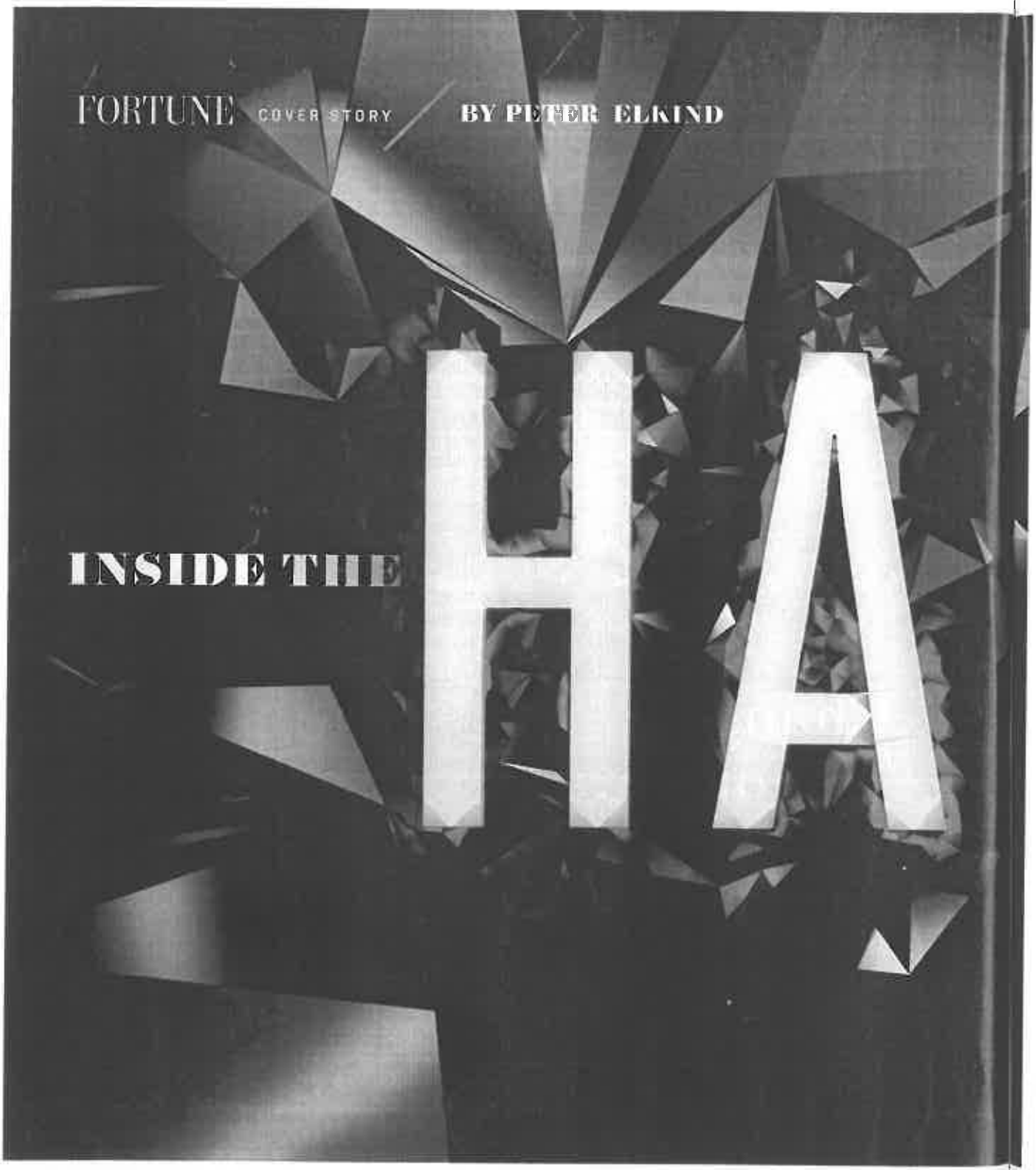
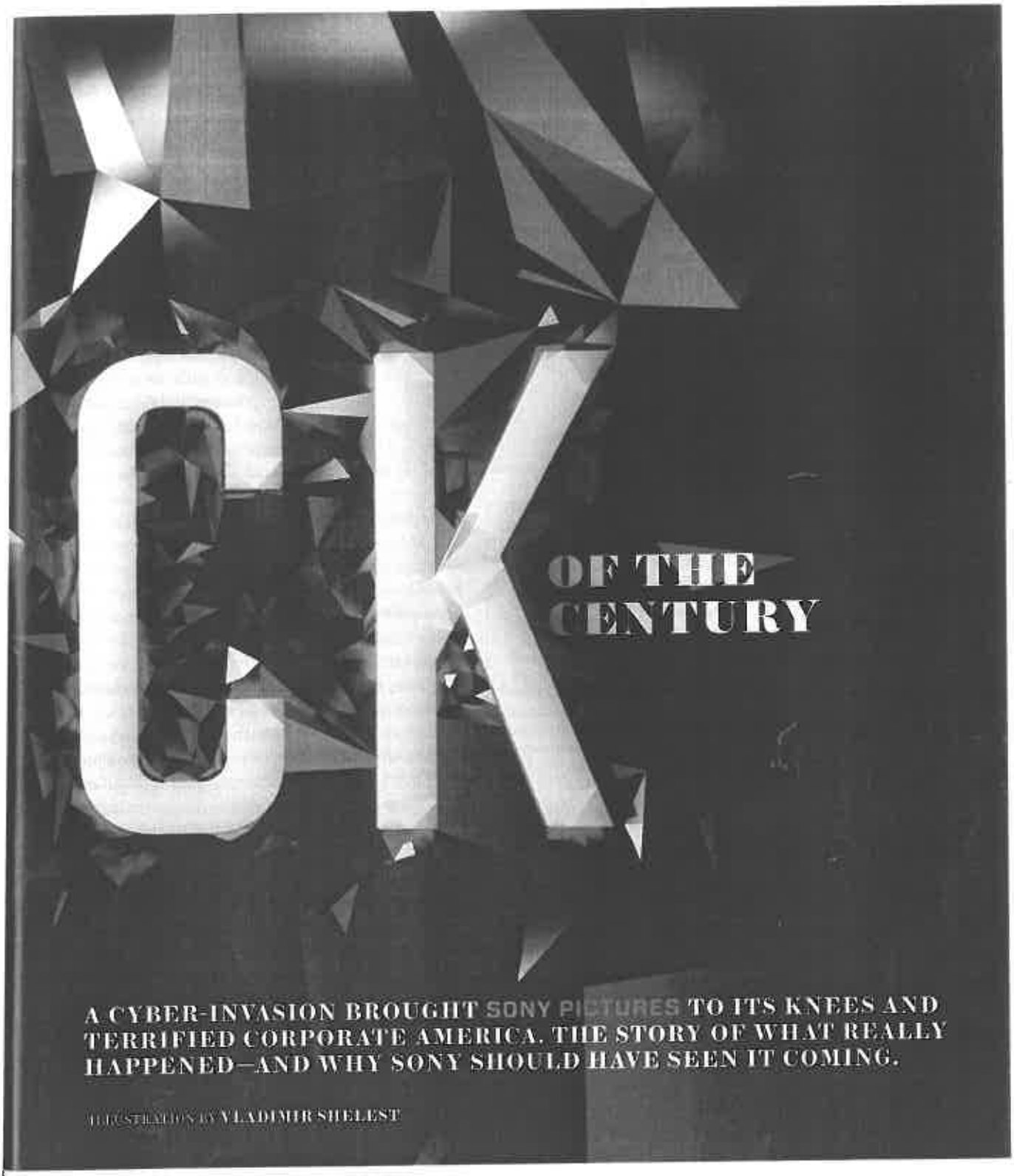

FORTUNE COVER STORY
BY PETER ELKIND
INSIDE THE
HA



# CK OF THE CENTURY

**A CYBER-INVASION BROUGHT SONY PICTURES TO ITS KNEES AND TERRIFIED CORPORATE AMERICA. THE STORY OF WHAT REALLY HAPPENED—AND WHY SONY SHOULD HAVE SEEN IT COMING.**

ILLUSTRATIONS BY VLADIMIR SHELEST

# On Monday, Nov. 3,

**2014, a four-man team from Norse Corp., a small "threat-intelligence" firm based in Silicon Valley, arrived early for an 11:30 a.m. meeting on the studio lot of Sony Pictures Entertainment, in the Los Angeles suburb of Culver City. They were scheduled to see Sony's top cybersecurity managers to pitch Norse's services in defending the studio against hackers, who had been plaguing Sony for years.**

After a quick security check at the front gate and then proceeding to the George Burns Building on the east side of the Sony lot, the Norse group walked straight into the unlocked first-floor offices of the information security department, marked with a small sign reading INFO SEC. There was no receptionist or security guard to check who they were; in fact, there was no one in sight at all. The room contained cubicles with unattended computers providing access to Sony's international data network.

The visitors found their way to a small sitting area outside the office of Jason Spaltro, Sony's senior vice president for information security, settled in, and waited. Alone. For about 15 minutes.

"I got a little shocked," says Tommy Stiansen, Norse's co-founder and chief technology officer. "Their Info Sec was empty, and all their screens were logged in. Basically the janitor can walk straight into their Info Sec department." Adds Mickey Shapiro, a veteran entertainment attorney who helped set up the meeting and was present that day: "If we were bad guys, we could have done something horrible."

Finally Spaltro, who's worked at Sony since 1998, showed up and led them to a nearby conference room, where another studio information security executive was waiting. The meeting began, and as Stiansen described how Norse scopes out potential threats, Spaltro interrupted: "Boy, that could really help us with that North Korean film!" According to the four Norse representatives, Spaltro explained that he was worried about a Seth Rogen comedy called *The Interview* that the studio was preparing to release on Christmas Day. It featured a plot to assassinate Kim Jong-un, the country's actual leader. Recalls Stiansen: "They said North Korea is threatening them." (Sony denies any mention of a North Korean cyberthreat.)

After about an hour the Sony team declared the session "very productive," according to the Norse team, and promised to be in touch. They departed, leaving the visitors to find their own way out.

THREE WEEKS LATER—starting at about 7 a.m. Pacific time on Monday, Nov. 24—a crushing cyberattack was launched on Sony Pictures. Employees logging on to its network were met with the sound of gunfire, scrolling threats, and the menacing image of a fiery skeleton looming over the tiny zombified heads of the studio's top two executives.

