AFTER TARGETING OPM, HACKERS MOVED ONTO UNITED?

Bloomberg reports that the same people who hacked OPM then went on to target United, which does a lot of business with the government (and, though the story doesn't say it, a lot of flights to China).

> United, the world's second-largest airline, detected an incursion into its computer systems in May or early June, said several people familiar with the probe. According to three of these people, investigators working with the carrier have linked the attack to a group of China-backed hackers they say are behind several other large heists — including the theft of security-clearance records from the U.S. Office of Personnel Management and medical data from health insurer Anthem Inc.
>
> [snip]
>
> The timing of the United breach also raises questions about whether it's linked to computer faults that stranded thousands of the airline's passengers in two incidents over the past couple of months. Two additional people close to the probe, who like the others asked not to be identified when discussing the investigation, say the carrier has found no connection between the hack and a July 8 systems failure that halted flights for two hours. They didn't rule out a possible, tangential connection to an outage on June 2.

But what I find most interesting is that OPM developed a list of potential victims, including United, and alerted them of the signatures related to the hack.

> The China-backed hackers that cybersecurity experts have linked to that attack have embedded the name of targets in web domains, phishing e-mails and other attack infrastructure, according to one of the people familiar with the investigation.
>
> In May, the OPM investigators began drawing up a list of possible victims in the private sector and provided the companies with digital signatures that would indicate their systems had been breached. United Airlines was on that list.

That's interesting for two reasons. First, OPM alerted United *before* it alerted even the less exposed OPM victims, those whose personnel data got stolen; OPM has yet to formally alert those whose security clearance data got taken. I get that you might want to alert additional targets before confirming publicly you know about the hack (potentially to learn more about the perpetrators).

But it also shows that data sharing — alleged to be the urgent need calling for CISA — is not a problem.

UNDER CISA, DATA WOULD AUTOMATICALLY GET SHARED WITH AGENCIES WITH WORSE CYBERPREPAREDNESS

THAN OPM

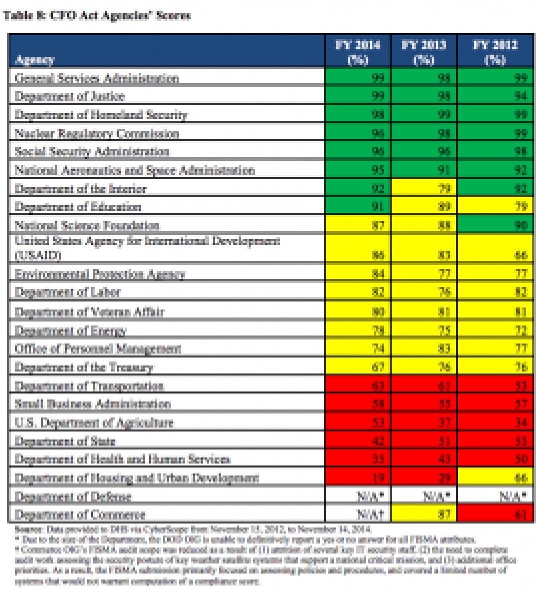


Table 8: CFO Act Agencies' Scores

Agency	FY 2014 (%)	FY 2013 (%)	FY 2012 (%)
General Services Administration	99	98	99
Department of Justice	99	98	94
Department of Homeland Security	98	99	99
Nuclear Regulatory Commission	96	98	99
Social Security Administration	96	96	98
National Aeronautics and Space Administration	95	91	92
Department of the Interior	92	79	92
Department of Education	91	89	79
National Science Foundation	87	88	90
United States Agency for International Development (USAID)	86	83	66
Environmental Protection Agency	84	77	77
Department of Labor	82	76	82
Department of Veteran Affair	80	81	81
Department of Energy	78	75	72
Office of Personnel Management	74	83	77
Department of the Treasury	67	76	76
Department of Transportation	63	61	53
Small Business Administration	58	55	57
U.S. Department of Agriculture	53	37	34
Department of State	42	51	53
Department of Health and Human Services	35	43	50
Department of Housing and Urban Development	19	29	66
Department of Defense	N/A*	N/A*	N/A*
Department of Commerce	N/A†	87	61

Source: Data provided to DHS via CyberScope from November 15, 2012, to November 14, 2014.
* Due to the size of the Department, the DOD OIG is unable to definitively report a yes or no answer for all FISMA attributes.
† Commerce OIG's FISMA audit scope was reduced as a result of (1) attrition of several key IT security staff, (2) the need to complete audit work assessing the security posture of key weather satellite systems that support a national critical mission, and (3) additional office priorities. As a result, the FISMA submission primarily focused on assessing policies and procedures, and covered a limited number of systems that would not warrant computation of a compliance score.

In the wake of the OPM hack, Congress is preparing to *do something!!!* Unfortunately, that "something" will be to pass the Cyber Information Sharing Act, which not only wouldn't have helped prevent the OPM hack, but comes with its own problems.

To understand why it is such a bad idea to pass CISA just to appear to be doing something in response to OPM, compare this table from this year's Federal Information Security Management report with the list of agencies that will automatically get the data turned over to the Federal government if CISA passes.

> (A) The Department of Commerce.
>
> (B) The Department of Defense.
>
> (C) The Department of Energy.
>
> (D) The Department of Homeland Security.
>
> (E) The Department of Justice.
>
> (F) The Department of the Treasury.
>
> (G) The Office of the Director of National Intelligence.

