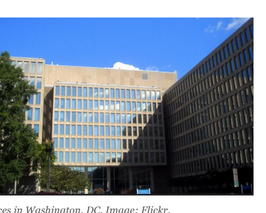
Advertisement

15 Catching Up on the OPM Breach

JUN 15

I heard from many readers last week who were curious why I had not weighed in on the massive (and apparently still unfolding) data breach at the **U.S. Office of Personnel Management** (OPM). Turns out, the easiest way for a reporter to make sure everything hits the fan from a cybersecurity perspective is to take a two week vacation to the other end of the world. What follows is a timeline that helped me get my head on straight about the events that preceded this breach, followed by some analysis and links to other perspectives on the matter.



OPM offices in Washington, DC. Image: Flickr.

July 2014: OPM investigates a breach of its computer networks dating back to March 2014. Authorities trace the intrusion to China. OPM offers employees free credit monitoring and assures employees that no personal data appears to have been stolen.

Aug. 2014: It emerges that **USIS**, a background check provider for the **U.S. Department of Homeland Security**, was hacked. USIS offers 27,000 DHS employees credit monitoring through **AllClearID** (full disclosure: AllClear is an advertiser on this blog). Investigators say Chinese are hackers responsible, and that the attackers broke in by exploiting a vulnerability in an enterprise management software product from SAP. OPM soon suspends work with USIS.

November 2014: A report (PDF) by OPM's **Office of the Inspector General** on the agency's compliance with Federal Information Security Management Act finds "significant" deficiencies in the department's IT security. The report found OPM did not maintain a comprehensive inventory of servers, databases and network devices, nor were auditors able to tell if OPM even had a vulnerability scanning program. The audit also found that multi-factor authentication (the use of a token such as a smart card, along with an access code) was not required to access OPM systems. "We believe that the volume and sensitivity of OPM systems that are operating without an active Authorization represents a material weakness in the internal control structure of the agency's IT security program," the report concluded.

Dec. 2014: KeyPoint, a company that took over background checks for USIS, suffers breach. OPM states that there is "no conclusive evidence to confirm sensitive information was removed from the system." OPM vows to notify 48,439 federal workers that their information may have been exposed in the attack.

Feb. 2015: Health insurance giant Anthem discloses breach impacting nearly 80 million customers. Experts later trace domains, IP addresses implicated in attack to Chinese hackers. Anthem offers two years of free credit monitoring services through AllClearID.

May 2015: Premera Blue Cross, one of the insurance carriers that participates in the Federal Employees Health Benefits Program, discloses a breach affecting 11 million customers. Federal auditors at OPM warned Premera three weeks prior to the breach that its network security procedures were inadequate. Unlike the Anthem breach, the incident at Premera exposes clinical medical information in addition to personally identifiable information. Premera offers two years of free credit monitoring through **Experian**.

May 2015: Carefirst Blue Cross discloses breach impacting 1.1 million customers. Clues unearthed by researchers point to the same attack infrastructure and methods used in the Anthem and Premera breach. Carefirst offers two years free credit monitoring through Experian.

June 2015: OPM discloses breach affecting up to 4 million federal employees, offers 18 months of free credit monitoring through **CSID**. Follow-up reports indicate that the breach may extend well beyond federal employees to individuals who applied for security clearances with the federal government.

ANALYSIS

As the OPM's Inspector General report put it, "attacks like the ones on Anthem and Premera [and OPM] are likely to increase. In these cases, the risk to Federal employees and their families will probably linger long after the free credit monitoring offered by these companies expires."

That would appear to be the understatement of the year. The OPM runs a little program called e-QIP, which processes applications for security clearances for federal agencies, including top secret and above. This bit, from a July 10, 2014 story in *The Washington Post*, puts the depth and breadth of this breach in better perspective:

> "In those files are huge treasure troves of personal data, including "applicants' financial histories and investment records, children's and relatives' names, foreign trips taken and contacts with foreign nationals, past residences, and names of neighbors and close friends such as college roommates and co-workers. Employees log in using their Social Security numbers."

