Influencers: Obama's info-sharing plan won't significantly reduce security breaches

Even if it passes Congress, 87 percent of Passcode's Influencers say President Obama's push for more information sharing between the government and the private sector will not significantly reduce security breaches.

By Sara Sorcher

February 25, 2015

In the wake of several high-profile cyberattacks, President Obama pushed a plan to increase the exchange of information about threats between the private sector and the government. Even if it passes Congress, however, a strong 87 percent majority of Passcode's Influencers say this initiative will not significantly reduce security breaches.

"Yawn. This is the 99th time I've heard of this idea," wrote technologist and author Dan Geer.

"The private sector in various places (like high end banks) is doing such a better job of information sharing that the US government has nothing to add unless it wants to just give all the chief information security officers a clearance – which, incidentally, they have largely done for the bigs but not for the littles," said Geer, chief information security officer for In-Q-Tel, a not-for-profit investment firm that works to invest in technology that supports the missions of US intelligence community.

"Banks are way, way ahead," he said. "The big data breaches are so often the result of not paying attention by the victim."

If the solution to significantly reduce security breaches is information sharing, said Jeff Moss, president of DEF CON Communications, "then the market would have addressed it years ago with a crowded field of info exchange tools, but [it] hasn't. Information sharing allows better and faster bandaids but doesn't address the core problem."

The Obama administration's plan, designed to pool threat information and improve response times to cyberattacks, would put the Department of Homeland Security as the central repository of the information coming from the private sector. It came on the heels of major security breaches at companies such as Sony Pictures and Target.

The plan would have helped in just a "small subset of cases to provide information sharing and smarter defenses, but that alone won't significantly stop attacks," said one Influencer, who chose to remain anonymous. "If private sector companies set up the infrastructure, training, and process to defend their networks using this – and lots of other intelligence – then it will indeed start to provide significantly greater protection. All that being said, the smartest and most sophisticated adversaries will continue to penetrate what are in many cases inherently vulnerable systems."

The Passcode Influencers Poll brings together a diverse group of more than 70 security and privacy experts from across government, the private sector, academia, and the privacy community. To preserve the candor of their responses, Influencers have the choice to keep their comments anonymous, or voice their opinions on the record.

Relying on information-sharing to prevent attacks "presumes that hackers will evidence the same signature over a long period of time," wrote Martin Libicki, senior management scientist at RAND. "If it functions at all (as a signature-passing device), its primary effect will be to force hackers to modify their signatures. After the hackers do so, this expensively-wrought measure will be fairly useless."

There is momentum on Capitol Hill to pass a version of Obama's information-sharing plan, which did have some defenders within Passcode's pool of experts. Thirteen percent of Influencers said the plan would significantly reduce security breaches, even as some acknowledged it's not a panacea.

"While important, information sharing won’t solve everything," said Congressional Cybersecurity Caucus co-chair Rep. Jim Langevin (D) of Rhode Island. "What it will do, though, is enable companies to discover and respond to threats of which they may not have been aware - and provide badly needed situational awareness to the government. It’s a first step, but an important one, and will allow us to broaden the conversation to other important cybersecurity policy matters."

Who are the Passcode Influencers?

For a full list, check out our interactive masthead here.

We want to hear from you, too.

Vote in the readers' version of the Passcode Influencers Poll.

Comments: No

"Information sharing and other efforts to reduce our vulnerability to attack cannot by themselves solve our nation's cybersecurity problem. Vulnerability mitigation – building taller fences and stronger locks – will not protect against attacks by nation-states and other determined actors." – Melanie Teplinsky, American University Washington College of Law

"No, it will not. This is a flawed security paradigm because the emphasis is on keeping adversaries out (an impossible task) instead of keeping valuable IP safe, which is much easier to do." – Jeffrey Carr, Taia Global

"Maybe in the short term... as the 'commodity' attacks get weeded out. But information sharing is only as good as the information that is being shared, and right now it is still the case that more sophisticated attacks place the defender at a distinct disadvantage." – Influencer

"Info sharing will only be useful for highly sophisticated companies; the vast majority are still operating at an elementary level." – Jacob Olcott, BitSight Technologies

"We need to move beyond just information sharing to true collaboration between private sector and the government. A lot of information sharing already occurs today. What we need most is action, not sharing." – Influencer

"More information sharing will probably have some modest benefits, but it's not at all clear that legal barriers are the primary obstacle to increased sharing. Even if we see significant buy-in, I'd expect it to be of limited value against sophisticated, targeted attacks." – Julian Sanchez, CATO Institute

"It needs to be more than just legislation. It need to be executed on by all parties to be effective. It needs a credible evangelist. The US Government has to lead by example. Then it may make a difference." – Rodney Joffe, Neustar

"It really depends on the definition of the word 'significantly.' It may offer a small reduction but that has to be balanced with the down side, letting NSA walk through the front door of America's vast domestic telecom system." – Influencer

"Information sharing is an important component of cybersecurity, but will not reduce security breaches by itself. Strong security practices and digital hygiene will also be critical. The sheer number of security breaches is also likely to naturally rise with time as technology continues to spread and create more data." – Influencer