So not only will information automatically go to DOJ, DHS, and DOD — all of which fulfill the information security measures reviewed by Office of Management and Budget — but it would also go to Department of Energy, which scores just a few points better than OPM, Department of Commerce, which was improving but lost some IT people and so couldn't be graded last year, and Department of Treasury, which scores *worse* than OPM.

Which is just one of the reasons why CISA is a stupid idea.

Some folks have put together this really cool tool that will help you *fax* the Senate (a tool they might understand) so you can explain how dumb passing CISA would be. Try it!

IN SUPPORT OF BEN WITTES

Over at Lawfare, Ben Wittes does some brainstorming about what other databases the Chinese may be hacking after ingesting all its OPM winnings. He thinks they might target:

- FDA New Drug Applications
- VA patient records
- Visa applications (State Department)
- Export control applications (Commerce)
- SEC investigative files

For each description of why he thinks they might be juicy targets, he ends with this statement:

> Fortunately, the [XXX] Department is a highly competent counterintelligence agency with first-rate cybersecurity expertise, whose employees are scrupulous about cybersecurity and never do business on their own email servers. I am sure it is fully competent to

> protect these records.

As it happens, there's plenty of support for most of Wittes' speculative targets, especially if you consult this year's FISMA report from OMB.

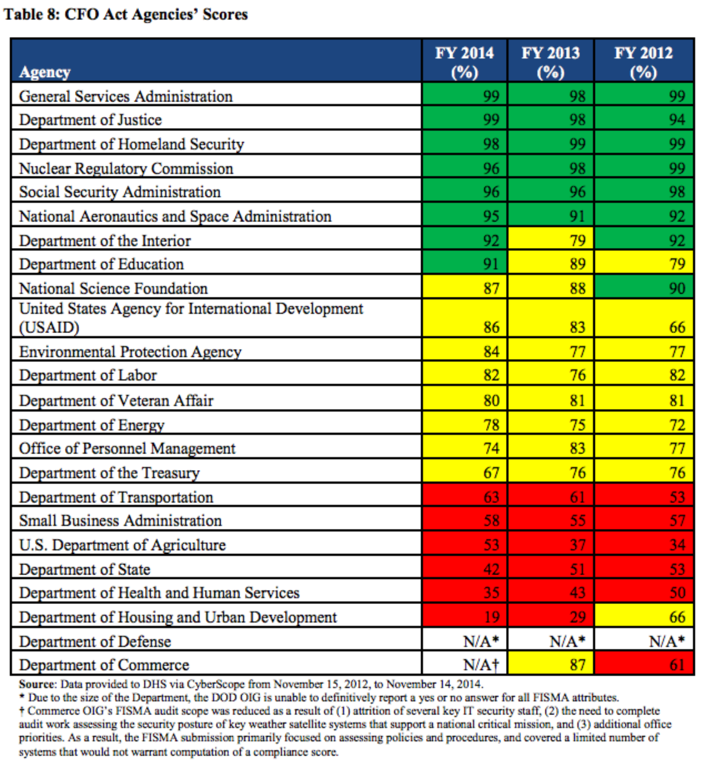


Table 8: CFO Act Agencies' Scores

Agency	FY 2014 (%)	FY 2013 (%)	FY 2012 (%)
General Services Administration	99	98	99
Department of Justice	99	98	94
Department of Homeland Security	98	99	99
Nuclear Regulatory Commission	96	98	99
Social Security Administration	96	96	98
National Aeronautics and Space Administration	95	91	92
Department of the Interior	92	79	92
Department of Education	91	89	79
National Science Foundation	87	88	90
United States Agency for International Development (USAID)	86	83	66
Environmental Protection Agency	84	77	77
Department of Labor	82	76	82
Department of Veteran Affair	80	81	81
Department of Energy	78	75	72
Office of Personnel Management	74	83	77
Department of the Treasury	67	76	76
Department of Transportation	63	61	53
Small Business Administration	58	55	57
U.S. Department of Agriculture	53	37	34
Department of State	42	51	53
Department of Health and Human Services	35	43	50
Department of Housing and Urban Development	19	29	66
Department of Defense	N/A*	N/A*	N/A*
Department of Commerce	N/A†	87	61

Source: Data provided to DHS via CyberScope from November 15, 2012, to November 14, 2014.

* Due to the size of the Department, the DOD OIG is unable to definitively report a yes or no answer for all FISMA attributes.

† Commerce OIG's FISMA audit scope was reduced as a result of (1) attrition of several key IT security staff, (2) the need to complete audit work assessing the security posture of key weather satellite systems that support a national critical mission, and (3) additional office priorities. As a result, the FISMA submission primarily focused on assessing policies and procedures, and covered a limited number of systems that would not warrant computation of a compliance score.

Several of the agencies — especially the State Department, but also especially Commerce — rated very poorly in OMB's summary of the Inspector Generals reviews from last year.

I'd add two agencies to Wittes' list: USDA (China has allegedly been stealing seed corn, so why not Ag records?) and Treasury generally (though in some other areas Treasury is pretty good, and it has mostly been "hacked" via old style means — including PII "spillage" — of late).

This list is particularly notable, however, given that the debate over CISA is about to start again. Both Treasury and Commerce are among the agencies that get automatic updates of the data turned over under the law. But their security is, in some ways, even worse than

OPM’s.

