard-liners, who see it as a prelude to betraying the referendum mandate). Meanwhile, the DUP's desire to avoid reerecting a border with the Republic of Ireland is in direct conflict with popular pressure for tighter control of immigration.

U.K. politics was a mess even before June 8. It's an unholy one now.

TURNOVER

IS GE DUE FOR A COMEBACK?

As one of the world's biggest public companies, GE gets maximum scrutiny from investors—and two of its last three CEOs disappointed the Street. Will new CEO John Flannery deliver?

REGINALD H. JONES
DEC. 1972–APRIL 1981

UNDERPERFORMED THE MARKET BY **19 PERCENTAGE POINTS**

JOHN F. WELCH JR.
APRIL 1981–SEPT. 2001

OUTPERFORMED THE MARKET BY **2,036 POINTS**

JEFF IMMELT
SEPT. 2001–JUNE 2017

UNDERPERFORMED THE MARKET BY **155 POINTS**

JOHN FLANNERY
JUNE 2017–PRESENT

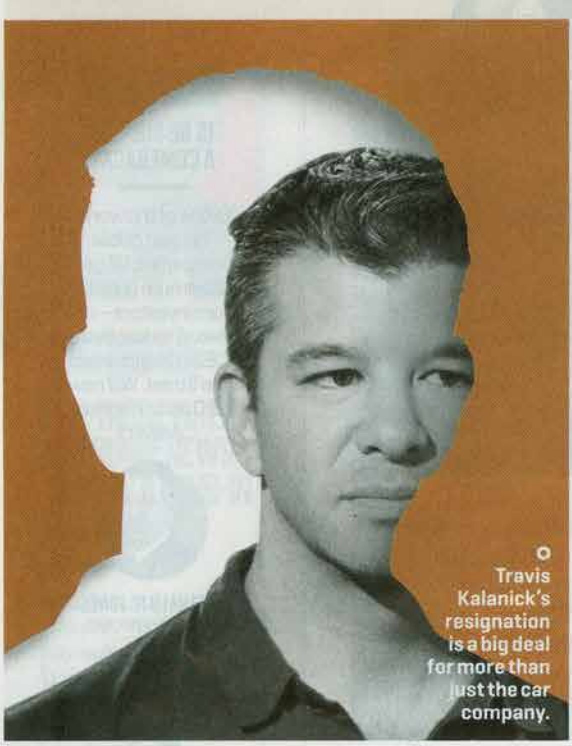
STOCK PERFORMANCE: **TO BE DETERMINED**

TOTAL ECLIPSE OF HOTEL AVAILABILITY

TOURISM

A SWATH of small towns across Middle America are getting their moment in the sun (kind of). Aug. 21 will see the first coast-to-coast total solar eclipse in the U.S. since 1918—but it will be visible only from a few places. The result? Hotels and Airbnbs are jammed in towns like St. Joseph, Mo., which will close its airport for a 100,000-person viewing party. In Carbondale, Ill., a football stadium will become a viewing center. And Hopkinsville, Ky., will rename itself Eclipseville for the day. Nightly rooms at the Sheraton Grand hotel in Nashville start at $359 but include a penthouse eclipse fete. And in Jackson Hole, Wyo., the well-heeled can take a gondola up to the peak of a mountain for a viewing party at 10,450 feet, complete with a resident astronomer, telescopes, and mimosas.
—JENNIFER ALSEVER

MAY: ADRIAN DENNIS—AFP/GETTY IMAGES; ECLIPSE: DAVID LOH—EYEEM/GETTY IMAGES; JONES, WELCH, IMMELT: COURTESY OF GE; FLANNERY: HEMANT MISHRA—MINT VIA GETTY IMAGES



Travis Kalanick's resignation is a big deal for more than just the car company.

What Uber Means for the Valley

The company's self-inflicted wounds are likely to have a wide-ranging impact on startup culture, regulations, and more. BY ERIN GRIFFITH

UNICORNS

UBER CEO TRAVIS KALANICK'S resignation marks the beginning of a new era for the company—raising major questions about the ride-sharing giant's future and its $68 billion valuation. But it could also herald a new chapter for Silicon Valley itself. The age of so-called startup unicorns has had its share of meltdowns, including onetime blood-testing darling Theranos and insurance software notable Zenefits. But Uber is different: It's the largest, most valuable, most global, most disruptive, most quintessential Silicon Valley success story.

Kalanick's departure has the potential to affect the way local regulators view disruptive startups that operate in legal gray areas, the way labor regulators look at Silicon Valley workplaces, and the way securities regulators view low-information startup stock sales. (Before, Uber was "controversial." Now its bad behavior could serve as justification for tighter regulation.)

Uber's moment of truth could also influence startup valuations and the way investors assess risk for companies with founder-controlled boards. It could affect the kinds of executives that want to leave cushy jobs in mainstream sectors to become "the adult" at Silicon Valley startups. And it could deter would-be entrepreneurs who might otherwise have been seduced by the cult of personality surrounding unicorn CEOs.

This wake-up call for the tech industry has been at least six months in the making. Uber was not the only company with a reportedly toxic culture, an obsession with disruption over following the rules, and a win-at-any-cost strategy; it was just the most successful. Because those characteristics had worked so well, others emulated the formula. Scores of "Uber for X" companies hoping to re-create its success may now be rethinking their plans. Uber's story is no longer a playbook. It's a cautionary tale.

PHARMA

COULD NEW TECH (FINALLY) DESTROY THE PILLBOX?

PILLS HAVE BEEN popped for aches, pains, and other maladies for millennia, but their days as the holy grail of drug delivery could soon be ending.

A new class of pharmaceutical implants, matchstick-size devices that deliver drugs over a period of weeks or months, are coming into their own. Titan Pharmaceuticals and Braeburn Pharmaceuticals have an FDA-approved implantable that, inserted in patients' upper arms, treats opioid addiction by providing continuous doses of buprenorphine. Braeburn is also developing an implant for schizophrenia. Biotech Intarcia, too, has one for diabetes now under FDA review.

If such devices take off, experts say they could save billions in medical nonadherence costs (it's hard to remember to take those pills) and save chronic sufferers even more pain. —ERIKA FRY

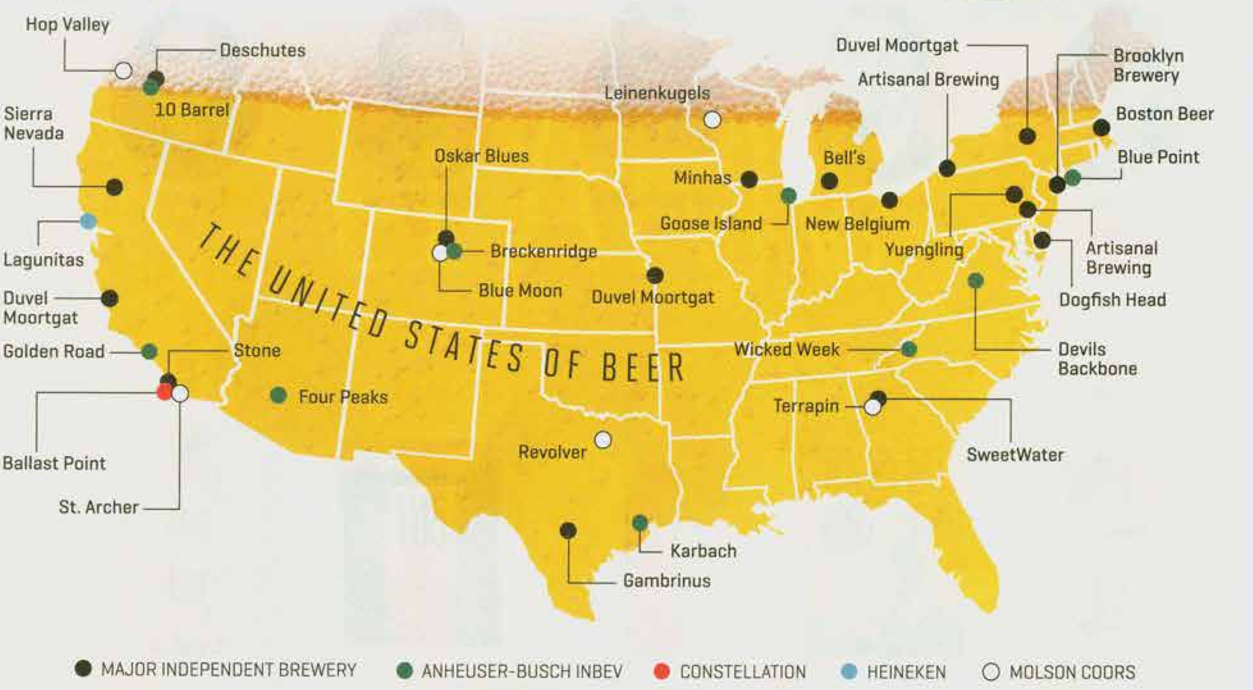
○ KALANICK: BRENT LEWIN—BLOOMBERG VIA GETTY IMAGES; PROBUPHINE: COURTESY OF BRAEBURN PHARMACEUTICALS

TURF

Drink Local, Buy Global

BY JOHN KELL

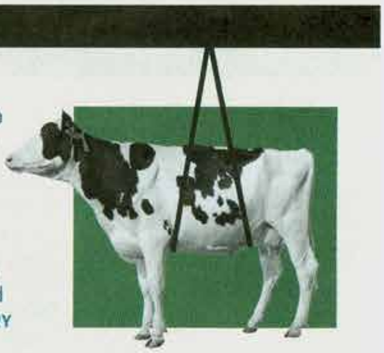
THERE'S A GOOD CHANCE that locally brewed beer you're drinking is actually a part of a giant multinational corporation. With Bud and Miller sales cooling, Big Beverage inked at least 15 craft-beer deals in recent years. Craft snobs call foul, but beer execs say they're just giving drinkers what they want: more fuller flavored ales. Craft buyouts tend to lead to broader expansion—Goose Island and Blue Moon became national brands; Elysian and Ballast Point aren't far behind.



MIDDLE EAST

HOW A PETRO STATE HANDLES AN EMBARGO

QATAR IS the world's richest country per capita. But when Saudi Arabia and its Gulf State neighbors cut ties with the geographically isolated, Connecticut-sized kingdom in June, allegedly for funding terrorism, it got food-poor fast. The result: Qatar is adopting a spirit of (deep-pocketed) self-reliance: One Qatari businessman plans to airlift in 4,000 U.S. and Australian cows to boost the Qatari dairy industry. Still, Qatar is feeling the pressure: Poor workers are particularly affected, and regional tensions will remain heightened indefinitely. —**ERIKA FRY**



© COW: ANDIA—UIG VIA GETTY IMAGES; BEER IN MAP: GETTY IMAGES; BOTTLES: COURTESY OF BALLAST POINT; ELYSIAN BREWING; MOLSON COORS

Celebs Dabble in Weird Food

Perfume sponsorship is *so* last season.

BY JOHN KELL

STYLE **HOLLYWOOD'S** next starring role: food investor.

A-listers from Beyoncé to Leonardo DiCaprio are amassing stakes in buzzy, offbeat food and beverage startups. The barrier to entry can be low—consumer product startups can often get off the ground with $5 million or less in early financing rounds. And it's a natural fit: Food brands get a bigger boost than most from stars' huge social media followings.

Healthy fare is a celebrity favorite. Gwyneth Paltrow has invested in a frozen-food maker; actress Olivia Munn is backing specialty jerky (good for weight loss!); and DiCaprio supports organic chickpeas. The more original the better. "Disruptive brands—that's what I look for," says Munn.

While the financial bets are often small, a payoff can be massive. 50 Cent reportedly pocketed as much as $100 million after Coca-Cola bought the maker of Vitaminwater, which the rapper had invested in. And just a month after Justin Timberlake took a stake in Bai Brands, it sold to Dr Pepper Snapple for a cool $1.7 billion.

BEYONCÉ
1

LEONARDO DICAPRIO
2

GWYNETH PALTROW
3

JUSTIN TIMBERLAKE
4

OLIVIA MUNN
5

MATCH THE STAR WITH THE STARTUP

A
DAILY HARVEST

B
HIPPEAS

C
WTRMLN WTR

D
CHEF'S CUT

E
BAI

UOCAB CHECK

OLA

\'ō-el-ē\

SIX MONTHS AGO, only the wonkiest policy nerds knew what OLA was; now it's about to be at the heart of the angry debate over repealing Dodd-Frank. The OLA, or the Orderly Liquidation Authority, gives regulators the ability to intervene in the event of a bank failure that would impact the larger economy. The GOP-controlled House voted in June to dismantle it, arguing it enables bailouts. But economists say the OLA is necessary to prevent crises (and that any losses would be borne by the private sector). At the moment, it looks unlikely that much of the House's bill will get past the Senate. And the Treasury Department is currently reviewing the issue. Regulation foes are watching carefully.

ANSWER KEY: 1: C; 2: B; 3: A; 4: E; 5: D

O BEYONCÉ: JASON LAVERIS—FILMMAGIC/GETTY IMAGES; MUNN: STEVE GRANITZ—WIREIMAGEGETTY IMAGES; TIMBERLAKE: MICHAEL TRAN—FILMMAGIC/GETTY IMAGES; DICAPRIO: WALTER MCBRIDE—FILMMAGIC/GETTY IMAGES; PALTROW: JB LACROIX—WIREIMAGE/GETTY IMAGES; PRODUCTS: COURTESY OF THE COMPANIES

READ.
WATCH.
THE BROADSHEET
BROAD STROKES
LEARN.

Fortune on the Global Stage

FROM NEW YORK TO LONDON

In June, we gathered some of our favorite thinkers and doers in two global hubs. First, at the Northside Festival, founders and VCs dropped knowledge in Brooklyn, the U.S. capital of hipster cool. Days later, the sixth annual Most Powerful Women International Summit kicked off in London, covering everything from geopolitical upheaval and Brexit to hacking and space travel. While the confabs were an ocean apart, they did share a common thread: We live in an age of disruption. Let's embrace it.

—KRISTEN BELLSTROM AND CLAIRE ZILLMAN

MOST POWERFUL WOMEN

"I KNOW SOMETHING ABOUT EGO."

—SUPERMODEL NAOMI CAMPBELL

NAOMI CAMPBELL spoke about how she persuaded some of the biggest names in business, including Donald Trump, to donate to Fashion for Relief, the charity fashion show she launched to benefit victims of Hurricane Katrina. Pop icon **Annie Lennox** also talked philanthropy—her nonprofit, The Circle, helps women in developing countries—and how an interview with Charlie Rose reminded her that "there's something more important than my fashion sense" and inspired her to use her fame for good.

SOCIAL NETWORK TO SOCIAL PARIAH?

AFTER THE London Bridge terrorist attack, British Prime Minister Theresa May lashed out at big Internet companies for giving extremist ideology "the safe space it needs to breed." **Nicola Mendelsohn,** Facebook's vice president of EMEA, responded to the charge on the London stage, saying that the company plans to add 3,000 employees to scrub offensive content: "We want to be a hostile environment for terrorists."

NORTHSIDE FESTIVAL

"WE BOUGHT A WHITEBOARD—IT WAS THE MOST BUSINESS-Y THING I'D EVER DONE."

—**KICKSTARTER CEO YANCEY STRICKLER,** telling the Northside crowd about his transition from music journalist to entrepreneur

"THE ONLY WAY YOU COMBAT A STRONG IDEA IS TO COME UP WITH A STRONGER IDEA."

—**IAN SCHRAGER,** on the hotel industry's underwhelming reaction to the rise of Airbnb

© MPW SUMMIT: PETER DENCH; NORTHSIDE FESTIVAL: COLE GIORDANO

Slack CEO Stewart Butterfield

TECH

SLACK'S QUEST TO MAKE WORK EASIER

CEO Stewart Butterfield on saving you time and hassle on the job.

BY MICHAL LEV-RAM

SINCE DEBUTING three years ago, Slack has become a popular alternative to that quaint workplace communication tool known as email. Meanwhile, its founder and CEO, Stewart Butterfield, has become a guru of sorts on the evolution of work, including about things like chatbots (those automated attendants that increasingly respond to your customer service questions online).

Butterfield, a philosophy-major-turned-techie, isn't just pontificating—Slack's customers and its own workforce have provided a massive ▷▷

▲ PHOTOGRAPH BY BENJAMIN RASMUSSEN

sandbox for his observations. More than 5 million workers use his emoji-friendly app daily to message their teams, track and share documents, and yes, send one another dancing bananas. Giants like IBM, Capital One, and eBay (not to mention thousands of startups) are Slack customers. As a result, the privately owned company has ballooned into an 800-person tech player, currently valued at nearly $4 billion.

At press time, media reports said technology giants including Amazon.com were interested in acquiring Slack, which was seeking additional funding at an even higher $5 billion valuation. Slack declined to comment.

We caught up with Butterfield to hear more about workplace trends—not just chatbots, but also artificial intelligence, crowdsourcing, and why you need your own virtual chief of staff.

FORTUNE: You built and used Slack at your now defunct video game startup, Glitch. Was the original vision in line with what Slack is today?

BUTTERFIELD: Yes, we started a company to do something totally different and along the way we had invented this "proto" of Slack. It didn't have a name. But when we shut down Glitch we realized that this may be something that would be useful to other people because we would never work without it again. So we wrote a proposal for our investors. The mission was exactly what we ended up doing—to make peoples' working lives simpler, more pleasant, and more productive.

More recently, you've been working on adding artificial intelligence features. How so?

This might seem like a weird analogy at first, but we're trying to do what Google Maps did for the physical world. Inside all the computers of any large corporation is every decision that gets made. But people spend a huge amount of time trying to find the correct piece of information.

Like what?

Often it's simple, factual questions like, Who was responsible for this project? Who is so-and-so's manager? Where is the document relevant to today's meeting? This is so taken for granted that people don't really see it. And the degree of effort that people put into it is like the degree of effort that people put into finding geographic information back in the day—like pulling over at a gas station and asking the attendant how you get here or there, or folding and unfolding a map. Now you can just pinch and zoom into the world. Slowly, that will happen for people's experience at work. Anything we can do that lets people find information more quickly is something we're interested in.

How will we work five to 10 years out? And what's Slack's role in that future?

One way to describe it is that we are giving everyone a virtual chief of staff—someone who has infinite patience and infinite memory. It will proactively recommend things you should pay attention to. For example, we are working on something called "Highlights." Of all of the messages you haven't looked at yet, which are the ones that seem most important? Another example: Performance reviews can be handled by bots.

Wait, what?

A lot of companies lock up for a few weeks once a year for performance reviews. But there's a way to collect feedback in real time from Slack so that by the end of the year you've already stored up all of this information.

What does Slack, the company name, actually mean?

I used to say internally that it stands for "searchable log of all communications and knowledge," and then everyone forgot it. But there are two other meanings. The first one that often comes to mind is slacking off or slackers. The second one—and I think the more important one for us—is the idea of picking up the slack or cutting me some slack. As organizations have moved to increase efficiency, they've removed all the room for creativity and exploration from the system. Slack is actually a technical term in product management that means the excess capacity the system has to absorb any failures or to take on new work. That's something that was really on our minds when we came up with it. ■

STEWART BUTTERFIELD

FOUNDER AND CEO, SLACK

AGE: 44

FROM: Lund, British Columbia

EARLY LIFE: Until he turned 3 years old, Butterfield and his family lived in a log cabin with no running water. When he was still a kid, he taught himself how to code. He later studied philosophy at the University of Cambridge.

CLAIM TO FAME (PRE-SLACK): The entrepreneur cofounded photo-sharing site Flickr along with his ex-wife. The "Web 2.0" company sold to Yahoo in 2005 for a reported $35 million.

ORIGIN STORY: Both Flickr and Slack were "pivots"—they originated out of gaming companies Butterfield attempted but that ultimately failed. He has said he's unlikely to found another gaming startup.

A FORERUNNER IN VENTURE CAPITAL

Kirsten Green founded a one-woman VC firm in 2003—and has piled up the investing hits ever since. BY LEENA RAO

AMERICAN VOICES

PHOTOGRAPH BY ELISABETH FALL

KIRSTEN GREEN FOUNDER AND MANAGING PARTNER, FORERUNNER VENTURES

Stone Cold Numbers
As an analyst covering Safeway, Green once spent hours in a store's meat freezer counting inventory.

Heavenly Touch
As an angel investor, Green cashed in on hipster eyeglasses maker Warby Parker and menswear purveyor Bonobos.

Recent Favorites
Green has invested in Reese Witherspoon's clothing line, Draper James, and online makeup site Glossier.

VENTURE **AT AGE 18,** Kirsten Green sold women's clothes at the Nordstrom in Walnut Creek, Calif. Twenty years later, the retailer backed her fund, Forerunner Ventures. Green, 45, has made a name by investing in a handful of e-commerce supernovas, including razor-delivery startup Dollar Shave Club, which was acquired by Unilever in 2016 for $1 billion and e-commerce marketplace Jet.com, bought by Walmart for $3.3 billion.

Green started as a retail analyst and always felt "safe in numbers." Eventually she took more risk and in 2002 invested in a little-known company called Deckers Brands, which owned Teva sandals and had acquired a boot company called Ugg. Within a year, the stock went from $2.50 to $42 per share.

Green was new to Silicon Valley, so she did research projects for VCs and made angel investments before forming Forerunner in 2003. "To be a good investor you have to think differently from others," says Green—who if only for her gender stands out in the industry. Just 7% of U.S. VCs are women, according to Axios. Eight of the other nine people in her firm are women or minorities. "We want different perspectives and believe in the benefit," she says.

"I don't love it when people come in and say, 'We need a woman on our board,' or 'Can you invest in this new shopping app because you like to shop?'" she admits. "But whatever gets me in the deal." F

The reception lobby at Villa Kennedy—a five-star retreat in the center of Frankfurt.

COURTESY OF ROCCO FORTE HOTELS

DOING BUSINESS IN: FRANKFURT

Known for its modern skyline and financial vigor, this city on the Main River is well versed in international business—and poised to become an even bigger powerhouse post-Brexit. "After the U.K., this is the easiest place in Europe to do business," says Sir Rocco Forte , the English hotelier who has spent the past 13 years going back and forth to Frankfurt. "It's certainly a strong financial center—but there's also quite a lot to do." Here are some tips for your next business trip. **BY ADAM ERACE**

Getting around

Home to Europe's second largest airport by passenger volume [over 60 million annually], Frankfurt is a transportation juggernaut with nonstop service from 13 U.S. cities. Its airport is also a refreshingly convenient 20 minutes from downtown and well connected to public transportation. On arrival, you can get around on foot or by train, bus, or subway, but Forte notes, "it's a driving city, and parking isn't a problem," so you may want to rent a car if you plan to spend more than a few days.

Best business hotels

Situated on the southern bank of the Main River, Forte's Villa Kennedy resides in a late-19th-century mansion with a garden courtyard, a first-class, four-floor spa, and the suave JFK Bar. Closer to the financial center [just a 10-minute walk from Deutsche Bank HQ], the Sofitel Frankfurt Opera opened last October with urbane suites and an indoor pool.

Stay in shape

Frankfurt's full name is Frankfurt am Main, for its location on the jogger-and-cyclist-friendly waterway. Hemmed in on either side by pedestrian parks and laced like a high-top sneaker with slender bridges, the river makes an ideal location for getting some exercise, as well as your geographical bearings.