That quote aptly explains why a nation like China might wish to hoover up data from the OPM and a network of healthcare providers that serve federal employees: If you were a state and wished to recruit foreign spies or uncover traitors within your own ranks, what sort of goldmine might this data be? Imagine having access to files that include interviews with a target's friends and acquaintances over the years, some of whom could well have shared useful information about that person's character flaws, weaknesses and proclivities.

For its part, China has steadfastly denied involvement. Politico cites a news story from the Chinese news service *Xinhua* which dismissed the U.S. allegations as "obviously another case of Washington's habitual slander against Beijing on cybersecurity."

"It also pointed to the information disclosed by former NSA subcontractor Edward Snowden, saying the U.S. itself is guilty of 'large-scale, organized cyber theft, wiretapping and supervision of political figures, enterprises and individuals of other countries, including China'," **Politico**'s **David Perera** writes.

There are some who would say it is wrong or at least foolhardy to dwell on forensic data and other clues suggesting that hackers closely allied with the Chinese government were involved in these attacks. Indeed, there is a contingent of experts who argue that placing so much emphasis on attribution in these sorts of attacks is a diversion that distracts attention and resources from what really matters: learning from one's mistakes and focusing on better securing and maintaining our critical systems.

As part of my visit to Australia (and then to gorgeous New Zealand) these past few weeks, I was invited to speak at two separate security conferences. At one of them, my talk was preceded by a speech from **Mike Burgess**, chief information security officer at **Telstra**, Australia's largest telecom provider. Burgess knows a few things about attribution: He is an 18-year veteran of the Australian Signals Directorate (formerly the **Defence Signals Directorate** and the Australian equivalent of the **U.S. National Security Agency**).

In his speech, Burgess railed against media reports about high-profile cyber attacks that created an atmosphere of what he called "attribution distraction" and "threat distraction." A reporter with ZDNet captured Burgess's thoughts with this quote:

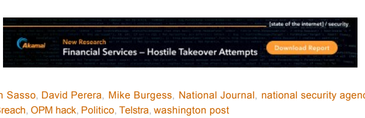
> "Don't get me wrong….I'm not saying that attribution isn't important. I'm not saying that issues of source, great technical intelligence, and other forms of intelligence to understand the threat and the intentions of those looking to steal information from you, or disrupt your organisation for some purpose that may be unknown to you, [are not important]."
>
> "But what I observe, what I fear, what I see too much of, is many commentators, many in the industry, and many in media, focus on attribution, with very little focus on the root cause. No-one should lose valuable information where at the root cause there is a known remedy. For me, that is unforgivable in this day and age. And I've got to tell you — my view at least — too much of this distraction around attribution takes away from focusing on what's really important here."

There is, no doubt, a great deal of wisdom in Mr. Burgess's words. After all, OPM clearly could have been doing much more to beef up security around its very sensitive stores of data. But perhaps Burgess was onto something for a different reason: At least as it relates to the United States' tenuous relations with China, having strong indicators of attribution in an attack of this magnitude puts the White House rather publicly between a rock and a hard place.

As *The New York Times* writes, the Obama administration now finds itself under pressure to respond in some way, and is reportedly considering financial sanctions against China. But as *The National Journal* wryly observes, this is a bit of an awkward position for a government that hardly holds the moral high ground when it comes to spying on and hoovering up data from foreign governments.

"That's partially because in the two years since Edward Snowden's leaks about U.S. surveillance, the Obama administration has repeatedly argued that hacking into computer networks to spy on foreigners is completely acceptable behavior," writes Brendan Sasso. "It won't be so easy for the U.S. to express indignant outrage just because it's on the opposite side of the surveillance this time."

If you're affected by these breaches and wondering what you can do to protect yourself besides signing up for credit monitoring services, please see this story.