Update: Paul Rosenzweig takes a shot. He picks CFIUS, NRC, FERC, state license DBs, and university research. There is some correlation with weak agencies there, too.

OUR DEFINITIONS OF NATIONAL SECURITY CRIMES ARE FUCKED

I realized something the other day.

For the purposes of hacking, a theater (or at least any mall it was attached to) might count as critical infrastructure that would deem it a National Security target, just as Sony Pictures was deemed critical infrastructure for sanction and retaliation purposes after it got hacked.

But if a mentally ill misogynist with a public track record of supporting right wing hate shoots up a movie showing, it would not be considered a national security target. Given his death, DOJ won’t be faced with the challenge of naming John Russell Houser’s crime, but they would have even less ability to punish Houser for his motivation and ties to other haters than they had with Dylann Roof.

DOJ had no such problem with Joseph Buddenberg and Nicole Kissane, who got charged with terrorism (under the Animal Enterprise Terrorism Act) yesterday because they freed some minks. And a bobcat.

So shooting African Americans worshipping in church is not terrorism, but freeing a bobcat is.

Meanwhile, most of the 204 mass shootings — averaging one a day — that happened this year have passed unremarked.

I laid out some of the problems with the disparity between Muslim terrorism and white supremacist terrorism (to say nothing of bobcat-freeing “terrorism”) the other day.

> “This should in no way signify that this particular murder or any federal crime is of any lesser significance.” [than terrorism, Loretta Lynch claimed while announcing the Hate Crime charges against Roof
>
> Except it is, by all appearances.
>
> When asked, Lynch refused to comment on how DOJ is allocating resources, but reporting on the increase in terrorism analysts since 9/11 suggests the FBI has dedicated large amounts of new resources to fighting Islamic terrorism, domestically and abroad. In addition, there are a number of spying tools that are tied solely to international terrorism — but DOJ has managed to define, in secret, domestic terrorism espoused by Muslims in the U.S. as international terrorism. That means FBI has far more tools to dedicate to finding tweets posted by Muslims, and fewer to find the manifesto Roof wrote speaking of having ”the bravery to take it to the real world” against blacks and even Jews.
>
> Perhaps most importantly, because of vastly expanded post-9/11 information sharing, local law enforcement offices have been deputized in the hunt for Muslim terrorists, receiving intelligence obtained through those additional spying tools and sharing tips back up with the FBI. By contrast, as one after another confrontation makes clear — most recently the video of a white Texas trooper escalating a traffic stop with African American woman Sandra Bland that ultimately ended in her death, purportedly by suicide — too many

> white local cops tend to prey on African Americans themselves rather than the police who target African Americans for their race.
>
> [snip]
>
> Finally, the FBI has an incentive to call Roof's attack something different, as it makes a big deal of its success in preventing "terrorist" attacks. If the Charleston attack was terrorism, it means FBI missed a terrorist plotting while tracking a bunch of Muslims who might not have acted without FBI incitement. That would be all the worse as the FBI might have stopped Roof during the background check conducted before he bought the murder weapon, if not for some confusion on a prior charge.
>
> [snip]
>
> I'm certainly not saying we should expand the already over-broad domestic dragnet to include white supremacists espousing ugly speech (but neither should hateful speech from Muslims be sufficient for a material support for terrorism charge, as it currently is). Yet as one after another white cop kills or leads to the death of unarmed African Americans, we have to ensure that we call like crimes by like names to emphasize the importance of protecting all Americans. DOJ under Eric Holder was superb at policing civil rights violations, and there's no reason to believe that will change under DOJ's second African American Attorney General, Loretta Lynch.
>
> But hate crimes brought with the assistance of DOJ's Civil Rights division (as these were) are not the same as terrorist crimes brought by national security prosecutors, nor

> are they as easy to prosecute. If our nation can't keep African Americans worshipping in church safe, than we're not delivering national security.

But I'd add to that. If we're discussing mass killings with guns (remember, earlier this year Richard Burr tried to include commission of a violent crime while in possession of a gun among the definitions of terrorism) then it suggests far different solutions than just calling terrorism terrorism.

What if we focused all our energy on interceding before crazy men — of all sorts — shoot up public spaces rather than just one select group?

What if our definitions of national security started with a measure of impact rather than a picture of global threat?

MICHAEL CHERTOFF MAKES THE CASE AGAINST BACK DOORS

One of the more interesting comments at the Aspen Security Forum (one that has, as far as I've seen, gone unreported) came on Friday when Michael Chertoff was asked about whether the government should be able to require back doors. He provided this response (his response starts at 16:26).

> I think that it's a mistake to require companies that are making hardware and software to build a duplicate key or a back door even if you hedge it with the notion that there's going to be a court order. And I say that for a number of reasons and I've given it quite a bit of thought and I'm working with some

> companies in this area too.
>
> First of all, there is, when you do require a duplicate key or some other form of back door, there is an increased risk and increased vulnerability. You can manage that to some extent. But it does prevent you from certain kinds of encryption. So you’re basically making things less secure for ordinary people.
>
> The second thing is that the really bad people are going to find apps and tools that are going to allow them to encrypt everything without a back door. These apps are multiplying all the time. The idea that you’re going to be able to stop this, particularly given the global environment, I think is a pipe dream. So what would wind up happening is people who are legitimate actors will be taking somewhat less secure communications and the bad guys will still not be able to be decrypted.
>
> The third thing is that what are we going to tell other countries? When other countries say great, we want to have a duplicate key too, with Beijing or in Moscow or someplace else? The companies are not going to have a principled basis to refuse to do that. So that’s going to be a strategic problem for us.
>
> Finally, I guess I have a couple of overarching comments. One is we do not historically organize our society to make it maximally easy for law enforcement, even with court orders, to get information. We often make trade-offs and we make it more difficult. If that were not the case then why wouldn’t the government simply say all of these [takes out phone] have to be configured so they’re constantly recording everything that we say and do and then when you get a court order it gets

