



📷 Lead image by AP Photo.

IN THE ARENA

How Obama Fell Short on Cybersecurity

Under the president's proposals, we'll remain America the Vulnerable.

By JOEL BRENNER | January 21, 2015

Our nation is being turned inside out electronically and we seem helpless to stop it. The Russians have broken into a [White House network](#) and [JPMorgan Chase](#). The Chinese have stolen blueprints, manufacturing processes, clinical trial results and other proprietary data from [more than 140 companies](#) and have utterly penetrated [major media](#). The [Iranians attack our banks](#), our electric [grid is assaulted](#) with frightening frequency and North Korea has brought [Sony](#) to its knees. Meanwhile, credit card data from big retailers such as Target and Home Depot are [for sale electronically](#) by the boatload. Infrastructure is at risk. Last month, attackers [disrupted production at a German steel plant](#) and damaged its blast furnaces, using only cyber methods.

The fact that network attacks are getting worse, even after vast sums have been invested in defense, should tell us something fundamental about the deeply flawed nature of our networks. Unfortunately, the [measures just announced by President Barack Obama](#) do not address these flaws. He's right that better information-sharing between the private sector and the government is overdue; Congress should finally pass legislation to make it possible. But it would not address underlying weaknesses in the Internet. Stiffer sentences for cyber crime may be useful, but they would not make our infrastructure harder to attack or our communications more secure. His proposal for a uniform breach-notification law would simplify companies' legal compliance, but it would do nothing to prevent breaches.

The Internet was created as a powerful tool for collaboration among a small group of scientists in the government and a few American universities, but it had no security built in. What this meant—and still means—is that on the Internet there's no way to be sure that the person you think you're communicating with really is that person. It also means that code that causes a computer to do things—and which can include malware that you can inadvertently import—is

difficult to distinguish from ordinary passive data files. Malicious code is therefore easy to hide. At first, these characteristics didn't matter because only a small community of trusted people could use the network. In fact, until 1992 it was against the law to use the Internet for commercial purposes.

After 1992, we took this same porous and insecure network and turned it into the backbone of international finance, personal finance and controls on critical infrastructure. We unleashed a revolution in productivity and pleasure, but we also unleashed pervasive vulnerabilities. Critical infrastructure now runs on the same network your teenager uses to surf websites you'd rather not know about. Virtually all our communications, including military command and control, run on this insecure network. Government affairs in all advanced nations run on it. Air traffic control and railroad switches are exposed to it. Factories rely on it. Offshore drilling rigs in the North Sea and the Gulf of Mexico and local water treatment plants run on it. They are all vulnerable, and they have all been hacked.

We have been walking backward on cyber defense while ignoring the real issues. First, we adopted a moat-and-drawbridge approach. This didn't work for two reasons. We had barbarians inside the gates, and the gates themselves, which we fancied as "firewalls," were merely flimsy filters. New malware enters the market at the rate of about *160,000 per day*. Filters can't keep up.

Some clever defenders therefore thought that if we can't keep the bandits from getting in, let's keep our data from getting out. This is still an important tactic, but it requires 24/7 awareness of the traffic in your network. Most companies can't do that, and in any case we are *woefully short of qualified experts* to man watch floors in every organization. Sophisticated thieves have also developed ways to exfiltrate data that are hard to catch. In really advanced organizations, this tactic has matured into a constant hunt for anomalies in their systems, but that's difficult, expensive and imperfect. Few organizations can do it.

All defense strategies are variants on these models, and all of them are variants of Whac-A-Mole. We are playing a losing game. Obama's proposals may be marginally useful, but they won't change the game. Here are five commercial,

political and technical challenges that the president should have addressed that could make a real difference:

First, we should sharply increase funding for research into a more secure Internet in which computer instructions could be separated from data storage. Online identity is also too easy to spoof. Anonymity may be desirable when you're browsing the Web or sounding off politically, but we need identity assurance in secure communications, in credit transactions and in other contexts in which a counterparty demands it. Figuring out where an attack came from may not be impossible, but it is difficult, expensive and time consuming, and few organizations have the resources to try.

Second, industrial control systems should be designed for simplicity. We can test a chip to ensure that it will reliably do what it was meant to do but no can assure us that a device with a million gateways will not do things it is not supposed to do. Industrial control systems should be able to execute only the minimum functions required to operate the system. But we don't make simple devices like that. Our infrastructure relies on multipurpose chips with a million or more gateways, and as engineers know, more bells and whistles mean more vulnerability. Changing the current approach would take time, but it would be doable if there were a market for simpler devices. The federal government should make that market with its own purchases.

Third, utilities and other infrastructure operators must be able to factor the cost of security into their rates—including the cost of implementing robust controls. This could be politically contentious. State utility commissioners should know, however, that a successful attack on our water supply, sewage system or especially our electric grid is likely to occur. When it does, many of the efficiencies gained by exposing the grid to the Internet will prove to have been illusory, and the cost of making infrastructure more robust now will look cheap compared with the cost of a major blackout or sewage cleanup.

Fourth, most Internet crime occurs through botnets. These are networks of computers that, unknown to their owners, are vehicles for spreading malicious code. Botnets can involve a million or more machines under criminal control. They're used to spread poisoned software, to spam you with Viagra ads or porn or to launch destructive attacks


through other people's machines. Internet service providers can see these botnets at work, but taking them down might disrupt subscribers' communications, and service providers don't want a customer revolt. That's why they don't tell you when you're infected. That's why they don't help you refuse emails from computers they know are infected and that could infect your machine. They do cooperate with the Justice Department to take down the most dangerous botnets, but much criminal activity is allowed to flourish. The providers understandably feel squeezed. Resolving this dilemma will require transparency from the providers about the level and types of botnet activity in their networks—a good subject for congressional hearings. But the point is simple: To become significantly more secure, we must take the botnets down.

Fifth, security cannot continue to be left to consumers, or even to most businesses. Users don't understand the complexities of their communication systems any more than they understand what happens under the hoods of their cars. But security will increasingly be a commodity, and commodities will find markets. Data center companies, which manage huge volumes of traffic efficiently, will increasingly exploit the growing market for high-level security management in the commercial sector. Huge economic benefits, for example, can be achieved by using data centers to securely manage power generation and transmission. Similarly, a partnership between data center operators and telecommunication providers could raise the security bar in the consumer telecommunications market. It could also play a major role in suppressing botnets.

These five measures will require imagination and political resolve as well as technological improvement. The White House has come to this fight with too little, too late. Let's stop playing Whack-A-Mole. There are too many moles to whack them all.

Joel Brenner is a former senior counsel at the National Security Agency and author of America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime and Warfare (Penguin 2011), which is now available in paperback as Glass Houses: Privacy, Secrecy and Cyber Insecurity in a Transparent World (Penguin 2013).

Additional credits:

 Lead image by AP Photo.