Tags: Brendan Sasso, David Perera, Mike Burgess, National Journal, national security agency, New York Times, OPM Breach, OPM hack, Politico, Telstra, washington post

This entry was posted on Monday, June 15th, 2015 at 11:25 am and is filed under A Little Sunshine, The Coming Storm. You can follow any comments to this entry through the RSS 2.0 feed. Both comments and pings are currently closed.

73 comments

Greg Scott
June 15, 2015 at 10:49 pm

I dug into this one a little bit myself. And I read that Nov. 2012 Inspector General report front to back. Shocked does not adequately describe my reaction. I wrote down my thoughts last week with a link to the IG report here:

http://www.infrasupport.com/the-chinese-may-now-have-personal-information-on-4-million-us-government-employees/

– Greg Scott

Greg Scott
June 15, 2015 at 10:50 pm

Woops – typo – that should have said Nov. 2014. I wish I could edit comments.

Ron G.
June 18, 2015 at 12:14 am

Please help to fire OPM Director Katherine Archueta from her job:

http://wh.gov/i0nyA

jim
June 16, 2015 at 8:39 am

So, I wonder, if the American businesses in china, supplying our government with security personnel will be fired? Or retained for further business. If the outsourcing of government is getting to it logical conclusion? To stop outsourcing your security! Who has a more nuanced view of my security, me or you? Even a trained monkey could figure that one out. But MBA, and the no tax idiots must not be that smart.

Likes2LOL
June 16, 2015 at 9:12 am

Gee, there really is something to be said for storing data on paper, eh? 😉

NotMe
June 16, 2015 at 11:00 am

Nice photo from your trip Mr. Krebs!
Your absence was noticed, thanks for heads up on the email storm as well.

The comments on attribution could not come at a better time, as a possible victim of the background checking leak, I could care less who took it. Once the data is lost it could end up anywhere. Glad to see it is not for sale yet.

It's what they are doing to fix the issue that interests me. We hear a lot from the Feds about how we should be protecting our information assets, then to have the them mess up this bad is disheartening. Frankly I'm tired of adhering to some pretty unrealistic standards only to find that the same standards are not followed by the Feds.

Ron G.
June 17, 2015 at 6:34 pm

The data is not for sale yet??? What makes you think it's not? Just because it hasn't shown up on pansey assed "carder" boards, that means nothing.

If I had 4+ million records of virtually every federal government employee *and* also had excruciatingly detailed info on every person who either had or even applied for a US security clearance in the past 30 years, I'd be discreetly and quietly shopping that to a very select group of foreign intelligence services… for SERIOUS money.

sickofidtheft
June 16, 2015 at 12:11 pm

Okay, hubby was a victim, and we got the letter in the mail from OPM yesterday, offering CSID monitoring. This is the Fourth theft of our identity info in LESS than one year, with no fault of our own. 1st Medical records CMS data base, target, home depot, and now this. Ours was having worked at the USPS years ago.. like 20! I will not be using CSID to monitor us, because, they will eventually be hacked.. I mean, it is the obvious next step, if one were a hacker. So, we are dumbing down our lives, getting rid of credit cards, etc.. in hopes of at least being smart. What I wish our politicians would do, is realize that once somebody's info is stolen, it is a lifelong monitoring issue for the individual, not just "18" months of watching, as CSID is offering. At anytime, somebody can attempt to be you, it could be today, next year, or when you attempt to collect your social security checks. I am disgusted that our government, which interestingly has the knowledgeable ability to attack with drones, cannot safeguard information. What a joke! Are monkeys the Gov. I.T. guys? (although perhaps they may DO a better job). I would like to see fines, and punishments for those companies, and gov. entities who REFUSE to spend the money to protect information, because their system is, "good enough." ENOUGH IS ENOUGH!

Lee Church
June 16, 2015 at 12:48 pm

Burgess is correct that folks can be distracted with attribution, as attribution includes answering the question 'why would party x do y?'.

I will repeat one of my recent posts to Brian's carefirst breach entry:
……….