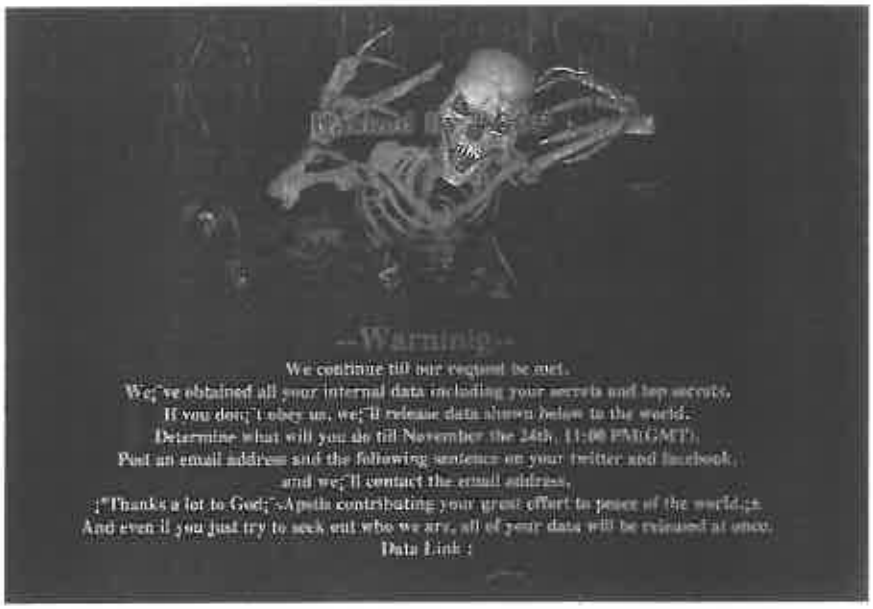
Before Sony's IT staff could pull the plug, the hackers' malware had leaped from machine to machine throughout the lot and across continents, wiping out half of Sony's global network. It erased everything stored on 3,262 of the company's 6,797 personal computers and 837 of its 1,555 servers. To make sure nothing could be recovered, the attackers had even added a little extra poison: a special deleting algorithm that overwrote the data seven different ways. When that was done, the code zapped each computer's startup software, rendering the machines brain-dead.

From the moment the malware was launched—months after the hackers first broke in—it took just one hour to throw Sony Pictures back into the era of the Betamax. The studio was reduced to using fax machines, communicating through posted messages, and paying its 7,000 employees with paper checks.

That was only the beginning of Sony's horror story. Before destroying the company's data, the hackers had stolen it. Over the next three weeks they dumped nine batches of confidential files onto public file-sharing sites: everything from unfinished movie scripts and mortifying emails to salary lists and more than 47,000 Social Security numbers. Five Sony films, four of them unreleased, were leaked to piracy websites for free viewing. Then the hackers threatened a 9/11-style attack against theaters, prompting Sony to abandon *The Interview*'s Christmas release. A week later, after an uproar, the studio announced it would make the movie available, after all, through video on demand and in a few hundred theaters.

On Dec. 19 the FBI blamed the hack on North Korea, which had issued threats over the film. The White House followed with economic sanctions. Sony was pilloried both for horrendous judgment (for making a comedy depicting the killing of North Korea's sovereign leader) and its seeming capitulation (for its initial refusal to show the film). In its darkest hours Sony drew zero support from Hollywood—and a blast from President Obama. Sony's traumatized employees face an ongoing threat of identity theft.

The studio and its Tokyo-based parent, Sony Corp., were already under siege. "Big Sony"—as studio executives refer to it—is facing a prolonged crisis after losing money for six of the past seven years. Sony Pictures remains one of its few moneymaking businesses. But as interviews and internal emails reveal, the studio was a deeply unhappy place, beset by pressures over disappointing profits, cost cutting and layoffs, the scorn of an activist investor, and tribal infighting. Sony Pictures CEO Michael Lynton pursued four separate opportunities to leave the company during the 18 months before the hack.




**The screen that greeted Sony Pictures employees after they logged on to their computers on Nov. 24. The hack not only stole massive quantities of documents and emails, but it also erased all the data on half the company's computers and servers.**

In Sony's view, the company is a blameless victim. In a December interview with National Public Radio, Lynton insisted his company was "extremely well prepared for conventional cybersecurity," but faced "the worst cyberattack in U.S. history." He has repeatedly described it as a "highly sophisticated attack." Sony Pictures provided written responses to questions through Robert Lawson, its chief spokesman. He says Lynton has no plans to fire or discipline anyone. The CEO's reasoning rests on the belief that because Sony's assailant was a foreign government, with far more resources than a renegade band of hackers, what happened was unstoppable. The studio simply faced an unfair fight.

In a statement, Lawson argues that "any suggestion Sony Pictures Entertainment should have been able to defend itself against this attack is deeply flawed and ignores essential findings and comments made by the FBI and [Sony's cybersecurity consultant] Kevin Mandia—the two parties most knowledgeable of the nation state threat and the evidence in this investigation. Joseph Demarest, then assistant director of the FBI's cyber division, could not have been clearer when he told a U.S. Senate hearing that 'the malware that was used would have slipped, probably would have gotten past 90% of the net defenses that are out there today in private industry, and I would challenge to even say government.'" Mandia, the statement continues, "has also explained how the sophistication of the exfiltration methods used in this attack made them virtually undetectable. And both Mandia and the FBI have stated that the malware used was undetectable by industry standard antivirus software."

In truth, there is no way to know whether Sony's attackers would have prevailed over even impeccable cyberdefenses. Experts say Sony's electronic security probably wasn't worse than that of many others; weak, outmoded practices are the norm at far too many companies. But it's clear that Sony, which failed to employ several basic safeguards, didn't put up much of a fight.

As it was, the company had ample reason to have bolstered its defenses: For years, culminating with its release of *The Interview*, Sony Corp.'s business decisions have made it a virtual piñata for cyberassailants. And North Korea had been blamed for devastating high-profile electronic attacks in the past. Despite that, the company's leadership failed repeatedly to take greater precautions.

"No company is ever going to say, 'We were just sloppy, so people got in,'" says cybersecurity expert James Lewis, senior fellow at the Center for Strategic and International Studies. "The fact that it's a nation-state and is hard to defeat doesn't mean you have to leave the doors wide open and put out the welcome mat."

This article is based on more than 50 interviews with current and former high-level executives at Sony (all of whom insisted on not being identified by name), cybersecurity experts, and law-enforcement officials. It is also based, in large part, on Sony emails and documents stolen by the hackers. Beyond generating Hollywood gossip, which they already have, they offer a remarkable window into the business of Sony Pictures at the time of the hack: the personalities of its leaders, the pressures they faced in their relationship with the business's Tokyo-based parent, and the challenges of running an entertainment studio in the 21st century. (We've preserved the emails' original punctuation and often sloppy spelling.)

The emails also reveal myriad surprises and previously unreported anecdotes, including one episode in which Sony spied on its own employees' emails. Paradoxically, the hacked emails and documents provide a telling window into how and why such a disastrous hack succeeded and what companies need to do to protect themselves—which is precisely why *Fortune* has chosen to use this material. (For more on our thinking, see Editor's Desk in this issue.)

What happened at Sony stands as a landmark event. It struck terror in boardrooms throughout corporate America, and for all the unique elements in Sony's situation, the lessons apply to every company. After all, to use an old line, there are only two kinds of companies: Those that have been hacked, and those that don't yet realize they've been hacked. Countless behemoths have been victimized on a massive scale, including Target, Anthem, Home Depot, and J.P. Morgan, suffering incursions for profit-oriented data theft or corporate espionage.

The peril for corporate America seems to be growing even faster than the immense resources now mobilized to combat electronic crime. (The government has hardly been immune, with high-profile infiltrations of the IRS, the White House's email system, and the U.S. Office of Personnel Management.) But for the most part, previous corporate invasions have afflicted customers, not businesses.

INSIDE THE HACK OF THE CENTURY

Sony Pictures CEO MICHAEL LYNTON and studio chief AMY PASCAL, photographed on Sony's lot in 2010, were emotional opposites but collaborated productively for a decade.

ROBERT GALLAGHER—CORBIS OUTLINE

This one hit home because it showed how attackers could steal even executives' most precious secrets—and bring a company to its knees.

## The Humbled Giant

THE IMPROBABLE COMBINATION of a Japanese electronics giant and a Hollywood studio dates back to 1989. Sony Corp. was then the most dominant electronics company on the face of the earth, at a moment when Japanese business dominance seemed permanent. Sony paid an eye-popping $4.8 billion for struggling Columbia Pictures, declaring movies the equivalent of "software" needed to boost sales of its premium "hardware"—TVs, videocassette recorders, and music players. The studio was renamed Sony Pictures Entertainment but continued to struggle, forcing a $2.7 billion write-down five years later.

The next quarter-century was not kind to Sony Corp., which clung to its consumer electronics business as it became commoditized. Today the company remains a Goliath, with 132,000 employees and $74.7 billion in revenues for the fiscal year ending in March. But Sony has lost $12.1 billion over the past seven fiscal years. When Kazuo Hirai became CEO in April 2012, he declared "a very severe sense of crisis" and announced a turnaround strategy, including thousands of layoffs. In the change-averse Japanese corporate culture, it has unfolded far too slowly.

Hirai, who succeeded Howard Stringer, Sony's first non-Japanese CEO and a man frustrated by his inability to reenergize the sclerotic company, rose through its PlayStation videogames division, which he helped make a reliable moneymaker. Just 51 when named CEO, Hirai dressed casually, encouraged employees to call him Kaz, and, after years in the U.S., pitched products in perfect English.

Like his predecessors, Hirai kept his hands off Sony Pictures, run for more than a decade through a delicate yin-yang partnership. Sony's studio chief was Amy Pascal, who reigned as the most powerful woman in Hollywood. Masterly at stroking celebrity egos, Pascal cultivated relationships with filmmakers and stars, who returned the affection. "I adore you, Amy," George Clooney wrote her last year. "You are literally the only person running a studio that loves film." Raised middle class in Los Angeles, Pascal was frenetic, thin-skinned, and unfiltered, given to long, stream-of-consciousness emails. Paid $9.1 million

for 2014, she proudly presided over her domain from a majestic office once occupied by Louis B. Mayer. She had a reputation for dispensing overly generous deals and falling in love with ambitious movies that had dubious commercial prospects.

