Are D.C. Insiders Stoking Cyber Fears?
Interview with Jim Harper of The Cato Institute
Eric Chabrow, Managing Editor
July 21, 2009

Except for national defense, Jim Harper doesn't think the government needs to secure its IT any more than does the private sector. But the director of information policy studies at The Cato Institute, a libertarian think tanks, says Washington officialdom, contractors and pundits are painting a false, doomsday scenario if federal government IT assets aren't quickly secured.

"I am most concerned with the Washington, D.C., mentality that we need to secure it all right now or we will suffer enormous calamity," Harper says in an interview with GovInfoSecurity.com (transcript below). "We may suffer some because of some cyber attacks or because of some weaknesses, but we have just got to know that that is going to be par for the course. Throughout the physical world, we continue to suffer losses of assets and losses of people because we don't know perfectly well how to secure all of these things. "

Harper analogizes the digital world with the real world, contending that as everything in the real world isn't secured, not all things in cyberspace must be safeguarded, too.

In the interview, with GovInfoSecurity.com Managing Editor Eric Chabrow, Harper also:

Assets that cyber terrorism does not exists, believing it's a creation of Washington insiders who who try to make the problem of securing government IT bigger than it really is. "There's no such thing as cyber terrorism because cyberattacks can't cause terror," he says. "They don't scare us, and that's an essential element of terrorism as the name implies."
Proposes IT vendors assume more responsibility - and liability - for the products they sell in event of cyberattacks, even if that should raise the price of wares the government, businesses and consumers pay.
Explains the failure of the Federal Information Security Management Act to truly secure government IT, in part, on lawmakers and policymakers not fully understanding the challenges faced when the law was written in 2002, a matter they must consider when reforming FISMA.

ERIC CHABROW: In your congressional testimony, you analogized the real and virtual worlds, saying that cybersecurity, as security in the real world, consists not of a small universe of problems but thousands of different problems that will be handled in thousands of different ways by millions of people over the coming decades. Securing cyberspace means tackling thousands of technology, business economics and law enforcement problems and like the real world, it will take time, perhaps decades, and that doesn't worry you. Why not?

JIM HARPER: There is a broad analogy between cyberspace and real space and the conclusion is that we should secure cyberspace, but we don't really secure real space. We secure specific things in real space. I think it is just a sort of turner phrase that has turned into a policy that we should secure all of cyberspace and that is just not the case. We should secure our houses, our cars, our locker at the gym, our bikes, our

money, and we use systems that have been developed over hundreds, and in many cases, thousands of years to do so. We know what we can keep in a house behind windows and doors, which have certain physical properties.

We suspect that we could create an analogical world that is a parallel world in a matter of years or certainly not months or even decades, it will take a long time to secure all of this stuff. Nothing I say is meant to diminish the importance of working on security; we will suffer losses, but we have got to understand that it is going to take a long time to figure all of this stuff out and I am most concerned with the Washington, D.C., mentality that we need to secure it all right now or we will suffer enormous calamity. We may suffer some because of some cyber attacks or because of some weaknesses, but we have just got to know that that is going to be par for the course. Throughout the physical world we continue to suffer losses of assets and losses of people because we don't know perfectly well how to secure all of these things.

CHABROW: Are there too many doomsayers out there making cyber threats seem more menacing than they really are?

HARPER: I think there are. It is an illustration that Washington, D.C., had that where people try to sort of outbid each other in doomsaying. Take any issue area, any controversy, and you tend to see the Washington, D.C., pundit class, politicians and government contractors step up and try to make the problem sound bigger than it is.

We get that in this area with the discussion of cyber warfare and cyber terrorism. Cyber terrorism, in particular, I think cannot exist. I think there is no such thing as cyber terrorism because cyber attacks can't cause terror. They don't scare us and that is an essential element of terrorism as the name implies.

There is a limited realm in which there might be such a thing as cyber warfare, that is attacking networks during wartime to prevent and dismantle the war making apparatus of our country. Other than that there really isn't a strategic logic to cyber warfare. The upside for "attacker" is very minimal and the downside is rather vast so I don't think there is even a real logic to general cyber attacks.

So anyway, these terms are thrown about more and more commonly in D.C., suggesting that there is an emergency underway. There is not an emergency. There is an important problem that we need to continue to work on.

CHABROW: We are talking the week after Independence Day, when there have been assaults on websites in the federal government, some commercial institutions, as well as South Korea, with some suggesting that it may be coming from North Korea. Is this an illustration of overreaction?

HARPER: I think this is a good illustration actually of the nature and scope of the threat. Now, there is always going to be on the horizon some more serious concern. We have to always be looking for that and working to address that, but this was a cyber attack of substantial significance and most Americans won't know about it. Those that do know about it will know about it from your publication and from reading about it elsewhere.