> turned over and we wind up convicting ourselves. So I don’t think socially we do that.
>
> And I also think that experience shows we’re not quite as dark, sometimes, as we fear we are. In the 90s there was a deb — when encryption first became a big deal — debate about a Clipper Chip that would be embedded in devices or whatever your communications equipment was to allow court ordered interception. Congress ultimately and the President did not agree to that. And, from talking to people in the community afterwards, you know what? We collected more than ever. We found ways to deal with that issue.
>
> So it’s a little bit of a long-winded answer. But I think on this one, strategically, we, requiring people to build a vulnerability may be a strategic mistake.

These are, of course, all the same answers opponents to back doors always offer (and Chertoff has made some of them before). But Chertoff’s answer is notable both because it is so succinct and because of who he is: a long-time prosecutor, judge, and both Criminal Division Chief at DOJ and Secretary of Homeland Security. Through much of that career, Chertoff has been the close colleague of FBI Director Jim Comey, the guy pushing back doors now.

It’s possible he’s saying this now because as a contractor he’s being paid to voice the opinions of the tech industry; as he noted, he’s working with some companies on this issue. Nevertheless, it’s not just hippies and hackers making these arguments. It’s also someone who, for most of his career, pursued and prosecuted the same kinds of people that Jim Comey is today.

Update: Chertoff makes substantially the same argument in a WaPo op-ed also bylined by Mike

McConnell and William Lynn.

WAS CHRYSLER’S VEHICLE HACKING RISK AN SEC DISCLOSURE REPORTABLE EVENT?

Remember the data breach at JPMorgan Chase, exposing 76 million accounts to “hack-mapping“? Last October, JPMorgan Chase publicly disclosed the intrusion and exposure to investors in an 8-K filing with the Securities and Exchange Commission. The statement complied with the SEC’s CF Disclosure Guidance: Topic No. 2 – Cybersecurity.

Other companies whose customers’ data have been exposed also disclosed breaches in 8-Ks, including Target, TJX Companies, Heartland Payment, EMC and Google. (Firms NASDAQ, Citigroup and Amazon have not.)

Disclosure of known cybersecurity threats or attacks with potential material risks allows investors to make informed decisions. Stock share pricing will fluctuate and reflect the true market value once risk has been factored by investors – and not remain artificially high.

Fiat Chrysler America (FCA; NYSE:FCAU) has known for nearly a year about the risk that Chrysler vehicles could be hacked remotely, according to Fortune magazine Thursday.

Yet to date no filing with the SEC has been made, disclosing this specific cyber risk to investors, customers, and the public.

The SEC’s Disclosure Guidance, though, is just that – guidance. There aren’t any firm rules yet in place, and the guidance itself was published in October 2011. A lot has happened and changed about technology and cybersecurity risks since then; the guidance has not reflected the increasing threats and attacks to business' data.

Nor does the SEC's guidance distinguish between cybersecurity threats to service products (like banking services), versus hardlines or manufactured goods (like automobiles which offer software as an additional, non-essential feature). The software industry's chronic security patching confuses any distinction; should software companies likewise include all security patches in their SEC filings, or continue as they have without doing so? It's easy to see how revelations about Adobe Flash after Hacking Team was hacked have materially hurt Adobe and all companies relying on Flash — yet Adobe hasn't released a statement at its website. (Only a statement addressing the 2013 threat to customer accounts is posted.)

Are financial services firms any more obligated than software firms? Are automobile companies, which claim ownership of on-board software, any more obligated than software companies?

It's likely FCA chose not to reveal the vehicle hacking threat until efforts to mitigate potential damage had been completed. The now-released security patch for Chrysler vehicles is an obvious indication of this attempt.

Less visible to the public and to investors is any financial effort to reduce future financial exposures. Has FCA established a protocol for investigating any suspect vehicle accidents? Were reserves set up for future claims should there be (or have been) an accident caused by hacking of their vehicle software?

Can investors adequately account for their own financial risk if they do not know what actions FCA has taken? At this point, investors only know what Chrysler owners and the public know: FCA issued a recall Friday on 1.4 million vehicles at risk, in order to patch their UConnect systems.

Senators Richard Blumenthal (D-CT) announced Friday that he and Ed Markey (D-MA) are working on new legislation, to ensure the National Highway Traffic Safety Administration (NHTSA) and the Federal Trade Commission (FTC) establish new safety standards for software features in vehicles, in response to the kind threat revealed this week. This is problematic – members of Congress have proven repeatedly they are not able to grasp technological subtleties and details. We'll have to hope for the best.

But business reporting must likewise keep up with technology; the SEC should revisit cybersecurity disclosure guidance immediately, given the size and scope cybersecurity threats pose to the public. Disclosure to investors and the public should not be a hit-or-miss proposition.