To inject fiscal discipline, Stringer in 2004 had forced Pascal to team up with Lynton, who had left a job as head of AOL Europe to join Sony Pictures as CEO. Raised in the Netherlands by a wealthy German-Jewish family that fled Hitler, Lynton attended Exeter before earning his undergraduate degree and MBA at Harvard, where he played rugby; he'd done a stint as an investment banker. Cool, cerebral, and measured, Lynton was an East Coast intellectual with artistic interests that he viewed as more refined than the crassly commercial fare typically peddled by Hollywood. In 1998, after leaving Disney Studios and moving back east to run Penguin Books, he told a *New Yorker* writer of his "horror" at "living in a town where everything is about movies."

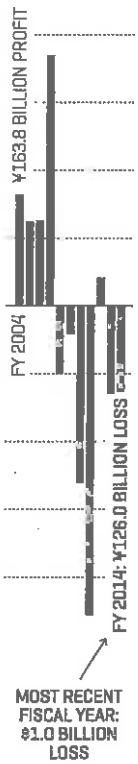
A consummate networker, Lynton avoided drama and the spotlight, preferring to pull strings behind the scenes. He arranged a film audition for billionaire Leon Black's actress-niece, dined with President Obama on Martha's Vineyard, and plotted with Facebook COO Sheryl Sandberg to see if they could find a blind date for Malcolm Gladwell, one of his many writer buddies.

Despite his personal wealth (which included 2013 Sony pay of $9.6 million), Lynton made a show of being frugal. He drove a Volkswagen Golf GTI. Pascal described him in one leaked email as "the kind of guy who wears the same pair of shoes every day but what you wouldn't know is that they were made by the poshest most expensive cobbler in switzerland."

Lynton and Pascal had survived together for a decade—an eternity in Hollywood. Both in their mid-fifties, they lived two miles apart and even attended the same synagogue. When Lynton first took the job, he diplomatically vowed to steer clear of Pascal's turf and rarely stood in the way of a film she wanted—even one he loathed—where the bottom line seemed to make sense. After reading the script for a movie called *Money Monster*, for example, he wrote Pascal: "I hate it... It is simplistic, bombastic, wrongheaded, and stupid. All that being said... if the numbers work and there is no risk then I am ok." Sony moved forward with the film; its release date is undetermined. (Says Sony spokesperson Lawson: "Initially [Lynton] was not supportive, but what you don't see in the stolen emails is that through further discussion, his position changed and he ended up supporting the project.")

INSIDE THE HACK OF THE CENTURY

SONY CORP.'S LOSS YEARS




Hirai maintained a similar posture. In June 2014, after forwarding enthusiastic European screening reports for the Cameron Diaz comedy *Sex Tape* (which would later bomb), Lynton joked with the Sony Corp. CEO about their mutual dislike for it. "Something tells me that I should keep my day job," wrote Hirai.

"The box office will be the judge," Lynton replied. "But you and I have the same view of the movie!!"

## Fending off Dan Loeb: "No cost is too sacred to cut."

IN MAY 2013 a new consideration altered "Big Sony's" dealings with the studio and shook its fragile management partnership: The parent company came under pressure from Dan Loeb. Loeb, who runs the New York City–based hedge fund Third Point, had acquired a $1.1 billion stake in Sony Corp.—more than 6% of its Tokyo shares—and placed Sony Pictures in his crosshairs.

Loeb is rough on his targets, often accusing executives of personal misconduct in an attempt to drive them out. In a letter he urged Sony Corp.'s board to spin off up to 20% of the studio (as well as its music business, which Lynton also oversees) through a public offering to help fund its turnaround. Loeb publicly charged that Sony Pictures was "famously bloated" and "poorly managed," with profit margins far below those of rival studios. Hirai, he asserted, was giving Lynton and Pascal "free passes."

The movie business is volatile. But in truth the studio was not only experiencing a bad run but also poorly positioned for the future. Its two pricey would-be summer blockbusters for 2013, *White House Down* and *After Earth*, flopped. Sony's pipeline was short on "tentpoles," the big franchises that generate lucrative sequels and tie-in products, such as action figures and videogames. The studio produced few animated hits for the family market. And too many of its movies had limited appeal overseas, now two-thirds of total box-office receipts.

Still, Hirai had no intention of doing what Loeb wanted. Despite its problems, the movie studio, with about 11% of the parent's revenues, remained one of Sony Corp.'s few profitable realms. A spin-off would also undermine Hirai's "One Sony" strategy—his re-

CHART SOURCE: S&P CAPITAL IQ

vived notion of the old software-hardware synergy.

What followed was a strange form of misdirection. Although many at Sony feared and loathed Loeb (an executive vice president, in a leaked email, called him a "douchebag"), the company's chiefs launched a public charm offensive in hopes of persuading him to walk away. Hirai had breakfast with Loeb in Tokyo. Lynton and Pascal hired a new $600,000-a-year studio PR chief, Charlie Sipkins, from a crisis-management firm where he'd helped Yahoo deal with Loeb successfully. And Sony announced it was responding to Loeb's calls for increased transparency with its first-ever "Entertainment Investor Day," to be held on Nov. 21, 2013.

Executives prepared for this event, which was to be webcast, as if it were Oscar night. Pascal drafted her presentation three weeks early, then emailed Lynton and others: "LET'S START REHEARSING NOW." When Loeb, during a CNBC interview, expressed pleasure with promised Sony actions, company executives tweaked their scripts to highlight those steps. PR man Sipkins even sent everyone an email on preferred attire: "We want to project a consistent image... men should wear dark suits, nonpatterned shirts, and simple ties. If possible, women should wear suits or long skirts/dresses."

In five hours of presentations Sony executives labored to display their commitment to fiscal discipline and consistent earnings. Lynton and Pascal promised tighter policies for green-lighting films. Talent would get less generous deals, more dependent on financial results. Sony was reducing its annual slate from two dozen movies to 18. And the studio vowed to slash $250 million in expenses over the next two years, a process that would result in hundreds of layoffs. "No cost is too sacred to cut," Lynton declared.

By then Lynton had hired management consultants Bain & Co. to find at least another $50 million in cuts, for a total of $300 million. Sony labored to "spin" this bloodletting, privately instructing the executive team, according to hacked meeting minutes: "Going forward, everyone should use the name 'Build for Tomorrow' when referring to the project... the process can be enormously productive, and we need everyone to embrace it wholeheartedly." But Bain's hiring leaked into the press before Sony even announced it internally. This, TV chief Steve Mosko complained to Sony's CFO, had generated "a major shit storm... I had people in my office all day yesterday asking if they were losing their job."

PHIL MCCARTEN—REUTERS

DAN LOEB

> SONY PICTURES WAS "FAMOUSLY BLOATED" AND "POORLY MANAGED," THIRD POINT'S LOEB SAID AFTER TAKING A STAKE IN SONY CORP. THE INVESTOR'S AGITATION CAUSED FEAR AND LOATHING INSIDE THE STUDIO. ONE EXEC REFERRED TO LOEB AS A "DOUCHEBAG."

Yet it appeared to have the desired effect on Loeb. In January 2014 he emailed Hirai and Lynton that he'd fed friendly comments about the company to the *New York Post*. "Hope they were helpful," he said. When *Variety* called him for a story, Loeb gave Sony executives a heads-up. "I'm talking on background only," he confided. (Loeb declined to speak with *Fortune*.)

Still, Nicole Seligman, Sony Corp.'s New York–based general counsel was wary, according to leaked emails. Was a mole inside Sony talking to Loeb? She decided to find out. At her direction the studio's top lawyer, Leah Weil, secretly arranged for the IT department to unearth all email traffic between Loeb and anyone at Sony since January 2013, then forwarded the messages to Seligman. The search turned up just a dozen innocuous exchanges between Loeb and two Sony executives, Lynton and Mosko, who had already told Seligman about them.

"Nothing new," Seligman wrote Weil in a confidential email. "Should not be shared beyond you."

"Understood," Weil replied.

## "Why is everyone freaking out... what is the big deal?"

THE FALLOUT from Loeb's campaign caused widespread unhappiness at Sony Pictures. At Investor Day, with flat profits projected for the movie business, Lynton promised "a significant shift in emphasis" to the studio's real moneymaker: television. Driven by hits like *Breaking Bad* and *Blacklist*, syndication, and a growing portfolio of overseas channels, TV was already producing more than half the studio's operating profit. Sony was projecting that figure to climb to 75% by 2018.

Pascal was beside herself at the resulting coverage in the trade press, according to leaked emails: that TV was now paramount, that her job was in jeopardy, and—in a *Hollywood Reporter* story—that she had only recently parted ways with a personal assistant paid "well over" $250,000 a year. (Actually, it was $300,000.) "This is truely the most ridiculous inaccurate article I have ever read"... "absurd"... "so stupid"... "insane," she vented in a series of emails to Sony executives, industry friends, and family. "I dont get whats going on," she wrote Lynton. "Why is everyone freaking out... what is the big deal?"

"Because we said no cost is too small," shot back Lynton. "An assistant paid that amount suggests a lack of controls. We claim to have those controls."

"Michael all the stories are about how we are concentraing on tv and how you have ultimate greenlight authoruty... it was two fucking movies... how long does this go on?"

"Until we can show a real turn around or they focus on the next studio," Lynton replied.

The executives running television, who reported to Pascal, also felt maligned. Mosko, a yoga-practicing fitness buff who had been at Sony for two decades and rebuilt its TV business, accused Pascal and Lynton of supporting a "personal attack" in the media on him and his group. In a February email to Pascal, he wrote, "I've always delivered for you guys... and getting thrown under the bus and treated like the help... it's fucked up." Mosko vented to Lynton, too, after the CEO scolded him about startup costs for new shows. "I feel a ton of hostility coming my way and I'm not sure why... every year we find a way to deliver... and then some..."

In late summer Lynton even came to suspect the TV chief was attempting a power play. "Steve Mosko is actively campaigning to be made COO of SPE," he advised Seligman, then vacationing in Prague. "Steve/COO? Oy," she replied.

Lynton, facing growing pressure to boost profits, wasn't happy either. "Work has been very taxing lately," he confided to a friend in November 2013. "All a bit more than I signed up for, but I will persist..."