Where to entertain clients

It might seem strange to dine on American meat and potatoes in Frankfurt, but M-Steakhouse, from the city's prolific Mook Group, is a popular place for business dinners. The logo looks like something out of Guy Fieri's camp, while the cozy interior [white linens, candles, wood wainscoting] conjures New York City's Minetta Tavern. The menu includes "The Butterknife," a Nebraska-sourced filet mignon, and no less than eight types of potatoes.

After work

"Everyone thinks of Berlin as Germany's music center," says Forte, "but Frankfurt has quite a scene," which ranges from variety theater at Tigerpalast and international musicians at the underground Jazzkeller—Armstrong and Gillespie played there—to shows at the city's two opera houses. Rebuilt to its pre-WWII glory, the original Alte Oper hosts concerts, while the Oper Frankfurt company, whose soprano Louise Alder was named 2017's Young Singer by the International Opera Awards in May, performs in the modern glass hall by the river.

Local gifts

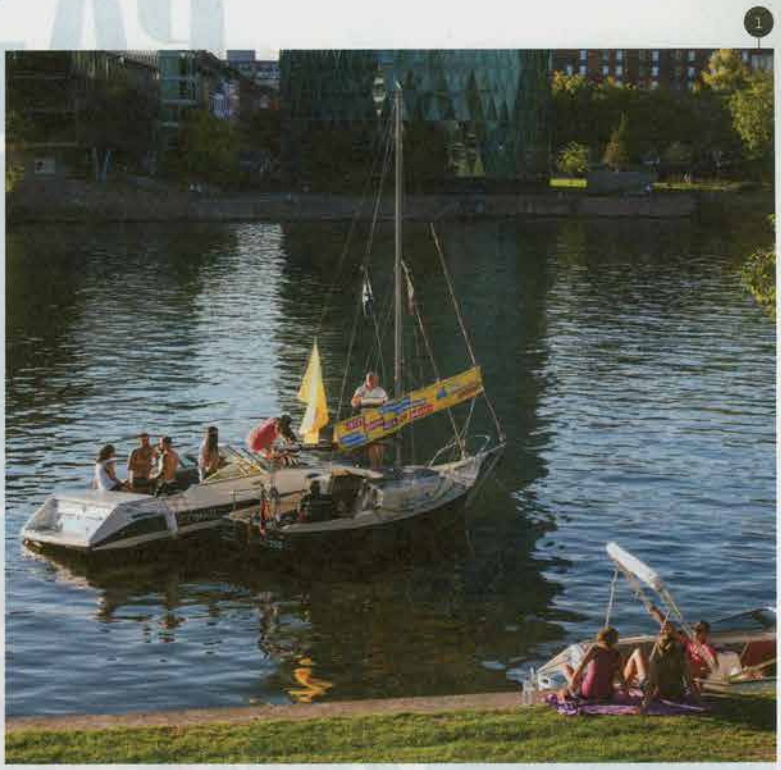
Frankfurt's deep distilling and brewing tradition means there are many delicious drinkable souvenirs to ship home. Local favorites include *apfelwein*, akin to dry French cider; Gin Sieben, a Frankfurt-style gin infused with seven specific herbs, including borage and sorrel; and *mispelchen*, a brandy made with medlar, a persimmon-like fruit.

Extending your stay

Heritage wine estates dot the sloping green hillsides of the Rheingau region, just west of Frankfurt, which is famed for its 20-mile stretch known as the Rheingauer Riesling Route. As the name suggests, Riesling is queen here [about 78% of production], but also look out for the region's elegant, lesser-known pinot noirs, called *spätburgunder*.

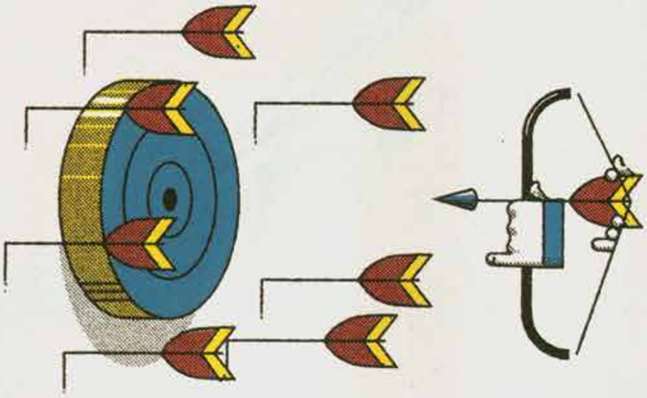
Etiquette 101

German politesse and discipline are famous, so "don't be aggressive and put a rush on [a business deal]," says Forte, who notes that despite Frankfurt's modernity, "old-fashioned" traditions still command respect: "When you shake hands, it's a done deal." With regard to politics, the U.S. has many issues in common with Germany [immigration, Russia], so respectful discussion is completely permissible. As at home, though, it helps to get a feel for your audience before launching into a more vigorous debate. ■



[1] When the work is done, Frankfurters enjoy an afternoon on the Main River. [2] A trumpet player performs for a discerning audience at the world-renowned Jazzkeller.

O MAIN RIVER: HORACIO VILLALOBOS—CORBIS/GETTY IMAGES; TRUMPET PLAYER: MANFRED ROTH—ULLSTEIN BILD/GETTY IMAGES



ON MESSAGE, OFF TARGET

The world is eager to adopt startup-style business practices. But what if they're wrong? BY ERIN GRIFFITH

WHEN ENTERING an unfamiliar society, it is wise to learn the local customs, the unspoken rules, and the names of its heroes, villains, and gods.

The same rule applies to Startup Land. To an outsider, the world of venture-backed startups might feel impenetrable. But don't despair: The Internet is littered with free guides to The Startup Way. Look first to the luminaries known by their acronyms: PG, TK, @AVC, a16z. (That would be Y Combinator founder Paul Graham, Uber CEO Travis Kalanick, Union Square Ventures partner Fred Wilson, and venture capital firm Andreessen Horowitz.) Follow their blogs, listen to their podcasts, repeat their catchphrases, learn the Acronymed Ones' acronyms. (FNAC stands for "feature, not a company." HENRY means "high earner, not rich yet.") You can even consume precious nuggets of startup wisdom through mobile push notifications thanks to products like Startup Funding Bot, Startup Patterns, Startup Quotes, and the website Great Fucking Startup Advice. (Sample counsel: "Don't ask for permission, ask for fucking forgiveness.")

FOR MORE
Follow Erin Griffith on Twitter (@eringriffith) or at fortune.com/boom.

Startup Land's collective knowledge is one part mythology, one part advice, one part inspiration, and zero parts business school–sanctioned case study. (As universities add courses on entrepreneurship, Peter Thiel pays students to drop out.) Its catchphrases have been repeated so much that they are now clichéd punch lines, oversimplified to the point of meaninglessness.

But that doesn't mean they're not true. So what happens when a piece of startup gospel is flat-out wrong?

I recently found myself carelessly repeating a statistic that I'd heard dozens of times in private conversations and on public stages: "Nine out of 10 startups fail." The problem? It's not true. Cambridge Associates, a global investment firm based in Boston, tracked the performance of venture investments in 27,259 startups between 1990 and 2010. Its research reveals that the real percentage of venture-backed startups that fail—as defined by companies that provide a 1X return or less to investors—has not risen above 60% since 2001. Even amid the dotcom bust of 2000, the failure rate topped out at 79%.

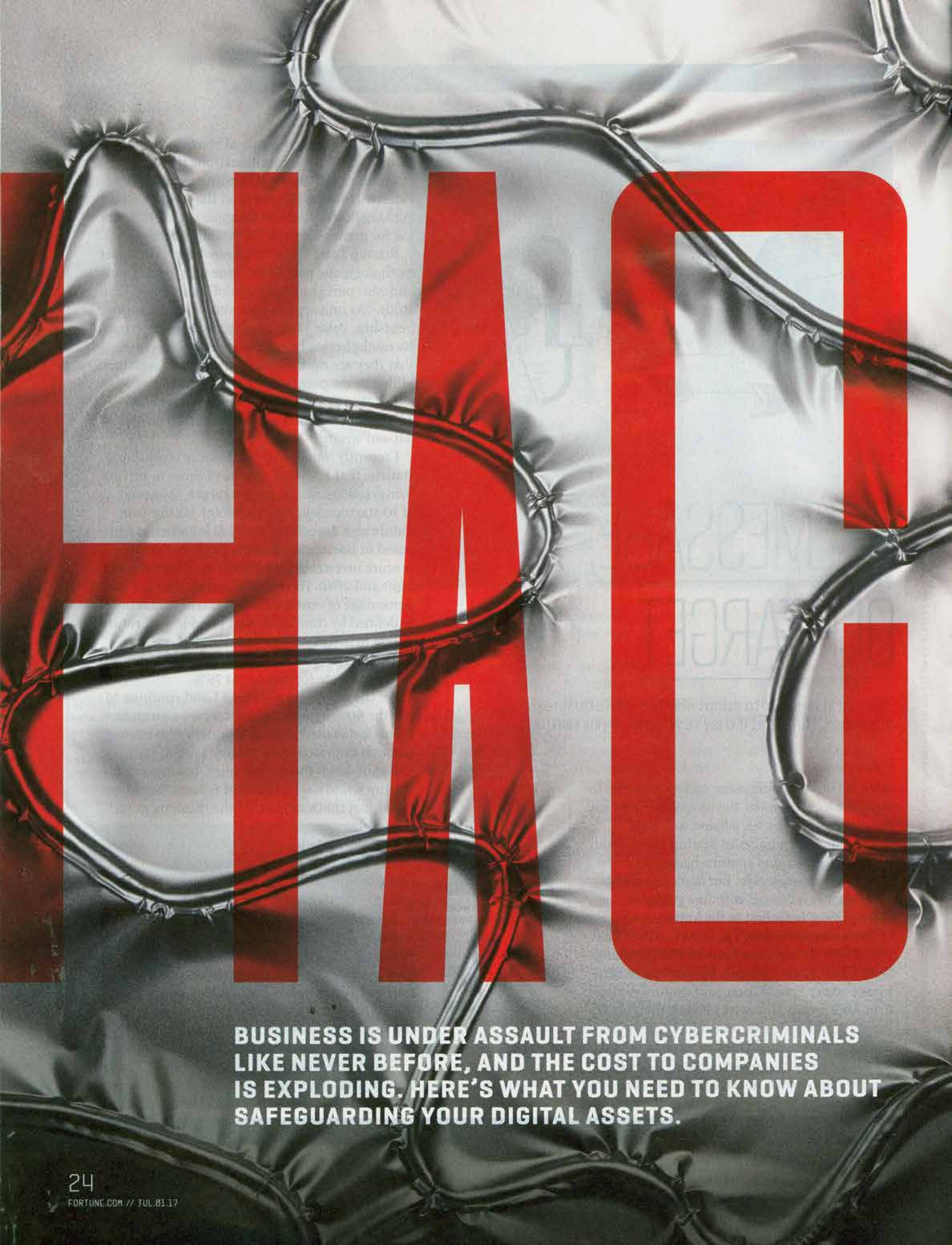
Yet the denizens of Startup Land continue to cite the 90% figure because it serves a purpose. It comforts failed startup founders who burned through their investors' money, laid off staff, and shut down their companies. It supports the startup world's celebration of failure. "Sure, you failed, but that's the norm," the thinking goes. "The odds were against you."

But startup failure isn't a natural law like gravity. It's not a given. Normalizing the failure narrative only conceals the truth, misleads founders, and in certain cases, explains away bad behavior.

So here's some wisdom of my own: Take a skeptical view of the widely accepted knowledge in Startup Land. It's especially necessary in an environment where entrepreneurship is fetishized on television shows like *Shark Tank,* old-economy corporations are desperately trying to imitate their disrupters, and *Fortune* 500 execs are jumping ship to "unicorn" startups.

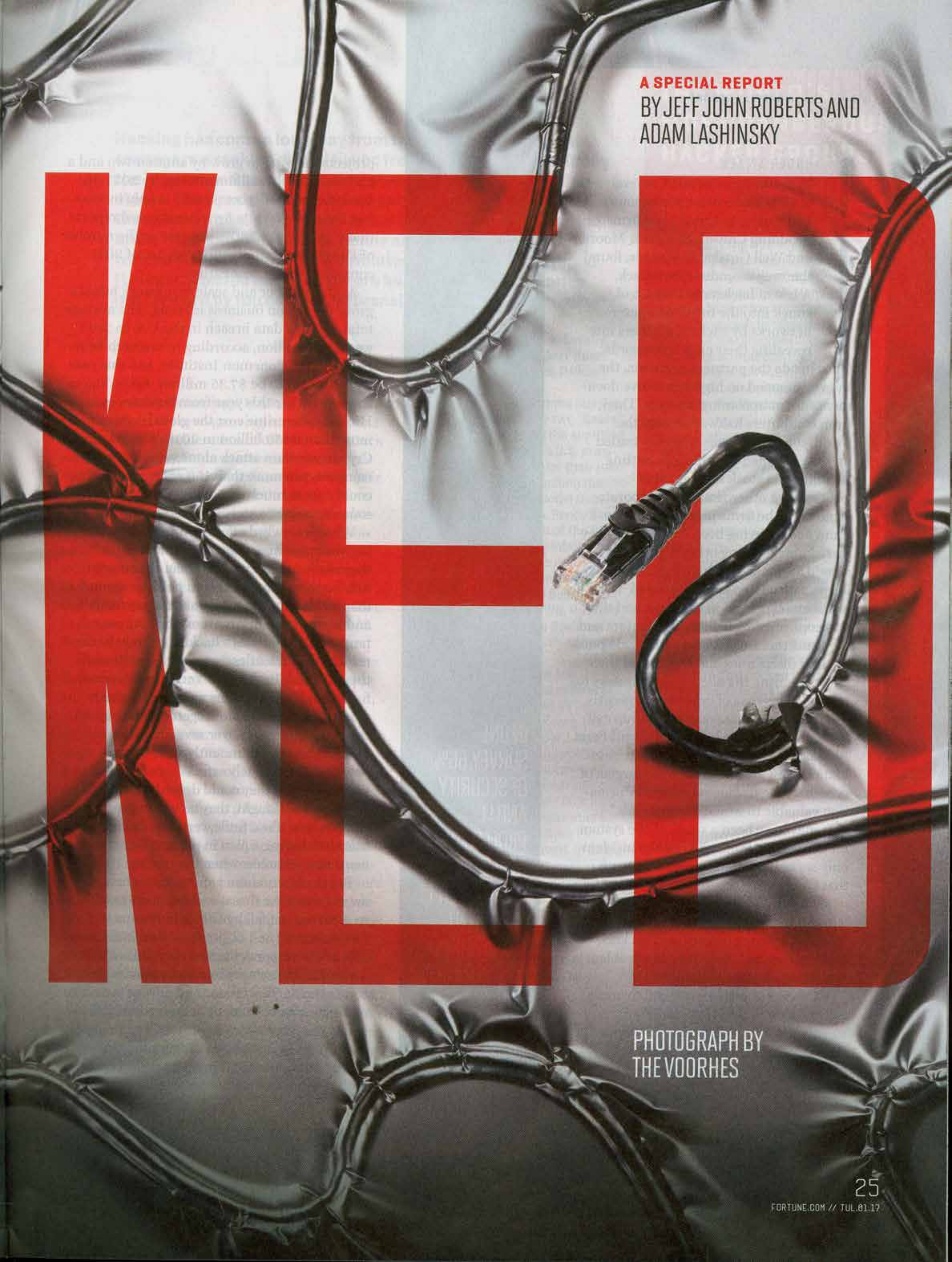
Soak up the mantras inside the Silicon Valley bubble. But do so with a grain of salt. ■

▲ ILLUSTRATION BY **MICHAEL GEORGE HADDAD**



HAC

BUSINESS IS UNDER ASSAULT FROM CYBERCRIMINALS LIKE NEVER BEFORE, AND THE COST TO COMPANIES IS EXPLODING. HERE'S WHAT YOU NEED TO KNOW ABOUT SAFEGUARDING YOUR DIGITAL ASSETS.



KED

A SPECIAL REPORT

BY JEFF JOHN ROBERTS AND ADAM LASHINSKY

PHOTOGRAPH BY THE VOORHES

1 UNDER ATTACK

In the summer of 2015, several of New York's most prestigious and trusted corporate law firms, including Cravath Swaine & Moore and Weil Gotshal & Manges, found themselves under cyberattack. A trio of hackers in China had snuck into the firms' computer networks by tricking partners into revealing their email passwords. Once inside the partners' accounts, the thieves snooped on highly sensitive documents about upcoming mergers. Then, from computers halfway around the world, the cybercrooks allegedly traded on the purloined information, netting $4 million in stock market gains.

Like most other victims of corporate espionage, the firms preferred to keep mum about having been victimized. They feared antagonizing other digital thugs as well as damaging their reputations as keepers of clients' secrets. Instead, word of the attack leaked in the press and then was confirmed by federal prosecutors and the firms themselves. The Feds made public their discoveries and trumpeted their efforts to bring the alleged perpetrators to justice. "This case of cyber meets securities fraud should serve as a wake-up call for law firms around the world," said Preet Bharara, then the U.S. Attorney in Manhattan. "You are and will be the targets of cyberhacking because you have information valuable to would-be criminals."

It may have been a shock to the system for the legal community, but the incident only served to underscore a hard truth that CEOs, company directors, and network security experts have been grappling with for some time now: Business is under assault like never before from hackers, and the cost and severity of the problem is escalating almost daily.

The latest statistics are a call to arms: According to Cisco, the number of so-called distributed denial-of-service (DDoS) attacks—assaults that flood a system's servers with junk web traffic—jumped globally by 172% in 2016. Cisco projects the total to grow by another two and a half times, to 3.1 million attacks, by 2021. Indeed, the pace of cyberassaults is only increasing. Internet security firm Nexusguard reports that it observed a 380% increase in the number of DDoS attacks in the first quarter of 2017 compared with a year earlier.

IN ONE SURVEY, 66% OF SECURITY AND I.T. PROFESSIONALS REPLIED THAT THEY WEREN'T CONFIDENT THAT THEIR ORGANIZATION COULD RECOVER FROM A CYBERATTACK.

As the number and scale of network attacks grow, the toll on business is rising. The average total cost of a data breach in the U.S. in 2014 was $5.85 million, according to research from IBM and the Ponemon Institute, and this year it's estimated to be $7.35 million. According to a report earlier this year from business insurer Hiscox, cybercrime cost the global economy more than $450 billion in 2016. The WannaCry ransomware attack alone, which crippled computers in more than 150 countries in May, could cost as much as $4 billion according to some estimates.

What is slowly dawning on corporate hacking victims is how vulnerable and defenseless they really are, even when their opponents may be three guys in a room halfway around the world. Expensive data-security systems and high-priced information security consultants don't faze today's hackers, who have the resources to relentlessly mount assaults until they succeed. In the New York law-firm case, for example, prosecutors said the attackers attempted to penetrate targeted servers more than 100,000 times over seven months.

It has become abundantly clear that no network is completely safe. Where once companies thought they could defend themselves against an onslaught, they're now realizing that resistance is, if not futile, certainly less important than having a plan in place to detect and neutralize intruders when they strike.

But there remains a gaping chasm between awareness of the threat and readiness to address it: A survey last fall by IBM and Ponemon of 2,400 security and IT professionals found that 75% of the respondents said they did not have a formal cybersecurity incident response plan across their organization. And 66% of those who replied weren't confident in their organization's ability to recover from an attack.

Cybercrime is metastasizing for the same reason online services have become so popular with consumers and businesses alike: Ever-

more-accessible technology. Hacking is easier than ever thanks to the ever-growing number of online targets and the proliferation of off-the-shelf attack software. The very Internet networks that were built for convenience and profit are exposing their users to a steady stream of new threats.

What's more, the tense state of affairs is a glaring example of how the entire nature of business has changed in the digital age. In most cases, technology is much more than just a supplement to a company's core operations. For scores of the world's most valuable companies—from Alphabet to Amazon to Facebook to Uber—the assets that live on their networks *are* their core operations.

No sector of corporate America is safe. Hackers have plundered big retailers like Neiman Marcus and Home Depot for credit card and customer information. They've burrowed into banks like JPMorgan Chase. Even tech companies can't seem to protect themselves. Yahoo's ineptitude in repelling (or even being aware of) hackers forced it to reduce its sale price to Verizon. Google and Facebook recently fell victim to a hacker who conned their accountants into wiring him a total of more than $100 million. And OneLogin, a startup that bills itself as a secure password management service, recently lost certain customer data to hackers.

It's not like companies aren't trying to play defense. (Or sometimes even going on the offensive: See the following story, "Google's Elite Hacker SWAT Team vs. Everyone.") Accenture estimates that companies worldwide spent $84 billion in 2015 to protect against attacks. That spending is an acknowledgment that every company needs to safeguard its digital assets, which in turn requires *knowing* about the criminals that keep coming at them and what defenses they can build to minimize the damage.

THE WORLD'S MOST DANGEROUS HACKER GROUPS

Hacking has come a long way from the days of maladjusted teenagers wreaking digital havoc from their basements. Today the biggest and baddest hacker groups are backed by nation-states. They're called "advanced persistent threats" or APTs, in the cyber jargon, a phrase meant to convey their supreme and underlying quality: ferocity. Below are a few of the most notorious—and feared—state-affiliated hacking groups around. (Links to specific hacks below are based on leading theories put forward by top computer forensic firms.) —Robert Hackett

Fancy Bear (a.k.a. Sofacy, Pawn Storm) / Cozy Bear (a.k.a. CozyDuke, Office Monkeys)
Rival agencies in the Russian spy services, the two "Bears" were thrust into the spotlight during last year's U.S. presidential election for their roles in allegedly breaching the Democratic National Committee's system. Fancy Bear, which comes out of the GRU, Russia's military intelligence agency, has been meddling in European elections since then. Cozy Bear, which represents the FSB, Russia's successor to the Soviet-era KGB, has hit U.S. think tanks.

Lazarus Group (a.k.a. DarkSeoul, Guardians of Peace)
Widely believed to be associated with North Korea, this gang refuses to die. Lazarus got its start by pummeling American and South Korean websites with denial-of-service attacks in 2009. Five years later, it perpetrated a massive hack of Sony Pictures Entertainment. In 2016, Lazarus stole $81 million in a heist targeting Bangladesh's central bank and the SWIFT financial network. And it has been linked to the WannaCry ransomware worm that ground businesses around the globe to a halt in May.

Equation Group
This is the nickname given by Russian antivirus firm Kaspersky to a team believed to be associated with the U.S. National Security Agency—specifically the NSA's Tailored Access Operations unit, or TAO. They're the good guys, right? Not in everyone's eyes. Many experts believe the Equation Group successfully attacked Iran's nuclear program in the mid-aughts. But recently a selection of the squad's hacking tools were stolen and leaked by the Shadow Brokers, another mysterious hacker group (believed to be Russia-affiliated), and are now being used to cause mayhem.

Comment Crew (a.k.a. APT1, Shanghai Group)
China sponsors a plethora of hacking groups. One of the most notorious, believed to be part of the People's Liberation Army, came to be known as Comment Crew for its habit of hiding comments on web pages. The group was involved in Operation Aurora, a campaign that hacked big U.S. tech companies like Google in 2009. Chinese industrial espionage has been on the decline since former U.S. President Barack Obama and Chinese President Xi Jinping agreed to cool it on the cyber front last year.

