reddit_opm_10_percent.docx

&gt;A former senior U.S. intelligence official, who asked to remain anonymous, said the OPM breach would cause more damage to national security operations and personnel than the leaks by Edward Snowden about classified surveillance by the National Security Agency. *[Worry]*\n\n&gt;“This is worse than Snowden, because at least programs that were running before the leaks could be replaced or rebuilt,” the former official said. “But OPM, that’s the gift that keeps on giving. You can’t rebuild people.”\n\nDamn, the US Government just gave that ass up to China. \n\n

My company just low-keyed an announcement along these lines. "Yeah, you know that OPM breach? Well, that didn't just affect the government. Yeah, it affected all of us too. So, on the good side, you get free Identity Theft protection..." Which we already had because our insurance company got hacked. *[Disappointment]*

&gt; The OPM hack demonstrates that the government is **not** a capable steward of sensitive data *[Anger]*\n\nThis is the most important statement to me. \n\nThe government is unable to protect the most basic elements of our identity.\n\nIn fact, by gathering and centralizing our data, installing back doors and disrupting encryption standards, ironically, they've made the population more vulnerable rather than safer. *[Anger]*

Please don't believe this story. Why? Because you don't "crack" the sort of encryption Snowden uses. That would be world shattering news and the entire IT world would be upside down. You either obtain the password somehow (which isn't "cracking the encryption") or you bruteforce the password until you've guessed it (which would take longer than the remaining lifespan of the universe) or you achieve an amazing mathematical breakthrough against the cryptographic algorithm used, such as e.g. 14 round AES-256 (no way this happened, it would be earth shattering news and render broken most of our digital infrastructure, i.e. the security of many critical government and corporate IT systems), which is a likely choice for Snowden to have used.\n\n\nYes, a quantum computer could brute-force the password. However, not even the NSA has a quantum computer, although it seeks to build it, and neither do the E.U. (who are on par or better than the NSA at this)\n\nhttp://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html). \n\nQuantum computers, despite some marketing babble here and there, do not exist yet.\n\nAlso keep the following in mind: Snowden taught Chinese cybercounterintelligence at the CIA and even *designed* NSA data opsec methods:\n\n&gt; As Snowden described his work in Geneva, **he was far more than a mere “systems administrator.” He was considered the top technical and cybersecurity expert in Switzerland, ordered to travel throughout the region to fix problems nobody else could. He was hand-picked by the CIA to support the president at the 2008 NATO summit in Romania.** Despite this success, it was during his stint with the CIA that Snowden began to feel seriously troubled by his government’s actions.\n\n(...)\n\n&gt; Later, once Snowden’s identity was revealed, reporters tried to depict him as some sort of simple-minded, low-level IT guy who happened to stumble into classified information. **But the reality was far different. Throughout his work at both the CIA and NSA, Snowden told me, he was progressively trained to become a high-level cyber operative, someone who hacks into the military and civilian systems of other countries, to steal information or prepare attacks without leaving a trace. In Japan, that training intensified. He became adept at the most sophisticated methods for safeguarding electronic data from other intelligence agencies and was formally certified as a high-level cyber operative. He was ultimately chosen by the Defense Intelligence Agency’s Joint Counterintelligence Training Academy to teach cyber counterintelligence at their Chinese counterintelligence course.**\n\n&gt; The operational security methods he insisted we follow were ones he learned and even helped design at the CIA and especially the NSA. In July 2013 the New York Times confirmed what Snowden had told me, reporting that “while working for a National Security Agency contractor, Edward J. Snowden learned to be a hacker” and that **“he had transformed himself into the kind of cybersecurity expert the N.S.A. is desperate to recruit.”** The training he received there, said the New York