After a decade as CEO and uncertain of his future after the departure of Stringer (who had hired him), Lynton had already begun exploring opportunities to leave. In early 2013 he had two conversations with Time Warner CEO Jeff Bewkes about running the Warner Bros. studio. Then, in October 2013, Ilene Nagel, a Russell Reynolds headhunter advising Tulane University on its search for a new president, contacted Lynton about the job. Although Lynton lacked a Ph.D. and had never been an academic, he agreed to fly to New Orleans to meet with the search committee. Before that could happen, Nagel informed Lynton that Tulane had canceled after deciding that his lack of traditional credentials would make it a "challenge for you to gain acceptance."

By then Lynton was pursuing a third position: as secretary of the Smithsonian Institution, its top management job. Lynton met with Smithsonian board members on Jan. 8, and Nagel emailed him a "hugely confidential smiley" the next day.

"Wow. Great news!" Lynton replied.

INSIDE THE HACK OF THE CENTURY

"Mum's the word," she advised.

Once again, though, it didn't work out. In February he got word from Nagel that the board had "opted for the more traditional candidate."

In his most concerted effort to leave, Lynton spent more than a year pursuing the presidency of New York University, being vacated in 2016, when Lynton's Sony contract was up. In November 2013, after a meeting with John Paulson, a hedge fund billionaire on the NYU board, Lynton agreed to submit a letter promoting his candidacy. With editing suggestions from relatives and friends—including *New Yorker* writer Gladwell—he drafted a three-page pitch in December. "While I may not at first glance be a logical candidate to be the next president of NYU, I think that on closer inspection my qualifications for

Sony Corp. CEO KAZUO HIRAI (above left) tried to shake the company from its "crisis." Inset: Hirai, then overseeing Sony's PlayStation business, bowing in apology in 2011 after a damaging hack.

ETHAN MILLER—GETTY IMAGES; INSET: SHIZUO KAMBAYASHI—AP

the position are excellent..." Lynton wrote. He touted his experience "managing disruptive, egotistical, and difficult personalities who are very talented, driven, innovative, and stubborn. It is not that very different from the academic environment of a university."

Lynton would continue to campaign for the position during 2014. In August he met with attorney Marty Lipton, NYU's board chairman, who bluntly advised him that he was a "long shot." Lynton didn't take the hint, telling Lipton he would still "very much like to put my name forward for the position." In September, Lynton met with billionaire Ken Langone, another member of the search committee.

Meanwhile the pressures at Sony Pictures intensified. Sony was counting on big box-office numbers from the latest installment of *Spider-Man*, its biggest franchise, whose previous four films had grossed a combined $3.25 billion. (Lynton invited Loeb to the New York premiere but instructed his staff to make sure that the investor's seats be "nowhere near Amy or me.") But at $709 million in worldwide ticket sales, *Amazing Spider-Man 2* disappointed; Sony had projected $865 million. An outright flop came two months later, with the comedy *Sex Tape*. "I think it kills the year," Lynton emailed Pascal, as the depressing results arrived. "We keep putting our heads in the sand. I fear that this may just be one too many."

## "Totally floored by this movie. And by you."

EVEN AS SONY'S film business struggled through another rocky year, Pascal hoped her skill at building relationships with emerging stars would help turn things around. Seth Rogen was perhaps her favorite.

Rogen and his collaborator Evan Goldberg had been making profitable movies with Sony since 2007, starting with *Superbad*, which they had written as teenagers in Canada. The pair's hits included *Pineapple Express* and *This Is the End*. By early 2014, Pascal was working to line up Rogen for three more Sony projects. *The Interview*, which Rogen and Goldberg had directed and already filmed, was set for wide release on Oct. 10, 2014.

Rogen didn't always plan a comedy about a plot to kill the actual ruler of North Korea. Early scripts employed a fictional character named Kim Il-hwan, according to *Interview* screenwriter Dan Sterling. He maintains it was a studio executive (he declined to give the person's name) who originally suggested using Kim. Rogen and Goldberg loved the idea. Unlike, say, China, an important film market and thus one Sony didn't want to alienate, North Korea was regarded as fair game for provocative material in Hollywood. Pascal and Lynton blessed this change.

In hindsight it's easy to second-guess this decision. North Korea is a rogue state (with nuclear missiles) led by a volatile, unpredictable dictator. "Why is it necessary to name Kim Jong-un?" a filmmaker who has worked with Sony asks *Fortune*. "Is it going to mean that much more at the box office? If you're doing a serious film it's one thing. But it's a fart movie!"

The plot of *The Interview* is now well known. A doltish tabloid talk-show host played by James Franco and his bosom-buddy producer (Rogen)

are invited to North Korea to interview Kim Jong-un, who's a secret fan of their program. The CIA then enlists the pair to assassinate Kim. Some laughs ensue. It all ends with Kim's fiery death in a helicopter, which Franco's and Rogen's characters gun down from a commandeered tank.

*The Interview* cost $44 million to make ($8.2 million went to Rogen) and had a $32 million marketing budget. Sony had hefty box-office expectations for the R-rated comedy: $100 million to $135 million. The movie featured tigers, military hardware, and expensive special effects. Even Rogen marveled at the latitude he'd enjoyed, telling *Rolling Stone* before its release, "They're giving us insane amounts of money to do whatever the fuck we want."

Given the pair's commercial success, Sony was deeply motivated to keep Rogen and Goldberg happy and on the studio lot, where they worked out of a suite of offices and strolled the grounds smoking weed. "We love your movies and frankly yours is the most important relationship we have," Dwight Caines, Sony's president of theatrical marketing, told Rogen in an email. Test screenings for *The Interview* were strong. "Totally floored by this movie. And by you," Pascal wrote Rogen and his team in April. "Thanks for letting us make it," Rogen replied. "Nobody else would do that."

Rogen and his collaborators seem to have genuinely wanted to make a statement about the loony and oppressive ways of the Kim regime. "I was thrilled by the opportunity to make a mass appeal studio movie with a bit of political commentary in between the dick jokes," says Sterling. Sony executives seemed onboard. "The movie is doing something bold that I'm not sure any other movie has done before—taking on as its subject matter a real persona of this notoriety," Caines wrote Rogen in May. "This is the kind of angle that makes this notable... fun with a dash of smarts."

## We will take "a merciless counter-measure."

ON JUNE 17, leaked emails show, Sony's appetite for mocking a "real persona" instantly diminished. Days after the film's first trailer appeared online, Hirai, who had just screened the movie, called Lynton, concerned about roiling already fraught relations between Japan and North Korea. As Hirai saw it, this made *The Interview* dangerous fare for a Japanese company.

From left: actor JAMES FRANCO, co-director EVAN GOLDBERG, and co-director and actor SETH ROGEN on the set of *The Interview*

ROGEN ON SET AND *THE INTERVIEW* STILL: ED ARAQUEL—COLUMBIA PICTURES/COURTESY OF EVERETT COLLECTION

Lynton scrambled, first by yanking the trailer from the Internet for re-editing. As part of Hirai's One Sony initiative, the studio had just added the Sony logo to the credits for all films released under the studio's brands, which include Columbia Pictures, TriStar, and Screen Gems. Now orders went out to erase "Sony" from everything associated with *The Interview* in an attempt to downplay its Japanese parentage. Plans for a limited Asia release were also scrapped. "Have to keep whole interview thing under wraps," Lynton told Pascal.

That wouldn't be easy. Within days a North Korean government spokesman warned that *The Interview*'s release would represent "the most blatant act of terrorism and war," and threatened "a merciless counter-measure." (The government later filed formal complaints with the White House and the United Nations Security Council.) North Korea has long been known for its threats against other countries, but most have turned out to be mere bluster.

Still, the Kim regime had been widely blamed for a series of cyberattacks, especially against its arch-enemy, South Korea, and was believed to employ a


From top: a scene from *The Interview*, with the movie's Kim Jong-un at right; the scene outside one theater in Los Angeles on opening night, Dec. 25, 2014

THEATER: JUSTIN BAKER—WIREIMAGE/GETTY IMAGES

cadre of several thousand army hackers. The worst incident had occurred in March 2013. Known as the DarkSeoul attack, it caused $700 million in damage to South Korean banks and broadcasters, freezing ATMs and erasing the hard drives of 30,000 computers. The hackers in this episode, which received considerable press coverage in the U.S., posted a notice featuring images of skulls.

Yet Sony Pictures executives were caught off guard by the growing storm over their film. They tried to assess the danger. Reached in Europe after Hirai's call, studio executive Doug Belgrad advised Lynton that he was now "doing the homework on whether there is precedent on depicting and/or killing a living leader on film." Emails show Lynton tapped his personal network, conferring informally with two outside experts. (Rogen brushed it all off with a jocular tweet: "People don't usually wanna kill me for one of my movies until after they've paid 12 bucks for it.")

In a written statement on behalf of Lynton, Sony spokesman Lawson insists that the "extremely knowledgeable" experts the CEO consulted "gave no hint or warning of the possibility of a cyberattack." Indeed, one expert Lynton spoke with, Daniel Russel, assistant secretary of state for East Asian and Pacific affairs, made no mention of hacking risk, according to a note Lynton prepared memorializing their conversation.

But Lynton got a different message from the expert he consulted most extensively. Bruce Bennett, a North Korea specialist with the Rand Corp.—where Lynton serves on the board—says he did warn the Sony CEO that a cyberattack was "a possibility."

After watching *The Interview*, Bennett sent him a three-page memo assessing the situation even before the Koreans began protesting the film, then had several follow-up exchanges with Lynton. Bennett advised him that the North Koreans frequently made empty threats, and there probably wasn't much to fear.

Bennett's memo noted the likelihood that North Korea would probe Sony's computer systems: "Even if North Korea doesn't know about the film yet, as soon as they do find out about it, they will likely explore Sony's computer systems to see if Sony is ready to deal with North Korean criticism." (The memo was not retrievable from the hacked documents; Bennett read the passage to *Fortune*.)

In their follow-up conversations, Bennett says, he went further. He says he told the CEO that the Kim regime employed hackers "who could potentially cause damage," described the DarkSeoul episode, and counseled: "You need to realize something could happen in that area." Lawson denies this: "If [Lynton] had received any kind of warning, his next call would have been to a cyberexpert to ask about it... In their many phone conversations, Bennett never mentioned the possibility of a cyberattack on the studio..."

