Steven M. Bellovin
Columbia University

Toward a National Cybersecurity Policy

What should a country do? Software seems terminally insecure, and the consequences of insecurity seem large. In the past few months alone, we've seen reports about ransomware infecting hospitals, attacks on power grids, code apparently designed to blow up chemical plants, election meddling, and of course massive spyware. All of these have been attributed to one government or another. What is the proper policy response? I obviously cannot give a full answer in this small a space, but there are some directions to purse and some to avoid.

The most obvious bad idea is a national firewall. There are crystal clear scaling and privacy issues, plus a serious loss of functionality, but a big reason to eschew it is that it just won't work. Perimeter firewalls don't work well for enterprises; the notion of one that can protect a country is risible.

An oft-touted idea is to separate critical infrastructure networks from the rest of the Internet. Again, it won't work. Apart from the difficulty of deciding what networks are that vital, there are too many utterly necessary interconnections.

Other frequently suggested bad ideas include strongly authenticating all packets or connections (those won't solve the real problems) and asking ISPs to act as cops (the problems are on the computers, not the wires). Nor will simple information sharing between companies do very much. We need a better path.

The obvious organizing principle is incentives. Because most security problems are due to buggy code, companies need incentives to create and run good code. That's an expensive process, though, and many organizations will do it if and only if it's cheaper than the alternative. Being hacked costs money, and so do liability settlements. Changes to liability laws and the elimination of disclaimers in software licenses are probably the best things that governments can do. Fines for negligence may also be appropriate.

If there is liability, there will be insurance, but for insurance to reduce the incidence of problems, actuaries need data. As I've written here in the past (November/December 2012), the creation of an analog to the National Transportation Safety Board will serve many useful purposes. Voluntary reporting schemes will also help.

An oft-overlooked issue in breaches is the role of system administrators. Most penetrations are attributable to bugs for which patches exist—but for various reasons, the victimized organization has not installed these patches. Sysadmins are your first line of defense against hackers of any sort, including foreign governments. Governments can require proper disclosure to investors of the quality of corporate system administration. That in turn will make auditors investigate the issue.

Strong cryptography plays an important role in security, but many governments don't like it. I understand their concerns, but the necessity for strong encryption is quite clear and computer scientists have been pointing out the dangers of exceptional access systems for 25 years.

There's plenty to do on the diplomatic front, of course. There are few clearly established norms of behavior in cyberspace, and there are often no repercussions for violation of those that do exist. This has to change, even if it means that some countries will have to surrender their online offensive and intelligence operations. "Preparing the battlefield"—prepositioning malware—is just another form of insecurity.

None of these are easy, none are quick, and all (and the ideas I haven't discussed) have far more inherent complexity than I can address here. But our society is increasingly reliant on our networked computer systems. Computer insecurity has to be seen as a national threat; we have to take it seriously and give it the time, attention, and money it requires. ■

Steven M. Bellovin is a professor of computer science and affiliate law faculty at Columbia University. Contact him via https://www.cs.columbia.edu/~smb.

Copublished by the IEEE Computer and Reliability Societies