We are really not in a crisis mode because of these cyber attacks. What doesn't kill us makes us stronger. I understand that most of this has been a clumsy denial of service approach and denial of service is important, but not devastating. So, we've got a problem and we seem to have it well in hand and we should continue to press forward on attacks and genres of attack to prevent them, to weaken them, to be able to respond to them and bring our systems back up after them. The United States is not in crisis because of this attack; it is relatively placid, frankly, despite the attack.

CHABROW: Your testimony suggests that FISMA - the Federal Information Security Management Act -

demonstrates the government's inability to secure IT. Bills offered by Senators Jay Rockefeller of West Virginia and Tom Carper of Delaware would, in part, change the way government governs cybersecurity. Do you see these measures as any improvements over FISMA?

HARPER: The problem with FISMA, and I think it is well understood, is that it is mostly about paperwork. You have to have processes in place; you have to have a plan and these kinds of things. Well, all of that planning and all of that process kind of stands in the way, because we are always in the limited resource environment, it kind of stands in the way of getting at real problems.

Now, the federal government isn't specifically disabled from doing cybersecurity; it is not worse than anyone else, but nobody really knows how to secure these problems. I wrote about FISMA in this context in response to a paper from CSIS - the Center for Strategic and International Studies - which sort of lent to the idea that the government should regulate cyberspace in order to secure it. That begs the question of what the regulation would say and FISMA was written in the absence of knowing what it takes to secure all of these assets, so they just punted and said let's do paperwork.

That's the same thing that we saw in the privacy area in the Gramm-Leach-Bliley Act (which deregulated the financial services industry), where the safeguards rule - I think is the name of it - requires financial institutions to have a plan. Well, plans are defeated and we don't have security; we just have plans that failed to secure us. All this just begs the question of how you actually secure these things. It is more important to get on with the process of learning how to secure our assets and infrastructure rather than paperwork that says we are thinking about how we secure them.

CHABROW: So, what is the role of government in securing IT and that of the critical national IT infrastructure?

HARPER: Government does have a role. I work at a libertarian think tank and we try to limit the size and scope of government, expanding the freedom that individuals have to live their lives as they want with their tax dollars in their pocket rather than in the government coffers. But we do have a large government, it is a substantial, if not the largest purchaser of technology products in the world, and it can help mature what is still a very immature marketplace for technology.

Many products are rushed to market without sufficient testing and the government can set standards in a couple of different ways to help make sure that more and more products are secure when they hit the market. For example, by requiring that regular products have the more secure settings on be default. Making it a little bit harder to use but a little bit more secure so the people have to overcome a little step in order to make their technology less secure/more useful.

Another way might be to shift the risk of loss from the government - from the purchaser to the seller - when technology products failed to secure so that in a contract they say this product that you are selling is guaranteed to work for this purpose, including securing data, securing the network, etc., etc. If it fails to do so, contract liability then accrues to the seller rather than as it does for the most part now to the buyer.

As a buyer of technology, you loose if it doesn't work for you, so you shift that risk and the seller will have to take more responsibility, and it will cost them more if their products fail. Accordingly, they will spend more money and time on security. Products may cost more in that environment but products that are more secure are more valuable, so letting them cost more is appropriate. Government, as a market participant, can help advance the market in these directions and I think that will make things more secure across the cyberspace ecosystem, if you will.

CHABROW: But is there some danger if the government doesn't guarantee some of that security because

of the nature of government's responsibilities to its citizens?

HARPER: There isn't much danger. Now, a security breach in the private sector is equivalent to a security breach in the public sector, except for the areas that we really do ask government to take a special role. Things like defense, military defense, defense of the nation against physical attacks by others is a public good that the federal government is supposed to provide. If it fails to provide it, we are in a really bad situation. It is not something that could be provided in the private sector. In that field, it would be very dangerous for our security to be weak and accordingly that is the priority, and I think it is a priority that the Department of Defense and other entities are working on very hard right now, and appropriately so.

I cited, frankly, some successes where a lot of people are touting failures. The practice of keeping true critical infrastructure offline, not connected to the internet nor managed over the public internet, is working. In the case of the joint strike fighter, which now everybody seems to know for a small security breach, the important stuff was kept offline and wasn't breached so I think that is a success.

The really important stuff that is really an appropriate role for government must be kept secure like military infrastructure. I think they are doing a good job with it. When it comes to benefit and transfer payment and all the other stuff that the government does, the risks are the same between the private and public sector. There isn't special danger if the public sector fails at its security efforts. It should try to be secure, to be more secure with parties who loose money when they fail to secure, and that is not the case in government agencies.

Also see these other articles about Harper:

Is Term Cybersecurity Meaningless?
Is Cyber Threat Overstated?
Free Market Seen as FISMA Alternative

Close Window