Sandworm (a.k.a. Electrum)
Named for allusions to the sci-fi classic *Dune* found in its code, Sandworm is another group believed to be associated with the Russians. The crew has hacked people affiliated with NATO and the Ukrainian government, presumably to gather intelligence. Sandworm is also known for breaking into companies that deal with critical infrastructure. Last year the group shut down a power grid in Ukraine.

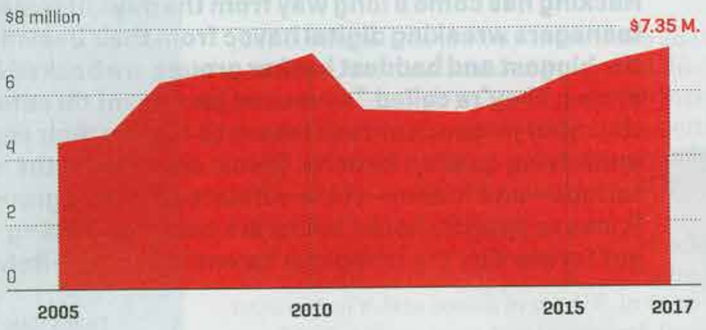
2

A NEW BREED OF CRIMINAL

Hacking is particularly frustrating for corporate executives who don't understand their enemy. Embezzlers or extortionists? Sure. But faceless gangs of nasty nerds? It's often harder for CEOs to wrap their brains around the motivation of their antagonists—or their audacity. "At the C-level they feel violated," says Jay Leek, a venture capitalist pursuing cybersecurity investments and a former chief information security officer at private equity giant Blackstone. "I witness this emotional 'What just happened?' You don't walk in physically to a company and violate it."

The brazenness Leek describes is a hallmark of hackers who—despite their mystique in popular culture—are basically everyday thieves, like bank robbers. Where hackers are different, however, is that they rarely meet in person. Instead, they convene in online forums on the "dark web," an anonymous layer of the Internet that requires a special browser to access. Deep in the forums, crooks hatch hacking plots of all sorts: breaking into corporate databases or selling stolen Social Security numbers or purchasing inside information from unscrupulous employees.

AVERAGE COST OF A DATA BREACH FOR U.S. COMPANIES



SOURCE: PONEMON INSTITUTE (FISCAL YEARS)

Cybercriminals have proved adept at adopting successful corporate strategies of their own. A recent development has seen the cleverest crooks selling hacking tools to criminal small-fry. It's analogous to semiconductor companies licensing their technology to device manufacturers. According to a report from security software giant Symantec, gangs now offer so-called ransomware as a service, a trick that involves licensing software that freezes computer files until a company pays up. The gangs then take their cut for providing the license to their criminal customers.

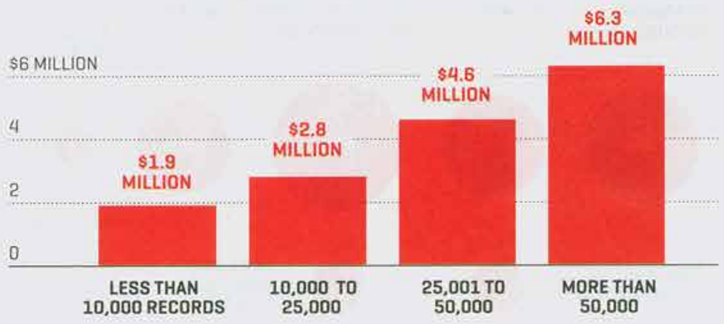
If it weren't all blatantly illegal, the practices would be laudably corporate. "Cybercriminals no longer need all the skills to complete any particular crime," says Nicole Friedlander, a former assistant U.S. Attorney in charge of the key Southern District of New York's complex fraud and cybercrime unit. "Instead, they can hire other cybercriminals online who have those skills and do it together." In that sense, hackers have become service providers like doctors or lawyers or anyone else, says Friedlander, who joined the New York office of law firm Sullivan & Cromwell last year.

But the bad guys aren't all freelancers. In fact, some of the most sinister hacking outfits operating today are "state-sponsored" groups supported, or at least loosely supervised, by

Nicole Friedlander, a New York lawyer specializing in cybercrime, says hackers collaborate more today and "no longer need all the skills to complete any particular crime."

▲ PHOTOGRAPH BY REBECCA GREENFIELD

AVERAGE COST PER SIZE OF DATA BREACH, GLOBAL, F.Y. 2017



SOURCE: PONEMON INSTITUTE

governments. That includes the Russians who are believed to have hacked into the Democratic National Committee last year and the North Korean team credited with unleashing the WannaCry malware as a moneymaking scheme. (See the box on "The World's Most Dangerous Hacker Groups.")

3 PLAYING DEFENSE

In early March, the information security team at ride-hailing giant Uber leaped into action: An Uber employee had reported a suspicious email message, and similar reports were flooding in from all over the company.

Uber's databases contain the email addresses and personal information of millions of riders around the world, making security a particularly pressing issue. And the company has had its share of problems as a caretaker of sensitive data. In 2014, Uber suffered a breach that exposed the insurance and driver's license information of tens of thousands of drivers; it took the megastartup months to discover and investigate the incident and fully notify its drivers.

As soon as the alarm was raised in March, Uber established an "incident commander" to manage the developing situation. The job of the incident commander—a term of art in cybersecurity circles—is to keep the company informed about potential attacks. It turned out that the attack was targeting users of Google's Gmail service, not Uber itself. But anyone with a Gmail address was vulnerable. Later that same day Google fixed the vulnerability in its Gmail service, allowing Uber's incident commander to stand down.

"DURING AN INCIDENT, THE ROLE OF EXECUTIVES IS TO GIVE SUPPORT," SAYS UBER'S CHIEF INFORMATION SECURITY OFFICER. "THERE'S NO ROOM FOR CONFUSION ABOUT WHO'S IN CHARGE."

Uber's reaction is an example of the vigilance with which companies must treat the torrent of threats coming at them every day. John "Four" Flynn, a former Facebook executive who now is chief information security officer for Uber, says the key to cybersecurity incidents—which he defines as everything from a data breach to a stolen laptop—is to have a clear communication strategy. "During an incident, the role of executives is to give support," says Flynn. "There's no room for confusion about who's in charge."

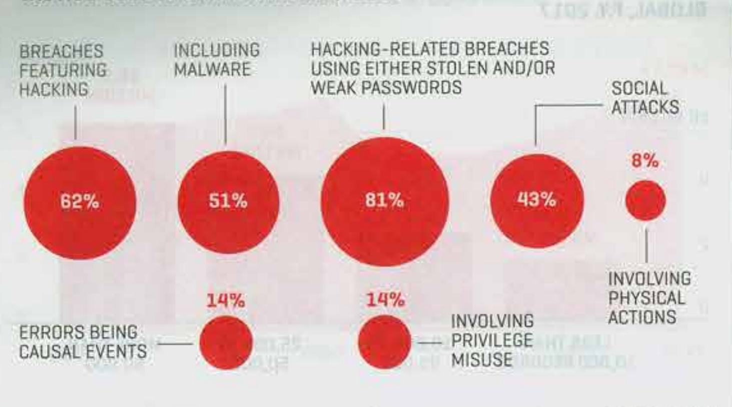
Flynn has every right to sound confident in his authority. The chief information security officer, or CISO, is possibly the hottest job in the C-suite today. Cybercrime is so serious that these formerly little-known and unloved executives now typically have a direct line to boards of directors—a big break from the past. Before, the CISO would report to the chief information officer, who was responsible for buying and operating computers, not obsessing over flies in the ointment. If the CISO sounded the alarm over a breach, too often he or she ended up being the one sacrificed to appease top management. "It was my job to tell my boss his baby was ugly," one former information security executive laments.

These days, though, smart companies treat hacking threats like other existential risks to their business—recessions, terrorist attacks, and natural disasters come to mind—and plan accordingly. The CISO is pivotal in maintaining readiness. "If you're a *Fortune* 500 company, you already have a response," says Leek, the former executive at Blackstone, which had several portfolio companies that suffered breaches, including arts-and-crafts merchant Michaels Stores. "But people forget to take it out, blow the dust off, and recall: 'Let's do what we decided when we had a sound mind.' "

Having a clear line of authority and a good action plan take a company only so far. At some point it has to call the cops, specifically the Federal Bureau of Investigation or the U.S. Secret Service. Both agencies have reach and power that allow them to take the fight to foreign cybercrooks. On several occasions, U.S. law enforcement agents working undercover on the dark web have managed to lure presumed offenders out of hiding with phony deals, and then had them apprehended in and extradited to the U.S.

Calling law enforcement has downsides, however. The likely outcome—an investigation—imposes burdens on the victim company in terms of money and time. And it increases the chance that sensitive details about the hack will leak publicly. That's why the best course of action is for companies to avoid FBI-level hacking incidents in the first place. A new, multibillion-dollar industry has sprung up to help.

TACTICS USED IN DATA BREACHES, 2016



SOURCE: VERIZON

4 AN INDUSTRY IS BORN

The videoconference camera looked like any other. But unbeknownst to its corporate owner, the device was working overtime: Hackers had captured the microphone remotely and were using it to spy on every meeting that took place in the boardroom. The company, which does not want to be identified, finally got wise to the spying scheme thanks to Darktrace, a global cybersecurity company that uses artificial intelligence to detect aberrant activity on client networks. Darktrace CEO Nicole Eagan says her company noticed the camera had been gobbling abnormal amounts of data. This raised a red flag, enabling Darktrace to notify its client that something was amiss.

Darktrace is just one of hundreds of firms that offer help to combat the hacking epidemic. Once a stodgy corner of enterprise software, cybersecurity has become a hot sector for venture capitalists. Investors put some $3.5 billion into a total of 404 security startups last year, according to New York research firm CB Insights. That's up from $1.8 billion

A BRIEF HISTORY OF MAJOR CORPORATE HACKS

LINKEDIN
2012

In 2012, the professional network said 6.5 million accounts had been hacked. In 2016, it emerged that the breach was much worse: Hackers were selling name and password info for more than 117 million accounts.

TARGET
2013

In December 2013, 110 million customers' personal and financial information was exposed. CEO Gregg Steinhafel later resigned as part of the fallout from the massive breach.

JPMORGAN
2014

Hackers hijacked one of JPMorgan Chase's servers and stole data about millions of the bank's accounts, which they allegedly used in fraud schemes yielding some $100 million.

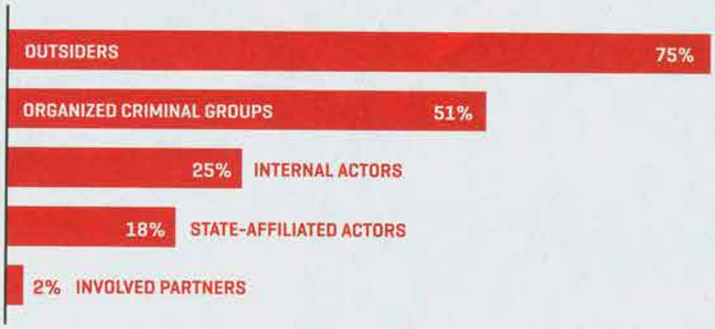
HOME DEPOT
2014

Hackers stole email and credit card data from more than 50 million customers. The breach cost the retail chain at least $179 million in settlements with consumers and credit card companies.

SONY
2014

Hackers believed to be associated with North Korea rampaged through the servers of Sony Pictures Entertainment in retaliation for a film comedy showing North Korean leader Kim Jong-un's face being melted off.

DATA BREACH PERPETRATORS, 2016



SOURCE: VERIZON

for 279 investments in 2013.

For executives, all of this entrepreneurial activity translates into a dizzying array of security options. There are newcomers like Tanium, for instance, which offers a service that lets companies see who is on their network. Publicly traded Palo Alto Networks makes a kind of intelligent firewall that uses machine learning to thwart intruders. There are also a host of niche security firms such as Area 1 (which specializes in defending against phishing scams) and Lookout (which is a mobile-phone-focused security service).

With all of this firepower arrayed against it, how can cybercrime continue to grow so fast? One answer is that some of the glitzy defense systems don't work as advertised. Security insiders grumble about firms bamboozling clients with "blinky lights" in order to sell "scareware"—software that plays to customers' insecurities but doesn't protect them.

At the end of the day, though, humans are as much to blame as software. "The weak underbelly of security is not tech failure but poor process implementation or social engineering," says Asheem Chandna, an investor with Greylock Partners and a Palo Alto Networks director. Chandna notes that most hacking attacks come about in two ways, neither of which involves a high level of technical sophistication: An employee clicks on a booby-trapped link or attachment—perhaps in an email that appears to be from her boss—or someone steals an employee's log-in credentials and gets access to the company network.

While cyberdefense tools can mitigate such attacks, some will always succeed. Humans are curious creatures and, in a big organization, there will always be someone who clicks on a message like, "Uh-oh. Did you see these pictures of you from the office party?" When it comes to hacking, a penny of offense can defeat a dollar's worth of defense. That's why the fight against hacking promises to be a never-ending battle. F

HILTON HOTELS
2015

Hackers got inside the chain's payment system and reportedly stole customer credit card data from dozens of Hilton and Starwood chains from across the country.

LAW FIRMS
2015

Chinese hackers accessed email accounts at firms Cravath Swaine & Moore and Weil Gotshal & Manges—and learned about upcoming corporate mergers. They allegedly made $4 million trading on the information.

SWIFT
2016

North Korean hackers reportedly exploited weaknesses in the SWIFT payment system to steal $81 million from the Bangladesh Central Bank's account at the New York Federal Reserve.

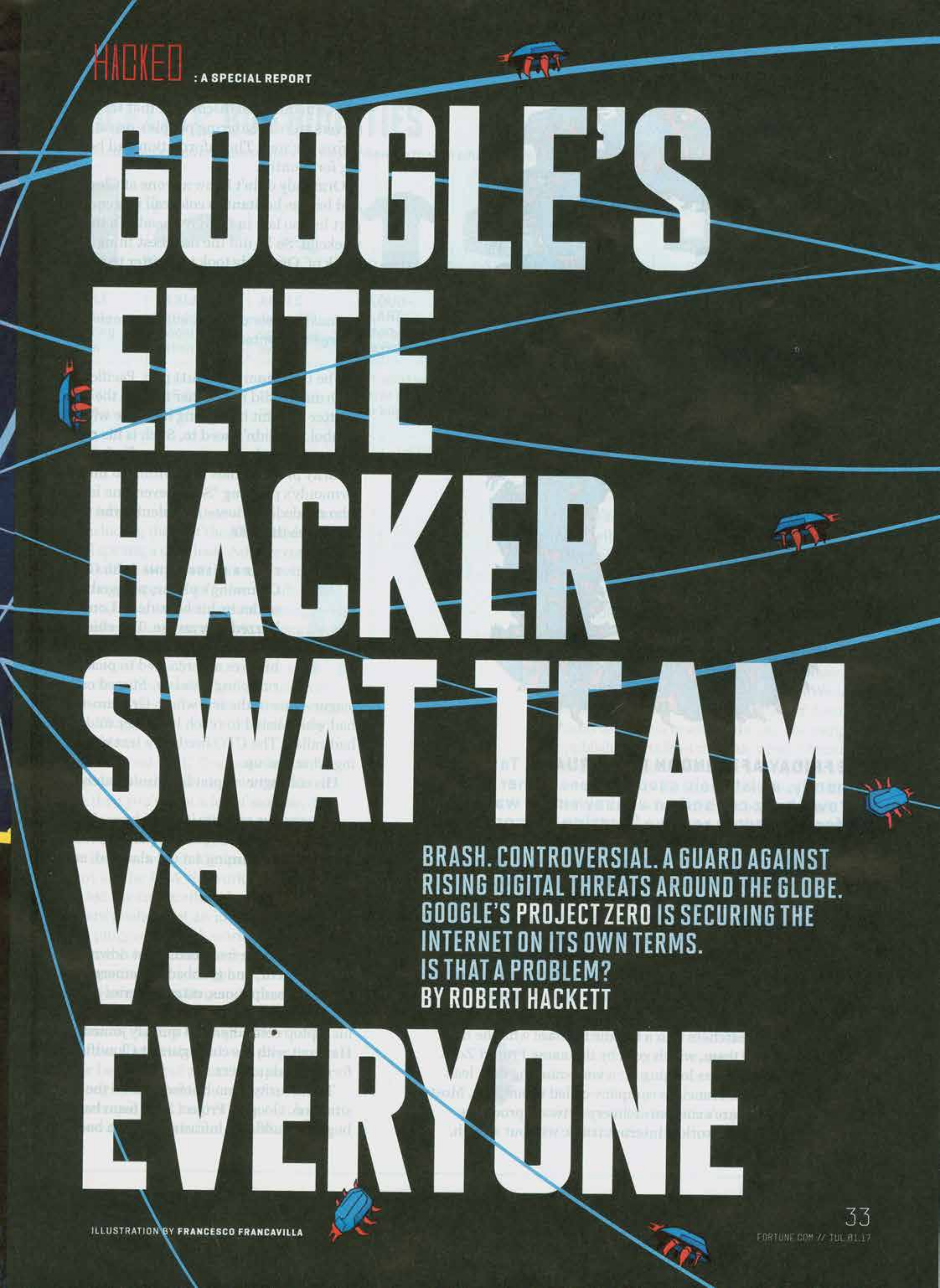
TESCO
2016

Hackers drained a total of around $3.2 million from more than 9,000 accounts in Tesco Bank, the bank run by the giant grocery chain. Tesco was forced to reimburse customers for the stolen money.

CHIPOTLE
2017

An Eastern European criminal gang reportedly used phishing to steal the credit card information of millions of Chipotle customers. The breach was part of a larger scam targeting restaurants.

G
FRAN
CAVIL
LA F.17

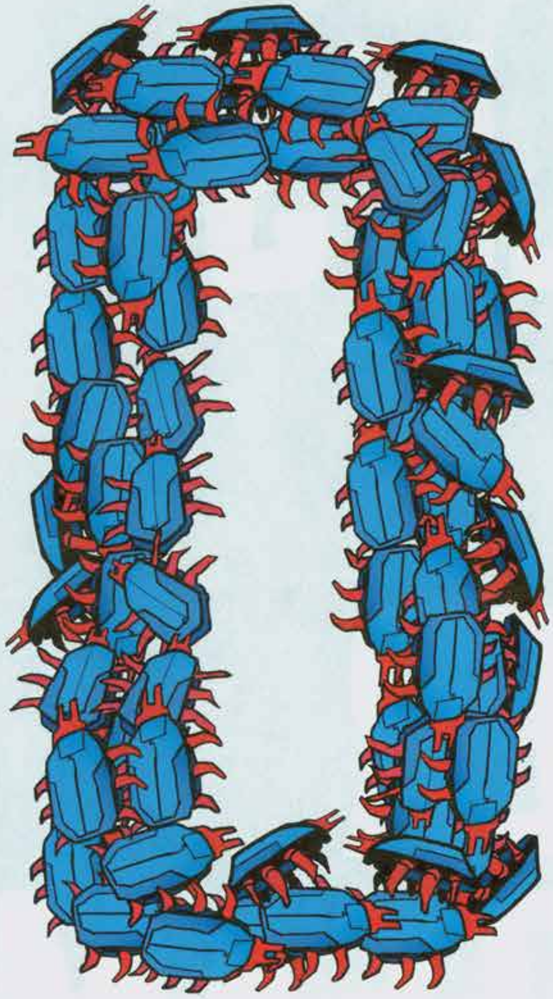


GOOGLE'S ELITE HACKER SWAT TEAM VS. EVERYONE

BRASH. CONTROVERSIAL. A GUARD AGAINST RISING DIGITAL THREATS AROUND THE GLOBE. GOOGLE'S PROJECT ZERO IS SECURING THE INTERNET ON ITS OWN TERMS. IS THAT A PROBLEM?

BY ROBERT HACKETT

ILLUSTRATION BY FRANCESCO FRANCAVILLA



ONE FRIDAY AFTERNOON IN FEBRUARY, Tavis Ormandy, a virtuosic security researcher with a brown buzz cut and an uneasy smile, was performing some routine "fuzzing," a common code-testing technique that blasts software with random data to expose faults, at his desk at Google headquarters in Mountain View, Calif. The process was going as expected when he spotted something amiss in the data set. *Weird,* he thought. *This isn't typical corrupted data.* Instead of the expected output, he saw bizarrely configured anomalies—strange chunks of memory strewn about. So he dug deeper.

After assembling enough information, Ormandy called his fellow security researchers into a huddle to share what he had found. The Google team, which goes by the name Project Zero, soon realized what it was looking at: a wide-ranging data leak spouting from a San Francisco company called Cloudflare. Most of the time, Cloudflare's content-delivery network processes roughly a tenth of the world's Internet traffic without a hitch. But Ormandy had discovered that the company's servers were splattering people's private data across the web. The information had been leaking for months.

Ormandy didn't know anyone at Cloudflare, and he was hesitant to cold-call its generic support line so late in the day ahead of a three-day weekend. So he did the next best thing he could think of. Ormandy took to Twitter to appeal to the tens of thousands of people who follow him there.

Could someone from Cloudflare security urgently contact me

The time stamp was 5:11 p.m. Pacific Time.

Ormandy did not bother to alert the company's Twitter account by tagging its name with an "@" symbol. He didn't need to. Such is his reputation among the zealous community of information-security professionals that within 15 minutes of Ormandy's pressing "Send," everyone in the world who needed to know—and plenty who didn't—would see the note.

AT 1:26 A.M. LOCAL TIME John Graham-Cumming's phone, plugged into an outlet by his bedside in London, buzzed him awake. The chief technology officer of Cloudflare rubbed his eyes and reached to pick up the rumbling handset. Missed call. A colleague—one of the few whom Graham-Cumming had white-listed to reach him after midnight—had called. The CTO fired off a text message asking what was up.

His colleague responded immediately.

very serious security issue

Graham-Cumming sat up, alarmed, and replied.

I will get online

The CTO rose from bed, went downstairs to the basement, and grabbed the emergency bag—charger, headphones, extra batteries—that he had stowed for such an occasion. He booted up his laptop computer and quickly joined a Google Hangout with his colleagues at Cloudflare's California headquarters.

The security team briefed him on the unfolding situation. Google's Project Zero team had found a bug in Cloudflare's infrastructure—a bad one. The

PRICE LIST: BUG BOUNTIES

○ Some companies reward researchers for finding flaws in their products. Here's a sampling of the spoils.

GOOGLE Android operating system	**TESLA** Tesla Model S sedan	**APPLE** Apple iOS operating system	**CLOUD-FLARE** Internet services	**DEPT. OF DEFENSE** Public DoD websites	**UNITED AIRLINES** Website and apps	**NETGEAR** Routers, apps, and services	**ORACLE** Any product or service
○ Up to $200,000 per bug	○ Up to $10,000 per bug	○ Up to $200,000 per bug	○ T-shirt and a free trial for bugs	○ Portion of $150,000 pool for all bugs	○ Up to 1 million miles per bug	○ Up to $15,000 per bug	○ "Thanks," a.k.a. credit in advisory about the fix

○ GOOGLE: MICHAEL SHORT—BLOOMBERG VIA GETTY IMAGES; TESLA: COURTESY OF TESLA; APPLE: COURTESY OF APPLE INC.; CLOUDFLARE: AMRIPHOTO—GETTY IMAGES; PENTAGON: LIBRARY OF CONGRESS/CORBIS/VCG VIA GETTY IMAGES; UNITED: COURTESY OF UNITED; NETGEAR: BUSINESS WIRE; ORACLE: KIMIHIRO HOSHINO—AFP/GETTY IMAGES

servers that help run more than 6 million customer websites, including those of the FBI, Nasdaq, and Reddit, had sprung a data leak. Anyone could access a Cloudflare-supported site and retrieve in certain circumstances the intimate details—authentication tokens, cookies, private messages—of users of another site on its network, among them Uber, 1Password, OKCupid, and Fitbit.