Rogen and Goldberg also received warnings of a possible cyberattack, according to their spokesman, Matt Labov. Even before they began shooting the film the pair sought the advice of Rich Klein, whose Washington, D.C.–based consulting firm, McLarty, advises Hollywood on sticky geopolitical problems. After reading their script, Klein tells *Fortune*, he advised the filmmakers to expect North Korean "blowback," possibly in the form of an electronic assault. He urged them to change their banking and email passwords and closely monitor their Internet accounts, and passed on the name of a cybersecurity adviser.

Klein says he also feared that North Korea might unleash a cyberassault on the studio to try to block *The Interview*'s release. Rogen and Goldberg relayed that message to Sony executives, according to Labov. "We felt that everybody involved in this had to protect themselves—the studio and the filmmakers," says Klein. "The North Koreans are pretty aggressive cyberwarriors... It's just surprising to me that there wasn't a more robust sense of alarm and caution." (Sony's spokesman also denies receiving a warning from Rogen and Goldberg.)

Instead of hardening its network defenses, emails show, Sony focused on somehow trying to offend the North Koreans less. Their actions befit a Hollywood farce. Never mind that Sony was planning to release a film that portrayed the violent death of a real head of state; the company spent $550,000 to digitally alter the movie's images of Kim family members shown on a wall mural and jacket pins worn by movie characters. It banished marketing materials for *The Interview* from Sony websites. And the studio prepared a statement insisting the movie was "a fictionalized comedy that is not in any way related to current events."

In early August, Pascal departed with her family for a long vacation through Asia. Lynton decamped to Martha's Vineyard. By then they'd decided to postpone *The Interview*'s release until Christmas Day, buying time to tackle another issue. On Hirai's orders, studio executives had begun a three-month battle with the filmmakers to soften the movie's gory climactic scene, in which a tank shell strikes Kim's helicopter and kills him in a slow-motion, head-popping, flesh-dripping ball of fire.

The *Hollywood Reporter* caught wind of this, Sony Pictures PR executive Jean Guerin advised Pascal and other executives in an email. It was preparing to report that "Corporate Sony" had asked for "a few key edits," including "that the melted face of Kim Jong-un will now be taken out of the final cut..." The studio denied that changes were being made in response to outside pressure. "We are dismissing [the reporter's] premise and letting her know off the record that this is normal/what happens in the filmmaking process," Guerin told the executives.

The article, which appeared on Aug. 13, suggested that Sony was changing the movie to appease the North Koreans. Rogen was livid. As he saw it, this painted him as a sellout. Executives convened an emergency call to plan damage control. Asked to join the session, Lynton said he was at a dinner on Martha's Vineyard and couldn't get up to leave. "I am sitting between president obama and Hillary Clinton... If we need a change of strategy then I don't want anything done until we speak."

Hirai and Lynton, who found the movie more offensive than funny, wanted the "head-popping scene" eliminated entirely. "We cannot be cute here," Lynton wrote in one email. "What we really want is no melting face and actually not seeing him die." But Rogen was fiercely resisting major changes in what he called the "awesome" shot.

Sony had final authority over the editing of the movie. But according to interviews and leaked emails, the studio feared that if it imposed its will, Rogen would disassociate himself from the film, creating a box-office and PR debacle. "This movie is supposed to be controversial," he emailed Pascal. "That was your pitch to us amy. There's nothing controversial about a movie that has been tempered to appease the very people it's mocking." (Rogen barraged Pascal, then vacationing through Vietnam and Bali, with messages, insisting they talk "as soon as humanly possible." Pascal forwarded one email to a colleague, asking, "Can I be lost in the jungle?")

On Sept. 25, Pascal, back in L.A. and sitting in tem-

ple on the Jewish New Year holiday, emailed Rogen an emotional personal plea to make the scene "a little less gory." "No one has backed you more than I have," she wrote. "And this isn't some flunky it's the chairman of the entire sony corporation who I am dealing with. You must know there are very few relationships and film makers I would let myself be in this situation for."

Rogen relented, agreeing to reduce Kim's "flaming hair by 50%," cut "three out of four of the face embers," and alter "the color of the head chunks to try to make them less gross." On Sept. 28, after viewing the new version, Hirai gave his blessing, according to emails, with the understanding that the scene would be removed entirely from any overseas release. Plans to release and promote *The Interview* moved forward. "I would love working for you and Sony no matter what you decided," Pascal emailed Hirai, "but I just needed to tell you how important this was for me and the studio Thank you for being an amazing leader and a very cool boss With much gratitude and devotion Amy."

## "From a single injection, we accessed EVERYTHING."

LOOKING BACK, it's hard to understand how Sony Pictures could have been so ill-prepared for an electronic invasion. It was part of a tech company that sells digital products—films, TV shows, videogames, and music—readily subject to online theft. Angered by Sony Corp.'s heavy-handed tactics to protect intellectual property, hackers have long targeted the company's various divisions. Says cybersecurity guru Bruce Schneier, a fellow at Harvard's Berkman Center for Internet and Society: "Sony is a company that hackers have loved to hate for 10 years."

This dates back to the "rootkit scandal" of 2005, when Sony's music division, seeking to combat piracy, manufactured millions of CDs that surreptitiously installed software on users' computers that blocked illegal copying—but also spied on their listening habits, slowed their PCs, and created security vulnerabilities. After a tech blogger exposed this, Sony faced state attorneys-general lawsuits, class-action cases, and Federal Trade Commission charges (later settled). The episode outraged consumers—especially privacy-sensitive hackers—who urged a boycott of Sony products.

In the years that followed, the antagonism only grew. In 2011, Sony launched what became known as its "war on hackers." Citing copyright and computer fraud laws, the company sued a celebrated 21-year-old hacker named George Hotz (a.k.a. "geohot") for "jailbreaking" his PlayStation 3 console so it could run pirated games and free software, then posting a video showing how to do it. Sony even subpoenaed server logs showing who had visited Hotz's website. The company sued a second hacker in Germany; police raided his home and seized his computers.

Blowback swiftly followed. In April hackers, declaring this crackdown "wholly unforgiveable," breached Sony's PlayStation Network and exposed personal information for 77 million customers and credit card records for 10 million of them. The episode forced Sony to shut down its network for 24 days and cost it $171 million. In congressional testimony, Tim Schaaff, the chief of Sony's PlayStation Network, used language that was strikingly similar to what Sony Pictures would employ years later: The company, he insisted, had fallen victim to a "highly sophisticated" breach, "unprecedented in its size and scope," despite "very, very strong" security.

Outside experts disagreed. They concluded that shoddy IT practices, including a failure to install software security updates, left Sony wide open. British regulators later fined the company the equivalent of $396,100 for failing to protect private information, saying the breach "could have been prevented" and calling Sony's security measures "simply not good enough." The company blamed the episode on Anonymous, but the group—which has taken responsibility for other hacks—insisted it had been framed; the guilty party was never determined.

Before 2011 was out, various Sony businesses suffered 20 more breaches, making a mockery of the company's claims of strong defenses. Sony Pictures fell victim in June, when LulzSec, an Anonymous splinter group, broke into its network using a simple technique and revealed personal information for some customers. LulzSec boasted that it had obtained information on a million Sony customers and had invaded just to show how easy it was: "From a single injection, we accessed EVERYTHING. Why do you put such faith in a company that allows itself to become open to these simple attacks?" Sony's defenses were viewed as so pitiful by Internet bloggers that they inspired a derisive term: "Sownage," as in "being totally owned like Sony."

SETH ROGEN

"THERE'S NOTHING CONTROVERSIAL ABOUT A MOVIE THAT HAS BEEN TEMPERED TO APPEASE THE VERY PEOPLE IT'S MOCKING," ROGEN WROTE AS HE RESISTED CHANGING *THE INTERVIEW.*

MICHAEL TRAN—FILMMAGIC/GETTY IMAGES

In the aftermath of the PlayStation attack, Kaz Hirai, then presiding over Sony's gaming and consumer products businesses, formally bowed in apology at a Tokyo press conference. He vowed new measures to toughen cyberdefenses across the company. In September 2011, Sony Corp. also announced the hiring of its first global chief information security officer, former Department of Homeland Security cybersecurity czar Philip Reitinger.

**"I will not invest $10 million to avoid a possible $1 million loss."**

IT'S NOT KNOWN precisely what new safeguards Sony Pictures implemented in the wake of Hirai's promises; the company declined to provide examples. But it's painfully clear whatever steps it took weren't enough.

The studio's email system, for example, didn't employ a fundamental protection called two-factor authentication, which many companies have used for years. This requires anyone logging in to use two forms of identification—for example, a personal password and a one-time password randomly generated on a mobile phone or electronic key-chain fob—making it far harder for hackers to steal a user's identity.

Lax email practices weren't new at Sony. In a 2007 article titled "Your Guide to Good-Enough Compliance" in *CIO*, a trade publication for IT professionals, studio cybersecurity chief Spaltro told the writer how an auditor, citing Sarbanes-Oxley requirements to protect personal info, had warned him that Sony had multiple security weaknesses, including lax password procedures. "If you were a bank, you'd be out of business," the auditor told him. Spaltro talked the auditor out of noting the deficiency, according to *CIO*'s phrasing, by arguing "that if his people had to remember those non-intuitive passwords, they'd most likely write them down on sticky notes and post them on their monitors. And how secure would that be?"

Spaltro seemed more afraid of the costs than the risks. "We literally could go broke trying to cover for everything," he told *CIO*. "I will not invest $10 million to avoid a possible $1 million loss," he reasoned. "It's a valid business decision to accept the risk." Although Spaltro's statements were made eight years ago, before Sony became the prominent repeat target of hackers (and he insisted "Sony is over-compliant in many areas"), there's little sign the company's attitude changed.

Pascal was known for her close relationship with actors, producers, writers, and others. "I adore you, Amy," wrote GEORGE CLOONEY. "You are literally the only person running a studio that loves film."

CLOONEY, SMITH, MAGUIRE, WITHERSPOON, AND DAMON: KEVIN WINTER—GETTY IMAGES

There was a litany of laxity. Sony's email-retention policy left up to seven years of old messages on servers, unencrypted and ripe for the taking. The company was essentially using email for long-term storage of business records, contracts, and documents saved in case of litigation. When Sony announced plans, in the fall of 2014, to reduce how long emails would be stored to two years—to make the system run better, according to emails, not because of hacking risk—howls of protest erupted at the studio.