THE BULLSHIT EXCUSES FOR NOT RETALIATING FOR OPM

A handful of anonymous sources have given Ellen Nakashima some bullshit explanations for why the Administration is not retaliating against China for the OPM hack.

Most laughable is that they're willing to retaliate for "economic" spying but not "political" spying. While also mentioning the Sony example, Nakashima points to the DOJ case against Chinese hackers for eavesdropping on discussions about trade disputes from the steel industry.

> As a result, China has so far escaped any major consequence for what U.S. officials have described as one of the most damaging cyber thefts in U.S.

> government history — an outcome that also appears to reflect an emerging divide in how the United States responds to commercial vs. traditional espionage.
>
> Over the past year and a half, the United States has moved aggressively against foreign governments accused of stealing the corporate secrets of major U.S. firms. Most notably, the Justice Department last year filed criminal charges against five Chinese military officers accused of involvement in alleged hacks of U.S. Steel, Westinghouse and other companies.

Nakashima doesn't say whether her sources made this connection or she did, but it's an inapt example. As I pointed out at the time, spying on trade negotiation adversaries is precisely the kind of "commercial" spying we embrace. We do this *all the time*. DOJ chose to indict on those trade dispute discussions but not on a never-ending list of hacks against more sensitive targets — like the F-35 development team — that fit more comfortably (though still not entirely) in the kind of "economic" spying we fancy others do but we don't; DOJ probably made that choice because both the target and the evidence was segregable from more sensitive issues (the Chinese government and our clusterfuck of DOD contracting cyberdefense). In other words, it is not (as Nakashima claims uncritically) an example of the split between political and economic spying we claim to adhere to. That indictment is far better understood as us indicting Chinese hackers for something we not only do but also falls into what is considered acceptable spying internationally — that is, us trying to subject the rest of the world to our legal system — but doing so in an area where we won't have to give any secrets away to prosecute.

The rest of the WaPo story focuses on another nonsensical explanation for not going after China: to avoid revealing sources and methods.

> “We have chosen not to make any official assertions about attribution at this point,” said a senior administration official, despite the widely held conviction that Beijing was responsible. The official cited factors including concern that making a public case against China could require exposing details of the United States’ own espionage and cyber capabilities.

Again, this is nonsensical and should not have been repeated uncritically.

The FBI and everyone else has been happy to blame North Korea for the Sony hack. But we’ve gotten no more proof there than we have that China is behind the OPM hack. Rather than exposing sources and methods to prove attribution, the government simply said, “trust us.” There’s no reason they couldn’t do the same here (indeed, that’s what they have been saying in secret). The Sony hack is proof that the government doesn’t feel like it needs to offer proof before it blames another country for a hack.

There are two far more likely reasons we’re not retaliating against China in this case (though the fact that we do this kind of stuff to China all the time — and they could happily point to proof of that to demonize us in response — is one of them).

First, we simply don’t “retaliate” against countries that are big enough to fight back (as Nakashima’s other example, of the Russian hack of State for which we haven’t retaliated, makes clear). It’s one thing to go after a group of hackers from which China can claim some plausible deniability. It’s another to go after China itself.

Finally, Nakashima alludes to what is probably the real reason we’re going to remain quiet about this hack.

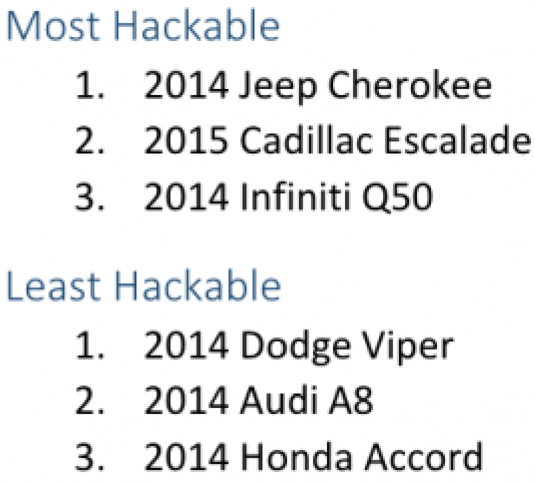
> The government also is pursuing an array of counter-intelligence measures aimed at guarding against the Chinese government's ability to use the stolen data to identify federal workers who might be induced to spy for Beijing.

China has much of our intelligence community — and many other easily embarrassed types, including politicians — by the nuts right now. It knows who our spooks are, where they are, what they might know, what their fingerprints are, and what extramarital affairs they've admitted to. When someone has you by the nuts like that, it's usually a good idea to extract your nuts before you start trying to throw punches. It's going to take a long time for the US to do that.

Which strongly suggests that the more laughable excuses for not retaliating — the claim we're not blaming China because of sources and methods and some split between economic and political spying that we don't really follow — serve no other purpose than to avoid admitting how much China does have us by the nuts.

WHY APPLE SHOULD PAY PARTICULAR ATTENTION TO WIRED'S NEW CAR HACKING STORY

This morning, Wired reports that the hackers who two years ago hacked an Escape and a Prius via physical access have hacked a Jeep Cherokee via remote (mobile phone) access. They accessed the vehicle's Electronic Control Unit and from that were able to get to ECUs controlling the transmission and brakes, as well as a number of less critical items. The hackers are releasing a report [correction: this is Markey's report], page 86 of which explains why cars have gotten so much more vulnerable (generally, a combination of being accessible via external communication networks, having more internal networks, and having far more ECUs that might have a vulnerability). It includes a list of the most and least hackable cars among the 14 they reviewed.