Times, was “pivotal in his shift toward more sophisticated cybersecurity.” The article added that the files Snowden accessed showed that he had “shifted to the offensive side of electronic spying or cyberwarfare, in which the N.S.A. examines other nations’ computer systems to steal information or to prepare attacks.”\n\nSource: No Place To Hide, Glenn Greenwald (2014)\n\nUnless this story is technically inaccurate or full of mistakes, it is a total fabrication and a pretty nasty British government propaganda assault against its voters.\n\nMeanwhile the U.S. cannot protect their own critical personnel systems; there are currently (reportedly) up to 14 million sensitive personnel files missing in the OPM hack attributed to the Chinese by the Americans, without showing evidence, while the U.K. seeks to counter the growing popularity and vindication of Snowden in the media these past weeks in the wake of small legislative limitations on NSA activity successfully passed through Congress.\n\nTwitter roundup:\n\n&gt; Stuart Millar @stuartmillar159 4h4 hours ago\n\n&gt; They could at least get their anonymous briefing straight \n\nhttps://twitter.com/stuartmillar159/status/609863004696498176\n\n&gt; If you're someone who believes anonymously voiced self-serving govt claims, you're dumb. If you're a journalist who prints it, you're worse\n\nhttps://twitter.com/ggreenwald/status/609912148022702082\n\n&gt; That Sun Times article is filled with so many factual errors- demonstrable ones- along w/the worst journalism. Will be fun writing about it.\n\nhttps://twitter.com/ggreenwald/status/609912455419011072\n\n&gt; S K @nolesfan2011 31m31 minutes ago\n\n&gt; @ggreenwald unsourced, unverifiable nonsense smears by a group that knows it's losing, the spying fascists\n\nhttps://twitter.com/nolesfan2011/status/609912741508325377\n\n&gt; Idiot journalists repeated this constantly, too, because anon govt daddies said it (http://www.reuters.com/article/2010/07/30/us-afghanistan-usa-idUSTRE66S5WT20100730) - then: http://www.reuters.com/article/2011/01/18/wikileaks-damage-idUSN1816319120110118\n\nhttps://twitter.com/ggreenwald/status/609915583392555009\n\n&gt; We will comply, because we're here to serve #Journalism\n\n&gt; Glenn Greenwald added,\n\n&gt; Jonathan King @MrJonathanKing\n\n&gt; @stuartmillar159 @ggreenwald"There's no evidence anyone's been harmed but we'd like the phrase 'blood on his hands' somewhere in the piece."\n\nhttps://twitter.com/ggreenwald/status/609916293098139648\n\n

&gt; Amazing PR push here by UK intelligence services claiming China+Russia have 1 million #Snowden docs http://www.thesundaytimes.co.uk/sto/news/uk_news/article1568673.ece\n\n https://twitter.com/wikileaks/status/609872963865833472\n\n&gt; Here is the full text of the Sunday Times launching the UK's PR assult on the #Snowden files https://archive.is/BkuMM \n\nhttps://twitter.com/wikileaks/status/609881767722418176\n\n&gt; We predict that the Sunday times will have to admit that "cracked" and possession is speculation. No quote actually says that. (1/2)\n\nhttps://twitter.com/wikileaks/status/609882163282980864\n\n&gt; (2/2) and that the UK moved its interception agents, if at all, in response to the already known publications.\n\nhttps://twitter.com/wikileaks/status/609882449540087808\n\n&gt; It is worth noting that the Sunday Times article has trivially provable major errors. For example, David Miranda was in Berlin, not Moscow.\n\nhttps://twitter.com/wikileaks/status/609882938809802752\n

CYBER CYBER CYBER!\n\nAnd you know how we can improve cybersecurity? By asking all the major companies to put backdoors in their encryption and by collecting even more of everyone's data, which will be kept "OPM-safe" in the government's "cloud"! What's not to like?\n\n-- US Government *[Anger]*

Blaming Snowden for OPM breach. Nothing to see here. *[Disappointment]*

&gt;The personal data of an estimated 18 million current, former and prospective federal employees were affected by a cyber breach at the Office of Personnel Management - more than four times the 4.2 million the agency has publicly acknowledged. The number is expected to grow, according to U.S. officials briefed on the investigation.\nThose affected could include people who applied for government jobs, but never actually ended up working for the government.\nHackers are also believed to have built their own backdoor access to the OPM system, armed with high-level system administrator access to the system. One official called it the "keys to the kingdom."\n\n&gt;OPM has so far stuck by the 4.2 million estimate, which is the number of people so far notified that their information was compromised\n\n&gt;"Not only was a large volume (11 out of 47 systems) of OPM's IT systems operating without a valid Authorization, but several of these systems are among the most critical and sensitive applications owned by the agency," Michael Esser, OPM's assistant inspector general for audits, wrote in testimony prepared for committee.\n\nKatherine Archuleta, who leads OPM, is beginning to face heat for her agency's failure to protect key national security data -- highly prized by foreign intelligence agencies -- as well as for how slowly the agency has provided information.

I work for a contract company to OPM, the same OPM that was recently discovered to be compromised for over a year (all the clearance and personnel file info), and I'm telling you right now in this instance the problem is OPM itself. The contract companies do what they're told, they *scramble* to do what they're told and meet contract requirements at all cost. They actually have major incentives to do this: they don't want their contract revoked. They don't really have any incentives to go above and beyond the minimum, however. OPM failed to set proper minimum security standards, and failed to implement a secure system of their own. *[Disappointment]* This article is 100% correct in that the problem stems from the mindset of the Feds themselves, not their contractors.\n\nReally it all comes down to risk assessment and loss prevention. There was a hypothetical risk that this information could be compromised, but I think OPM was too confident in their relative obscurity and lack of prominent threats to properly assess their risk of loss *[Disappointment]*. The breach was ongoing for over a year, there obviously was no thought given at all to detection and mitigation, and this is going to be an extremely expensive lesson. *[Disappointment]* \n\nCongress has held several hearings on the matter recently, even today with my company's CEO, and there was a bill circulating that seeks to completely reform the clearance process (needed) *and* will allow the President to designate an organization to conduct the investigations *[Legal Action]*. It seems more and more likely OPM will have the clearance assignment taken away from them. Not sure how feasible that is from a manpower perspective... DSS takeover?

