Silver Bullet Talks with Nicole Perlroth

Nicole Perlroth covers cybersecurity for the New York Times and the Bits Blog. Before joining the San Francisco bureau in 2011, she was deputy editor at Forbes, where she covered venture capital and web start-ups. Perlroth is the recipient of several journalism rewards for her reporting on efforts by the Chinese government to steal military and industrial trade secrets.

According to rumor, the first pitch you ever did landed you on the front page of Sunday’s Post, so do tell.

Yes, at the time, I hadn’t done anything in journalism. I didn’t work for a student paper or have ambitions of being a journalist. After Princeton, I took some jobs that a lot of graduates take. I was a consultant for a little while. I worked on Capitol Hill for a little while. I worked in marketing for Coach, the handbag company, for a little while. And I just thought all of these jobs were completely mind-numbing. I just missed any kind of intellectual stimulation.

So I ended up taking one of those adult continuing-studies classes at NYU at night—a feature-writing class. The guy who taught it, a business columnist at the New York Post, said “you know you have some skills here, I think you should try freelancing.”

Actually, he gave me an assignment. Some of your listeners may remember someone found rats doing cartwheels in the back of this Taco Bell/KFC. So he said, “Why don’t you do a freelance story for the New York Post about how it’s not just Taco Bell. All these expensive restaurants probably have rat problems too.” So I said, “Okay.”

By day I’m working at this luxury handbag company and by night I’m going through the Department of Health’s restaurant records to see which of these nice restaurants had rat problems. And I found that a restaurant that I really like had one of the most horrific health records I’d seen; it was horrendous. I couldn’t wrap my head around it because I’d just been there, and it was really clean.

So I called them and I said, “I happened upon your health record, and I really can’t parse this because I was just at your restaurant. It seemed pretty clean and sanitary to me.” And they said, “Well, thanks for calling. Actually, the health inspector came to our restaurant to do his review, and he ended up getting drunk at the bar and passing out for two hours. And we think he just made a bunch of stuff up on our report to justify to his supervisor why it took him so long to do the inspection.” So I said, “You have got to be kidding. If only there were proof of this. We should get this guy.” And they said, “Well actually, we have a camera in the restaurant that caught some of this.”

So there was proof?

There was proof. I had no idea what kind of story I had. I sheepishly walk into the New York Post and say, “I’m really sorry I didn’t get to do this assignment the way you envisioned it, but I did end up getting video footage of the health inspector drunk, passed out at the bar, and making up this whole report.” It went on the cover of the Sunday’s New York Post with a great headline that said something like “Rat Nap Inspector Snoozoo.”

After that I was hooked. The guy was fired. The Department of Health had to have new rules for inspections, and there had to be some follow up with the restaurants. To see the impact of something that started out as such a silly assignment was pretty cool.

I was going to ask you what got you into covering information security, but if you start with rats, why not just keep on going?

Exactly. I mean I didn’t choose information security. While at Forbes, I was based in Silicon Valley,
Nicole Perlroth covers cybersecurity for the New York Times and the Bits Blog (www.nytimes.com/column/bits). Before joining the San Francisco bureau in 2011, she was deputy editor at Forbes, where she covered venture capital and web start-ups. Perlroth is the recipient of several journalism rewards for her reporting on efforts by the Chinese government to steal military and industrial trade secrets. She has a BA in political science and near Eastern studies from Princeton and an MA in journalism from Stanford, and is a native of the Bay Area where she still lives.

covering venture capital during the heat-up ahead of Facebook’s IPO, including a lot of the investors and some of the private-share sales. So I got a few cover stories in Forbes. One day, I got a call from a blog editor at the New York Times, who said, “We’re looking at you for a job; it’s cybersecurity.” And I remember thinking, you want to take me off this gravy train to cover cybersecurity. I honestly didn’t think I was qualified. I told myself, well it’s an honor to get invited into the New York Times building and go to New York for these interviews, so I’ll just be myself and see what comes of it.

But lo and behold, I ended up getting the job, and the rest is history.

So how does venture capital compare to the others you’ve covered?

Venture capital is interesting because it’s very self-promotional. I get a lot of calls from venture capitalists trying to get me to write them a glowing profile, which is similar in some ways to information security because we constantly get pitched by cybersecurity firms or firms that want to slap the word cyber onto their website, looking for promotion. Dealing with the self-promoters was very good training for me.

It’s no longer even the reporting and writing that’s the hardest part of my job these days. It’s the day after the story publishes, on Twitter. When you’re writing for a layperson audience, the technical audience is never going to be happy with how you’re covering information security.Dealing with such a hypercritical, vocal, philosophical, almost religious-like community has been the hardest part; nothing prepared me for that.

You’ve been involved with some really big stories, including the recent “Russian Election Hacking Efforts, Wider Than Previously Known.” As you know, you can look out ahead of the 2018 elections and see what’s being done to prevent another situation like the one we had in 2016. I started digging around and found that there were still many more unresolved issues from the 2016 election than had been covered by the mainstream media.