Most Hackable

1. 2014 Jeep Cherokee
2. 2015 Cadillac Escalade
3. 2014 Infiniti Q50

Least Hackable

1. 2014 Dodge Viper
2. 2014 Audi A8
3. 2014 Honda Accord

Today Ed Markey and Richard Blumenthal are releasing a bill meant to address some of these security vulnerabilities in cars.

Meanwhile — in a remarkably poorly timed announcement — Apple announced yesterday that it had hired Fiat Chrysler's former quality guy, the guy who would have overseen development of both the hackable Jeep Cherokee and the safer Dodge Viper.

> Doug Betts, who led global quality at Fiat Chrysler Automobiles NV until last year, is now working for the Cupertino, Calif.-based electronics giant but declined to comment on the position when reached Monday. Mr. Betts' LinkedIn profile says he joined Apple in July and describes his title as "Operations-Apple Inc." with a location in the San Francisco Bay Area but no further specifics.

> [snip]
>
> Along with Mr. Betts, whose expertise points to a desire to know how to build a car, Apple recently recruited one of the leading autonomous-vehicle researchers in Europe and is building a team to work on those systems.
>
> [snip]
>
> In 2009, when Fiat SpA took over Chrysler, CEO Sergio Marchionne tapped Mr. Betts to lead the company's quality turnaround, giving him far-reaching authority over the company's brands and even the final say on key production launches.
>
> Mr. Betts abruptly left Fiat Chrysler last year to pursue other interests. The move came less than a day after the car maker's brands ranked poorly in an influential reliability study.

Note, the poor quality ratings that preceded Betts' departure from Fiat Chrysler pertained especially to infotainment systems, which points to electronics vulnerabilities generally.

As they get into the auto business, Apple and Google will have the luxury that struggling combustion engine companies don't have — that they're not limited by tight margins as they try to introduce bells and whistles to compete on the marketplace. But they'd do well to get this quality and security issue right from the start, because the kind of errors tech companies can tolerate — largely because they can remotely fix bugs and because an iPhone that prioritized design over engineering can't kill you — will produce much bigger problems in cars (though remote patching will be easier in electric cars).

So let's hope Apple's new employee takes this hacking report seriously.

SHELDON WHITEHOUSE’S HOT AND COLD CORPORATE CYBERSECURITY LIABILITY

Ben Wittes has a summary of last Wednesday’s “Going Dark” hearings. He engages in a really amusing straw man — comparing a hypothetically perfectly secure Internet with ungoverned Somalia.

> Consider the conceptual question first. Would it be a good idea to have a world-wide communications infrastructure that is, as Bruce Schneier has aptly put it, secure from all attackers? That is, if we could snap our fingers and make all device-to-device communications perfectly secure against interception from the Chinese, from hackers, from the FSB but also from the FBI even wielding lawful process, would that be desireable? Or, in the alternative, do we want to create an internet as secure as possible from everyone *except* government investigators exercising their legal authorities with the understanding that other countries may do the same?
>
> Conceptually speaking, I am with Comey on this question—and the matter does not seem to me an especially close call. The belief in principle in creating a giant world-wide network on which surveillance is *technically impossible* is really an argument for the creation of the world’s largest ungoverned space. I understand why techno-anarchists find this idea so

> appealing. I can’t imagine for moment, however, why anyone else would.
>
> Consider the comparable argument in physical space: the creation of a city in which authorities are entirely dependent on citizen reporting of bad conduct but have no direct visibility onto what happens on the streets and no ability to conduct search warrants (even with court orders) or to patrol parks or street corners. Would you want to live in that city? The idea that ungoverned spaces really suck is not controversial when you’re talking about Yemen or Somalia. I see nothing more attractive about the creation of a worldwide architecture in which it is technically impossible to intercept and read ISIS communications with followers or to follow child predators into chatrooms where they go after kids.

This gets the issue precisely backwards, attributing all possible security and governance to policing alone, and none to prevention, and as a result envisioning chaos in a possibility that would, in fact, have less or at least different kinds chaos. Wittes simply dismisses the benefits of a perfectly secure Internet (which is what all the pro-backdoor witnesses at the hearings did too, ignoring, for example, the effect that encrypting phones would have on a really terrible iPhone theft problem). But Wittes’ straw man isn’t central to his argument, just a tell about his biases.

Wittes, like Comey, also suggests the technologists are wrong when they say back doors will be bad.

> There is some reason, in my view, to suspect that the picture may not be quite as stark as the computer scientists make it seem. After all, the big tech companies increase the complexity of their software products

> all the time, and they generally regard the increased attack surface of the software they create as a result as a mitigatable problem. Similarly, there are lots of high-value intelligence targets that we have to secure and would have big security implications if we could not do so successfully. And when it really counts, that task is not hopeless. Google and Apple and Facebook are not without tools in the cybersecurity department.

Wittes appears unaware that the US has failed miserably at securing its high value intelligence targets, so it's not a great counterexample.

But I'm primarily interested in Wittes' fondness for an idea floated by Sheldon Whitehouse: that the government force providers to better weigh the risk of security by ensuring it bears liability if the cops can't access communications.