May 24, 2015 at 9:59 pm

RE: decouple the 'why' from likelihood of the 'what' (probability of event does not depend on our understanding of why an event happens)

As human beings we try to make sense of the world. In doing so, we often fall to a mental error of requiring the 'why' before we can accept the 'what'. In general, just because the 'why' of something is not understood should not influence our assessment of the probability of a scenario. In other words, our own understanding does not make the 'what' more or less likely.

I often hear folks discuss the 'why' as a modifier to the likelihood of an event, and it's a huge logical mistake. It's whether it's possible and the consequences, not whether we understand 'why' it would happen. Coupling them basically multiplies the odds of the event and our understanding, making the result even less clear.

Brian Krebs has succumbed to this error as well (notably in his NK attribution posts), so it's by no means a rare mistake. Our analysts missed 9/11 in part due to dismissing an event because it had no known 'why' answer to why would anyone want to do such a thing.

A corollary to demanding 'why' to accept 'what' is that we are also tricked by a false 'why'. Once we think we understand 'why' we assign a greater likelihood to the event, even if the 'why' is false. We all know people who just want an answer, and any answer is fine with them.. but until they get an answer they are not satisfied. So another exploitation is to present a false but plausible 'why' and it leads to errors on the flip side, or over estimating likelihood.

So please folks, particularly Infosec and security people, when you find yourself giving up on a scenario because of lack of clarity on 'why', resist the natural human urge to dismiss a probability of the event, particularly if the consequence of the event is large or unknown. And when we think we know 'why', remember we can be wrong as much, if not more than if we don't know 'why' at all.

Sometimes, the 'why' presents itself much later after an event… and sometimes never. This is the nature of tail event risks and I would suspect that most tail events have the 'it could not have been otherwise' though pre-event analysis never sees it coming.

One final thought for those that are interested. When the 'black hats' know folks dismiss events that have no readily answerable 'why', they can design events that exploit that behavior. So it's up to the Infosec and security folks to make sure we take away that bit of human behavior exploitation.

anyway, hope this was of use.

regards

Stienke
June 16, 2015 at 3:12 pm

This particular breach made me laugh,
1. I am a Veteran; Strike one
2. Applied for serveral government postions; Strike two
3. recieved letter from Homeland Security RE: Keypoint Breach.

I am wiating for the notification that my security clearance information was breached…

3 cheers for….oh wait nevermind!

Allyn Kirkham
June 16, 2015 at 4:33 pm

As a federal employee with constant reminders about the need to keep everything secure, encrypted laptop, forced encryption on removable media, etc. this is just ridiculous. OPM was pretty careless when they did their background check for my hiring – they shared my SSN with a neighbor who protested that they should not be showing her that info.

CS
June 17, 2015 at 10:53 am

Your comment "If you're affected by these breaches and wondering what you can do to protect yourself besides signing up for credit monitoring services, please see this story." is the all too common response to this breach. Not all concerns are financial. The amount of security data provided depends in no small part on the level of clearance requested. Whoever has this data can cull through it to find those with the highest levels. Those people might be exposed to extortion, intimidation or even kidnapping in order to get what they know.

Patrick
June 17, 2015 at 4:29 pm

I agree with CS on this one. In many cases credit monitoring is useless for breaches like this. If the hackers don't intend to open up credit accounts in your name then the credit bureaus probably won't see anything anyway. And the cost for this monitoring is likely covered by cyber insurance, so offering the monitoring may not even be very painful for the breached organization. The sad part is that technologies exist that can detect and/or stop most of the breaches (I didn't say 'all') if used correctly but organizations choose to not use them. Sometimes it is because they don't think anyone will attack them ("We sell hammers"). Other times their security folks may not know about them and other times it is just budgetary priorities. Unfortunately it can also be because the org thinks it is secure when it really isn't. It is often difficult for finance folks to calculate the ROI on incremental security spend, so I think we will continue to see these breaches happen until everyone is forced to raise their security standards. Maybe the cyber insurance companies can start nudging folks in the right direction. I also agree that too much attention is being paid to attribution and not enough on good ol' security 101. Companies get wrecked because they are wreckable and hacked because they are hackable (hat-tip to Gordon Gekko). Just be sure you are at least less hackable than everyone else.