The information was hidden in plain sight. Worse, search engines and other web crawlers had been storing the leaked data in their caches for months. Plugging the leak would not fully solve the problem.

"I liken it to an oil spill," Graham-Cumming says. "It's easy to deal with a hole in the side of a tanker, but then you've got a lot of seabeds that need to be cleaned up."

So Cloudflare's engineers got to work. Security chief Marc Rogers, who in his spare time serves as a consultant for the USA Network hacker drama *Mr. Robot*, led the triage effort. In less than an hour the team pushed out an initial mitigating update that plugged the leak worldwide. After several hours the technicians successfully rolled back functions that had contributed to the error. Almost seven hours after Ormandy fired off his tweet, Cloudflare's engineers managed to enlist the major search engines—Google, Microsoft, Yahoo—to clear their historical web page caches.

It was the beginning of a very long weekend. Cloudflare engineers spent the rest of it evaluating how much and what kind of data had leaked as well as how far the mess had spilled.

Google's Project Zero team was initially impressed with the rapid response of Cloudflare, which has a reputation for transparency when it comes to security matters. But the relationship began to fray as the teams negotiated when they would publicly reveal what had transpired. The companies tentatively agreed to make an announcement as early as Tuesday, Feb. 21. As the day waned, Cloudflare decided it needed more time for cleanup. Tuesday became Wednesday. Wednesday became Thursday. Google put its foot down: Thursday afternoon would be the day the companies published details of the leak, which Ormandy dubbed "Cloudbleed," whether or not Cloudflare had completed its assessment and ensured that the leaked data was clear from online caches.

Both advisories went up on Feb. 23. A weeklong Internet panic ensued.

YOU DON'T HAVE TO BE a member of Google's Project Zero to know that security crises are on the rise around the globe. Every company has become a tech company—and so hacks are increasingly becoming commonplace, draining corporate bank accounts, spying on individuals, and interfering in elections. The headlines are sobering: More than 1 billion Yahoo accounts compromised. Tens of millions of dollars stolen through the SWIFT financial network. Countless private emails from the Democratic National Committee exposed ahead of the 2016 U.S. presidential election. (For more on how business is responding, read "Hacked," p. 24.)

U.S. companies and government agencies reported 40% more breaches in 2016 than in 2015, and that's a conservative estimate, according to the Identity Theft Resource Center. At the same time, the average cost of a data breach now runs organizations $3.6 million, according to an IBM-sponsored study conducted by the Ponemon Institute, a research group.

Whether the result of a programmer's error or hackers working for a nation-state, data leaks are the new norm. So executives are coming to terms with the idea that it might be more economical to nip coding issues in the bud before they lead to bigger—and messier—problems down the road.

But it's not that simple. Too many organizations either don't prioritize security or view it as an impediment to meeting product development and delivery deadlines. According to Veracode, an application-security firm acquired by CA Technologies earlier this year, 83% of the 500 IT managers it surveyed admitted that they had released code before testing for bugs or resolving security issues. At the same time, the security industry faces a talent shortage. Cisco estimates that there are 1 million unfilled security jobs worldwide, and Symantec predicts that will increase to 1.5 million by 2019. Some estimates believe that figure will grow to 3.5 million by 2021.

Even if a company has the funds, initiative, and cachet to support a proper security staff, it's not immune to shipping flawed code. The best quality-assurance programs and agile development practices can't catch every bug.

So many companies, including Microsoft and Apple, have internal security-research teams that investigate their own software. But few have teams that focus on the software made by other companies. That is what makes Google so unusual. To Ormandy and the dozen or so ace computer crackers that make up Google's Project Zero, there are no boundaries to their jurisdiction—anything that touches the Internet is fair game. Policing cyberspace isn't just good for humanity. It's good for business too.

GOOGLE OFFICIALLY formed Project Zero in 2014, but the group's origins stretch back another five years. It often takes an emergency to drive most companies to take security seriously. For Google, that moment was Operation Aurora.

In 2009, a cyberespionage group associated with the Chinese government hacked Google and a number of other tech titans, breaching their servers, stealing their intellectual property, and attempting to spy on their users. The pillaging outraged Google's top executives—enough so that the company eventually exited China, the world's biggest market, over the affair.

The event particularly bothered Google cofounder Sergey Brin. Computer-forensics firms and investigators determined that the company had been hacked not through any fault of Google's own software, but via an unpatched flaw in Microsoft Internet Explorer 6. Why, he wondered, should Google's security depend on other companies' products?

In the months that followed, Google began to get more aggressive in demanding that rivals fix flaws in their software's code. The battles between Google and its peers soon became the stuff of legend. At the center of several of these spats was none other than bug hunter Tavis Ormandy, known for his smashmouth approach to getting flaws fixed. (Ormandy declined to be interviewed for this story.)

For example, not long after Operation Aurora became public, Ormandy disclosed a flaw he found months earlier in Microsoft's Windows operating system that could allow attackers to commandeer people's PCs. After waiting seven months for the company to issue a patch, he took matters into his own hands. In January 2010, Ormandy posted details of the flaw on a "full disclosure" mailing list where security researchers notify peers of new vulnerabilities and attack methods. His thinking: If Microsoft wasn't going to address the problem in a timely manner, people should at least know about the issue so they can develop their own solutions. A few months later, he did the same for a bug affecting Oracle's Java software as well as for another big Windows flaw, the latter just five days after reporting it to Microsoft.

Critics of the practice censured Ormandy's behavior, claiming it damaged people's security. (Apple, Microsoft, and Oracle would not comment for this story.) In a corporate blog post, two Verizon security specialists called researchers who choose the full disclosure route "narcissistic vulnerability pimps." Ormandy ignored the flak. In 2013 he again chose to make a Windows bug public before Microsoft developed a fix for it. Without the threat of a researcher going public, he reasoned, companies have little pressure to fix a flaw in a timely manner. They can sit on bugs indefinitely, putting everyone at risk.

FROM ZERO TO HERO

TAVIS ORMANDY
Researcher, Google

○ **A member of Google's Project Zero team of hackers who scour the Internet for broken software.**

JOHN GRAHAM-CUMMING
CTO, Cloudflare

○ **An exec at a San Francisco company that runs a network that underpins a sizable chunk of the Internet.**

○ GRAHAM-CUMMING: COURTESY OF CLOUDFLARE; ORMANDY: COURTESY OF BLACK HAT

Google quietly began to formalize what became Project Zero in 2014. (The name alludes to "zero-day" vulnerabilities, the term security pros used to describe previously unknown security holes, ones that companies have had no time, or zero days, to prepare for.) The company established a set of protocols and allowed Chris Evans (no relation to Captain America), former head of Google Chrome security, to take the helm. Evans in turn began recruiting Googlers and others to the team.

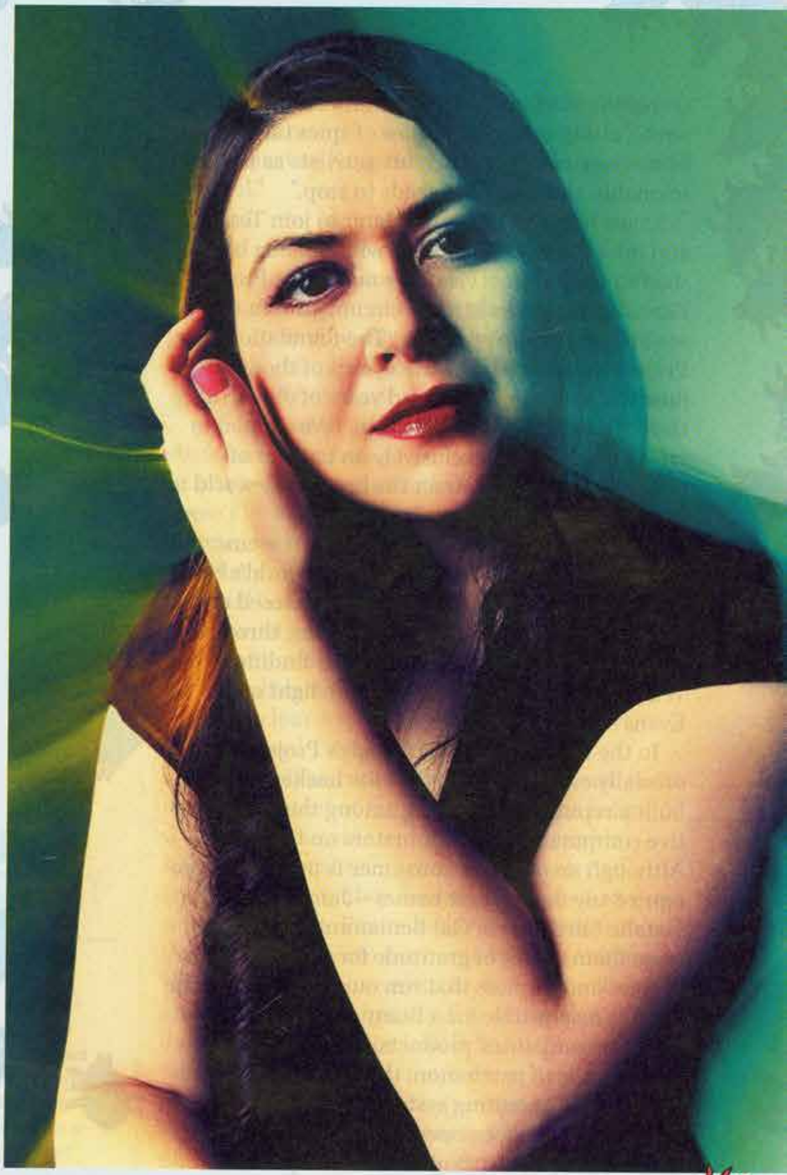
He signed on Ian Beer, a British-born security researcher based in Switzerland, who had demonstrated a penchant for sussing out Apple's coding errors. He brought on Ormandy, a British bruiser known for his highly publicized skirmishes with Microsoft. Evans enlisted Ben Hawkes, a New Zealander known for stomping out Adobe Flash and Microsoft Office bugs. And he invited George Hotz, a precocious teenager who had earned $150,000 after busting open the Google Chrome browser in a hacking competition earlier that year, to be an intern. (Current members of Project Zero declined multiple requests to be interviewed about their work for this story.)

The first sign that Project Zero had arrived came in April 2014 when Apple credited a Google researcher in a brief note for discovering a flaw that would allow a hacker to take control of software running Apple's Safari web browser. The note thanked "Ian Beer of Google Project Zero."

On Twitter, the information-security community openly wondered about the secretive group. "What is Google Project Zero?" asked Dan Guido, cofounder and CEO of the New York–based cybersecurity consultancy Trail of Bits, in a tweet posted April 24, 2014. "Employee of mysterious 'Google Project Zero' thanked in Apple security update changelog," noted Chris Soghoian, then the chief technologist at the American Civil Liberties Union.

More credits soon appeared. In May, Apple credited the discovery of several bugs in its OS X operating system to Beer. A month later, Microsoft patched a bug that made it possible to defeat its malware protection, noting the help of "Tavis Ormandy of Google Project Zero" in an advisory.

By then, the team had generated considerable buzz among those who track security issues. Evans finally made its presence officially known in a blog post on the company's website. "You should be able to use the web without fear that a criminal or state-sponsored actor is exploiting software bugs to infect your computer, steal



JOE PUGLIESE—AUGUST

BUG BARONESS AND LUTA SECURITY CEO KATIE MOUSSOURIS EXPLAINS THE ECONOMY OF EXPLOITS

THERE ARE TWO MARKETS FOR BUGS: offense and defense. The former is made of nation-states, organized crime groups, and other attackers. The latter consists of bug-bounty programs and companies that sell security products. The offense market pays higher prices and doesn't have a ceiling. They're not just buying a vulnerability or an exploit; they're buying the ability to use it without being detected. They're buying silence. The defense market can't pay as much. It's not like vendors are going to compensate their top developers a million dollars. Even though major companies' code quality is improving, complexity continues to increase. That means more bugs. What security researchers do with a particular bug may depend on their financial needs, their dispositions about a piece of software or vendor, and their own personal risk. It's not black-hat sellers vs. white hat. *—As told to Robert Hackett* secrets or monitor your communications," he wrote, citing recent examples of spies targeting businesses and human-rights activists as unconscionable abuses. "This needs to stop."

Evans left the team a year later to join Tesla and now serves as an adviser with the bug bounty startup HackerOne. (Hawkes now leads Project Zero.) Today Evans is more circumspect in describing the group's origins. "The foundations for Project Zero were laid across years of thoughtful lunchtime conversations and years of observing the evolution of attacks," he says. "We wanted to create jobs focused exclusively on top-tier offensive research, to attract the best in the world to the public research space."

It's a more difficult challenge than it seems. Private money soaks up many of the world's best hackers, luring them to work behind closed doors, where governments and other entities, through brokers, will pay top dollar for their findings. When that research doesn't see the light of day, Evans says, people suffer.

In the three years since Google's Project Zero officially came together, the elite hacker squad has built a reputation for being among the most effective computer bug exterminators on the planet. Although an ordinary consumer is unlikely to recognize any one of their names—James Forshaw, Natalie Silvanovich, Gal Beniamini—the world owes them a debt of gratitude for sealing up the devices and services that run our digital lives. The team is responsible for a litany of improvements in other companies' products, including finding and helping to patch more than a thousand security holes in operating systems, antivirus software, password managers, open-source code libraries, and other software. Project Zero has published more than 70 blog posts about its work to date, some of the best public security research available on the web today.

The team's work indirectly benefits Google's primary business: online advertising. Protecting Internet users from threats means protecting the company's ability to serve those users ads. Project Zero's effort to hold vendors' feet to the fire also forces them to fix bugs that cause Google products to crash.

"This is a dorky name for it, but it's like a sheepdog," says Dino Dai Zovi, a cybersecurity entrepreneur, noted Apple hacker, and former head of mobile security at Square. "A sheepdog is not a wolf. It's kind of benevolent, but it still chases the sheep into line to get them back into the pen."

THE WORLD OWES PROJECT ZERO A DEBT OF GRATITUDE FOR SEALING UP THE DEVICES AND SERVICES THAT RUN OUR DIGITAL LIVES.

IN APRIL three members of Project Zero traveled to Miami to attend the Infiltrate security conference, a gathering focused entirely on the offensive side of hacking.

In a city built on suntans and sports cars, the computing cohort look somewhat out of place. Hawkes, Ormandy, and Thomas Dullien, a German security researcher and member of the Project Zero team who is better known by the hacker moniker "Halvar Flake," gather on the lawn of the swanky Fontainebleau hotel to sip mojitos under the rustling palm trees. Seated at a table with a handful of other conference attendees, the Googlers chat about current affairs, favorite sci-fi tales, and how shameful it is that more is not done to preserve hacker history.

At one point Ormandy swipes a pair of gaudy Versace sunglasses left on a table by Morgan Marquis-Boire, a former Google employee, well-known malware researcher, and current head of security at eBay founder Pierre Omidyar's media venture First Look Media. The Florida sun has subsided, but Ormandy places the shades over his blue eyes and mugs. He looks ridiculous.

Infiltrate organizer Dave Aitel, an ex-NSA hacker who runs Immunity, an offensive hacking shop, whips out his phone to take a photo. His subject contorts his hands into a heavy metal fan's "sign of the horns." Behold Tavis Ormandy: online, a quarrelsome critic who suffers no fools; offline, a genial geek who happily horses around.

"People give you a lot of shit, Tavis," Aitel says, referring to the frustrating battles Ormandy must endure while prodding vendors to fix their code. "You know, you don't have to deal with that." With an impish grin, Aitel proceeds with a facetious attempt to persuade Ormandy to join the "dark side" of hacking—researchers who find bugs and then sell them for a profit rather than report them to the affected companies, rendering the bugs kaput.

Ormandy shrugs off Aitel's offer, laughs, then sets the glasses back on the table. He may be a troublemaker, but his aims are pure. (Ormandy allowed this reporter to hang around, but later declined to comment.)

Despite its hard-edged reputation, Project Zero has had to become more flexible as its high-minded ideals collide with the complexities of the real world. The team initially kept to a strict 90-day disclosure deadline, or just seven days for "actively exploited" bugs, but several instances of disclosure shortly before companies had scheduled to release updates, such as Microsoft and its recurring "Patch Tuesday," caused the group a lot of backlash. (It has since added a 14-day extension after the 90 days in the event that a vendor has a patch prepared.)

Project Zero has some of the most explicit disclosure policies in the technology industry, says Katie Moussouris, who helped create the disclosure policy at Microsoft and now runs her own bug-bounty consulting firm called Luta Security. That's a good thing, she says. Many companies fail to establish guidelines on how to report bugs or lack policies on how or when a researcher should expect a bug to go public. Some organizations provide companies with even less time to fix their software. Cert CC, a group run out of Carnegie Mellon University, has a stated 45-day policy—half that of Project Zero, though the group allows for more leeway on individual bases.

And Project Zero is as quick to praise a company's actions to fix a bug as it is to criticize a sluggish response. Earlier this year, Ormandy tweeted that he and colleague Natalie Silvanovich had "discovered the worst windows remote code exec in recent memory," meaning a way to take over a Windows-based system from afar. "This is crazy bad," he wrote. The two worked with Microsoft to patch the bug. "Still blown away at how quickly @msftsecurity responded to protect users, can't give enough kudos. Amazing," he wrote in a follow-up tweet. Apparently, it's never too late to improve.

Technology companies may cringe at Project Zero's audacity, but they should take comfort in the fact that its hackers are willing to resist the urges that drive some researchers to put their findings up for sale. In the years since hacking became professionalized, markets have sprouted for the bugs that Project Zero discloses. Governments, intelligence services, criminals—everyone wants them for themselves and is willing to pay top dollar. The growing adoption of bug bounty programs at software companies is a slight tip of the scale in the other direction, offering compensation to researchers for their time, effort, and expertise. But the payment on the bounty side will never meet the compensation one can get from murkier markets.

"Whatever Google's bug bounty rewards are, the Chinese government will pay more for it," says Bruce Schneier, a well-known security guru and executive at IBM.

Back at the Fontainebleau, Dullien tells me he is amazed at how in-demand the skills of hackers have become. What was once a hobby done in dark basements is now a profession at home in the halls of government.

"This was all a '90s subculture, like hip-hop or break dancing or skateboarding or graffiti," he says. "It just so happened that the military found it useful."

ACCORDING TO MATTHEW PRINCE, CEO and cofounder of Cloudflare, the leak uncovered by Google's top bug hunters initially cost his company about a month of growth. (The setback was temporary, he says: Cloudflare's transparency during the process helped it attract new business.)

If he's at all sour about the experience, Prince doesn't let it show. He knows what it's like to be targeted by truly malicious hackers. A few years ago a hacker group called "UGNazi" broke into Prince's personal Gmail account, used it to gain control over his corporate email account, then hijacked Cloudflare's infrastructure. The hooligans could have done significant damage. Instead, they decided to redirect 4chan.org, a common hacker hangout, to their personal Twitter profile for publicity.

Prince still regrets not informing his customers of the full extent of the Cloudbleed issue before Google and Cloudflare published their initial findings. He wishes his company had alerted customers before they read about the leak in news reports. Even so, Prince believes in retrospect that the Project Zero team was right on the timing of when to go live with the disclosure. To his knowledge, no one has uncovered any significant damages related to the leak in the time since. No passwords, credit card numbers, or health records have turned up, despite their initial fears.

Prince says Cloudflare has put new controls in place to prevent such an incident from happening again. The company began a review of all of its code and hired outside testers to do the same. It also instituted a more sophisticated system that identifies common software crashes, which tend to indicate the presence of bugs.

"I have many more gray hairs and will likely live a year less than before as a result of those 14 days," Prince says about the discovery and the aftermath of the leak. "Thank God it was Tavis and that team who found it and not some crazy hacker."