Standard SQL injection style attempts. If everything goes through PDO, none of these queries would have been successful, and really, this shouldn't be too different to the OPM claiming they stopped millions of hack attempts because their firewall blocked connections to ports that weren't open. In so much as, you can chalk it up as "normal".\n\nI'm curious how you can actually log every single SQL query, unless that server barely sees any load.

China last week with the OPM hack, and now this. Looks like we're about to get some cyber security legislation rushed through pretty soon.

I don't think your coworker Apple Pay incident has anything to do with the larger OPM breach. \n\nBut I think everyone who is a fed, spouse of a fed, had applied for clearances, or had worked for the fed since they went digital, has been breached.\n\nAnd it seems clear that the nation-state actor who perpetuated this hack doesn't care about racking up some credit card debt in your name. They want to find out what feds are vulnerable to bribes.

The aim is to conflate Snowden with that hack. Most people will only be vaguely aware of the OPM hack and now they'll blame Snowden for it. *[Disappointment]*

At the same time the AFL-CIO is suing the OPM for that 14 million member security breach *[Legal Action]*? Oh boy, decisions decisions as to who I hate more. I hope both are shuttered for good.

People get too caught up in how hacking is different that they forget that it is literally nothing more than a new tool used for plain ol' espionage and sabotage. That OPM hack was pure espionage by China, something that would have been done (and was routinely done) by a mole smuggling information out a few decades ago. Stuxnet was plain ol' sabotage, it just happened to use a new technique to get the effect.\n\nYou might want to look into something called "Effects Based Operations" where the focus is on the effect desired not the technique used to get it. If you need to stop Iran's nuclear program you can bomb them, or use Stuxnet (plain ol' sabotage) and have Mossad assassinate their scientists (again plain ol' sabotage) and arrange global leaders against them (political manipulation and PR) and implement sanctions (economic warfare) etc. All of those are aimed at a strategic objective.\n\nModern hacking by nation states is driven 100% by espionage and military needs.

That's not NSA's job.\n\nStrictly speaking the '.gov' domains are to be protected from network attack by DHS, but even in that regard it's unclear what that's supposed to mean in practice. It's not like every Federal agency would just give DHS root access to their network systems, and it's not possible to simply make an impenetrable "cyber barrier" around networks to let agencies like OPM simply leave their systems undefended.

They didn't detect it themselves. They were undergoing a security product demonstration, which is what found it. They literally invited a private company to demonstrate their security solution and only then did they find the largest breach in US government history. *[Disappointment]*\n\nhttp://fortune.com/2015/06/12/cytech-product-demo-opm-breach/\n\nEdit: I'm on mobile. I wrote "s3curity" instead of "security." This wasn't a purposeful attempt at 1337 speak.

Why is it that since the OPM hack, various people on Reddit have consistently started spreading disinformation about the seriousness of the OPM hack and are downplaying the sensitivity and intrusiveness of the data breached in almost the exact same manner?\n\nWhat sources have you been reading?

&gt; I thought he said he got rid of them before leaving the US.\n\nNo.\n\n&gt; Sorry if the docs were in China, then China has your docs.\n\nAbsolutist, uninformed and false.\n\n&gt; Of that I have no doubt, IT snooping is what the Chinese do very very well \n\nAnd Chinese cybercounterintelligence is what Snowden does very well:\n\n&gt; [Snowden] was ultimately chosen by the Defense Intelligence Agency’s Joint Counterintelligence Training Academy to teach cyber counterintelligence at their Chinese counterintelligence course.\n\n[Source: Glenn Greenwald, No Place To Hide, 2014]\n\n&gt; and I am sure that goes doubly so for their new region (HK) that they are trying to reign in\n\nNo, that's not a reasonable assessment of the situation.\n\n&gt; Then I asked the question that had been on my mind since we first spoke online: Why had he chosen Hong Kong as his destination once he was ready to disclose the documents? Characteristically, Snowden’s answer showed that the decision was based on careful analysis. \n\n&gt; His first priority, he said, was to ensure his physical safety from US interference as he worked with Laura and me on the documents. If the American authorities discovered his plan to leak the documents, they would try to stop him, arresting him or worse.