One of the things that was so soothing after the election was we knew Russia had done a series of disinformation campaigns. We knew about the propaganda efforts, although at that point, we didn’t know the extent of them. But for the most part, the intelligence report that came out last January delivered the message: Despite all those efforts to influence the 2016 campaign, Russia stopped short of hacking the actual tallies.

What I’ve learned in the reporting is that this conclusion came predominantly from spies, spies that we have and digital intercepts of Russian communications. Someone likely told someone else, we didn’t hack the vote count, and they were really surprised that Trump had won without those efforts.

But no real forensic effort had been made to ensure that some of the systems that were hacked on the back end didn’t impact the votes.

One place that kept coming up in my conversations was Durham, North Carolina. The county used an electronic poll book vendor called VR Systems that we know, from a leaked NSA report, had successfully been hacked by the Russian GRU. A lot of the problems on Election Day fit the MO of someone trying to create chaos or prevent people from voting. Durham is a predominantly blue county in a swing state. As we dug deeper, we found that there were instances of people showing up with their registration cards and being told that they were no longer registered and they’ve been marked as inactive, or they voted early when they hadn’t, or they voted absentee when they hadn’t.

Fishy.

It was written off as a glitch, but no one had ever done a forensics investigation. Then I found out the county had hired a local security company to do some forensics investigation. I got my hands on that report; it was like an old cop report where they had gone to poll workers and written, “at 6:09 I interviewed Judy from precinct number three.” But there was no actual forensics analysis. The US Department of Homeland Security and FBI never analyzed the systems in Durham, because they have to be invited by the county and the state, and the state had rebuffed their efforts. I started unraveling this and realized that this tale was more common than we knew.

I hope that story gets more attention. It seems easy to cover spectacular failures like the Equifax breach, because humans love to read about disasters. But how do we get coverage for important but not really sexy computer security stuff like software security?

As far as software security, I think people are getting more interested in it. In the book I’m writing about the exploit market [This Is How They Tell Me the World Will
End], I’m hoping to end on software security because there’s now more awareness of vulnerabilities and how big an impact human error and sloppiness can have. And there was a big focus on the Equifax breach, at least initially, on the vulnerability.

Another thing that gave me hope was during Facebook’s IPO—I know this from my venture IP days—their philosophy was “move fast and break things.” And recently, while I was at Facebook headquarters, I saw that motto had been replaced: there were signs on the wall that said, “Move slowly and fix your sh*t.”

And the CSO at Facebook has had a good influence over there.

Oh yeah. And at Google, the amount of fuzzing that’s going on ... they say that their motto since the 2010 Chinese attack that happened there has been “never again,” that security and software security is extremely important to them. How that trickles down to Android I don’t know. But it’s something that’s getting talked about pretty seriously at the executive level at some tech companies, which is a good thing.

Do you think that CSOs are doomed to be the guy before the guy, or are you seeing forward progress?

I think that was the case in the past. But now that we’ve finally admitted that we’ve all been hacked, we want a veteran of serious nation-state attacks to protect our business because they understand that compliance checklists aren’t going to cut it. I think that now it’s not the CSO that gets fired; it’s the CEO.

From your perspective, what one thing should we all do to encourage more women to join cybersecurity?

I don’t think we play up the sex appeal of cybersecurity enough. You’re not just coding; you’re playing cops and robbers. I talked earlier about how little intellectual stimulation there was in some of the jobs I’ve had. The cybersecurity world is full of intellectual stimulation. It’s amazing—three days ago, I knew nothing about North Korean counterfeiting operations, but I had to go quickly study up on it because of the financially motivated attacks that North Korea has been launching to make up for the fact that it’s counterfeiting operations are no longer as effective.

There’s a real political bent to a lot of the nation-state attacks that we’re seeing. I don’t think people realize it’s not just code and it’s not just hackers in their basements—there are real opportunities here to be on the front lines of history. And talk about employment security. You know the problem is only getting worse.

I actually met a young woman the other day who was going to Johns Hopkins, and she had sought out an internship related to cybersecurity for the summer. That was the first I’d heard of a freshman co-ed seeking out a job like this. Most people just fall into it. That was a nice thing to hear.

All right, very last question: where’s your favorite place to dive on the planet?

I’ve skydived in really ugly places, so New Jersey and Lodi, California—I couldn’t tell you which one was better.

The Silver Bullet Podcast with Gary McGraw is cosponsored by Cigital (part of Synopsys) and this magazine and is syndicated by SearchSecurity.

Gary McGraw is vice president of security technology at Synopsys. He’s the author of Software Security: Building Security In (Addison-Wesley 2006) and eight other books. McGraw received a BA in philosophy from the University of Virginia and a dual PhD in computer science and cognitive science from Indiana University. Contact him via garymcgraw.com.