February 10, 2012

Traveling Light in a Time of Digital Thievery

By NICOLE PERLROTH

SAN FRANCISCO — When Kenneth G. Lieberthal, a China expert at the Brookings Institution, travels to that country, he follows a routine that seems straight from a spy film.

He leaves his cellphone and laptop at home and instead brings “loaner” devices, which he erases before he leaves the United States and wipes clean the minute he returns. In China, he disables Bluetooth and Wi-Fi, never lets his phone out of his sight and, in meetings, not only turns off his phone but also removes the battery, for fear his microphone could be turned on remotely. He connects to the Internet only through an encrypted, password-protected channel, and copies and pastes his password from a USB thumb drive. He never types in a password directly, because, he said, “the Chinese are very good at installing key-logging software on your laptop.”

What might have once sounded like the behavior of a paranoid is now standard operating procedure for officials at American government agencies, research groups and companies that do business in China and Russia — like Google, the State Department and the Internet security giant McAfee. Digital espionage in these countries, security experts say, is a real and growing threat — whether in pursuit of confidential government information or corporate trade secrets.

“If a company has significant intellectual property that the Chinese and Russians are interested in, and you go over there with mobile devices, your devices will get penetrated,” said Joel F. Brenner, formerly the top counterintelligence official in the office of the director of national intelligence.

Theft of trade secrets was long the work of insiders — corporate moles or disgruntled employees. But it has become easier to steal information remotely because of the Internet, the proliferation of smartphones and the inclination of employees to plug their personal devices into workplace networks and cart proprietary information around. Hackers' preferred modus operandi, security experts say, is to break into employees' portable devices and leapfrog into employers' networks — stealing secrets while leaving nary a trace.

Targets of hack attacks are reluctant to discuss them and statistics are scarce. Most breaches go unreported, security experts say, because corporate victims fear what disclosure might mean for their stock price, or because those affected never knew they were hacked in the first place. But the scope of the problem is illustrated by an incident at the United States Chamber of Commerce in 2010.

The chamber did not learn that it — and its member organizations — were the victims of a cybertheft that had lasted for months until the Federal Bureau of Investigation told the group that servers in China were stealing information from four of its Asia policy experts, who frequent China. By the time the chamber secured its network, hackers had pilfered at least six weeks worth of e-mails with its member organizations, which include most of the nation's largest corporations. Later still, the chamber discovered that its office printer and even a thermostat in one of its corporate apartments were still communicating with an Internet address in China.

The chamber did not disclose how hackers had infiltrated its systems, but its first step after the attack was to bar employees from taking devices with them "to certain countries," notably China, a spokesman said.

The implication, said Jacob Olcott, a cybersecurity expert at Good Harbor Consulting, was that devices brought into China were hacked. "Everybody knows that if you are doing business in China, in the 21st century, you don't bring anything with you. That's 'Business 101' — at least it should be."

Neither the Chinese nor Russian embassies in Washington responded to several requests for comment. But after Google accused Chinese hackers of breaking into its systems in 2010, Chinese officials gave this statement: "China is committed to protecting the legitimate rights and interests of foreign companies in our country."

Still, United States security experts and government officials say they are increasingly concerned about breaches from within these countries into corporate networks — whether through mobile devices or other means.

Last week, James R. Clapper, the director of national intelligence, warned in testimony before the Senate Intelligence Committee about theft of trade secrets by “entities” within China and Russia. And Mike McConnell, a former director of national intelligence, and now a private consultant, said in an interview, “In looking at computer systems of consequence — in government, Congress, at the Department of Defense, aerospace, companies with valuable trade secrets — we’ve not examined one yet that has not been infected by an advanced persistent threat.”

Both China and Russia prohibit travelers from entering the country with encrypted devices unless they have government permission. When officials from those countries visit the United States, they take extra precautions to prevent the hacking of their portable devices, according to security experts.

Now, United States companies, government agencies and organizations are doing the same by imposing do-not-carry rules. Representative Mike Rogers, the Michigan Republican who is chairman of the House Intelligence Committee, said its members could bring only “clean” devices to China and were forbidden from connecting to the government’s network while abroad. As for himself, he said he traveled “electronically naked.”

At the State Department, employees get specific instruction on how to secure their devices in Russia and China, and are briefed annually on general principles of security. At the Brookings Institution, Mr. Lieberthal advises companies that do business in China. He said that there was no formal policy mandating that employees leave their devices at home, “but they certainly educate employees who travel to China and Russia to do so.”

McAfee, the security company, said that if any employee’s device was inspected at the Chinese border, it could never be plugged into McAfee’s network again. Ever. “We just wouldn’t take the risk,” said Simon Hunt, a vice president.

At AirPatrol, a company based in Columbia, Md., that specializes in wireless security systems, employees take only loaner devices to China and Russia, never enable Bluetooth and always switch off the microphone and camera. “We operate under the assumption that we will inevitably be compromised,” said Tom Kellermann, the company’s chief technology officer and a member of President Obama’s commission on cybersecurity.

Google said it would not comment on its internal travel policies, but employees who spoke on condition of anonymity said the company prohibited them from bringing sensitive data to China, required they bring only loaner laptops or have their devices inspected upon their return.

Federal lawmakers are considering bills aimed at thwarting cybertheft of trade secrets, although it is unclear whether this legislation would directly address problems that arise from business trips overseas.

In the meantime, companies are leaking critical information, often without realizing it.

“The Chinese are very good at covering their tracks,” said Scott Aken, a former F.B.I. agent who specialized in counterintelligence and computer intrusion. “In most cases, companies don’t realize they’ve been burned until years later when a foreign competitor puts out their very same product — only they’re making it 30 percent cheaper.”

“We’ve already lost our manufacturing base,” he said. “Now we’re losing our R.& D. base. If we lose that, what do we fall back on?”