Thomas
June 17, 2015 at 5:10 pm

So I went to FBO.gov to see the contract for the OPM credit monitoring contract of $20mil, didn't see it but a couple of others like NARA (3200) and Maryland National Guard (79).

I set up an agent that tells me on a daily basis if there are new Government RFPs looking for credit monitoring services.

Thomas

Jeffrey Carr
June 17, 2015 at 6:32 pm

Brian, welcome to the dark side. You've finally acknowledged that we spend far too much time searching for who to blame instead of looking at what we need to do better. And thanks to Mike Burgess for evangelizing that viewpoint!

Ron G.
June 17, 2015 at 7:59 pm

EVERYBODY! PLEASE SIGN my brand new Whitehouse Petition! I am asking for the incompetent director of OPM to be fired. (In the private sector, this would have happened already, but she is your typical ethnic-checkbox political appointee and former Democratic party apparatchik hack operative who did a lot of work on Obama's campaign, so now Obama is defending her of course… just like Bush did for the director of FEMA during Hurricane Katrina. But the size of this breach is too big to push under the rug.)

Please sign my petition here and please spread this URL as far and wide as possible:

http://wh.gov/i0nyA

Note that the petition won't even be FULLY published on the Whitehouse web site until I get at least 150 signatures… SO I NEED YOUR HELP!

Another_Proposal
June 17, 2015 at 11:56 pm

(Signed)

Here is a petition for the heads of government and ICANN to disconnect select Chinese networks from the Internet, by signing on the right side if you are in agreement (digitally sign by submitting). Millions of people have been affected by compromised data (from OPM, Anthem, Home Depot, Target Corporation…) so you may wish to pass this along for more than one signature. https://www.change.org/p/icann-internet-corporation-for-assigned-names-and-numbers-tell-the-worldwide-internet-maintainers-to-disconnect-select-networks-in-china-from-the-internet-internet-2-0

Zelco Munye
June 18, 2015 at 5:50 pm

If you are going to do that to specific Chinese nets, let's also include our own spy service nets to that list. I don't want them snorting around in my life any more than the Chinese.

K-Dee
June 18, 2015 at 2:47 pm

A couple of us just realized something this morning that I haven't seen mentioned yet. OPM has my wife's and my children's personal information for TSP beneficiary information as well as health insurance coverage!! :-/

password protect pdf
June 20, 2015 at 1:14 pm

Similarly, secret questions and password hints cannot be hashed, as they want to have the ability to read them once more.

SLC
June 24, 2015 at 11:29 pm

Weighing in a bit late, but arrived home after a 3-week vacation to find my OPM letter in the held mail stack.

Given that I left Federal service in 1992, I suspect that the number of affected individuals is far, far higher than OPM has let on.

Will probably be instituting a credit freeze for the spouse & me. Not sure about using the "complimentary" CSID credit monitoring services but will look into it to see what's involved and if I have to do things like given them a credit card number "to keep on file."

Jim Mooney
June 26, 2015 at 6:28 pm

Oh gee, the idiots offer "credit monitoring" for a short period. When your bank account is emptied and you can't make your rent or pay your employees, and the bank, as usual, is stalling, that monitoring will be a big help.

PIV Guy
July 2, 2015 at 9:32 am

I have been involved in the authentication world for years. No credit agency is going to keep you secure. Two Factor Authentication (2FA) does. Not cell phone based as they are susceptible to Man in the Middle attacks. The Yubi key is the way to go and the vendors that use it. It's based on the FIDO and OpenID standards (Federal recognized). Don't retreat. Build your security fortress around 2FA. If the hacker doesn't have your token he doesn't get your data. Period.