Of course, Prince will never be able to rule out the possibility that another person or organization has copies of the leaked data. And that's just Project Zero's point. For every one of its team members, there are countless other researchers working in private with less noble goals in mind. It's the devil you know—or the devil you don't. ■

SECURITY: A GLOSSARY

BUG

○ **An unexpected error in computer code. The ones with security implications are called "vulnerabilities."**

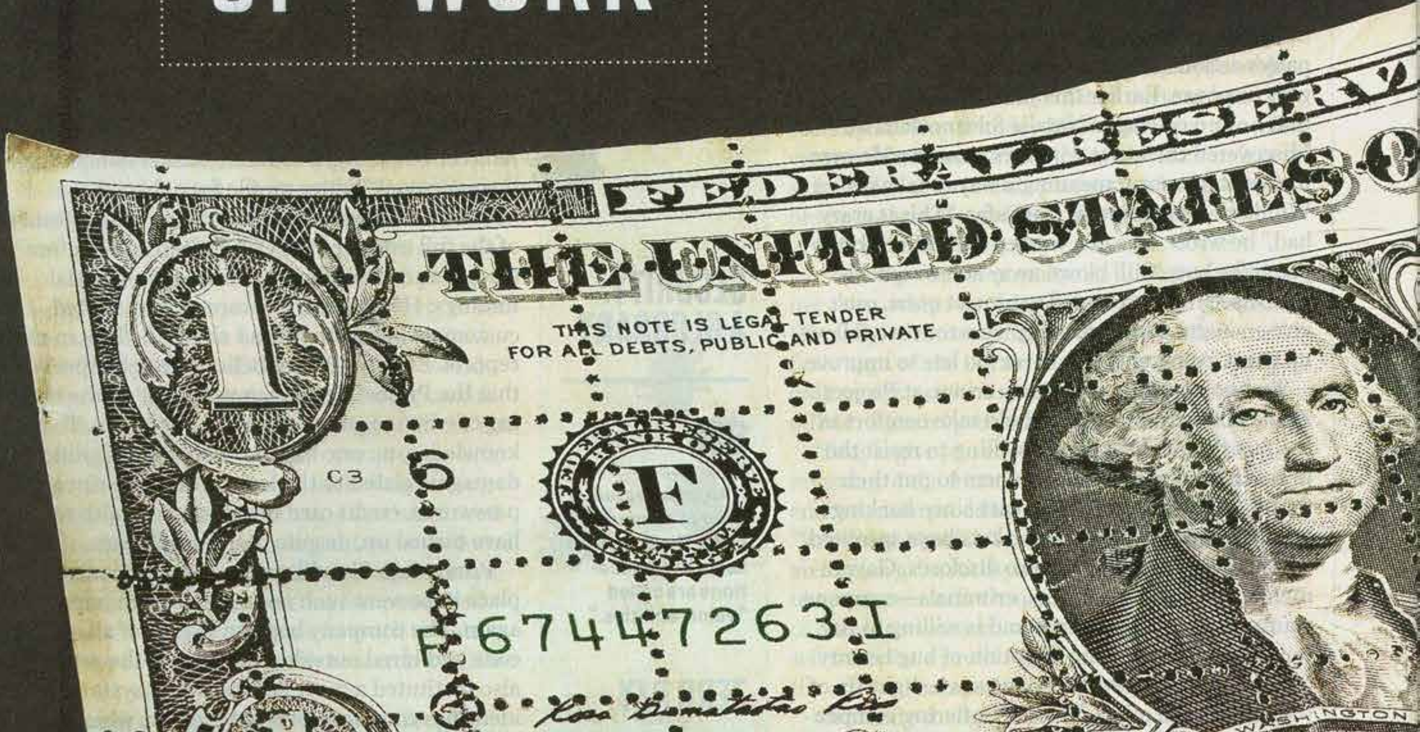
ZERO DAY

○ **A vulnerability that people and companies have had no time—"zero days"—to fix.**

EXPLOIT

○ **A computer program that a hacker crafts to take advantage of a known vulnerability.**

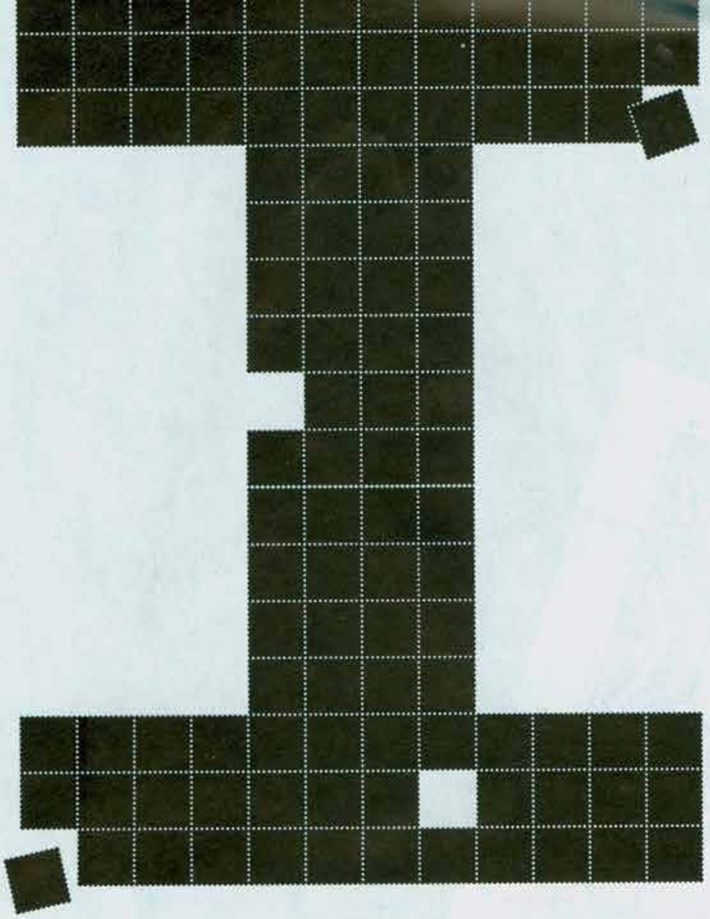
WHY *FREE MONEY COULD BE THE FUTURE OF WORK


FEDERAL RESERVE
THE UNITED STATES OF
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
C3
6
F
F 67447263 I
Treasurer of the United States.
WASHINGTON
ONE DO

BY
CLAY DILLOW
AND
BROOKS RAINWATER

SOME OF THE TOP LEADERS IN TECH BELIEVE THAT ARTIFICIAL INTELLIGENCE AND AUTOMATION WILL LEAVE TENS OF MILLIONS OF AMERICANS PERMANENTLY UNDEREMPLOYED. THEIR SOLUTION: A "UNIVERSAL BASIC INCOME" THAT COULD REDEFINE WHAT IT MEANS TO EARN A LIVING.

▲ PHOTOGRAPHS BY **SAM KAPLAN**



IMAGINE FOR A MOMENT having $1,500 extra in your bank account at the end of the month—$1,500 more than you've actually earned. It's not a bank error; the money is yours, no strings attached. You can travel, pay down bills, or offer it to a relative who needs a little help. You can leave it right where it is for some later day.

Now imagine that the $1,500 arrived every month. Would you put it toward a new car? Take a nicer-than-usual vacation? Would you go back to school, or start a business? Would you work fewer hours? Spend more time with family? Would you cease working altogether?

Sam Altman doesn't know what you would do, but he'd like to find out. The 31-year-old CEO of Silicon Valley startup accelerator Y Combinator believes that if economic trends continue on their current trajectory, that hypothetical deposit in your account may prove a critical part of your future. And he's currently paying about 50 households in Oakland up to $1,500 a month to see what that future might look like.

To understand why, complete the thought experiment above, with some darker shadings: Imagine that a robot has stolen your job and pushed you into a lower-wage occupation, if not out of the workforce altogether. Imagine that companies, choosing between keeping costly human workers or replacing them with less expensive software and machines, have made the most profitable decision. Imagine that you feel a little desperate.

For a growing number of business leaders and economists, this future no longer seems hypothetical. A University of Oxford study from 2013 estimated that 47% of U.S. jobs may be at risk within the next two decades because of advances in artificial intelligence and automation. Last year, the White House Council of Economic Advisers estimated that workers making below $20 an hour would have an 83% chance of losing their jobs to robots in that span. Those odds dropped as workers' education and income levels grew. But as software gets smarter, that too is subject to change: Companies will eliminate even jobs that were long considered immune from technological displacement.

That's where Altman's $1,500 comes in. One potential means of blunting the impact of automation involves providing each person—working or not—with a minimum payment, for life, regardless of income or other mitigating factors. Universal basic income (UBI) would insulate displaced workers from poverty and quell the potential for unrest during a profound and painful economic transition. Theoretically, it might spur innovation and encourage people to take entrepreneurial risks. It would almost certainly alter the definition of "work" by attaching compensation to whatever people choose to do with their time, including absolutely nothing.

Floated by economists and political theorists for decades, the notion of basic income is enjoying new prominence today. That's particularly true in Silicon Valley, where several of the entrepreneurs developing the very technologies that fuel fears of a dystopian future—and often profiting handsomely from them—have endorsed UBI as a potential fix. Governments in developed and emerging nations alike have warmed to the concept, launching a bushel of pilot projects. And the inherently "lefty" idea has drawn growing support from libertarians and conservatives, particularly those who view traditional welfare mechanisms as bloated, wasteful, and inefficient.

Of course, the widening support by no means makes UBI politically palatable. Critics have a buffet of objections to choose from—it undermines productivity, it rewards laziness, it's socialism by another name. There's no doubt that it would be unprecedentedly, astronomically expensive. The concept also violates a core tenet of capitalism, by assuming that this technological revolution, unlike others before it, won't create better jobs tomorrow to replace the ones it erases today.

Altman, the precocious investor and new-company coach whose firm helped launch stars like Airbnb, Zenefits, and Dropbox, is using real-world experimentation to learn whether UBI can stand up to such critiques. Y Combinator's research arm has launched a pilot program in which up to 100 recipient households will get $12,000 to $18,000 this year, in exchange for ... nothing. They're asked to submit to occasional surveys, but there's no

penalty for failing to do so. The idea is to give people money without preconditions and observe what they choose to do. If the pilot is successful, Y Combinator will launch a much larger study, likely a five-year experiment involving thousands of households in multiple states. Within a few years, Altman hopes his team will have something that has thus far proved elusive: proof of whether UBI can have a long-term positive impact.

"It's not for me to tell policymakers what to do, and I don't know what the best policy is," Altman says. But in a time of unprecedented disruption, it's time to find out; after all, he adds, "People can smell automation on the horizon."

YOU KNOW AN IDEA has gone mainstream when one of the world's best-known CEOs invokes it in an Ivy League commencement speech. In May, speaking to Harvard's graduating class, Facebook founder Mark Zuckerberg made a case for UBI as a means to mitigate automation's downsides and as a catalyst for entrepreneurship. "We should have a society that measures progress not just by economic metrics like GDP, but by how many of us have a role we find meaningful," Zuckerberg said. "We should explore ideas like universal basic income, to make sure that everyone has a cushion to try new ideas."

▽ THE FUTURE OF WORK

WITH UBI, "EVERYONE HAS A CUSHION TO TRY NEW IDEAS," ZUCKERBERG SAID IN HIS HARVARD COMMENCEMENT SPEECH.

That idea is gaining currency among tech leaders. In November, Tesla and SpaceX CEO Elon Musk told CNBC "there's a pretty good chance we end up with a universal basic income ... due to automation." Facebook cofounder Chris Hughes helped launch the Economic Security Project last year to fund UBI research. And in February, eBay founder Pierre Omidyar donated nearly half a million dollars through his philanthropic organization to support a basic-income experiment in Kenya. The tech elite's burgeoning concern could be described as part moral obligation, part enlightened self-interest. Many of them share the view that technologies that have generated huge amounts of concentrated wealth will soon be responsible for devastating labor market upheavals. The fact that a middle class gutted by unemployment doesn't bode well for gadget sales likely isn't lost on them either.

That said, the concept of UBI is hardly new. Sometimes called a "guaranteed minimum income" or simply "basic income," the notion has cycled through the political consciousness for centuries, rising during times of technological and economic revolution. The idea was floated by Sir Thomas More (in his 1516 *Utopia*) and Founding Father Thomas Paine (in his 1797 pamphlet

Agrarian Justice). In the 20th century, the concept got a boost from the political right: Conservative economists Milton Friedman and Friedrich Hayek endorsed it as a more efficient alternative to sprawling social service bureaucracies. In the 1960s, even as liberal thinkers like Martin Luther King Jr. championed a minimum income for moral reasons, conservatives like Richard Nixon considered it on practical grounds. Led by director of the Office of Economic Opportunity Donald Rumsfeld (and his special assistant, Dick Cheney), the Nixon administration even conducted basic income experiments in several U.S. states.

What's different about the current moment is this: In technological revolutions past, rapid and irreversible changes caused massive dislocation, but over time those revolutions created new and often better kinds of work. The automation revolution, however, could break that pattern, says Martin Ford, software entrepreneur and author of *Rise of the Robots.* Workers won't be able to shift to new kinds of predictable, routine work, because it's exactly that kind of work that's being automated, not just in agriculture or manufacturing or service industries but across all of them simultaneously. "This time around, maybe we can't educate our way out of this," Ford says.

Indeed, many commentators agree that the education system and policy environment are not keeping up with the disruption at hand, increasing the odds of dark days ahead. "As technology takes away more and more good-paying jobs, we are going to have more and more people that are working but are very poor," says Robert Reich, who served as labor secretary to President Clinton.

Many who fear this scenario believe it's already playing out. They see it manifested in the widening income gap in the U.S., and in the economic mood of the middle class, which is anxious even though unemployment is historically low—an anxiety that became unignorable during last year's elections. Between 1979 and 2013, the income of America's top 1% grew 192%, while income for the bottom 20% expanded only 46%. The effects have been felt acutely in coastal cities, where the creation of vast wealth has driven costs of living to levels that strain all but the top earners.

"POLITICIANS LIE AND SAY THEY'RE GOING TO STOP JOBS FROM GOING AWAY," SAYS ALTMAN. "THAT'S NOT GOING TO HAPPEN."

If the core problem in a robotics-led world is the average worker's lack of income, the thinking goes, then UBI could—theoretically—mitigate it by providing a financial floor below which people cannot fall. It's the rare kind of societal problem for which the solution may be to simply throw money at it.

Of course, how much to throw, and to whom, is a point of enormous contention. In the U.S., a number oft-cited by critics is $3.2 trillion—the cost of giving $10,000 a year to each and every citizen. (That's about 19% of GDP; for perspective, the federal government will spend about $4 trillion in fiscal 2017 on all of its programs and obligations combined.) Advocates of UBI counter that much of that money could be recovered by rolling up existing social programs like welfare and Social Security, by excluding children, and so on. Even so, new costs could be measured in trillions for any program that could earn the label "universal."

Altman believes robots are likely to solve the cost problem, even as they eliminate jobs, by creating unprecedented productivity and wealth—perhaps even doubling GDP. "If we need it, we'll be able to afford it," he says of UBI. But cost isn't where he's focusing now: The Y Combinator team is far more concerned with collecting conclusive data about whether UBI can create the stability to allow people to find meaning in new kinds of work—the kind of data that could persuade policymakers to make a trillion-dollar bet.

THEY'RE NOT the only ones looking. Experiments are in the works in at least a dozen countries, including Spain, the Netherlands, Kenya, Uganda, and India. The city of Glasgow in Scotland has undertaken a feasibility study for the first UBI pilot in the U.K. In January, the Finnish social services agency Kela launched a program that selected 2,000 citizens who were already receiving unemployment benefits and offered them an extra 560 euros monthly. This summer the Canadian province of Ontario will begin a basic income trial involving up to 4,000 families.

MORE: FINE ART IMAGES/HERITAGE IMAGES/GETTY IMAGES; PAINE: HULTON ARCHIVE/GETTY IMAGES; FRIEDMAN: AP; KING: AGIP/RDA/GETTY IMAGES; NIXON: KATHERINE YOUNG—GETTY IMAGES; TRUDEAU: REG INNELL—TORONTO STAR/GETTY IMAGES

AN IDEA WITH A PEDIGREE

The concept of universal basic income has resurfaced repeatedly over the centuries at times of economic transformation, winning allies across the ideological spectrum.

THOMAS MORE

In his *Utopia* [1516], More advocated using basic income to share wealth created as public lands passed to private ownership.

THOMAS PAINE

In 1797 the Founding Father called for a "citizen's dividend"—a payment made to all U.S. citizens, paid for by a tax on landowners.

MILTON FRIEDMAN

The conservative economist endorsed basic income in 1962, arguing that it would be more efficient than the welfare bureaucracy.

DR. MARTIN LUTHER KING

In his final book, *Where Do We Go From Here?* [1967], the civil-rights leader called for a basic income "pegged to the median of society."

And Switzerland last year voted on the idea of a national basic income in a referendum. (It lost.)

This is all vindication for economists like Guy Standing. In 1986 the U.K. native cofounded the Basic Income Earth Network with what he describes as "a very young, radical group of philosophers and economists." It turns out they were a few decades early. "We were regarded as mad, bad, and dangerous to know," says Standing, a professorial research associate at SOAS University of London and author of *Basic Income: And How We Can Make It Happen*. "But in the last five years we've gained a huge increase in respectability."

That respectability has been boosted by pilot projects in communities where baseline living standards are low—and where basic income's impact looks correspondingly impressive. A 2011 pilot administered in part by UNICEF selected about 1,100 households, more than 6,000 adults and children altogether, spread across eight villages in rural India. Each received the equivalent of 20% to 30% of an average household's income—not a full ride, but a notable bump in spending power. Researchers, including Standing, surveyed recipients throughout the two-year experiment, comparing the results with a dozen similar villages that served as a control group.

The study found that people who used the money to curtail their working hours were rare. Most saved it for major improvements to their lives or livelihoods, things like building materials for a new house or new tools with which to ply a trade. Some pooled their grants with family or neighbors and launched new businesses. Across the board, money spent on education in the recipient villages rose, alongside school performance. "The only group for which it resulted in a reduction in labor was among children, because they were spending more time in school," Standing explains.

A similar pilot—the one funded in large part by Omidyar of eBay—began in October in Kenya. It will give 6,000 people across 40 villages 2,280 shillings per month—about $22—for a full 12 years (another 11,500 people across an additional 80 villages will participate in a shorter trial). The Kenya

RICHARD NIXON

His administration ran UBI experiments from 1968 to 1971, finding, among other things, that it had no negative effect on work ethic.

PIERRE TRUDEAU

The Canadian leader's mid-1970s' "Mincome" project remains among the largest UBI programs ever pursued in an advanced economy.

READY FOR THE ROBOTS?

***FORTUNE*'S ANDREW NUSCA ASKED SIX HUMANS—THREE EXECUTIVES, A RESEARCHER, AN ECONOMIST, AND A FUTURIST—HOW AUTOMATION WILL IMPACT SOCIETY.**

"This is a sophisticated problem, and it demands a call to intellectual arms to not assume that it's a binary situation. It's not just that jobs will be lost and that robots are taking over. It's much more sophisticated than that."

—Amy Webb, founder, Future Today Institute

"How do we create a mentality of agility and continuous learning? That's the challenge I see with a lot of this. It's very easy when you're 22 to make a career change. It's much harder in the middle of your career. The cost of transitioning is very high." —Bret Taylor, CEO, Quip, a Salesforce-owned company

"We need to keep relationship skills. I went to an automated, self-serve restaurant the other day, and I felt so empty when I left. Contrast that with my coffee shop. We are hard-wired for relationships—you want the smile, the connection." —Leighanne Levensaler, SVP of corporate strategy, Workday

© WEBB: MELISSA GOLDEN—REDUX; TAYLOR: COURTESY OF QUIP; LEVENSALER: COURTESY OF WORKDAY

"Most of us don't have the reflective time that allows us to be innovative and creative. So we've actually destroyed our capacity to go beyond computers. But computers are always going to be more efficient than us. For us to be better than technology, we have to find our inner human."
—Lynda Gratton, professor, London Business School

"There's a huge need to increase productivity around the world, the U.S. included, simply because of aging. Half of our economic growth has come from more people working: women in the workforce, growing population. That source is about to disappear. So we badly need to increase the economic output. One way to do that is to have the robots, the A.I., do the work. It has the potential to increase our productivity. And not only do we need robots working, but people too. So we need to make sure there's enough work for them to do."
—Michael Chui, partner, McKinsey Global Institute

"There's this assumption that it's going to be people or robots, all or nothing. My experience is that it doesn't operate that way. It's automating part of the job, but not the full job. Repetitive, manual work—no one who's doing it is really enjoying it. Technology replaces and creates. It replaces manual work and creates new opportunities—new tasks, if you will. And productivity creates growth, which creates new kinds of work. It is a virtuous cycle. It's so easy to talk about it in binary terms. I just don't think that's the reality." **—John Donahoe,** CEO, ServiceNow

effort aims to be the largest, most extensive basic income trial to date. While it's too new to have produced conclusions, there's already evidence that recipients, formerly impoverished, have used the cash to buy motorbikes, livestock, fishing nets, and other vehicles of economic empowerment.

There's far less UBI data available from European and North American nations with complex social welfare systems. Those systems themselves offer little insight into how UBI might impact their economies. That's largely because they're hedged with restrictions, requirements, and "incentive traps" that can penalize recipients financially if they earn more money through work—the way Americans, for example, can be disqualified from food stamp programs if their income crosses a minimum threshold. (This is what makes the "no strings attached" aspect of UBI so important to advocates.)

There's a notable exception to this data drought—though it's a program that has been defunct for about 40 years. In the 1970s, reformist Canadian Prime Minister Pierre Trudeau (father of current premier Justin) experimented with a project called Mincome, short for "minimum income." As proof of concept, Mincome provided a guaranteed income to over 1,000 lower-net-worth families scattered across the province of Manitoba. And one town, Dauphin (approximate metro population in 1974: 12,400), was chosen as a "full saturation site" where any resident could receive the benefit, regardless of income—a move designed to test what could happen in a context where everyone received the same cash benefit.

The political winds in Ottawa shifted a few years later, and Mincome lost its funding before it could yield definitive conclusions. But Evelyn Forget, an economics professor at the University of Manitoba, recently revisited the Dauphin data, publishing a report that extracted some wider insights. Forget found that in households that collected Mincome, primary earners on average didn't see a significant reduction in hours worked. "Secondary" and "tertiary" earners did work less, but in ways that were potentially beneficial. Working mothers took more time off around childbirth, "essentially using the stipend to buy themselves longer parental leave," she says. Working adolescents were more likely to finish school, Forget says, pointing to a "nice little bubble in high school completion rates" that coincided with the experiment. Hospital, doctor, and mental-health visits all declined.

A healthier, better-educated workforce would presumably be better armed than a control group to handle future economic disruption. Forget's study, alas, doesn't address what became of the Mincome families after the pilot ended. But Guy Standing isn't discouraged by the lack of firmer

GRATTON: LUKAS KROULIK; CHUI: KEVIN MOLONEY; DONAHOE: COURTESY OF SERVICENOW

conclusions. And he's bullish on what existing research shows about the relationship between UBI and work habits, regardless of what kind of economy recipients are immersed in. "Critics say that if you provide a basic income people will ... become lazy and surf on Malibu beach or something," Standing says. "In actual fact we've found very strong positive effects on the amount of work people were doing. It energized people [and] it increased entrepreneurial-type activities."

To be sure, examples of entrepreneurialism in a Ugandan village may not be replicable in a more advanced economy: It takes far more capital to open a fish-and-chips place than it takes to buy a fishing net. Still, many UBI advocates believe that the opportunism they've seen in Kenya or India could translate to developed economies. As Natalie Foster, cochair of the Economic Security Project, puts it, "Really interesting things start to happen when everyone has a bit more cash."

That range of "interesting things" may not include anything we currently recognize as a job. It's a certainty that some individuals would choose not to work, yet it's unclear how much that matters—in a labor market where good-paying jobs are scarce and unemployment is high, it's not necessarily a bad thing if some people opt out of the workforce. And policies like paid parental leave already recognize the value of tasks that fall outside the conventional definition of labor. UBI isn't money for nothing if "work" expands to include caring for an elderly parent, volunteering at a local school, or engaging in civic organizations and political life.

IF SUCH AN EXPANSION is worth paying for, UBI supporters say, it doesn't have to be unaffordable. Current social welfare programs spend vast sums extremely inefficiently—money that could be retasked to UBI. Though funding basic income involves the unpopular act of raising taxes, governments could avoid burdening individual taxpayers by taxing technology itself. Earlier this year Bill Gates suggested doing exactly that by placing a tax on companies' use of robots and directing the proceeds to fund worker retraining and other priorities.

CURSE OF THE WORKING CLASS

▽

Recent research suggests that better paid jobs, which generally correlate with higher education levels, are less likely to face displacement by automation. But there's no guarantee that advantage will last.

HOURLY WAGE	NUMBER OF U.S. JOBS IN WAGE RANGE	LIKELIHOOD OF JOB DISPLACEMENT BY 2036
LESS THAN $20	81 million	83%
$20 TO $40	39 million	31%
MORE THAN $40	10 million	4%

SOURCE: WHITE HOUSE COUNCIL OF ECONOMIC ADVISERS

Other would-be reformers are advocating policies that could amount to UBI by other names. A bill currently in play in California would create a progressive tax on carbon emissions, with revenue to be paid back out in equal installments to all Californians. In February, a paper authored by (among others) James Baker, Henry Paulson, and George Schultz—who variously served as cabinet secretaries for Presidents named Nixon, Reagan, and Bush—laid out a "conservative case for carbon dividends" calling for a similar scheme at the federal level. (Among its stated aims: curbing populism by boosting the incomes of frustrated working-class Americans.) And Democratic Congressman Ro Khanna—who represents much of Silicon Valley—has proposed an expansion of the earned income tax credit that would provide as much as $12,000 per year to working families.