An array of sensitive information—including user names and passwords for IT administrators—was kept in unprotected spreadsheets and Word files with names like "Computer Passwords." Sony's IT team had difficulty keeping track of all the hardware in its network, which included 30 data centers. In the fall of 2013, while transferring studio security monitoring from an outside vendor to a corporate Sony team, one firewall and 148 routers, switches, and web servers

Pascal with (clockwise from top left) actors WILL SMITH, JENNIFER ANISTON, and ADAM SANDLER, producer SCOTT RUDIN, agent BRYAN LOURD, actors MATT DAMON, REESE WITHERSPOON, BRAD PITT, and (center) TOBEY MAGUIRE

ANISTON AND SANDLER: CHRISTOPHER POLK—GETTY IMAGES; PITT: LESTER COHEN—WIREIMAGE; RUDIN: JEAN BAPTISTE LACROIX—WIREIMAGE/GETTY IMAGES; LOURD: ARAYA DIAZ—GETTY IMAGES

were left unwatched for months, according to a September 2014 PricewaterhouseCoopers audit included among the hacked documents. "As a result, security incidents impacting these network or infrastructure devices may not be detected or resolved timely," the report noted. Over a 10-month period, according to the audit, the corporate team had alerted the studio to 193 security "incidents."

In August 2014, Reitinger, the executive who had been hired to harden Sony Corp.'s defenses, quit as global chief information security officer. A Sony spokesperson says his departure was "long planned and not a surprise." Emails at the time paint a different picture. "Was this a surprise?" Sony Pictures general counsel Weil wrote security chief Spaltro. "Yes," he replied.

Reitinger, an advocate for stronger security during his time in government, declined requests for an interview. But his many admirers in the field believe he didn't accomplish more at Sony because he lacked adequate authority (the company disputes this) and because Tokyo didn't pay enough attention. Even today, they say, it can be hard for an American to wield significant influence in Sony's Tokyo headquarters. Says cyber-expert Lewis: "He felt a little frustrated."

## "We are just not making enough money."

BIG SONY'S WOES just kept getting more dire. In May 2014, after announcing a projected $489 million loss for the fiscal year ending the following March, Hirai disclosed that he and 40 other top executives would again forgo their annual bonuses. (Lynton wrote the CEO, offering to forfeit his own bonus "to show solidarity." Much to his relief, Hirai declined the offer. "He gave me the bonus, the bet paid off," Lynton exulted in an email to a friend.) In September 2014 the company revised its projections dramatically downward. The company now expected a $2.1 billion loss.

Lynton was feeling stress. On Oct. 3 he emailed Pascal: "We are virtually a public company and we have made promises to Sony and the street as to what we will deliver for the next three years. I did not want to be in this situation, but events have overtaken us and so here we are. It is therefore very very important that before we take risky or marginal bets in a given slate we have a rock solid foundation to build on... I am about to go next week and make some big promises to Sony and we have to deliver on them... I am only saying all this so you understand the enormous pressure I am under and why I really don't have much patience at the moment." Five days later he emailed Pascal from budget sessions with Hirai in New York: "Meeting pretty rough... We are just not making enough money... Too much overhead. Not enough hits."

The emails suggest Lynton was going through a trying period. "Work is drudgery," he wrote a friend in September. He told another, "I haven't read a script in a month... A weird block that I can't explain." Lynton seemed more excited about his personal investment projects, which included Snapchat (he and his wife had provided seed money, and Lynton served on the board) and a scheme to develop a Breathalyzer-type device for detecting marijuana use. Emails show he pitched billionaire Dr. Patrick

Soon-Shiong on this "very commercial idea" and wanted to patent the concept. ("Michael Lynton spent minimal time on these outside interests," maintains Sony's spokesperson.)

Lynton was also wrestling with chronic insomnia and a bad back, along with the latest in a series of tax audits in California. (Sony's Lawson says there is "absolutely no connection between work pressures and any assumptions you are making based on stolen emails about Michael's medical conditions or personal tax matters.") Unbeknown to anyone at Sony, Lynton was also making plans to move with his family back to New York.

On Oct. 21, Sony finally got some good news. After a rise in Sony stock, Loeb had sold his stake at a profit of nearly 20%. He had remained in friendly mode for months, visiting Culver City for a private lunch with Lynton and other executives, dining with Seligman, and sending his hopes that Hirai had enjoyed his summer vacation in Hawaii. Publicly, Sony had treated Loeb as a respected investor who had raised helpful "concerns." But when he exited, there was unabashed delight. "Champagne for all!!!!" declared CFO David Hendler.

While Lynton was angling to leave, Pascal grew increasingly anxious over slow-moving negotiations for a new contract to stay. Her agreement was set to expire in March 2015. "You know ml will be as rude as possible and try and make me feel AKWARD instead of loved...," she complained to Hollywood agent Bryan Lourd. "Tell me how to approach ml differently. Read art of war?"

She was already working with studio deputies and "vision" consultants to develop a plan to upgrade the anemic film pipeline. "I guess I [am] mad at him because this is our company and in some level I still think they are interlopers who are destroying it," she emailed studio president Belgrad on Nov. 12. "Isn't that silly? But I can tell you one thing. We will be there one way or another when everyone else has gone. I don't know if that is good or bad but I know it's true."

## "There weren't any extreme hurdles in place."

FBI DIRECTOR JAMES COMEY has said he believes Sony's cyberattackers first breached the studio's network in September, gaining access through a common tactic called "spear phishing"—duping an employee into clicking on an email attachment or a web link.

Sony's traditional virus-detection programs provided no protection from the hackers' malware, since they block only previously identified attacks, and hackers know to make small changes in their code. Indeed, it's now accepted wisdom in the cyberworld that attackers can penetrate the perimeter defenses of almost any company.

What's critical is detecting the intruders quickly, before they can do much damage. According to a 2015 report by Mandia's company, it typically takes a company 205 days to discover it has been penetrated, and less than a third of companies detect the breach themselves. This doesn't mean it's impossible to stop attacks; it's evidence that most companies haven't embraced the right precautions.

Once inside, the Sony attackers' next step was to "escalate privileges"—to gain wide access by stealing the credentials of system administrators. For more than two months Sony's hackers roamed freely, identifying what they wanted to steal. This was possible because the studio, with few exceptions, didn't segregate or provide extra security for even its most precious secrets. In effect, once the invaders made it past the network gates they could go anywhere they wanted because Sony hadn't locked any doors—much in the way that the company had left its information security department open and unattended.

It's "astounding" that the Sony hackers were able to remove so much without being noticed, says J. Alex Halderman, a University of Michigan computer science professor. Most corporate networks employ intrusion-detection software, which is designed to sound alarms about unusual file transfers—big files sent to strange places at unusual times—or odd behavior by system users accessing stuff they don't usually touch. This has fed suspicions that the Sony attackers had inside help providing access to its system—that someone downloaded its secrets onto portable hard drives (as Edward Snowden did at NSA), rather than sent them through the Internet.

Kevin Mandia, the prominent forensic expert Sony hired to investigate the hack, insists there is no evidence of that. The hackers, he contends, escaped detection by patiently moving data out in chunks over several weeks from different company servers to various attacker-controlled locations

INSIDE THE HACK OF THE CENTURY

MICHAEL LYNTON

LYNTON ARGUES SONY WAS BLAMELESS, INSISTING IT WAS "EXTREMELY WELL PREPARED FOR CONVENTIONAL CYBER-SECURITY" BUT FACED "THE WORST CYBERATTACK IN U.S. HISTORY."

LYNN GOLDSMITH—CORBIS

around the world. As a media company, Sony routinely transfers giant files, making it harder to spot the theft.

Sony would not permit Mandia, chief operating officer of FireEye, to be interviewed by *Fortune*, allowing him to provide only a brief written statement. Sony has often cited a note Mandia provided to Lynton that asserts that no company could have been "fully prepared for" the attack. But that note was carefully worded. For example, it notes that "industry standard antivirus software" wouldn't have detected the malware. That's not saying much. To a cyberexpert, traditional antivirus protection offers the hacking equivalent of being able to repel a musket ball when today's villains are firing AK-47s.

Indeed, several cybersecurity vendors—including FireEye—claim their products would have prevented (or at least dramatically reduced) the devastation at Sony. Says FireEye spokesman Vitor De Souza: "If they had our solution, we probably would have spotted the malware used in the attack." De Souza says two-factor authentication also would have made a big difference at Sony. "It creates a big hurdle of the attackers," he says. "If you don't have two-factor authentication and they penetrate your network, you're in big trouble." If blocked, De Souza acknowledges, hackers might have employed other methods. "If a state actor wants to get in, he'll get in," he says. "The question is, How fast do you respond? Instead of, say, taking 10 terabytes of data, they might have gotten one."

After pilfering Sony documents, the invaders turned to swiping emails for five top studio executives; the most recent messages are dated just two days before the hackers detonated their attack. By that point they had stolen seven sets of credentials for system administrators and mapped the studio's entire network. This information was "hard-coded" into the destructive malware, allowing it to infect all the computers those IT managers were authorized to touch.

On Monday, Nov. 24, the attackers unleashed their customized wiper malware—igfxtrayex.exe—into Sony's network. On each machine the malware reached, it deleted everything on the hard drive while installing the threatening web page, with its skeletal imagery and warning. Anyone already logged in helplessly watched their files disappear. The malware also erased the software instructions that tell the computer how to operate. Two hours later the computer would restart to display another chilling message: "Operating system not found."



To avoid detection the hackers immediately exited Sony's network after launching their destruction. The malware reported back to "command and control" servers out in cyberspace, allowing the intruders—wherever they were—to tally up their digital toll. Hackers typically use the simplest means necessary to accomplish their mission, and experts say there was nothing particularly sophisticated about the Sony attack. Ed Skoudis, a "white hat" hacker who teaches cyberdefense testing for corporate IT security professionals at the SANS Institute, says the skill level deployed at Sony looks "pretty average." He puts its perpetrators on par with students in his mid-level classes. "It shows the defenses of Sony were not particularly good," says Skoudis. "I didn't see the bad guys jumping over any extreme hurdles, because there weren't any extreme hurdles in place."

What *was* extreme was the destruction.

## "Pay the damage, or Sony Pictures will be bombarded."

FROM THE OUTSET, the management and employees at Sony Pictures didn't have a clue as to what hit them—or what was on the way. The studio's initial public comment on Nov. 24 was a marvel of understatement: "We are investigating an IT matter."