Jonathan Jaffe
July 2, 2015 at 11:34 am

Yubi is another device to carry while imposing requirements and operational constraints on the consumer. See details at
https://www.yubico.com/products/yubikey-hardware/

It is an example of the traditional inverse relationship between security and ease of use where More Secure > Harder to Use. see http://nc3.mobi/about-us/

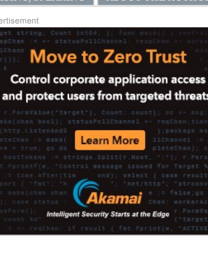
Why not use equipment many people *already* carry and increased security makes it easier to use?

There is a better way.

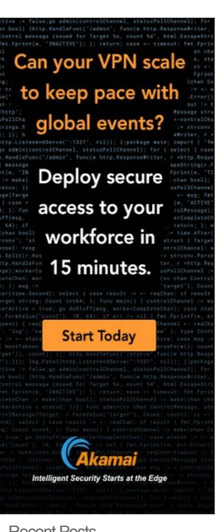
Jonathan @nc3mobi

← Older Comments

Advertisement



Mailing List
Subscribe here



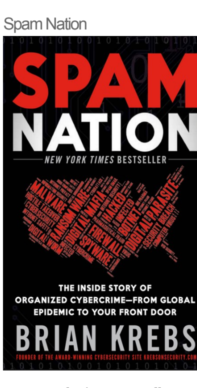
Recent Posts
Coronavirus Widens the Money Mule Pool
The Web's Bot Containment Unit Needs Your Help
Live Coronavirus Map Used to Spread Malware
Crafty Web Skimming Domain Spoofs "https"
Microsoft Patch Tuesday, March 2020 Edition

All About Skimmers

Click image for my skimmer series.

Donate with PayPal

Spam Nation



A New York Times Bestseller!

Buy at Amazon

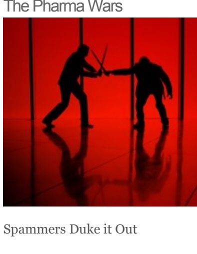
The Value of a Hacked PC

Badguy uses for your PC

Tools for a Safer PC

Tools for a Safer PC

The Pharma Wars

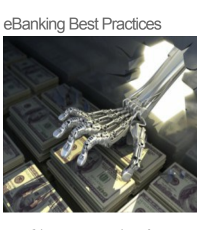


Spammers Duke it Out

Badguy Uses for Your Email

Your email account may be worth far more than you imagine.

eBanking Best Practices



eBanking Best Practices for Businesses

Most Popular Posts
Sextortion Scam Uses Recipient's Hacked Passwords (1076)
Online Cheating Site AshleyMadison Hacked (798)
Sources: Target Investigating Data Breach (620)
Cards Stolen in Target Breach Flood Underground Markets (445)
Reports: Liberty Reserve Founder Arrested, Site Shuttered (416)
Was the Ashley Madison Database Leaked? (376)
True Goodbye: 'Using TrueCrypt Is Not Secure' (363)
Who Hacked Ashley Madison? (361)
Following the Money, ePassporte Edition (353)
U.S. Government Seizes LibertyReserve.com (315)

Category: Web Fraud 2.0

Innovations from the Underground

ID Protection Services Examined

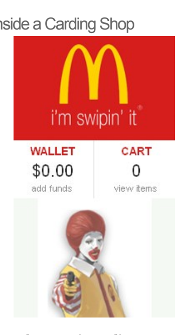
Is Antivirus Dead?

The reasons for its decline

The Growing Tax Fraud Menace

File 'em Before the Bad Guys Can

Inside a Carding Shop



A crash course in carding.

Beware Social Security Fraud

Sign up, or Be Signed Up!

How Was Your Card Stolen?

Finding out is not so easy.

Krebs's 3 Rules…

…For Online Safety.

© 2020 Krebs on Security. Powered by WordPress. Privacy Policy