With none of those proposals anywhere near fruition, the Y Combinator team is exploring what $1,500 per month can buy in Oakland. For most, it doesn't buy a free ride. The rising cost of living in the Bay Area has spilled over into what was until recently one of its rare affordable enclaves: Median rents in Oakland have crept toward $3,000 a month, ranking it among the nation's most expensive markets. But the money can still help residents cope with stagnant wage growth. And for Altman and his allies, it buys data-driven insight into human behavior. Will Oaklanders be more likely to become couch potatoes, or self-taught coders? To retrain, or tune out? The answers might help buy legitimacy for UBI—serious consideration of an idea long dismissed as practically unfeasible, politically untenable, or both.

Autonomous vehicles on the streets, automated traders on the floor, and factories where people are a distant memory. The benefits could be enormous, but this future—with artificial intelligence performing the business functions once reserved to us—is where basic income might make sense. "A lot of people, politicians especially, they'll lie and say they're going to stop jobs from going away," Altman says. "That's not going to happen. Technology is going to come. Jobs are going to change. I want to figure out how to make this new world work for everybody." F

Clay Dillow is a business and technology journalist. Brooks Rainwater is the director of the Center for City Solutions at the National League of Cities.

CAN BITCOIN'S FIRST FELON HELP MAKE CRYPTOCURRENCY A TRILLION-DOLLAR MARKET?

Charlie Shrem on the beach in Sarasota, where he lives.

After spending a year in prison, Bitcoin pioneer CHARLIE SHREM has a new job and a new mission: strengthening the ecosystem of blockchain assets—and, just maybe, helping build the future of the Internet.

By Brian Patrick Eha

Photograph By
Jeffery Salter

"My word is gold," says Charlie Shrem, glass of absinthe in hand, light winking off a pinkie ring he wears that is embossed with a Bitcoin symbol. "And I make sure everyone gets paid."

BITCOIN'S FIRST FELON IS IN HIS FAVORITE MODE: full-on bluster. We're in Sarasota, where he lives, perched on stools at Pangea Alchemy Lab, a faux-speakeasy tucked behind a curtain in the back of a sandwich shop. The bartender is a bearded anarchist who, after making our drinks—he drips water from a sort of four-armed decanter onto sugar cubes suspended on slotted spoons above glasses of French absinthe—asks if I've read *Debt: The First 5,000 Years,* by the anthropologist David Graeber. Shrem has been offering plenty for the bartender to eavesdrop on, a discourse that features words like *Bitcoin, blockchain, digital currency.*

Before his fall from grace, Shrem was living the high life as a Bitcoin millionaire. Now, at 27, he once again has something to prove. Ten months after his release from federal custody, he has a new job, and he's looking to mount a comeback.

It's happening just as digital currencies are in the midst of an epic explosion. Bitcoin and its ilk are now worth $107 billion, *six times* their value at the beginning of the year. It's either the beginning of a global financial realignment—or a bubble of historic proportions. These days as much as $6.6 billion in digital tokens changes hands every day, and even mainstream players such as Goldman Sachs, Visa, Capital One, Nasdaq, and the New York Stock Exchange have invested in the underlying technology.

Shrem saw value back when Bitcoins were worth only a few dollars each—they now trade above $2,600—and there was hardly anything to spend them on. In 2011 he cofounded a startup, BitInstant, that became one of the biggest early cryptocurrency companies. At one point, it was processing about a third of all Bitcoin transactions, before flaming out in 2013. "You talk to 10 people," says Shrem, "I guarantee you at least seven of them will say they got their first bitcoin from BitInstant."

Shrem is a natural-born impresario, a promoter's promoter, and he was one of the first public faces of the cryptocurrency phenomenon. In 2013, when *GQ* needed a "spirit guide" to the shadow realm of digital currency, it relied on Charlie Shrem. He was featured in the documentary *The Rise and Rise of Bitcoin.* He was a speaker and proselytizer at industry conferences. And he cofounded the Bitcoin Foundation, the first nonprofit advocacy group for digital currency.

But Shrem crashed as fast as he rose. In March 2015 he went to federal prison after pleading guilty to helping a customer acquire Bitcoins to resell on the underground marketplace Silk Road, where Bitcoin was used to buy drugs.

Today Shrem is a free man again, and his world has dramatically changed. Bitcoin was the only digital currency when he was first in the game. Now it's less important—not because it has imploded, as critics long predicted it would, but because it has given rise to hundreds of new digital assets.

He is embracing the transformation. There won't be one supreme digital currency, he and others agree. A kind of crypto-pluralism is taking hold. In early March, when I first catch up with Shrem, Bitcoin's share of the total market cap of all cryptocurrencies is about 85%. By June 12 it is 41%, an all-time low. To be clear, Bitcoin's price hasn't fallen; in fact, it has soared (see chart at right). But many leading rivals have soared even faster.

Shrem is a connector, not a coder, and he's positioning himself to play a key role in this newly diverse ecosystem. He has already stumbled once in his comeback, with one venture crashing almost instantly, before landing a job at Jaxx, a startup that allows users to hold separate balances of different virtual coins in digital wallets.

Shrem embodied the chaotic, legally questionable early days of cryptocurrency. But he says he's different now. He claims he's no longer operating mainly for himself and instead wants to use his talents to strengthen the crypto-community.

Charlie Shrem is nobody's image of a traditional financier, but that's precisely the point with alternative currencies: Their early leaders were the sorts of people who would never pass muster at, say, Morgan Stanley. That may just make Shrem the perfect messenger, as digital currencies transition from an off-the-grid form of exchange favored by people who reviled any established system into something that is fast becoming an established system of its own.

THE PROMISE OF BITCOIN, when it came into the world in 2009, was to be a universal currency, electronic cash that could be sent around the globe in minutes and that would work as well in New Delhi as it did in New York. Its scarcity is predetermined by the code: New bitcoins are introduced into the system at regular intervals through a process called mining. The word is misleading, since this form of mining consists of solving the complex math problems necessary to confirm transactions on the network. Successfully solving the problems triggers the creation of more digital currency.

Bitcoin's pseudonymous creator, Satoshi Nakamoto, built a decentralized system that no one would own but anyone could participate in. A constantly updated copy of the ledger recording all Bitcoin transactions—the blockchain—would be stored on the computer of anyone running the software. Although the ledger was open to all, Bitcoin transactions were meant to be anonymous.

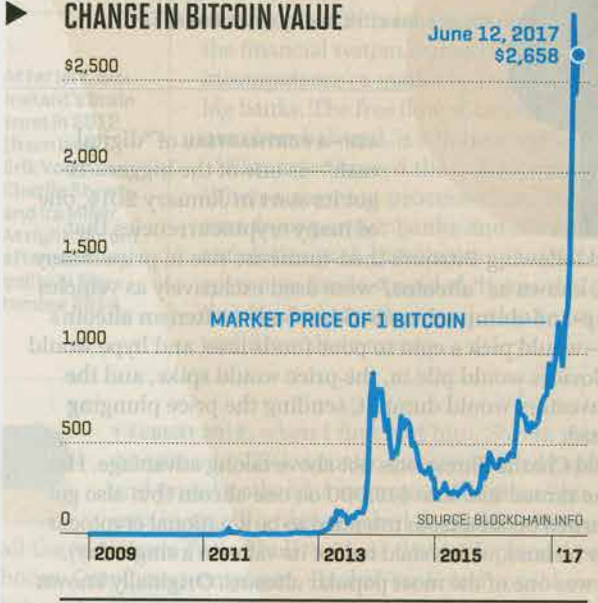
Blockchain technology is groundbreaking because it allows transactions to be processed without recourse to a central authority, such as a payments company, government, or bank. Businesses and services can be decentralized, cutting out costly middlemen and removing single points of failure.

But only eight years after its launch, Bitcoin is showing strain. A civil war has been raging over its future. Due to limitations in its code, the Bitcoin network can process only seven transactions a second—a trifling quantity for any system that aspires to serve the masses. (Visa handles thousands of transactions per second.) As the load has increased, the time it takes to confirm transactions has risen sharply, and users have been at odds over how to solve the problem. The bickering threatens to divide the currency into two competing versions of Bitcoin—or condemn it to obsolescence.

Not only is Bitcoin slower than some of its younger rivals, it's also more limited. Yes, Bitcoin allows the transfer of value. But many of the new systems can be used for much more. Ethereum's creators, for instance, have built a potentially more versatile network by incorporating a scripting language that allows developers to create "smart contracts"—agreements written into the software that can dispense funds and perform other functions automatically in response to preset triggers.

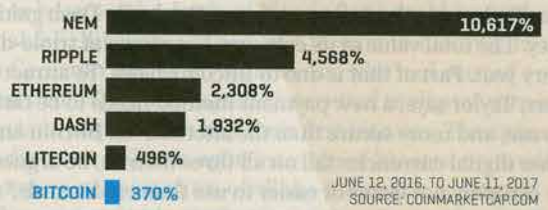
All of which means Bitcoin faces a threat from younger, more nimble rivals. Their names are legion: Litecoin. Zcash. Monero. Dash.

CHANGE IN BITCOIN VALUE



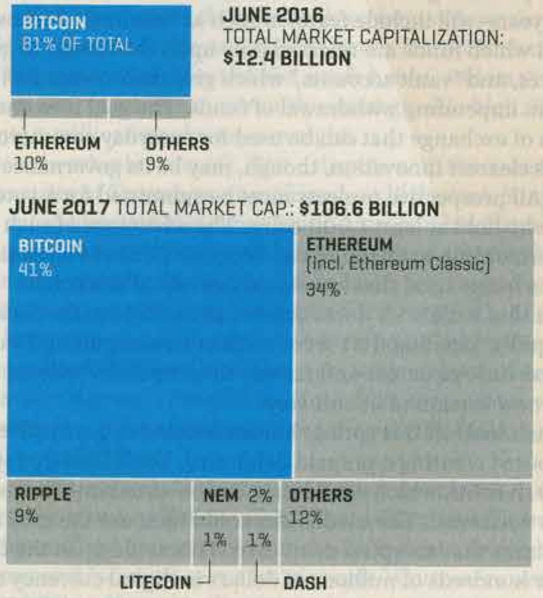
SOURCE: BLOCKCHAIN.INFO

ONE-YEAR CHANGE IN PRICES FOR TOP CRYPTOCURRENCIES



JUNE 12, 2016, TO JUNE 11, 2017
SOURCE: COINMARKETCAP.COM

CRYPTOCURRENCY MARKET SHARE



JUNE 12, 2016, TO JUNE 12, 2017 SOURCE: COINMARKETCAP.COM

DASH—A PORTMANTEAU of "digital cash"—is one of the biggest. It got its start in January 2014, one of many cryptocurrencies that emerged following Bitcoin's then-immense rise in price. Many of these, known as "altcoins," were used exclusively as vehicles for pump-and-dump schemes. Somebody—often an altcoin's creator—would pick a coin to pour funds into, and hype would build. Novices would pile in, the price would spike, and the major investors would dump it, sending the price plunging downward.

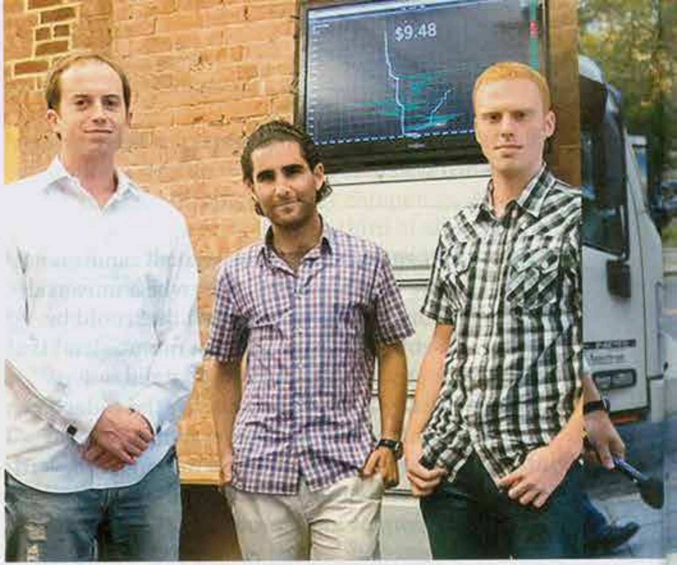
The old Charlie Shrem was not above taking advantage. He claims he turned $50 into $15,000 on one altcoin (but also got badly burned on an altcoin intended to be a national cryptocurrency for Iceland, which shed half of its value in a single day).

Dash was one of the most popular altcoins. Originally known as Darkcoin because it promised untraceable transactions, it saw plenty of pumping and dumping. But its creator continued to refine the software and add new features. In March 2015 it rebranded as Dash, so people wouldn't mistake it for a "single-feature coin," says Ryan Taylor, who leads its core team. Gradually Dash gained legitimacy. The total value of its currency has grown at triple-digit rates every year. Part of that is due to Bitcoin's flaws. To attract customers, Taylor says, a new payment method needs to be faster, easier to use, and more secure than the alternatives. Bitcoin and most other digital currencies fail on all three metrics, he argues. "They're certainly not faster or easier to use than credit cards," says Taylor, a former financial services consultant at McKinsey.

Dash has functions to address those weaknesses. It offers an "instant send" feature that Taylor says is "as fast as using a credit card." To protect against fraud or theft, Dash's next version—due out this year—will include features such as "moderated transactions," in which funds are released only upon the receipt of goods or services, and "vault accounts," which give their owner 24 hours to stop an impending withdrawal of funds. The goal is to create a medium of exchange that can be used for everyday commerce.

Dash's clearest innovation, though, may be its governance system. All prospective projects must be submitted for a vote by people who hold at least 1,000 coins. The advantage of such a system, according to Olaf Carlson-Wee, the CEO of Polychain Capital, a hedge fund that invests exclusively in blockchain assets, is that it allows a decentralized network to make decisions rapidly, avoiding the sort of conflict now engulfing Bitcoin, which has little structure and no way to compel anybody to, say, adopt a new version of its software.

As Dash took off this spring, Shrem decided to get involved. He proposed creating a prepaid debit card. You'd load in, say, three Dash coins, which would then be converted into dollars (or euros or whatever). The cardholder could then use the card at any business that accepts a debit card. This could open the floodgates for hundreds of millions of dollars in digital currency to enter the mainstream economy. "People only want to hold Dash if they can easily convert it to something of use," Taylor agrees.



There are several Dash-funded debit cards available, but Shrem's would be the first that could be used in the U.S. His plan garnered overwhelming support within the Dash universe. "Reputation plays an important role on the network," Taylor says. "When someone like Charlie comes along, people take it seriously."

CHARLIE SHREM GREW UP in Sheepshead Bay, a predominantly Russian and Jewish neighborhood in deep Brooklyn. His parents are Orthodox Jews, and his father worked for a jewelry retailer, while his mother cared for Shrem and his two sisters.

Shy and awkward, Shrem blossomed upon discovering a knack for computers. He taught himself to code and became a presence in online hacker forums. In 2009, while attending Brooklyn College, he cofounded a daily deals site for electronics called Daily Checkout. He found he loved sales.

Shrem has claimed, with characteristic hyperbole, that he was one of the first 10 people in the world to know what Bitcoin was. That is likely exaggerated. By the fall of 2011, however, he was sufficiently established in the Bitcoin community to be credible as the CEO of a startup (albeit one he launched from his parents' basement).

That startup, BitInstant, helped people acquire digital currency and move it between Bitcoin exchanges. Eventually it allowed customers to convert cash into bitcoins at banks such as Wells Fargo and Bank of America, and (via partners including MoneyGram) at 700,000 locations across the U.S., Russia, and Brazil, including Walmart, 7-Eleven, and CVS stores.

Shrem, who was partnering with a 23-year-old Welsh coder named Gareth Nelson, handled the business end. He raised $10,000 from his mom and $120,000 from an angel investor named Roger Ver.

At far left, BitInstant's brain trust in 2012 (from left): Erik Voorhees, Charlie Shrem, and Ira Miller. At right: Shrem after pleading guilty in September 2014.

FROM LEFT: BRIAN PATRICK EHA; CRAIG RUTTLE—AP

But one person who declined to invest warned him that BitInstant had no safeguards to prevent money laundering.

That was fine with Shrem. It was fine, too, with a substantial portion of BitInstant's clientele, users of Silk Road, who needed to exchange dollars for Bitcoins in order to buy drugs on the underground market. There was even a middleman, Robert Faiella, a plumber in Florida who had a sideline obtaining Bitcoins for Silk Road users.

Shrem soon figured out what Faiella was up to. But rather than shut him down, Shrem helped Faiella source money for drug transactions. BitInstant's cash-processing company and Shrem's partner wanted to put a stop to it. But Shrem simply encouraged Faiella to disguise his identity with a new username and email address.

The flow of money went on unimpeded. By the time Shrem finally cut him off, in late 2012, Faiella—who later pleaded guilty to operating an unlicensed money-transmitting business and was sentenced to four years in prison—had laundered nearly a million dollars through BitInstant.

The libertarian defense for Shrem's conduct—which he himself has advanced at times—has two parts: first, that individuals have the right to do what they want with their money and their bodies as long as they aren't harming anyone else; second, that at the time he began helping Faiella, the U.S. government hadn't determined how to classify or regulate Bitcoin. If the government hadn't even decided whether it viewed Bitcoin as money, the argument goes, how could one be laundering it?

The Bitcoin community in those days was united in its sense of righteous mission. Because the digital currency abjured central banks and other authorities, many of its first devotees were libertarians, anarchists, and black marketeers who wanted to do business away from the government's watchful eye. They were gleeful at any sign of Bitcoin's impending triumph over the financial system, enraged by any show of incompetence or malice by the government or big banks. The free flow of capital, community members believed, is a human right.

Shrem embraced the outlaw stance. When a payment processor, under pressure from partner banks and Mastercard, cut all ties with Bitcoin companies, leaving customer funds stranded, it was BitInstant that hacked together a solution to let them withdraw their money.

BY AUGUST 2012, when I first met him, Shrem was a 22-year-old CEO, a cocky, motormouthed capitalist and proud pothead. I interviewed him and his lieutenants in an office they dubbed the Bakery because of all the marijuana-fueled bull sessions that took place there after hours. One former employee, Rachel Yankelevitz, told me, "Charlie's main qualification for coworkers was if they could smoke weed or drink with him and chill together."

Shrem had swaggering ambitions. His company would soon be processing 30% of all Bitcoin transactions, and he wanted BitInstant to become "the Apple of Bitcoin," as he told me at the time.

That fall, BitInstant raised $1.5 million in funding, most of it from Cameron and Tyler Winklevoss, who had started a venture capital firm. They had become interested in digital currency, and BitInstant helped them buy their first bitcoins. The twins—who later disavowed Shrem upon learning of his arrest—would go on to scoop up a reported 1% of all the bitcoins in existence.

After raising funds, BitInstant's future looked bright. Because so much of the crypto-economy depended on fast money transfers in and out of the system, Shrem's company became a barometer of the industry. During the Cypriot financial crisis in early 2013, when it appeared that the bank accounts of regular citizens would be taxed at 6.75% as a condition of a European bailout deal, Bitcoin suddenly looked like a safe haven, and its price shot up from $50 to $266—a previously unimaginable high. Shrem became a millionaire almost overnight.

Then the wheels came off. First a dispute with the investors led to the ouster of Shrem's two best friends at BitInstant. Something went out of him with their departures. He was often distracted. He'd spend the night partying, then sleep in and show up late.

The site, meanwhile, was straining under the surge in users, leading to waves of customer complaints. An upgrade to the platform became mired in technical problems and legal concerns. It became clear BitInstant had been operating without state money transmitter licenses (which, it became clear, some states would require to serve their residents), and the cost of obtaining them would be prohibitive.

It was all too much. BitInstant shut down in July 2013. Alex Waters, the company's chief information officer, says Shrem "squandered" the opportunity to make BitInstant a world-beating company and "screwed over a lot of people." Customers were irate.

Shrem himself appeared at first to have gotten away unscathed. He was living on his own and enjoying his freedom. He and his girlfriend (now fiancée), Courtney Warner, took a vacation to Morocco, where he says he tried opium. He flew to Argentina on a mission for the Bitcoin Foundation. His life was a whirlwind of partying and dealmaking. "I have to take a lot of people out to clubs, buying bottles, buying dinners," he told a reporter in late 2013. His business now was not BitInstant but himself. He began to earn speaking fees—and all the while he kept talking like BitInstant was going to be rebuilt better than ever. "He was very arrogant," Warner says of her fiancé during that time.

In January 2014 it all caught up with him. On his way back from a speech in Amsterdam, he was arrested. He eventually pleaded guilty to aiding and abetting an unlicensed money transmitter, and was sentenced to two years. "I screwed up," he told the judge at his sentencing. Shrem had wanted to raise the issue of whether the law he had broken was just. But his lawyers discouraged it.

Other Bitcoiners had run afoul of the law, but Shrem was the first to serve time. This fact makes him, depending on your view, either a criminal who got his just deserts or a martyr. "A lot of people say that I took the first shot for Bitcoin," Shrem says. "The first person to walk through the door always gets shot, and then everyone else can come through."

SHREM ENTERED PRISON in March 2015. He had put weight on his slight 5-foot-4 frame, medicating himself with vodka in the nervous months before he was incarcerated. Now, in the minimum-security federal prison camp in Lewisburg, Pa., he detoxed and began frequenting the prison library. He found himself pondering the question of value. What made currencies—of any form—worth anything? As luck would have it, the prison economy provided the answer.

The prison had its own currency, one based on protein—mainly packets of mackerel in soybean oil. "Good-quality protein is very hard to come by in prison," Shrem says. "Tuna is good, but tuna doesn't have texture. Mackerel is meaty."

Inmates serving long sentences, he says, would stockpile mackerel, using it as a store of value, like a savings account. But those pouches of mackerel expire in three years. "People started transacting these mackerels that were expired," Shrem explains. "They called them money macks. The money mack had a value of about a dollar, whereas eating macks had a value of about $1.50. And they had exchangers. The money macks had no value—except that everyone said they had value."

Gradually he came to believe, as some monetary theorists do, that the acceptance of certain forms of money—shells, colored beads, pieces of paper—is largely a social convention, dependent upon what technologists would call their network effect.

But it was clear that certain features could make one type of currency more suitable than another. Money macks were an ideal form of money for inmates. "They were scarce," Shrem says. "The only way you could get money mackerels was from edible mackerels that expired. And the inflation rate of edible mackerels was set. You had 500 inmates—every inmate could only buy 14 mackerels every week in the commissary... That's how many mackerels at any time, at maximum, could come into the system. There's no arbitrary printing of mackerels; there's no flooding of the market with this food. It's like Bitcoin. There was no Federal Reserve of mackerel that was printing whenever they wanted."

Bitcoin, he knew, has qualities that make it a powerful currency, store of value, and payments network. But expecting it to do more than that was asking too much, he decided. "That's when it's going to fail," he says. "Trying to do smart contracts, and social media, and a distributed file-storage system, and all these different things on top of the Bitcoin blockchain—it's like trying to have your browser do everything for you." Better to let a thousand crypto-flowers bloom, each one focusing on what it does best.

MANY OF THE HOTTEST blockchain assets today are not digital currencies like Bitcoin or Dash, but so-called tokens, distinguished from true cryptocurrencies by their lack of a blockchain. They run instead on existing blockchains, primarily Ethereum's, and tend to be built for specific applications, such as a peer-to-peer marketplace for computation (Golem), a crowdsourced prediction market (Augur), or a blockchain-based advertising platform (Brave).

