The Wall Street Journal, Editorial, June 7, 2015

The Chinese Have Your Numbers

The U.S. government gives up personal data secrets with barely a fight

U.S. government incompetence seems to grow by the month, and now we know it's becoming a threat to national, and even individual American, security. The Obama Administration announced last week that Chinese hackers made off this year with personnel files that may have included those of all 2.1 million federal employees, plus former employees going back to the 1980s.

This is no routine hack. The Office of Personnel Management (OPM) lost background-check data to the Chinese nine months before this breach and still hadn't locked the cyber front door. OPM's inspector general issued a damning report last November that parts of its network should be shut down because they were riddled with weaknesses that "could potentially have national security implications." You can't ring the alarm much louder than that, but the failure to take basic precautions continued.

In other words this isn't a James Bond movie. It's a Dilbert cartoon. Despite years of warnings, and after the Bradley Manning and Edward Snowden debacles, the federal bureaucracy can't protect its most basic data from hackers. Private companies like Target are pilloried, not least by politicians, for their data leaks. But the feds have $4 trillion to spend each year plus access to the most advanced encryption systems. Will anyone in government take responsibility for this fiasco?

Speaking of Snowden, bipartisan Washington has been congratulating itself this month for supposedly protecting American privacy from the *potential* abuse of National Security Agency collection of metadata—that is, phone logs but not the content of calls. In the case of OPM we have an actual data breach of Social Security numbers and other records by malevolent foreign actors. Which do you worry more about?

The episode is one more confirmation that China is waging an unrelenting if unacknowledged cyber war against the United States. The main targets have been universities and private

Commented [i1]: Unauthorized disclosures by individuals with security clearances are not the same thing as the theft of data by external hackers.

Commented [i2]: According to public reports, Target's large 2013 data breach was detected by the company's own alert system, but no action was taken until federal officials contacted the company two weeks later. This suggests that the core problem was a lack of effective security procedures, rather than a lack of resources or technology.

See http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p1

Commented [i3]: Encryption technology is a critical part of strong cybersecurity. Encoding information to make it more difficult for unauthorized persons to read it makes that information much more secure.

Alarmingly, federal officials have recently begun to suggest that the US should prohibit American companies from providing encryption that federal agencies cannot overcome. This would require US hardware and software companies to sell less secure products.

See http://www.nytimes.com/2014/10/17/us/politics/fbi-director-in-policy-speech-calls-dark-devices-hindrance-to-crime-solving.html

Commented [i4]: Constantly collecting the private information of millions of law-abiding Americans is not a "potential" abuse – it is a serious violation of those Americans' fundamental rights.

While proponents of mass surveillance frequently suggest that collecting the records of phone calls is not intrusive, in reality phone records can reveal significant private and personal information, including medical issues, intimate relationships, and political and religious affiliations. For example, phone records revealing that someone called a psychiatrist three times in two days, and once after midnight, reveal quite a bit about that person.

Commented [i5]: In the case of both NSA mass surveillance and the OPM data breach, Americans are rightly worried that their personal information is not secure, and that it can be accessed without their knowledge or consent.

companies with the goal of stealing intellectual property, but attacks on the government are increasingly brazen.

Beijing can use the stolen OPM files to target employees with security clearances, current or past. It can attack their personal financial accounts, perhaps with blackmail in mind. It can trick them into helping hackers infiltrate other networks.

Michael McCaul, Chairman of the House Homeland Security Committee, said on CBS's "Face the Nation" Sunday that "it was done to get to personal information on political appointees in the federal government and federal employees to exploit them so that later down the road they can use those for espionage." Do Senators Rand Paul and Ron Wyden have some suggestions for countering this privacy threat?

The need for better defenses is obvious, but the Obama Administration has responded mainly with diplomacy and some indictments against Chinese hackers whom China's government won't even stop, much less arrest and extradite to the U.S. for trial.

Maybe President Obama still hopes to reach a "gentleman's agreement" with Chinese Supreme Leader Xi Jinping on hacking. He tried at the Sunnylands summit two years ago, but Mr. Xi refused even to admit the existence of his government's hacking.

White House spokesman Josh Earnest isn't much more forthcoming. He tried to change the subject last week by urging Congress to pass legislation that would allow information-sharing between companies and the government. But that has nothing to do with the OPM breach.

The main obstacle to the bill in the past two years has been Mr. Obama's insistence that it include new and costly government mandates on private companies. Congress seems poised to overrule the White House this year and pass the info-sharing bill without the mandates—if Mr. Obama and Democrats in the Senate will get out of the way.

Commented [i6]: The theft of personal information by foreign hackers poses a serious and continuing threat to Americans' privacy and information security.

The way to address this threat, with regard to OPM and other government-held data, is to ensure that federal agencies receive the funding and expertise to develop and implement robust security programs, and to ensure that these agencies have the technical and administrative controls that they need to combat a wide variety of cybersecurity threats. It is also important for the US to invest in the education of the next leaders in cybersecurity, and to recruit and retain a strong federal cybersecurity workforce by ensuring that cybersecurity professionals can find opportunities and career paths in government that are as rewarding as those in the private sector.

Mass surveillance of law-abiding Americans will not prevent data breaches. Weakening encryption technologies or stockpiling users' encryption keys will not prevent data breaches. And making it harder for individuals to sue large corporations inappropriately sharing their data will not prevent data breaches.

Commented [i7]: This point is absolutely correct. The cybersecurity "info-sharing" bill now pending in the Senate would make it harder for individuals to sue large corporations for inappropriately handing their data over to the government. It is difficult to see how this represents any sort of solution to the OPM data breach.

Commented [i8]: Previous versions of this bill would have required the government to propose cybersecurity standards for private companies to follow. This would have a much greater positive impact on American cybersecurity than handing corporations broad new protections against lawsuits from their customers.

By the way, what message does it send the rest of the federal bureaucracy when the rank-and-file read that Hillary Clinton was allowed to set up a personal email server for her official communications as Secretary of State in violation of her own department's rules?

***

The reality is that defenses alone won't work against determined adversaries like the Chinese, Russians and Iranians. The best cyberdefense is a good offense. U.S. intelligence services and the Pentagon will have to demonstrate the ability to punish Chinese institutions that continue to steal American secrets. That won't end the threat, but it might give the governments that are underwriting these hackers some pause.

The U.S. is already in a cyber war. The problem is that the Obama Administration doesn't want to admit it.

Commented [i9]: Cyberattacks represent a serious threat to fundamental American interests, including national security, economic competitiveness, and individual privacy. These security breaches can be caused in a variety of ways by a variety of actors, with varying knowledge and resources. The solutions to the problem are just as diverse.

Responses to aggressive actions by foreign governments should include the full range of US power, from multilateral diplomacy to economic sanctions to law enforcement action. It is a mistake to lump the many aspects of this problem into a single cyber threat that can be solved by a single cybersecurity bullet.