Steven M. Bellovin
Columbia University

What a Real Cybersecurity Bill Should Address

The US Congress is currently considering what to do about computer security. Unfortunately, it's concentrating on information sharing between the private sector and the government. Although information sharing isn't inherently bad, especially if done with enough attention to privacy, it won't solve the problem. At best, it's like downstream flood warnings based on what just happened upstream. What we really need is a stronger dam; better yet, we need to prevent the floods in the first place.

It's not likely that any law or set of laws will solve the problem. Nevertheless, there are some concrete things that can be done. Some of these can be addressed by legislation, though often only in the form of incentives for companies to do the right thing.

The biggest security problem we face stems from one simple fact: software is often buggy. These bugs are often exploitable by attackers. Even when better software is available, companies don't install patches promptly. We're not going to solve the software problem anytime soon, but we can do better. The single best thing Congress can do for cybersecurity is attack these problems.

It won't be easy. Favored tax treatment for software security efforts would help, but it's tricky to come up with correct definitions. A better approach would be to outlaw disclaimers of liability in end-user license agreements; most insist that the vendor isn't responsible for anything, up to and including software-related zombie outbreaks. If financial incentives for better software security exist, the market will be able to work its magic.

Improving system administration would be an immense help. Congress might not be able to do anything about it for the private sector, but it can and should do something for government organizations by raising the pay, status, and professionalism of the job.

The government should also encourage the use of cryptographic technology. Cryptography is hard for people to use properly, but much of its complexity arises from its relative rarity. If everything is supposed to be encrypted, life would be a lot simpler.

Encouraging cryptography can be done through both requirements and incentives. All storage devices and traffic going into and out of critical infrastructure computers (including those back-office desktops) should be encrypted. This is, by definition, a matter of national security. For less critical systems, companies could be liable for information theft, depending on what was or wasn't encrypted. Many state data breach notification laws already include similar provisions.

Using cryptography properly requires a secure way to store secret keys, preferably in tamper-resistant hardware. Industry-developed voluntary standards should suffice; if not, the National Institute of Standards and Technology could develop them. Furthermore, properly implemented cryptography could help stamp out passwords.

Finally, people need data on security failures. Airplanes are so safe today because every crash is investigated and the results are made public. Pilots, airlines, and manufacturers have all learned from past problems. In cybersecurity, we don't know if a particular penetration was due to lack of firewalls, bad passwords, employee mistakes, or any of a dozen other causes. Insurance companies need data, too, both as an actuarial basis for setting liability rates but also so they can adjust their rates based on risk factors. Congress should mandate external, published investigations for security problems at publicly traded companies.

None of these ideas is a panacea, and none is a short-term fix. Together, though, they'll help in the long run. ■

Steven M. Bellovin is a computer science professor at Columbia University. Contact him via www.cs.columbia.edu/~smb.

1540-7993/15/$31.00 © 2015 IEEE