Where digital currencies are generally "mined," tokens are usually distributed in crowd sales known as initial coin offerings (ICOs). (After that, they trade on public exchanges.) These crowd sales serve both to raise funds and to give potential investors their first chance to grab a piece of whatever service is being built. Dozens of ICOs have already been launched, raising more than $230 million last year, followed by more than $450 million just in the first half of 2017. (For more on investing in tokens, and their uncertain legal status, see "Investors Seek Sweet Coin," on page 56.)

The tokenization craze constitutes nothing less than "the second business model of the Internet," contends Carlson-Wee, whose hedge fund is backed by Andreessen Horowitz. Imagine if Facebook had issued a token to its users, with its value deriving from the content and connections generated on the social network. Early users might have scooped up large quantities of the token at rock-bottom prices, while those who joined later, as the network's value became widely apparent, might find themselves able to afford only a few. But all of them, by holding this digital asset, would be able to participate in Facebook's growing success.

This, of course, is not the case. The $435 billion value of Facebook is shared only among Mark Zuckerberg and other stockholders. Most other Internet platforms operate on the same principle. Their owners extract massive value from interactions between users.

With blockchain-based systems, by contrast, "there's no longer a division between users and owners," Carlson-Wee says. The tokens are a wealth-sharing mechanism, a way that everyone from hedge funders to consumers can take positions in—and place bets on—the future of the Internet.

SHREM'S REENTRY INTO CIVILIAN LIFE was a two-step process. He was transferred to a halfway house in Harrisburg, Pa., in March 2016. Shrem says living not merely with embezzlers, fraudsters, and drug dealers, as he had in Lewisburg, but also with "murderers, bank robbers, child molesters" was worse than prison. He cried his first night there. During this time, Shrem worked as a dishwasher at a restaurant for $8 an hour. Gainful employment was a condition of residency at the halfway house. Playing around with magical Internet money didn't qualify. "They were very specific," Shrem says.

If being a dishwasher humbled him, it was still more humbling to realize how much the Bitcoin community had changed in his absence. Familiar landmarks were gone. When he tried to visit one of his old haunts, an online exchange where he'd once speculated in altcoins, he found the site no longer existed. Even the lingo had changed.

Shrem set about catching up on what he'd missed. In prison the library had been his sanctuary: He would stay in there for hours. He says he read 137 books while incarcerated. Now he took the same approach with the blockchain industry. Marco Santori, a cryptocurrency attorney at the law firm Cooley, likens Shrem's reeducation to "that scene in *Austin Powers* where he's unfrozen after 40 years or whatever it is, and he just watches 40 years of history straight through to try to get his bearings."

That didn't stop Shrem from stumbling out of the gate. Having seen that token sales were the new frontier, he became the chief technology officer of a startup called Intellisys Capital, which he predicted was going to revolutionize the investment world. The idea was to raise funds for a portfolio of middle-market companies—and, later, blockchain startups—by issuing $25 million worth of tokens in an ICO. "It seemed like a really cool idea," Shrem says.

The problem was that their token would almost certainly be classified as a security under U.S. law. To avoid legal trouble, Intellisys decided to bar American and British citizens from participating in the sale. But the plan had drawbacks: They would have to rely on partners to vet prospective investors for them.

Shrem became the face of the venture. He was back in pitch mode, touting Intellisys to the press and the public. He described the fund's planned first investment, a 20-year-old waste-management company in Michigan, as a "proof of concept."

But as the date of the token sale was pushed back, from mid-January to the end of February, Shrem began to get cold feet. Selling a security could bring all kinds of scrutiny to a man already convicted of a financial crime. "I still get these nightmares I'm in prison sometimes," he tells me in March. He was becoming increasingly nervous.

Fortunately for him, fate intervened. The ICO, held at the end of February, was a bomb. "We had a bunch of technical problems," says Shrem. "We raised a few hundred thousand dollars, and then we refunded everyone's money." Shrem decided to walk away. It was easier to take the hit to his reputation than live in fear.

THAT'S ONE OF THE PARADOXES of cryptocurrency: Each new development seems to bring both great promise and great peril. ICOs are the next big chapter, after crowdfunding, in the democratization and decentralization of finance, says Brock Pierce, a managing partner at a San Francisco venture capital firm, Blockchain Capital, that invests in cryptocurrency startups. His firm recently raised $10 million by issuing its own blockchain token, becoming the first venture capital firm in the world to do so. (The token sold out in six hours.)

But many of the ICOs conducted so far have played fast and loose with regulations, he says, operating in a gray area. "I don't like the way that people are going about doing it," says Pierce. That the SEC hasn't yet cracked down means nothing, he says. "Good entrepreneurs with the best of intentions, who want to innovate and change the world, are going to end up in jail—or with fines."

Shrem agrees. "I try to explain to people that in any other industry it's okay to try new things and break shit, but in fintech, because you're talking about people's money, it's a lot more difficult," he says. "Especially in the Bitcoin and blockchain space. The government is always watching."

For now, though, the ICO market is surging—despite fears of a bubble and scams—and mainstream investors are entering. In May, billionaire venture capitalist Tim Draper, long bullish on Bitcoin, announced that he would take part in an ICO for the first time. The crowd sale, planned for July, is for the token powering Tezos, a smart-contracts platform that Draper says will be "more secure and more democratic" than Ethereum.

Draper says he expects in the future to see tokens for "everything from health care to insurance to commodities." Tokens, he says, are both "a brave new frontier" and a "Wild West."

THE FAILURE OF INTELLISYS cost Shrem. "I expended social capital on it," he says. "And I'll have to get that back." In March he tells me that he wants to make a comeback, but it has to be the right sort of comeback. "I need to show that I didn't just get lucky one time" with BitInstant, he says, "but that I know what I'm doing."

He had moved to Sarasota with his fiancée and was living with her and his future mother-in-law in a rented pink townhouse. He was spending his abundant off-hours relaxing on the beach, eating in nice restaurants, boating, Jet Skiing. He was mellower and more patient than in the past. He decided that if an opportunity came to get in on the ground floor of "something amazing," he would seize it. That turned out to be a full-time job as Jaxx's head of business and community development. The company's values appealed to him: Jaxx users are in control of their own funds. "It goes toward my vision of you being in control of your own money, you being in control of your own freedom," he says.

March was the first profitable month for Jaxx, which lets users (now more than 100,000) exchange one virtual coin for another. Now its founder, Anthony Di Iorio, who cofounded Ethereum, wants to expand to other countries, such as China, and Shrem will be a key part of that process. He is in charge of turning relationships into revenue, working with developers to add their cryptocoins to Jaxx's stable. Dozens of new partnerships are in the works.

But they have to be the right coins. Having helped Bitcoin grow from a stripling to a giant, Shrem is confident he can tell which crypto-projects have real promise—and which don't. He thinks if he can help build Jaxx, he'll "be a major industry player again."

His timing may be good. According to Carlson-Wee, "the real Cambrian explosion of tokenized assets" is still a couple of years away. That's when he expects to see technology that would let Bitcoin, Ethereum, Dash, and other blockchain networks communicate. As it stands, they're isolated from one another. (The concept has spawned another name in the argot: "parachains," a reference to the idea of bringing parallel blockchains together.)

Parachains would allow applications and smart contracts built on one system to interact with another system's assets. An Ethereum smart contract could be triggered by the balance in a Bitcoin wallet address, for instance. This would help overcome the network effect of the oldest cryptocurrency. Just as Bitcoin faces an uphill battle against currencies like the U.S. dollar, so new cryptocurrencies are at a disadvantage to Bitcoin, which has the broadest name recognition and biggest user base.

Forging bonds between blockchains would allow users to flow easily from Bitcoin to Dash to Ethereum to Zcash, strengthening the entire ecosystem and making all of it more valuable. "As long as you're keyed into any cryptocurrency, you'll have access to every cryptocurrency," Carlson-Wee says.

Bitcoin was created to be the money of the Internet. Its successors may build a new kind of Internet, a Web 3.0 of interconnected blockchains running countless applications. Charlie Shrem is determined to be in the middle of it all.

Brian Patrick Eha is the author of How Money Got Free: Bitcoin and the Fight for the Future of Finance.

INVESTORS SEEK SWEET COIN

ICOs are a white-hot way for tech companies to raise cash. But they may have more in common with gambling than investing.

BY JEFF JOHN ROBERTS

WHEN BRAVE, a privacy-focused Internet browser company, decided to raise money this May, it could have gone a traditional route by borrowing money or selling equity to investors. Instead it chose a third way: an initial coin offering, or ICO.

Like an initial public offering, an ICO lets a firm raise capital from multiple sources. But rather than issuing shares of ownership, the offering company sells digital tokens, or "coins," created through blockchain technology. In Brave's ICO, the startup raised $35 million from about 130 investors—in less than a minute.

Boosters believe that strategies like Brave's could be the future of investing, a transformative approach to fundraising that enables consumers to benefit more directly from the popularity of new technologies than they would if they owned a traditional stock. Critics, meanwhile, fret that ICOs occupy a regulatory gray area that could leave investors vulnerable to fraud and land startups in legal trouble. And at this early stage in ICO history, both sides may be right.

ICOs are among the big financial innovations to spring from blockchain technology, which uses revolutionary software and multiple computers to create tamper-proof record systems. Blockchain is central to the business models of most startups that use ICOs; Brave, for example, plans to use blockchain tokens to help its users earn money if they agree not to block online ads. By distributing tokens in an ICO, a startup gives buyers early access to its technology, to use however they see fit. If the service or product catches on—or in some cases, before it even launches, if it generates a lot of buzz—the buyers can sell their tokens on secondary markets. The startup, meanwhile, raises money without ceding any control to private investors or venture capitalists, and without the paperwork burdens of an equity IPO.

Perhaps the most famous ICO so far is that of Ethereum, which raised $18 million in 2014 by selling tokens that facilitate online contracts. Today Ethereum-powered contracts are proliferating, and the tokens had a market cap of $35 billion as of mid-June.

Indeed, with speculators' appetites for blockchain rapidly expanding—the combined market cap of the world's cryptocurrencies has grown almost ninefold in the past 12 months, to pass $100 billion—it's no surprise ICOs are having a moment. Renowned venture capitalists like Chris Dixon of Andreessen Horowitz and Fred Wilson of Union Square Ventures now tout ICOs as a new form of corporate financing. Even companies that are not blockchain-centric are getting in on the action. Messaging service Kik, founded in 2009, plans to conduct an ICO this year in hopes that tokens will spur more person-to-person payments and gaming on its platform. According to research firm Smith + Crown, dozens of firms have already completed ICOs this year, with dozens more to come; the 30 that reported their gains have raised about $400 million.

SO WHAT DO REGULATORS have to say about this brave new world? Right now, nothing. And that could become a problem, for investors and startups alike. In a traditional IPO, a company can't sell shares unless it gets approval from the Securities and Exchange Commission, which means disclosing extensive details about its business prospects and potential risks. For ICOs, there are no such requirements yet—and that could make them prone to abuse.

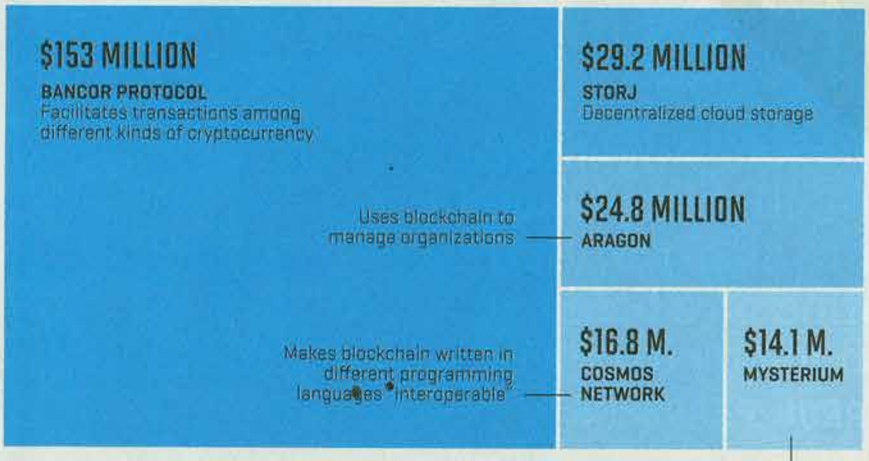
While no fraud investigations of ICOs have come to light, blockchain fans frequently warn one another about dubious offerings in online discussion groups. (One snide slide deck in wide circulation is dubbed "PonzICO.") And some companies have been able to issue tokens even though their business models are long shots at best. Jeff Garzik, a leading figure in the blockchain community who runs a consultancy called Bloq, sees ICOs as "transformative" but remains wary. "Ninety-nine percent of these ICOs will be garbage," he says. "It's like penny stocks but with less regulation."

Even the most legitimate and fiscally sound ICOs pose a potential threat for their issuers. "Coins" or tokens can look a lot like traditional securities, because they enable companies to take investors' cash while holding out the potential for profit. And selling securities without SEC approval violates federal law. "In the future, token sales won't be done in the same way as today, because of regulatory constraints," says Marco Santori, a digital currency lawyer with the firm Cooley. If regulators eventually determine that tokens are securities, Santori says, the SEC and Internal Revenue Service could impose sanctions on issuers; such a decision could also make it easier for investors to sue startups if their tokens become worthless.

Attorneys are now helping startups structure their ICOs to stay on regulators' good side. Lee Schneider, a securities lawyer with Debevoise & Plimpton who also hosts a fintech podcast, collaborated with digital currency exchange Coinbase on best practices for ICOs (Schneider prefers to call them "token launches"), and his advice offers good rules of thumb for would-be buyers too. The best token exchanges involve predictable pricing—a clear relationship between demand for tokens and their price. Issuers should be transparent about sharing the software code underlying the tokens.

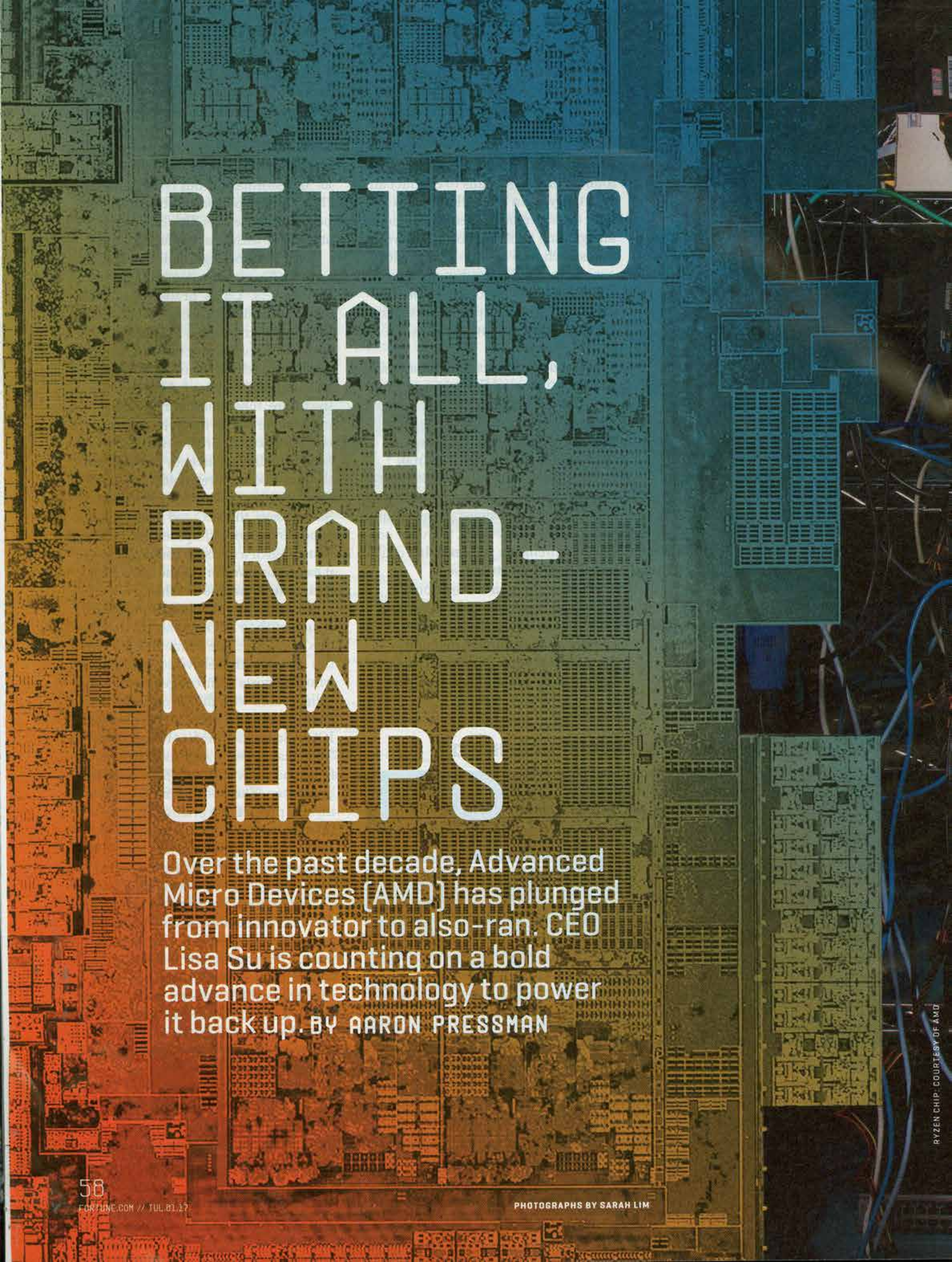
Perhaps most noteworthy: Schneider says ICO candidates shouldn't market tokens as the equivalent of an investment. They should pitch buyers on what the tokens can do, and not on what they could be worth. The bottom line: If a startup advertises its coins as something you can flip to get rich, its ICO is more likely to be "garbage" than "transformative." ■

5 STARTUPS THAT RAISED CASH THROUGH ICOs IN 2017



Offers privacy-protected VPN communication

SOURCE: SMITH + CROWN

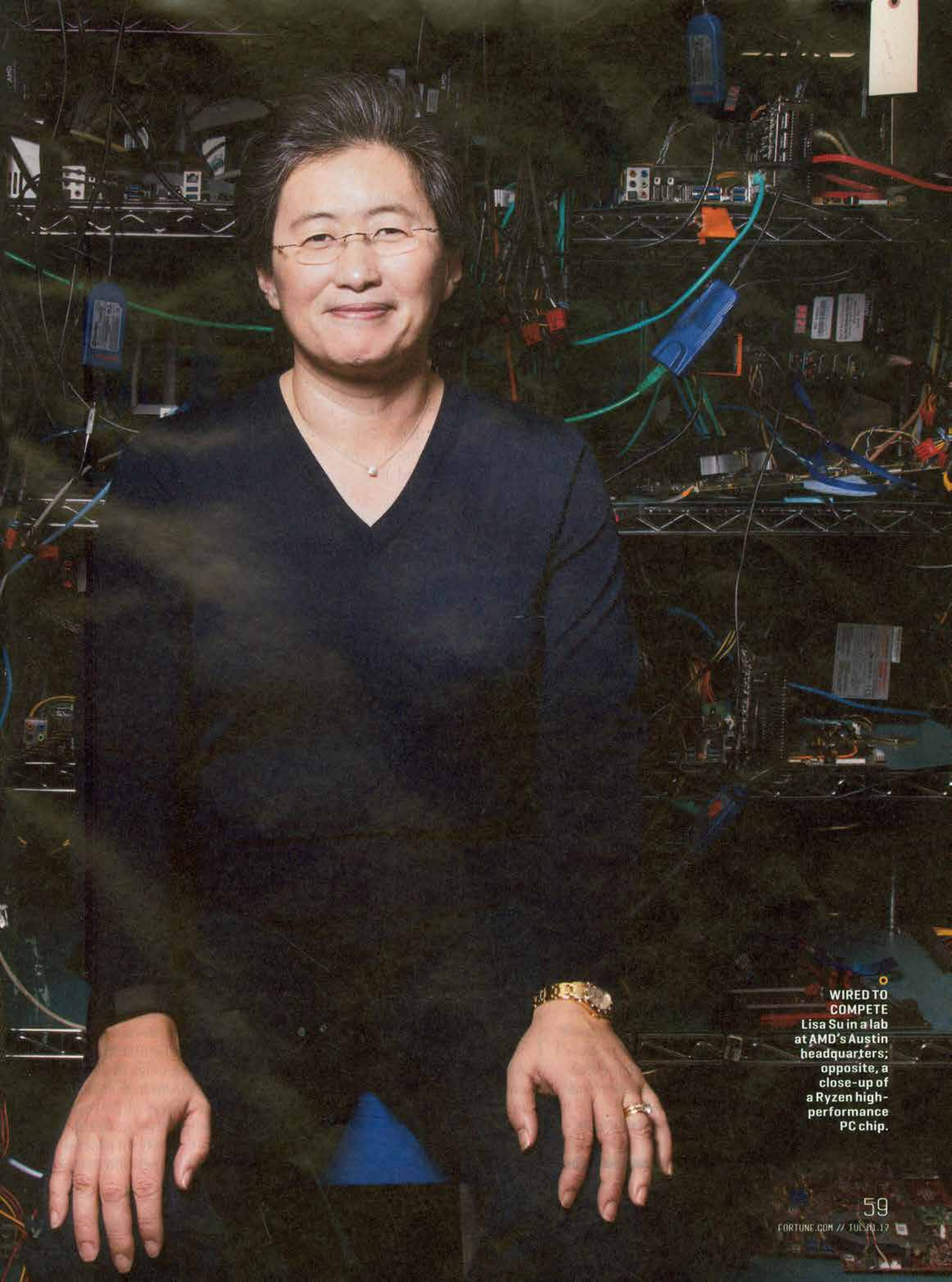


BETTING IT ALL, WITH BRAND-NEW CHIPS

Over the past decade, Advanced Micro Devices (AMD) has plunged from innovator to also-ran. CEO Lisa Su is counting on a bold advance in technology to power it back up. BY AARON PRESSMAN

PHOTOGRAPHS BY SARAH LIM

RYZEN CHIP: COURTESY OF AMD



WIRED TO COMPETE Lisa Su in a lab at AMD's Austin headquarters; opposite, a close-up of a Ryzen high-performance PC chip.

FROM THE WIDE WINDOWS OF HER FOURTH-FLOOR OFFICE, Lisa Su can look across the Austin campus of Advanced Micro Devices and see the laboratory building where the company's new chips get tested. In the spring of 2016, Su was looking in that direction quite often, not to mention texting, instant messaging, and calling the staffers who worked there. She was waiting eagerly for a Zeppelin to arrive.

Zeppelin was the code name for AMD's newest microprocessor, a flagship chip designed to run in personal computers and corporate servers—and the company's future was riding on its success. Su, a Ph.D. microprocessor engineer herself, had become CEO in 2014 in the midst of a dismal sales decline for the chipmaker. Zeppelin was the first fruit of her effort to revive AMD's product line, with redesigned-from-the-ground-up chips that could woo customers with intense computing needs, from finicky video gamers to tech companies running artificial intelligence and machine learning programs. If the new products thrived, AMD stood a chance of reversing years of losses, and even emerging from the shadow of rivals like Intel and Nvidia.

What Su didn't anticipate was that when the Zeppelin finally got to Austin, it would crash-land.

