Google and China: the attacks and their aftermath

Google's dramatic decision to call out Chinese hackers and its decision to stop censoring search results has prompted an extraordinary worldwide reaction. Here's what we know now.

By Nate Anderson | Last updated January 13, 2010 12:39 PM

Yesterday's announcement that Google would stop censoring its search results in China, and that the company had been the victim of sophisticated Chinese cyberattacks, was a Big Deal; Secretary of State Hilary Clinton even felt the need to weigh in on it with an official statement.

And she wasn't the only one with an opinion, insight, or suggestion to share.

Clinton weighs in. Her brief statement, in full, reads: "We have been briefed by Google on these allegations, which raise very serious concerns and questions. We look to the Chinese government for an explanation. The ability to operate with confidence in cyberspace is critical in a modern society and economy. I will be giving an address next week on the centrality of Internet freedom in the 21st century, and we will have further comment on this matter as the facts become clear."

Don't worry about your data, enterprise users! After the main Google announcement, Google Enterprise president Dave Girouard took to his own blog to reassure corporate and educational users of Google Apps that their hosted data was safe. "This incident was particularly notable for its high degree of sophistication," he wrote, then added, "This attack may understandably raise some questions."

Girouad stresses that the attack was "not an assault on cloud computing" and "we believe our customer cloud-based data remains secure." It is unusual for corporations to disclose such attacks precisely because of the uncertainty they might fuel among customers, but Google says it is opening up "because we are committed to transparency, accountability, and maintaining your trust."

Seriously, stop clicking on those e-mail links. According to security reports, a favorite technique of Chinese hackers relies on social engineering. Hackers might map out the relationships at a company or research lab, then spoof an e-mail to a worker that appears to come from his boss. Clicking the link could lead to a webpage with malicious software or a phishing attack. Other attacks might spoof a company-wide e-mail to everyone, hoping that at least a few non-savvy users will click the links and provide entry points into the network.

A Northrop Grumman report notes that this happened at a US research lab in recent years. Of the 1,100 people at the lab, only a handful were compromised by interacting with the e-mail, but that handful was enough to breach security. Google notes that something similar happened to it, though details are few. "The route the attackers used was malicious software used to infect personal computers," said the company. "Any computer connected to the Internet can fall victim to such attacks."

EFF calls for other firms to follow Google's lead. "Our hope is that other tech companies will follow Google's lead. Too many of them have been willing to comply with Chinese demands that they check their values at the border."

Not business as usual. William Moss, a public relations advisor who works (and blogs) from China, says that Google "has taken the China corporate communications playbook, wrapped it in oily rags, doused it in gasoline and dropped a lit match on it. In China, foreign companies tend to be deferential to the authorities to the point of obsequiousness, in a way that you would almost certainly never encounter in the United States or Europe. Scan any foreign company's China press releases and count the number of times you see the phrase, 'commitment to China.' Demonstrating 'alignment with the Chinese government's agenda' is an accepted tenet of corporate positioning and corporate social responsibility work in China."

Still, neither he nor anyone else seem to think the Chinese government is likely to cave on the censorship issue, especially when called out by Google in such a public and direct way.

The cynics scoff. A representative blog post questioning Google's real motives: "Cynic and all-around horrible person that I am, I wonder if Google would be doing this if they hadn't screwed the pooch on the China market several years ago and were still doing a fairly sh— job trying to catch up to Baidu. But that's just me, I can always find some a——— point of view for any story."

Did Google simply decide to cut off its small operations in China in return for currying favor just about everywhere else? Can complicated real-world decisions have multiple motivations behind them?

Welcome to Google PR! Marc Ambinder of *The Atlantic* points out that yesterday was the first day on the job for Jill Hazelbaker, John McCain's campaign communications director and new head of Google's public relations operation. "Suffice it to say that Hazelbaker is used to being thrust into chaotic situations," Ambinder remarks.

China enters its Bush-Cheney era. Also at *The Atlantic*, esteemed journalist James Fallows has just returned from several years of living in China, and he offers his usual platter of interesting observations. Chief among them: "In a strange and striking way there is an inversion of recent Chinese and US roles. In the switch from George W. Bush to Barack Obama, the US went from a president much of the world saw as deliberately antagonizing them to a president whose Nobel Prize reflected (perhaps desperate) gratitude at his efforts at conciliation. China, by contrast, seems to be entering its Bush-Cheney era. For Chinese readers, let me emphasize again my argument that China is not a 'threat' and that its development is good news for mankind. But its government is on a path at the moment that courts resistance around the world. To me, that is what Google's decision signifies."

Censorship and free trade agreements. The CCIA, a DC lobbying group for the tech sector that counts companies like Microsoft and Google as members, blasted China's censorship policies for violating trade agreements.

"It is increasingly apparent that censorship is a barrier to trade, and that China cannot limit the free flow of information and still comply with its international trade obligations," said CEO Ed Black. "The Chinese government has said it is gathering more information before deciding how to proceed and we would urge that they look at the issue holistically with government, economic and trade officials involved in the decision."

Google's Chinese HQ gets roses. At least some in China support Google's stance; flowers have already started to appear spontaneously at the company's China headquarters.

$600 million at stake? It's not clear how much revenue Google might leave on the table if it withdraws from China, but one analyst guestimates its yearly take at $600 million.

The official Chinese view. Xinhua, the country's official news outlet, is running a piece on its English-language site that comes at the issue from the perspective of the Chinese government. Xinhua got in touch with the head of China Internet Illegal Information Reporting Center, Xi Wei, who said only, "I am sorry I can't say anything. I am not clear about many problems in the case."

Guo Ke, a communications prof at Shanghai International Studies University, argued that Google can't leave the country because it "will suffer a huge economic loss from leaving the Chinese market." While the government is unlikely to yield, it could be "more moderate and smarter" about the way it handles Internet regulation, he said.

Everyone's getting hacked. The big search engine news in China over the last few days hasn't been Google, but number one search engine Baidu. Baidu was just hacked by a group calling itself the Iranian Cyber Army.

Why only subject lines? If the attackers could get access to subject lines, why couldn't they access entire e-mails? Apparently because the hackers infiltrated automated systems set up to provide such information to law enforcement in the

US and elsewhere. (Getting access to the contents of e-mail messages is harder under US law than getting access to addresses, subject lines, etc, which are considered to be on the "outside of the envelope" and subject to pen register searches).

According to a Macworld source, "Right before Christmas, it was, 'Holy s—, this malware is accessing the internal intercept [systems].'" Later, Google cofounder Larry Page supervised a Christmas Eve meeting on the security breach.

Fun fact: Google's security team managed to penetrate one of the servers being used by the attackers, which was how the full extent of the attack—more than 30 companies—was revealed.

Breaches by design. Former Ars writer Julian Sanchez, now covering security at the Cato Institute, sees a problem with these automated law enforcement tracking systems in place at most major ISPs and Web companies. "As an eminent group of security experts argued in 2008, the trend toward building surveillance capability into telecommunications architecture amounts to a breach-by-design, and a serious security risk. As the volume of requests from law enforcement at all levels grows, the compliance burdens on telcoms grow also—making it increasingly tempting to create automated portals to permit access to user information with minimal human intervention.

"The problem of volume is front and center in a leaked recording released last month, in which Sprint's head of legal compliance revealed that their automated system had processed 8 million requests for GPS location data in the span of a year, noting that it would have been impossible to manually serve that level of law enforcement traffic. Less remarked on, though, was Taylor's speculation that someone who downloaded a phony warrant form and submitted it to a random telecom would have a good chance of getting a response—and one assumes he'd know if anyone would."