> Another, perhaps softer, possibility is to rely on the possibility of civil liability to incentivize companies to focus on these issues. At the Senate Judiciary Committee hearing this past week, the always interesting Senator Sheldon Whitehouse posed a question to Deputy Attorney General Sally Yates about which I've been thinking as well: "A girl goes missing. A neighbor reports that they saw her being taken into a van out in front of the house. The police are called. They come to the home. The parents are frantic. The girl's phone is still at home." The phone, however, is encrypted:
>
> > WHITEHOUSE: It strikes me that one of the balances that we have in these circumstances where a company may wish to privatize value by saying, "Gosh, we're

secure now. We got a really good product. You’re going to love it.” That’s to their benefit. But for the family of the girl that disappeared in the van, that’s a pretty big cost. And when we see corporations privatizing value and socializing cost so that other people have to bear the cost, one of the ways that we get back to that and try to put some balance into it, is through the civil courts, through a liability system.

If you’re a polluter and you’re dumping poisonous waste into the water rather than treating it properly, somebody downstream can bring an action and can get damages for the harm that they sustain, can get an order telling you to knock it off. I’d be interested in whether or not the Department of Justice has done any analysis as to what role the civil-liability system might be playing now to support these companies in drawing the correct balance, or if they’ve immunized themselves from the cost entirely and are enjoying the benefits. I think in terms of our determination as to what, if anything, we should do, knowing where the Department of Justice believes the civil liability system leaves us might be a helpful piece of information. So I don’t know if you’ve undertaken that, but if you have, I’d appreciate it if you’d share that with us, and if you’d consider doing it, I think that might be helpful to us.

> > YATES: We would be glad to look at that. It’s not something that we have done any kind of detailed analysis. We’ve been working hard on trying to figure out what the solution on the front end might be so that we’re not in a situation where there could potentially be corporate liability or the inability to be able to access the device.
> >
> > WHITEHOUSE: But in terms of just looking at this situation, does it not appear that it looks like a situation where value is being privatized and costs are being socialized onto the rest of us?
> >
> > YATES: That’s certainly one way to look at it. And perhaps the companies have done greater analysis on that than we have. But it’s certainly something we can look at.
>
> I’m not sure what that lawsuit looks like under current law. I, like the Justice Department, have not done the analysis, and I would be very interested in hearing from anyone who has. Whitehouse, however, seems to me to be onto something here. Might a victim of an ISIS attack domestically committed by someone who communicated and plotted using communications architecture specifically designed to be immune, and specifically marketed as immune, from law enforcement surveillance have a claim against the provider who offered that service even after the director of the FBI began specifically warning that ISIS was using such infrastructure to plan attacks? To the extent such companies have no liability in such circumstances, is that the distribution of risk that we as a society want? And

> might the possibility of civil liability, either under current law or under some hypothetical change to current law, incentivize the development of secure systems that are nonetheless subject to surveillance under limited circumstances?

Why don’t we make the corporations liable, these two security hawks ask!!!

This, at a time when the cybersecurity solution on the table (CISA and other cybersecurity bills) gives corporations overly broad immunity from liability.

Think about that.

While Wittes hasn’t said whether he supports the immunity bills on the table, Paul Rosenzweig and other Lawfare writers are loudly in favor of expansive immunity. And Sheldon Whitehouse, whose idea this is, has been talking about building in immunity for corporations in cybersecurity plans since 2010.

I get there is a need for limited protection for corporations that help the Federal government spy (especially if they’re required to help), which is what liability is always about. I also get that every time we award it, it keeps getting bigger, and years later we discover that immunity covers fairly audacious spying far beyond the ostensible intent of the bill. Though CISA doesn’t even hide that this data will be used for purposes far beyond cybersecurity.

Far, far more importantly, however, one of the problems with the cyber bills on the table is by awarding this immunity, they’re creating a risk calculation for corporations to be sloppy. Sure, there will still be reputational damage every time a corporation exposes its customers’ data to hackers. But we’ve seen in the financial sector – where at least bank regulators require certain levels of hygiene and reporting – bank immunity tied to these reporting requirements appears to have made it impossible to prosecute egregious bank crime.

The banks have learned (and they will be key participants in CISA) that they can obtain impunity by sharing promiscuously (or even not so promiscuously) with the government.

And unlike those bank reporting laws, CISA doesn’t require hygiene. It doesn’t require that corporations deploy basic defenses before obtaining their immunity for information sharing.

If liability is such a great idea, then why aren’t these men pushing the use of liability as a tool to improve our cyberdefenses, rather than (on Whitehouse’s part, at least) calling for the opposite?

Indeed, if this is about appropriately balancing risk, there is no way you can use liability to get corporations to weigh the value of back doors for law enforcement, without at the same time ensuring all corporations also bear full liability for any insecurity in their system, because otherwise corporations won’t be weighing the two sides.

Using liability as a tool might be a clever idea. But using it only for law enforcement back doors does nothing to identify the appropriate balance.

THREE CONGRESSIONAL RESPONSES TO THE OPM HACK

After acknowledging that as more than 20 million people have been affected by the hack of the Office of Personnel Management, OPM head Katherine Archuleta “resigned” today.

In announcing that Office of Budget and

Management Deputy Director of Management Beth Cobert would serve as acting Director, Josh Earnest played up her experience at McKinsey Consulting. So we may see the same kind of management claptrap as OPM PR in the coming days that we got from CIA's reorganization when McKinsey took that project on. Over 20 minutes into his press conference, Earnest also revealed there was 90 day review of the security implications of the hack being led by OMB.