"There is no one single act that will serve to 'significantly reduce security breaches.' Better information will help on the margins to create a more informed defensive response to security threats and challenges, but it will do nothing to address insider threats, software corruption, hardware infiltration, and a dozen other cybersecurity threats and challenges." – Influencer

"Passing a bill, implementation, and successful implementation are very different things." – Jim Harper, CATO Institute

"President Obama needs to secure the US Government and Military before he can expect anyone to trust them with sensitive data. Hiring 6,000 IT administrators, giving them a few months of system administration and a pen-testing class won't move the needle, except for the SI's who land the huge contracts." – Chris Rouland, Bastille Networks

"It will not significantly reduce security breaches but it will be beneficial. Most organizations are not to the point where their security programs and cultures are mature enough to effectively use this type of sharing. It is a good move in the right direction that is needed and will encourage better practices and discussions within companies. Therefore it should be passed. It will significantly help the community but it should not be seen as a method to significantly reduce security breaches." – Robert Lee, Dragos Security

"The proposal will definitely help but we can't lose sight of two important facts: first, there is already significant and important information sharing occurring. Second, information sharing is not a panacea. Instead, it is one part of a larger solution." – Jeff Greene, Symantec

"This isn't 2004, the days of using signatures to keep hackers out of networks are long gone." – Chris Finan, Manifold Security

"Due to the expanding impact and influence of the Internet globally and the fact that billions more people are likely to be coming online in the future, many of them bad actors, while it is important that the private sector and government step up the sharing of immediate information about attacks and breaches this action will not effectively reduce the number of such actions. That is not likely to be possible at this point in the digital age or for the next few years at least." – Janna Anderson, author of Pew's "Future of the Internet" survey research series

"It will help, but this is a small and tentative first step." – Influencer

"As I noted in my 28 January 2015 testimony to the Senate: 'Threat intelligence can help defenders more quickly resist, identify, and respond to intrusions, but only if the organization is postured to succeed. Until one invests in sound strategy, processes, people and technology, no amount of information sharing or threat intelligence will be sufficient.'" – Richard Bejtlich, FireEye

"Sharing is just one of the process to defeat cyber adversaries. Teaching kids to share is just the start of making them a successful adult. Let's not imagine it'll be any different to get to successful cyber outcomes." – Jay Healey, Atlantic Council

"It cannot significantly reduce security breaches (by itself). However, cyber threat information sharing arrangements can help to manage cyber risks. To be effective, sharing arrangements require three properties: 1. Actionable: Information shared must be capable of being acted upon

in a meaningful way in the applicable environment. It also needs to have meaning to the recipient. 2. Timely: Meaningful information is perishable. Sharing and consumption of information needs to be done at speed or else it will be overcome by events. 3. Trusted: If there is no trust, information will not flow." – Influencer

"Without creating disincentives for poor operational security (i.e., fines and/or other liability), the private sector will continue to operationalize its IT in ways that privative profits while socializing risk." – Sascha Meinrath, X-Lab

"Coordination on the sharing of information does equate to reduced security breaches. Information sharing is designed to help orgnaizations prepare for attacks or share data on resutls of successful attacks. Information sharing needs to be tied to Cyber Intelligence (the understanding of the types of attacks, methods of attacks and what the bad actors are going after. With regard to the success of information sharing, we need to identify the information to be shared. There is some confusion regarding this. Specifically, companies do not have to share IP or private corporate data. What is shared is information such as type and classification of attack. Method of attack. And a recommended set of measures to block, eliminate, or remediate the attack or breach." – Geoff Hancock, Advanced Cybersecurity Group

"The initiative is good in that it brings to the forefront of public discussion the issues surrounding cyber, but the proposals are pablum and will be ineffective." – Influencer

"The proposal seriously undermines security research." – Influencer

Comments: Yes

"It cannot work in isolation, but is a critical step in any strategy to meet current cyberthreats. The bad actors are increasingly sophisticated, usually target multiple victims and benefit from the lack of coordinated and informed repsonses. We need robust, almost realtime sharing of threat data to minimize breaches and the damage they cause." – Jenny Durkan, Quinn Emmanuel

"Sharing of threats and latest intel is the easiest way to mitigate breaches." – Chuck Brooks, Xerox

"It’s worth commenting that the Senate Intelligence committee bill would better increase cybersecurity information sharing and thus lead to a reduction in security breaches. At the time of this writing, industry has not reviewed the latest CISA bill. However, when compared with the administration’s (inadequate) legislative proposal, released on January 13 (and the subsequent Sen. Carper bill introduced on February 11), the CISA bill would offer businesses more flexible, protected avenues for swapping threat data and countermeasures with industry partners and appropriate government entities in real time. CISA would also enable businesses to monitor their networks to spot intrusions and authorize a stronger package of safeguards—legal liability, regulatory, public disclosure, and antitrust matters. In short, CISA would make a bigger

difference in cybersecurity information sharing to stop future attacks. Nevertheless, the administration's willingness to engage on the issue is what's important. Let's hope that the administration won't threaten to veto cybersecurity information-sharing legislation a third time."
– Matthew Eggers, Chamber of Commerce