Louis Castro, who oversees testing, had assembled a team of 80 engineers to check out the first Zeppelin chip, dubbed the Ryzen. But the night before testing was to begin, in April 2016, the head of the chip design team called Castro. A flaw had slipped through the designers' computer simulations, and the first chip would be dead on arrival, incapable of even booting up a computer. Waiting for repairs could delay testing the chip—not to mention selling it—for weeks or even months. And to complicate matters, Su was 8,000 miles and 10 time zones away on a business trip in India. "You've never been part of something as big as this in your career," Castro recalls. "I sat and thought to myself, Oh, my gosh, what am I going to do?"

Lee Rusk, the engineer in charge of Zeppelin, called the foundry that was making the chip for AMD and told it to stop production immediately. Chief technology officer Mark Papermaster stepped up to call the CEO with the bad news. The conversation was urgent, but neither executive panicked. And Su's immediate reaction was decisive: Testing couldn't be delayed.

AMD's team quickly went into what Su calls "Apollo 13 mode." Four different teams of engineers brainstormed solutions for getting around the flaw in the prototype chip to start testing immediately. As soon as she got back to Austin, Su headed straight for the lab, encouraging the teams while reminding them that "failure was not an option."

The silicon chips at the heart of today's computers and phones are insanely complex. A single Ryzen chip the size of a nickel has five million transistors, laid out across 100 different layers. The flaw that Castro's team had found affected fewer than one-hundredth of one percent of the circuits. If it had been located deep in the chip, on one of the lowest layers, repairing it could have been fatally time-consuming. But AMD caught a break: The problem, it turned out, could be corrected at the foundry in a month. And Castro's team figured out how to get around the flaw for testing, avoiding losing even just that month.

It's hard to overstate how badly AMD needed a win, and a quick one to boot. The strategy it relied on over most of the past decade—building basic but essential chips, rolling out modest upgrades every year or two, and underpricing the competition—has broken down. Between 2007 and 2016, AMD's market share in PC chips sank from 23% to less than 10%, according to IDC; in server chips, it has dropped below 1%. At the same time the overall PC market has shrunk faster than anyone expected, losing ground to a mobile revolution that largely passed the company by. AMD has lost money for five years in a row, and revenue bottomed out at just under $4 billion in 2015, a 39% decline from its 2011 peak.

Bad news for AMD, arguably, is a loss for Silicon Valley. The company has never been anywhere near No. 1 in the semiconductor arms race. But AMD has been an innovator in countless ways—the first chipmaker to break the one-gigahertz speed barrier, the first to put two processing cores in a single chip for PCs. And in that role, it has helped keep costs down and ideas flowing for innumerable businesses that rely on processing power. "Competition drives

THEY LED "ZEPPELIN"
Su in the lab with Louis Castro (in Ryzen T-shirt), Lee Rusk (in polo), and other engineers on AMD's Zeppelin chip project.

innovation in every market I've ever seen," says Meg Whitman, CEO of Hewlett Packard Enterprise and now a veteran of the PC and server industries. "A broad ecosystem in the chip market," she adds, "is a good thing for the industry as a whole."

Today, AMD's extinction looks less likely—thanks in large part to Su. Her strategy hinges on radical redesigns that could help AMD leapfrog Intel and Nvidia in the market for supercomputer-like processors, chips that do more calculations simultaneously and speed access to data stored on other parts of a user's computer. At the same time, Su has begun weaning AMD from its dependence on PCs, focusing on deals to supply chips to the three leading video game console makers: Microsoft, Sony, and Nintendo. She has also boosted the bottom line by licensing server chip designs to a Chinese partner. To accomplish it all, Su is drawing on her experience as an engineer, on relationships she built over more than a decade at IBM—and on design talent poached from the glamorous confines of Apple.

The first Ryzen chips hit the market this March, and early reviews are strong. The chips easily exceeded AMD's promise of 40% faster processing than the previous generation. And they're matching the performance of comparable Intel chips at less than half the price; a top-end Ryzen 7 1800X chip for desktop computers, for example, sells for $499, while Intel's Core i7-6900K is $1,089. Investors are excited too: AMD's stock, which was barely treading water at under $2 a share in early 2016, now trades at about $12.

This summer will bring more debuts: Up next is a chip for servers called Epyc—taking on Intel's near monopoly in that category. Later comes Vega, a graphics chip, or GPU. Such chips have not only become important for gamers but also as the best way to run cutting-edge artificial intelligence and machine learning tasks—the kinds that fuel Siri and Alexa and are used by corporate giants like GE to analyze "big data" streams. Indeed, demand for GPUs is growing even as the PC market remains in a slump. The Vega's performance has been turning heads too: It convinced Apple to use the chip in its upcoming iMac Pro, the sleek, all-black computer it unveiled in June.

With those products still unproven, however, AMD is hardly out of the woods. Stacy Rasgon, the longtime chip industry analyst at Bernstein Research, believes Su has made the right bets and cleaned up the balance sheet but says she has yet to prove AMD can deliver. "In the context of a company where 18 months ago the concern was, are they going bankrupt or not, she's doing a really good job," Rasgon says. "But I have too much history with AMD to bet on their execution." It's Su's mission to vanquish such skepticism.

THAT HISTORY is tightly intertwined with that of AMD's far bigger rival, Intel. Both companies were founded by engineers and executives from semiconductor pioneer Fairchild. Robert Noyce, Gordon Moore, and Andy Grove struck out in 1968 to form Intel. The AMD group spun out a year later, under salesman Jerry Sanders, a self-proclaimed tough kid from Chicago's South Side. AMD's business took off in the 1980s largely because IBM decided it shouldn't rely only on Intel for chips for its new personal computer and designated AMD as its official second supplier. AMD remains the only major alternative source for PC chips compatible with Intel's x86 template—but even at its peak in the 2000s, when it sold nearly one out of every four chips found in PCs, it was always a distant second.

AMD reached its prime in the 1990s and 2000s under Sanders and his successor, Hector de Jesus Ruiz, introducing fast and innovative PC chips like the K6 that proved the company was more than an Intel clone. Its stock reached a high of over $42 a share in 2006. But Ruiz made the fateful decision that year to buy graphics-chip maker ATI for $5.4 billion. ATI's technology never gave AMD the boost it hoped for. What's more, the deal led to years in the red for the company as it juggled a heavy debt load and merger write-offs. From 2008 to 2011, AMD went through four CEOs.

That was the mess inherited by Su. Born in Taiwan, she moved to New York City with her family at age 2. Her parents told Lisa she could be a concert pianist, a doctor, or an engineer. The third choice resonated with a kid who regularly took apart her younger brother's electric cars and tried to put them back together. She attended the prestigious Bronx High School of Science, then MIT—where her interest in microprocessors first took root—for an undergraduate degree, master's, and Ph.D. in electrical engineering.

After a brief stint at Texas Instruments, Su went to IBM, where she spent more than a decade focused on the race for cheaper, faster chips. She also met a crucial mentor in Nicholas Donofrio, an IBM legend who had worked on everything from mainframes to the original PC. Donofrio arranged for Su's appointment as special technical assistant to Lou Gerstner, the then CEO who left the credit card industry to run Big Blue. Su's job was to keep Gerstner abreast of major technology developments and ensure his lack of technical training didn't hinder his decision-making. "What I got as a benefit from it was watching how the CEO of a major corporation thinks," Su recalls now. Gerstner's strength lay in simplifying the available options, homing in on how new technologies could actually help customers.

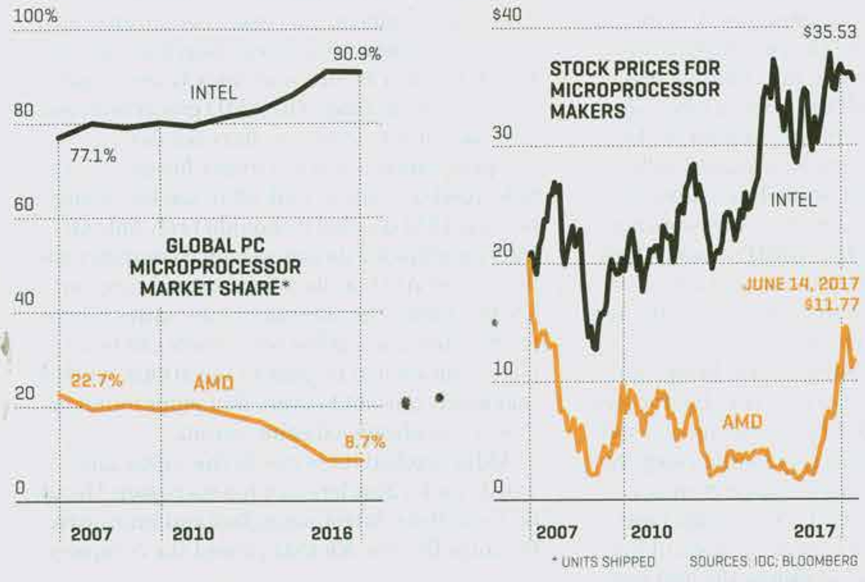
Su aspired to run a company, and as her star rose she felt she couldn't do that at IBM. (Being a woman, she stresses, was never an obstacle: If anything, she feels lucky to have always had bosses who were free of gender hang-ups.) In 2007, Freescale Semiconductor, a Motorola spinoff that made chips for the Apollo moon missions and was in need of an overhaul, offered Su the role of chief technology officer, and she seized the opportunity. She relocated to Austin, where she eventually ran Freescale's $1 billion networking chip division and helped the company go public in 2011.

By then, Donofrio had retired from IBM and joined AMD's board to help craft a turnaround strategy. In Austin for a board meeting, Donofrio invited Su to dinner at the tony Barton Creek Resort. Each worried that the other was angry over Su's departure from IBM. To break the tension, Donofrio ordered a very expensive California cabernet, Shafer Hillside Select, and as the wine flowed it became obvious that neither harbored a grudge. Remembering why Su had left IBM, Donofrio flipped the script. AMD had deeply rooted problems but also had incredible engineering talent and unique intellectual property. "It's so ripe for you," Donofrio recalls saying. "It's so right." Su jumped at the bait and joined the company in 2012. By 2014, she was CEO.

By then AMD had put together a design dream team that could reinvent its chips. Donofrio recruited Mark Papermaster, now the CTO, an IBM veteran whom Steve Jobs had wooed to help Apple develop its own line of chips for the iPhone. Papermaster in turn helped the company bring in other rock-star designers—most notably Raja Koduri in 2013. Widely respected as a graphics-chip visionary, Koduri was at Apple at the time, overhauling its product line to handle high-resolution Retina screens.

Jumping from Apple, at the height of its dominance, to struggling AMD seemed crazy to Koduri's friends and family. His wife thought he was having a midlife crisis. But Koduri had come to believe that other platforms might displace mobile as the locus for innovation in chipmaking. Staring at the display of an iPhone for hours on end, he had an epiphany. "Man eventually wants to carry this thing around with him all the time, not just in his pocket," Koduri recalls. "You want access

IN THE SHADOW OF INTEL



* UNITS SHIPPED SOURCES: IDC; BLOOMBERG

PAYING LEADERSHIP FORWARD Su with then IBM CEO Lou Gerstner (above, c. 2000); with MIT Ph.D. recipients in June.

to this information all the time." That might be attained through virtual reality or digital assistants fueled by artificial intelligence, or some mix Koduri couldn't foresee. But it was bound to boost demand for high-performance computing—and new kinds of chips. And AMD's desperation for renewal made it the place where he could design such chips with a clean slate. "If you work like you have nothing to lose, you can do some pretty interesting things," he says.

T**HE "NOTHING TO LOSE"** ethos is beginning to pay dividends. Last year AMD's revenue rose 7% over the previous year, to $4.2 billion. By the end of this year, the graphics business could be pulling more weight. In 2015, Su put all AMD's graphics-chip work under Koduri in a new unit called the Radeon Technology Group. Radeon's headcount has risen 60% since then, to 3,200, making it the largest team in the company. AMD's PC chips "had taken the limelight," Su says. "Now we're saying that graphics is also a first-class citizen."

Soon will come the real test of the strategy, as products with the new Vega chips go on sale this summer. Nvidia, under CEO Jensen Huang (another Taiwanese-born American trained as an electrical engineer), is a powerful player in graphics, particularly on the software side, where its proprietary CUDA platform dominates as a tool for big-data analysis. Although the market for what analysts call "GPU compute" is small, it's growing fast. From under $500 million in sales last year, it will hit close to $9 billion by 2020, Bernstein's Rasgon estimates. AMD is building an open-source software platform to catch up to CUDA. But by its executives' own admission, it's starting far behind.

Intel, meanwhile, is far from folding its tent in the competition for PCs and servers. CEO Brian Krzanich is focusing attention on data center customers, and in May Intel unveiled a higher-performance desktop line dubbed the Core i9. "We really stepped on the accelerator in this space a while back," says Greg Bryant, the new head of Intel's PC chip unit.

Meg Whitman, for one, thinks AMD will punch above its weight. Notably, Whitman and Su are among the few women who have reached the ranks of CEO at a *Fortune* 500 company (though AMD's recent revenue woes bumped it off that list in 2015), and Su consulted Whitman early on for advice about being a CEO. Whitman thinks Hewlett Packard Enterprise's core server business will be a big beneficiary (and buyer) of AMD's Epyc chip. "Why did Lisa succeed where others failed?" she asks. "She has focused that company on building great product. Beginning, middle, end of story."

S**U REGULARLY TRAVELS** the world to pitch that story. And on a sunny day this June she was back in the Boston area, mingling with some likely future customers. Almost 25 years after she earned her own doctorate, Su's alma mater, MIT, invited her to speak to the 500 or so graduates receiving a Ph.D. Apple CEO Tim Cook (an Auburn University and Duke business school grad) would address the school's full graduation the next day, but it was Su who spoke at the event where the doctoral recipients got their ceremonial hoods.

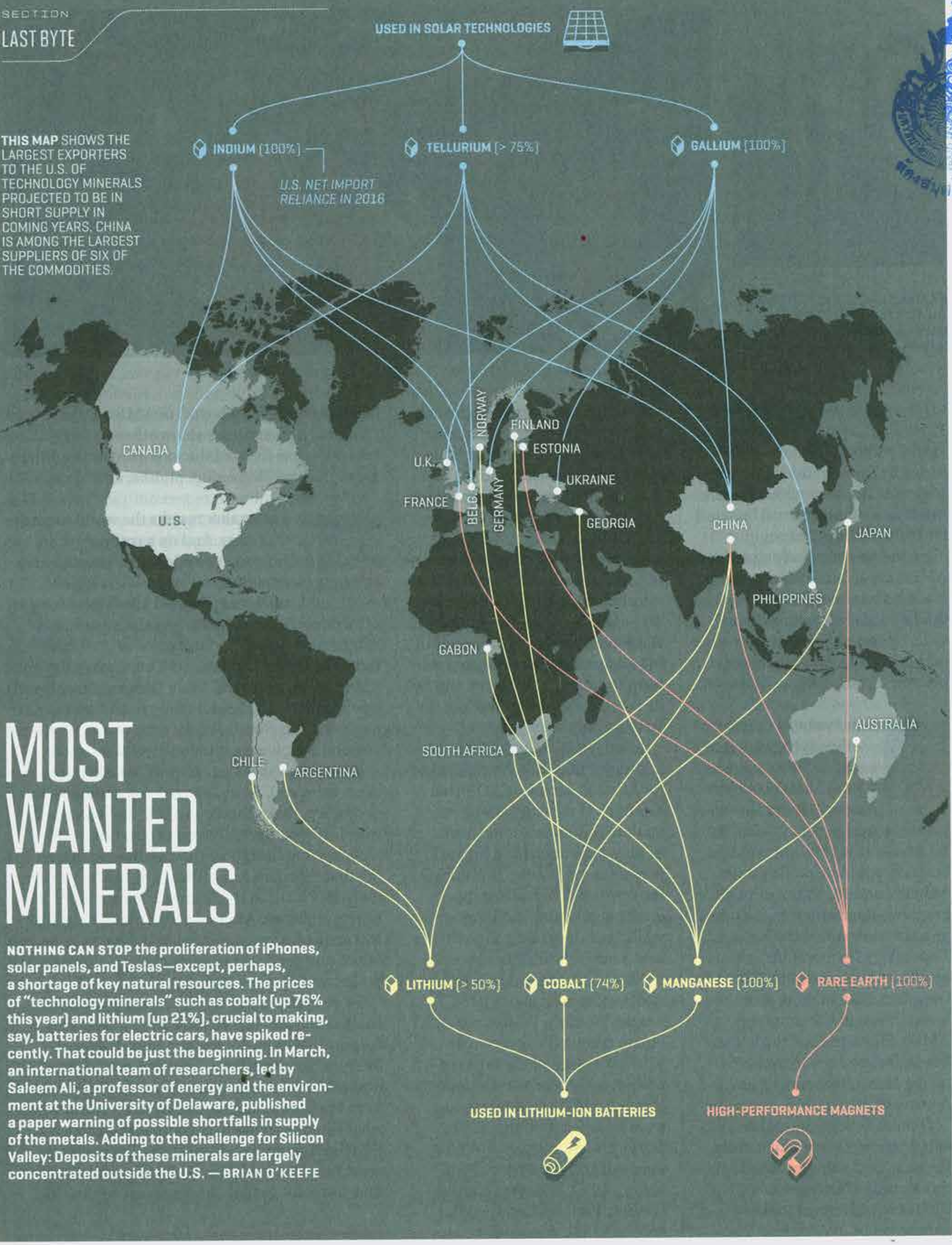
In a speech she wrote herself (a task many execs delegate), Su challenged the graduates to dream big, make their own luck, and change the world. Her competitive streak also came out. "Promise me that you will work hard at ensuring that there are lots of Harvard MBAs working for MIT Ph.D.s in the future," she concluded to hearty applause. Afterward her rock-star status was confirmed as graduates asked her to pose for selfies and professors approached to discuss chip design and Moore's law.

Su dutifully posed for the smartphones and chatted amiably before retreating to a nearby hole-in-the-wall Chinese restaurant, a favorite from her student days. Sitting next to her husband and ordering some of the spiciest dishes from the plastic menus, a relaxed Su summed up what she was trying to get across in her speech. "I'm fighting my set of wars, and I'm having a great time," Su said. "Each of you can pick a war that you want to fight, and you can win it." ■

SU AND GERSTNER: COURTESY OF AMD; SU AT MIT: AARON PRESSMAN

MOST WANTED MINERALS

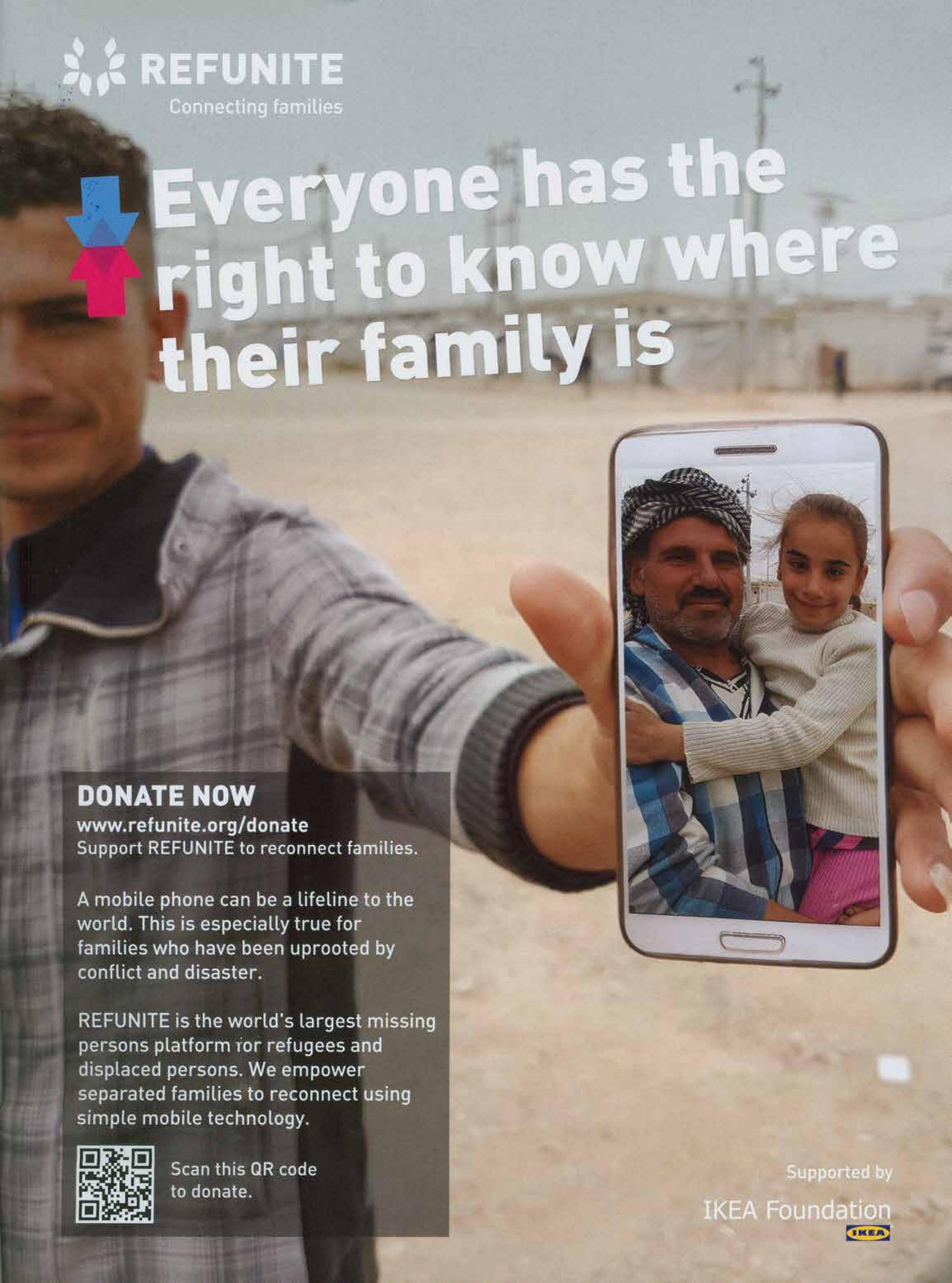
NOTHING CAN STOP the proliferation of iPhones, solar panels, and Teslas—except, perhaps, a shortage of key natural resources. The prices of "technology minerals" such as cobalt [up 76% this year] and lithium [up 21%], crucial to making, say, batteries for electric cars, have spiked recently. That could be just the beginning. In March, an international team of researchers, led by Saleem Ali, a professor of energy and the environment at the University of Delaware, published a paper warning of possible shortfalls in supply of the metals. Adding to the challenge for Silicon Valley: Deposits of these minerals are largely concentrated outside the U.S. — BRIAN O'KEEFE



THIS MAP SHOWS THE LARGEST EXPORTERS TO THE U.S. OF TECHNOLOGY MINERALS PROJECTED TO BE IN SHORT SUPPLY IN COMING YEARS. CHINA IS AMONG THE LARGEST SUPPLIERS OF SIX OF THE COMMODITIES.

SOURCE: U.S. GEOLOGICAL SURVEY; ENERGY AND ENVIRONMENTAL POLICY, UNIVERSITY OF DELAWARE

▲ GRAPHIC BY NICOLAS RAPP


REFUNITE
Connecting families
Everyone has the right to know where their family is
Supported by
IKEA Foundation
IKEA