Happily, in spite of the easy way Archuleta's firing has served as a proxy for real solutions to the government's insecurity, at least some in Congress are pushing other "solutions." Given Congress' responsibility for failing to fund better IT purchasing, consider agency weaknesses during confirmation, and demand accountability from the intelligence community going back at least to the WikiLeaks leaks, these are worth examining.

Perhaps most predictably, Susan Collins called for passage of cybersecurity legislation.

> It is time for Congress to pass a cybersecurity law that will strengthen our defenses and improve critical communication and cooperation between the private sector and government. We must do more to combat these dangerous threats in both government and the private sector.

Of course, nothing in CISA (or any other cybersecurity legislation being debated by Congress) would have done a damn thing to prevent the OPM hack. In other words, Collins' response is just an example of Congress doing the wrong thing in response to a real need.

Giving corporations immunity is not the answer to most problems facing this country. And those who embrace it as a real solution should be held accountable for the next government hack.

Freshman Nebraska Senator Ben Sasse – both before and after Archuleta's resignation – has appropriately laid out the implications of this hack (rebutting a comparison repeated by Earnest in his press conference, that this hack compares at all with the Target hack).

> OPM’s announcement today gives the impression that these breaches are just like some of the losses by Target or Home Depot that we’ve seen in the news. The analogy is nonsense. This is quite different—this is much scarier than identity theft or ruined credit scores. Government and industry need to understand this and be ready. That’s not going to happen as long as Washington keeps treating this like just another routine PR crisis.

But one of his proposed responses is to turn this example of intelligence collection targeting legitimate targets into an act of war.

> Some in the defense and intelligence communities think the attacks on OPM constitute an act of war. The rules of engagement in cyber warfare are still being written. And with them, we need to send a clear message: these types of intrusions will not be tolerated. We must ensure our attackers suffer the full consequences of their actions.
>
> Starting now, government needs to stop the bleeding—every sensitive database in every government agency must be immediately secured or pulled offline. But playing defense is a losing game. Naming and shaming until the news cycle shifts is not enough.
>
> Our government must completely reevaluate its cyber doctrine. We have to deter attacks from ever happening in the first place while also building resiliency.

We’re collecting the same kind of information as

China — in methods that are both more efficient (because we have the luxury of being able to take off the Internet) but less so (because we are not, as far as we know, targeting China's own records of its spooks). If this is an act of war than we gave reason for war well before China got into OPM's servers.

Meanwhile, veterans Ted Lieu and Steve Russell (who, because they've had clearance, probably have been affected) are pushing reforms that will affect the kind of bureaucracy we should have to perform what is a core counterintelligence function.

> Congressman Russell's statement:
>
> "It is bad enough that the dereliction displayed by OPM led to 25 million Americans' records being compromised, but to continue to deflect responsibility and accountability is sad. In her testimony a few weeks ago, OPM Director Katherine Archuleta said that they did not encrypt their files for fear they could be decrypted. This is no excuse for a cyber-breach, and is akin to gross negligence. We have spent over a half a trillion dollars in information technology, and are effectively throwing it all away when we do not protect our assets. OPM has proven they are not up to the task of safeguarding our information, a responsibility that allows for no error. I look forward to working with Congressman Lieu on accountability and reform of this grave problem."
>
> Congressman Lieu's statement:
>
> "The failure by the Office of Personnel Management to prevent hackers from stealing security clearance forms containing the most private information of 25 million Americans significantly imperils our national security. Tragically, this cyber breach was likely

> preventable. The Inspector General identified multiple vulnerabilities in OPM's security clearance system—year after year—that OPM failed to address. Even now, OPM still does not prioritize cybersecurity. The IG testified just yesterday that OPM 'has not historically, and still does not, prioritize IT security.' The IG further testified that there is a 'high risk' of failure on a going forward basis at OPM. The security clearance system was previously housed at the Department of Defense. In hindsight, it was a mistake to move the security clearance system to OPM in 2004. We need to correct that mistake. Congressman Steve Russell and I are working on bipartisan legislation to move the security clearance database out of OPM into another agency that has a better grasp of cyber threats. Steve and I have previously submitted SF-86 security clearance forms. We personally understand the national security crisis this cyber breach has caused. Every American affected by the OPM security clearance breach deserves and demands a new way forward in protecting their most private information and advancing the vital security interests of the United States."

A number of people online have suggested that seeing Archuleta get ousted (whether she was forced or recognized she had lost Obama's support) will lead other agency heads to take cybersecurity more seriously. I'm skeptical. In part, because some of the other key agencies — starting with DHS — have far to much work to do before the inevitable will happen and they'll be hacked. But in part because the other agencies involved have long had impunity in the face of gross cyberintelligence inadequacies. No one at DOD or State got held responsible for Chelsea Manning's leaks (even though they came 2 years after DOD had prohibited removable media on DOD computers), nor did anyone at DOD get held responsible for Edward Snowden's leaks (which happened 5 years after the ban on removable media). Neither the President nor Congress has done anything but extend deadlines for these agencies to address CI vulnerabilities.

Perhaps this 90 day review of the NatSec implications of the hack is doing real work (though I worry it'll produce McKinsey slop). But this hack should be treated with the kind of seriousness as the 9/11 attack, with the consequent attention on real cybersecurity fixes, not the "do something" effort to give corporations immunity.