The invaders had spelled out their intentions in the scrolling text that accompanied the scarlet skeleton. "Hacked By #GOP," it read. "We've already warned you, and this is just a beginning. We continue till our request be met. We've obtained all your internal data including your secrets and top secrets. If you don't obey us, we'll release data shown below to the world."

Exactly what "obey us" meant wasn't clear. The initial message from the hackers, who later identified themselves in emails to selected reporters as the "Guardians of Peace," also praised another group: "Thanks a lot to God'sApstls contributing your great effort to peace of the world."

As it turned out, "God'sApstls" had emailed Lynton, Pascal, and three other Sony executives three days before the attack, demanding a payoff. "We've got great damage by Sony Pictures. The compensation for it, monetary compensation we want. Pay the

damage, or Sony Pictures will be bombarded as a whole. You know us very well. We never wait long. You'd better behave wisely." The menacing messages did not specify how much of a payoff was being demanded. Sony executives forwarded the email to the FBI, according to spokesperson Lawson.

Neither "God'sApstls" (which was never heard from again) nor the GOP had mentioned *The Interview*.

Hours after Sony's computers went dark, Nicole Seligman notified the FBI. That afternoon a team of agents from the agency's Los Angeles cybersquad arrived on the lot. Sony also retained forensic investigator Mandia.

Inside Sony Pictures, employees were left to work with pens and paper. The studio issued 190 BlackBerrys to key employees. Shops on the lot took only cash. "It is possible that some or all of this disruption will continue over the Thanksgiving Holiday," the studio advised them. "We appreciate your efforts to find work arounds."

Then, starting on Dec. 1, after again alerting reporters through emails, the hackers began dumping heaps of stolen documents, many of them deeply personal, onto file-sharing sites. The first batches included confidential performance evaluations, family medical records, criminal background checks, disciplinary memos over workplace affairs, passport information, and salary details for everyone at Sony. The studio had maintained little control over even sensitive information prized by identity thieves. Analysis by a data protection firm called Identity Finder found, for example, that Sony had left Social Security numbers for 47,426 people (including many who hadn't worked at the company for years) in more than 600 files lacking password protection or encryption.

More dumps followed, one every few days, each triggering a new crisis as reporters pored through Sony's business and, especially, its dirty laundry. "It was a nightmare," says one executive working on the studio lot. "Just when you think you'd gotten over one—it was starting to get quiet and calm—boom, you'd get hit with something else that was even crazier."

Pascal's email exchanges with producer Scott Rudin proved especially cringeworthy and were widely disseminated in the press. They included nasty comments about celebrities like Angelina Jolie (Rudin called her a "minimally talented spoiled brat"); insensitive banter about President Obama's presumed taste for black-themed films ("Should I ask him if he liked DJANGO?" she wrote); and knockdowns over their film deals ("Do not fucking threaten me," Pascal warned Rudin at one point. As she routinely did, Pascal forwarded this last exchange to Lynton, who scolded: "You are both crazy to put this in an email.")

After the embarrassing headlines, Pascal issued a public apology, then sought forgiveness in meetings with Sony employees and the Rev. Al Sharpton, who had threatened to demand her head over the Obama comments. "I feel like I've been raped," she privately told a studio visitor. "And I was blamed for it."

Sony tried vainly to bottle it all up. In mid-December the studio retained attorney David Boies, who warned 40 media organizations (including *Fortune)* not to use the stolen information or they would be held "responsible for any damage or loss." Boies asserted the documents were, variously, "private," "confidential," and "trade secrets," and protected under an array of U.S. and foreign legal doctrines. Many news outlets, including the *Wall Street Journal*, Bloomberg, and Reuters, published articles using the emails nonetheless. (Boies even wrote Twitter, seeking to shut down Val Broeksmit, leader of an indie band called Bikini Robot Army, whose tweeted screenshots of hacked Sony emails had won him 19,000 followers. Twitter suspended his account for just a day. Broeksmit, who was contacted by Boies, blew him off.)

That was all a sideshow. Sony's biggest problem was *The Interview*. The media first raised the prospect that North Korea had hacked Sony because of the film on Nov. 28, four days after the attack. The GOP made no reference to *The Interview* until Dec. 8, when it demanded that Sony, having "refused to accept" its previous terms, "stop immediately showing the movie of terrorism." Rogen and Franco, meanwhile, had continued their promotional tour, maintaining the studio's line—as Rogen put it on *Good Morning America* on Dec. 15—that *The Interview* "wasn't meant to be controversial in any way."

The GOP intensified its threats. It had already made ominous statements about the safety of studio employees' family members if its demands were not met. Then, on Dec. 16, the hackers, vowing a "bitter fate" for "those who seek fun in terror," claimed it would attack movie theaters screening

KIM JONG-UN

> NORTH KOREAN HACKERS HAD BEEN BLAMED FOR THE "DARKSEOUL" ATTACK IN MARCH 2013. IT CAUSED $700 MILLION IN DAMAGE TO SOUTH KOREAN BANKS AND BROADCASTERS. THE ATTACKERS POSTED A NOTICE FEATURING IMAGES OF SKULLS.

KCNA—REUTERS

the "awful movie Sony Pictures Entertainment has made. The world will be full of fear," they warned. "Remember the 11th of September 2001. We recommend you to keep yourself distant from the places at that time."

The outrageous statements, made by an anonymous group seemingly able to wield great power, had their intended effect. Fear gripped the movie world. All five big theater chains, citing security concerns but also scared of ruining their holiday box office, told Sony they wouldn't show the film. *The Interview* had been scheduled to open on 3,500 screens. Lost in the anxiety: word from the Department of Homeland Security that it had "no credible intelligence to indicate an active plot against movie theaters."

On Dec. 17, Sony issued a statement, saying it was "deeply saddened at this brazen effort to suppress the distribution of a movie" and insisting, "We stand by our filmmakers and their right to free expression." But Sony wasn't standing by the movie; it was shelving it. "In light of the decision by the majority of our exhibitors not to show the film," the studio announced, it was scrapping the Christmas release.

Lynton would later insist that the chains' withdrawal had left him with no choice, commenting: "This was not our decision." In fact, a group of at least 150 independent theaters were eager to show the movie. Tim League, CEO of Austin-based Alamo Drafthouse Cinema, says he quickly notified Sony that his 19-location chain wanted to show *The Interview,* as did other members of the Art House Convergence, made up of theaters across the country. But Sony refused to let them have it.

Late in the day on Dec. 17, when journalists asked about releasing the film through video on demand (VOD) or streaming services like Netflix—a way to bypass the threat to theaters—the studio issued a second statement ruling out any option: "Sony has no further release plans for the film."

A day later the hackers demanded that Sony also yank "everything related to the movie, including its trailers." The studio did this too, pulling TV advertising, canceling press screenings, even abandoning promotional Facebook and Twitter accounts. (Sony's spokesperson says, "This was not an effort to appease hackers. There was no national release so the prudent thing to do was to stop the marketing efforts.") *The Interview*, the press reported, wasn't to see the light of day. The hackers had won.

INSIDE THE HACK OF THE CENTURY

BARACK OBAMA

OBAMA EXPRESSED SYMPATHY FOR SONY BUT SAID, "I WISH THEY HAD SPOKEN TO ME FIRST ... WE CANNOT HAVE A SOCIETY IN WHICH SOME DICTATOR SOMEPLACE CAN START IMPOSING CENSORSHIP HERE IN THE UNITED STATES."

## "Good thing they didn't publish *The Satanic Verses.*"

IT WASN'T UNDERSTOOD at the time, but commercial considerations, not just fear, were shaping Sony's actions. With the film's hefty marketing budget mostly spent, Lynton was desperate to avoid eating a $65 million investment. He also wanted to calm panicked employees. Lynton opted not to release the movie immediately.

Hoping the big chains would reverse course (or agree to an alternative date), Sony was reluctant to permit a narrow art-house release, which would generate a pittance in box-office revenues. And if Sony moved forward with video on demand, the big chains—which insist on an exclusive viewing window—would never screen the film. The "no further release plans" statement would have reassured the chains, surely furious about rumors of VOD, buying time for Lynton to get them back onboard.

Over the 48 hours after it pulled the film, Sony again became a target, as critics from Hollywood to Washington voiced alarm that the studio had caved. "Sony's decision to pull THE INTERVIEW is unsettling in so many ways," tweeted writer Stephen King. "Good thing they didn't publish THE SATANIC VERSES." At a press conference on Dec. 19, President Obama blasted Sony, saying the studio "made a mistake." Added the President: "We cannot have a society in which some dictator someplace can start imposing censorship here in the United States."

By this point the calculus had shifted. There was no sign of movement among the theater chains. Lynton had begun secretly exploring the VOD option as a backup immediately after canceling the Christmas release. But he had no takers; online services were reluctant to make themselves the hackers' next target. Sony could have offered the film on its own PlayStation Network, but it was also worried about security. (Both PlayStation and Microsoft's Xbox Live would face cyberattacks on Christmas Day; a group calling itself the Lizard Squad claimed responsibility.)

Conspicuously absent from the media since the hack, Lynton appeared on CNN hours after the President's comments, giving the first "exclusive" interview to Fareed Zakaria, a friend of Lynton's. There the CEO insisted, "We have not caved ... we have persevered, and we have not backed down." Sony, he said, remained committed to distribut-

ANDREW HARRER—BLOOMBERG VIA GETTY IMAGES

ing *The Interview* as soon as it could find a taker. "There has not been one major VOD—video on demand distributor—[or] one major e-commerce site that has stepped forward and said they are willing to distribute this movie for us," Lynton told Zakaria.

By Dec. 24, Lynton had given up altogether on the national chains—and found takers for VOD. Sony would allow the art-house theaters—ultimately, more than 300—to screen *The Interview* on Christmas Day. And he'd enlisted both Google and Microsoft, who'd first beefed up their cyberdefenses, to air the film on their VOD platforms. Starting that day, it would be available on Google's YouTube and Google Play and Microsoft's Xbox Video. Sony initially wanted to set a premium price—$17 for a 24-hour rental, Microsoft officials say. But ultimately, the studio recognized that would be another PR mistake and cut the price to $5.99 while touting the release as evidence of "our commitment to our filmmakers and free speech."

## "Very high confidence" North Korea was to blame.

WHODUNIT? Twenty-five days after the hack, the FBI attributed the Sony attack to North Korea. The determination came extremely fast, and it was rare for the agency to identify a government as the culprit.