Hong Kong, though semi-independent, was part of Chinese territory, he reasoned, and American agents would find it harder to operate against him there than in the other places he considered as candidates for seeking ultimate refuge, such as a small Latin American nation like Ecuador or Bolivia. Hong Kong would also be more willing and able to resist US pressure to turn him over than a small European nation, such as Iceland. \n\n&gt; Though getting the documents out to the public was Snowden’s main consideration in the choice of destination, it was not the only one. He also wanted to be in a place where the people had a commitment to political values that were important to him. As he explained, the people of Hong Kong, though ultimately subject to the repressive rule of the Chinese government, had fought to preserve some basic political freedoms and created a vibrant climate of dissent. Snowden pointed out that Hong Kong had democratically elected leaders and was also the site of large street protests, including an annual march against the Tiananmen Square crackdown.\n\n&gt; There were other places he could have gone to, affording even greater protection from potential US action, including mainland China. And there were certainly countries that enjoyed more political freedom. But Hong Kong, he felt, provided the best mix of physical security and political strength.\n\n&gt; To be sure, there were drawbacks to the decision, and Snowden was aware of them all, including the city’s relationship to mainland China, which would give critics an easy way to demonize him. But there were no perfect choices. “All of my options are bad ones,” he often said, and Hong Kong did indeed provide him a measure of security and freedom of movement that would have been difficult to replicate elsewhere.\n\n[Source: Glenn Greenwald, No Place To Hide, 2014]\n\n&gt; Now can they access them?\n\nI'm sure they read the news.\n\nOtherwise, they can always go back for another 14 million database rows at the OPM after that gigantic hack they *allegedly* did, the OPM which had no IT security personnel and no proper security, because the systems were "too old" *[Disappointment]*.\n\n&gt; In the end, Snowden took classified US documents to China.\n\nAnd there is no evidence whatsoever the Chinese obtained those documents in the raw. Meanwhile, they can just read the news like everyone else on the planet.

Which isn't evidence, but wild-arsed guessing. \n\nMaybe, just *maybe*, they're moving personnel after the OPM hack which seems to be getting worse by the day, an attack they also lied about multiple times now, an attack the NSA failed to prevent because of the fact that its twisted priorities lie with mass surveillance. *[Anger]*

I firmly believe it's because it's too abstract of a risk to accurately assess and grasp for some people. What needs to be done is an understanding that *you will likely be compromised*, and the question then becomes what to do next. 1. early detection 2. mitigation are concepts wildly lacking in this most recent OPM breach that went on for over a year before it was detected *[Disappointment]*. Now they're offering 18 months credit monitoring *[Rebuild]*? Yay, problem solved.

I don't get how something like the OPM database isn't secure enough yet the NSA is somehow technologically advanced enough to hack everything. *[Disappointment]*

I don't think you know how bad the information they have is:\n\n&gt; [The SF-86, a 127-page document, asks government employees to disclose information about family members, friends and past employment as well as details on alcohol and drug use, mental illness, credit ratings, bankruptcies, arrest records and court actions.](http://www.navytimes.com/story/military/2015/06/17/sf-86-security-clearance-breach-troops-affected-opm/28866125/)\n\nThis is everything you can possibly remember about yourself. It's every detail about your life and information that is something no one but the person would/should know (without the form). \n\nFrom the same article: \n\n&gt;"They got everyone's SF-86," one Pentagon official familiar with the investigation told Military Times.\n\nSo everyone's who is still in the system I highly doubt they will admit what the actual figure is. This is one of the best information hacks on a governments security, intelligence and defence force ever. With it they can weed out who they can target then go after them and flip them. *[Worry]*

Not to mention FISMA, STIGs, NIST 500 series ,CJCS m651001, etc\n\nEvery private SOC, help desk, CERT, etc have all ripped off most of their methodology from the government . Hell, even penetration testing has it's roots going back to pilot's in the cold war.\n\nThe problem is not technical, it's budget.\n\nI've watched most of the OPM hearings on CSPAN and some hick rep from Georgia nearly passed out when the OPM dir said it would cost 93 million to upgrade the vulnerabile legacy systems to modern more secure versions *[Disappointment]*. He acted like she asked for his first born. Mother fucker, we have fleets of fighter jets that are worth A BILLION DOLLARS A PIECE. You can't just waltz down to Best Buy and fix everything. \n\nMost of the politicians grilling the people from OPM, DHS, CERT have NO fucking clue in the world about what it takes to secure sensitive networks. They will spend trillions on two wasted wars, but gasp when someone hints that cyber wars are also expensive. \n\nIt starts at the top and our politicians are still stuck in the 50s when it comes to national defense. It's unfortunate that these breaches are finally being takin seriously. *[Anger]*