In a written statement and public comments, FBI officials cited similarities to the DarkSeoul episode, evidence that the Sony malware was constructed on computers with Korean language settings, Internet staging points for the attack, and—most intriguingly—intelligence from "sensitive sources and methods." At a Fordham University cybersecurity conference, FBI director Comey said he had "very high confidence" in this conclusion. (The *New York Times* later reported that U.S. intelligence, spying on North Korea, had found evidence of its role.)

Yet many experts remain unconvinced. It is easy, they note, for hackers to plant false clues. If the attackers' target was really Rogen's movie, why hadn't they mentioned it right away? How would North Koreans know what data to leak? How could they so skillfully navigate Sony's network? And why had they fallen silent after the release of *The Interview*?

"It's a dogpile," says Stuart McClure, CEO of cybersecurity firm Cylance. "'Well, that one is North Korea, and this one looks like it, so it must be North Korea.' There's no objective evidence."

Moreover, in the wake of revelations of secret government data gathering revealed by Edward Snowden, denizens of the electronic world are disinclined to take the government at its word. (The FBI has declined to make its evidence public.) Says Fordham law professor Joel Reidenberg, an information technology scholar who attended Comey's speech: "It was sort of 'Trust us, but we're not going to let you verify.'"

All this fed an alternative theory: Like an estimated one-quarter of cyberattacks, the Sony hack was an inside job. The most elaborate advocacy of this came from Norse, the firm that visited Sony to pitch its wares before the attack. Norse said its own investigation implicated a few bitter, laid-off Sony employees with IT savvy. On Dec. 29, Norse executives arrived at FBI headquarters in Washington to lay out their reasoning in a three-hour meeting. Immediately afterward the FBI issued a public statement, insisting there was "no credible information" to implicate anyone but the North Koreans.

Among the initial skeptics that North Korea was to blame: Amy Pascal, who didn't want to believe the film she backed had led to so much devastation. On Jan. 21 she met privately with Norse too, sitting down with her husband in their Los Angeles home to hear Stiansen detail his theories. Pascal later told a visitor that "for the longest time, I thought it was employees." Since then, Pascal has told friends, she is uncertain what to think. Norse officials say they now believe North Koreans pulled off the attack with "some assistance" from former Sony employees.

For Pascal, being studio chief hadn't been much fun for a while. But she wasn't ready to give it up, even after the public humiliation of having the world read her emails. After returning in late December from a family trip to Vermont, Pascal renewed her push for a new contract, which she'd told the company would be her last. She had made $47 million over the previous four years, and she wanted a comparable deal. She had been in negotiations with Sony for a new agreement since June.

But Lynton wasn't ready to move forward. After all, the film slate—the ultimate measure of Pascal's performance—hadn't met expectations for the past two years. And there was another consideration. As Lynton saw it, the events of the hack seemed to have

**SONY REVENUE BREAKDOWN BY SEGMENT (FY 2014)**


CHART SOURCE: SONY



FEEDBACK *peter_elkind@fortune.com*

traumatized her. Pascal hadn't been visible around the studio much since Christmas, an emotional time for everyone, he told others. To Lynton, this lack of leadership had irreparably damaged her standing with employees. (Pascal has privately called this account "nonsense.")

So in late January, when Pascal demanded a final answer, Lynton decided it was no. He conferred with Hirai about the move. Then, on Saturday, Jan. 31, he met with Pascal at her home. He wasn't going to offer her a new contract as studio chief, Lynton told her. It would be better for her to become a big producer for Sony, an option they'd also been discussing. According to a Pascal friend, she was "shell-shocked."

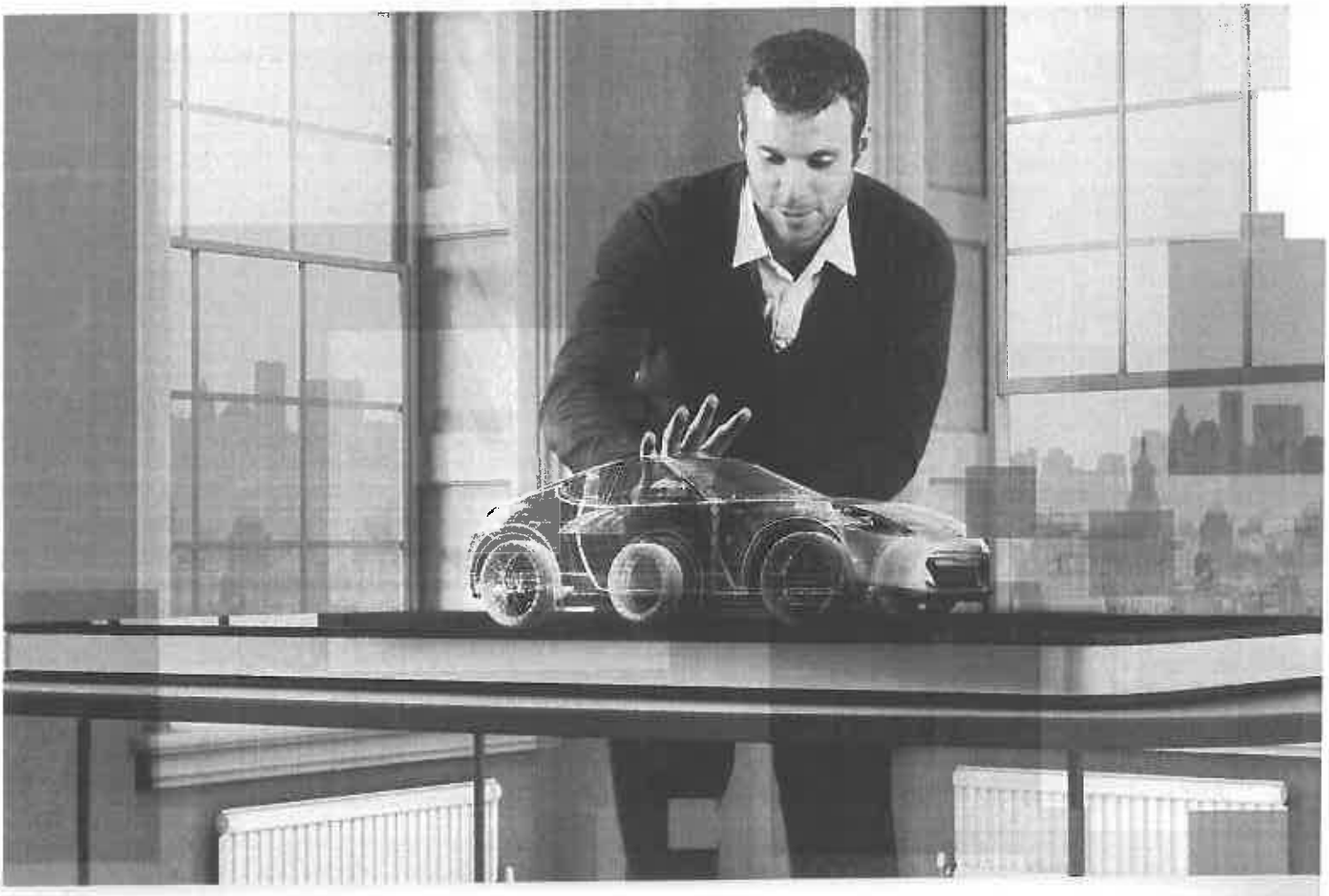
Pascal's departure was announced the following Thursday. In a press release both sides cast her departure as her decision. But at a women's conference in San Francisco days later, Pascal bluntly declared that she'd been "fired." Still, she'd enjoy a gentle landing, helping produce some of Sony's biggest films, including *Spider-Man*. Depending on how they perform, insiders confirm, Pascal's package will give her $30 million to $40 million over four years plus a percentage of the profits her movies generate. In February, Lynton named Tom Rothman, a budget-conscious former Fox chief who'd been running Sony's TriStar brand, as her replacement.



Lynton recommitted himself to Sony. He signed a contract extension in February. While his wife and daughters would be moving to Manhattan, he would commute between the two coasts. "You may have heard this rumor that I'm moving," he assured employees at an all-hands meeting on Feb. 25. "I'm not." Added Lynton: "I am here to stay."

*The Interview* made one additional bit of history. After several days on VOD passed with no calamitous consequences, other online providers, including Apple, PlayStation, then Netflix, began offering it. So far it has brought in more than $40 million on VOD, in addition to $12 million in theaters worldwide, making it Sony's biggest digital seller ever, though still a loser for the studio.

The financial calculus is grimmer if you add in the out-of-pocket costs stemming from the hack: $41 million through the end of March, according to the company. That's a bearable sum for a company of Sony's size. But there are a lot more costs to come. In



addition to expenses for investigation of the attack, IT repairs, and lost movie profits, Sony faces litigation blaming it for poor cybersecurity that exposed employees' private information. Seven cases have been consolidated into a proposed class action in Los Angeles federal court.

As Sony struggles to repair its reputation, it has also undertaken the challenge of reconstructing its blitzed computer network, this time with an array of precautions to resist—really resist—the next assault. Sony's "secure rebuild" strategy is expected to take a year, slowly returning the studio to normalcy while plugging the myriad weaknesses that its attackers so readily exploited.

The plan's premise is zero trust. It imposes precautions that Sony wouldn't previously countenance because they were too inconvenient and expensive. It's aimed at keeping bad guys out, preventing them from reaching anything valuable if they get in, and blocking them from stealing it if they do.

To resume operations safely, Sony began by building an entirely new "white network," completely segregated from the potential contagion of its old "black network." At the start Internet access was tightly restricted. Sony will keep as little information as possible on its active network; the rest will be stashed securely, encrypted and cut off from the Internet. Emails will be archived after just a few weeks. System administrators will have access only to areas required for their jobs. Employees will be barred from installing applications that aren't pre-approved. Sony will require everyone to use two-step login procedures. Firewalls will be put on the most restrictive settings. The studio will embrace an array of "next generation" cyberdefense technologies.

If implemented, it will represent a major step-up in cybersecurity for Sony. Will that be enough to prevent another cataclysm? Cyberexpert Lewis says that's the wrong question. "Think of it as a continuum of risk," he says. "You can do nothing, and you're at 100% risk. Or you can do a lot and you can get the risk down to 10% to 15%." The company was much closer to 100% risk last year and is heading much lower. That is undeniable progress. Now all Sony has to do is find a way to stop antagonizing hackers—and vindictive dictators.

*Research associates: Marty Jones and Robert Hackett*