DOI:10.1145/3180493

Fred B. Schneider

Viewpoint

Impediments with Policy Interventions to Foster Cybersecurity

A call for discussion of governmental investment and intervention in support of cybersecurity.

The list of cyberattacks having significant impacts is long and getting longer, well known, and regularly invoked in calls for action. Such calls are not misplaced, because society is becoming more dependent on computing, making cyberattacks more capable of widespread harm. Vardi's recent call[1] "it is time to get government involved, via laws and regulations" motivates this Viewpoint. Indeed, we do know how to build more-secure systems than we are deploying today. And governments can—through regulation or other mechanisms—incentivize actions that individuals and organizations are otherwise unlikely to pursue.

However, a considerable distance must be traversed from declaring that government interventions are needed to deciding particulars for those interventions, much less intervening. To start, we need to agree on specific goals to be achieved. Such an agreement requires understanding monetary and other costs that we as a society are willing to incur, as well as understanding the level of threat to be thwarted. Only after such an agreement is reached, does it make sense for policymakers to contemplate implementation details.

This Viewpoint reviews interventions often suggested for incentivizing enhanced cybersecurity. I discuss the trade-offs involved in the adoption of each. In so doing, I hope to facilitate discussions that will lead to agreements about goals and costs. It is premature to advocate for specific interventions, exactly because those discussions have yet to take place.

IMAGE BY ANDRIJ BORYS ASSOCIATES

Secure Systems Are More Expensive

Assurance that a system will do what it should and will not do what it should not requires effort during development. Somebody must pay. It could be consumers (through higher prices), government (through tax credits or grants), or investors (if developers will accept reduced profits). But realize that the consumers, taxpayers, and investors are just us. So before mandating expenditures for enhanced cybersecurity, we must decide that we are willing to pay and decide how much we are willing to pay.

Other priorities will compete. Some will advocate using "return on investment” (ROI) to set spending levels for cybersecurity versus other priorities. But ROI is problematic as a basis for justifying how much to spend here.

- There are no good ways to quantify how secure a system is. Measuring cybersecurity can be as difficult as establishing assurance for a system in the first place, which we know to be a hard problem for real systems.
- There are no good ways to quantify the costs of not investing in cybersecurity. To tally lost business or the work to recover data and systems ignores other, important harms from attacks. Disclosure of confidential information, for example, can destroy reputations, constrain future actions, or undermine advantages gained through technological superiority. Externalities also must be incorporated into a cost assessment—attacks can have both local and remote impact, because the utility of an individual computer often depends on, or is affected by, an entire network.

We should be mindful, though, that investments directed at other national priorities—defense, foreign aid, and social programs—are also difficult to evaluate in purely objective ways. Yet governments routinely prioritize across making such investments. Even in smaller, private-sector institutions, the “bottom line” is rarely all that matters, so they too have experience in making investment decisions when ROI or other objective measures are not available.

Any given intervention to encourage investing in cybersecurity will allocate costs across various sectors and, therefore, across different sets of individuals. A decision to invest in the first place might well depend on specifics of that allocation. We often strive to have those individuals who benefit the most be the ones who pay the most. But the nature of networked infrastructures makes it difficult to characterize who benefits from cybersecurity and by how much. For instance, civil government (and much of defense), private industry, and individuals all share the same networks and use the same software, so all benefit from the same security investments. Externalities also come into play. For example, should only the targeted political party be paying to prevent cyberattacks that, if successful, threaten the integrity of an election outcome?

The nature of networked infrastructures makes it difficult to characterize who benefits from cybersecurity.

Investments in cybersecurity will have to be recurring. Software, like a new bridge or building, has both an initial construction cost and an ongoing maintenance cost. It is true that software does not wear out. Nevertheless, software must be maintained:

- Today’s approaches for establishing assurance in the systems we build have limitations. So some vulnerabilities are likely to remain in any system that gets deployed. When these vulnerabilities are discovered, patches must be developed and applied to systems that have been installed.
- Unanticipated uses and an environment that evolves by accretion mean that assumptions a system developer will have made might not remain valid forever. Such assumptions constitute vulnerabilities, creating further opportunities for attackers.

Ideally, systems will be structured to allow patching, and software producers will engage in the continuing effort to develop patches. Some business models (for example, licensing) are better than others (for example, sales) at creating the income stream needed to support that patch development.

Cost Is Not the Only Disincentive

Secure systems tend to be less convenient to use, because enforcement mechanisms often intrude on usability.

- One common approach for obstructing attacks is based on monitoring. The system authenticates each request before it is performed and uses the context of past actions when deciding what requests are authorized to proceed. But user authentication requires (tedious) user interactions with the system; program authentication limits which software can be run on a system; and the role of context can limit a user’s flexibility in how tasks might be accomplished.
- Another common approach to defense is isolation. Here, effects of actions by users, programs, or machines are somehow contained. Isolation might be employed to keep attackers out or to keep attackers in. In either case, communications is blocked, which makes orchestrating cooperation difficult. We might, for example, facilitate secure access to a bank account by requiring use of a Web browser that is running in a separate (real or virtual) computer on which there is a separate file system and only certain “safe” application programs are available. The loss of access to other files or programs hinders attackers but it also hinders doing other tasks.

These enforcement mechanisms increase the chances that malicious actions will be prevented from executing, because they also block some actions that are not harmful. And users typically feel inconvenienced when limitations are imposed on how tasks must be accomplished. So nobody will be surprised to learn that users regularly disable enforcement mechanisms—security is secondary to efficiently getting the job done.

Security Can Be in Tension with Societal Values

Enhanced level of cybersecurity can conflict with societal values, such as privacy, openness, freedom of expression, opportunity to innovate, and access to information. Monitoring can undermine privacy; authentication of people can destroy anonymity; authentication of programs prevents change, which can interfere with flexibility in innovation and can be abused to block execution of software written by competitors. Such tensions must be resolved when designing interventions that will promote increased levels of cybersecurity.

Moreover, societal values differ across countries. We thus should not expect to formulate a single uniform set of cybersecurity goals that will serve for the entire Internet. In addition, the jurisdiction of any one government necessarily has a limited geographic scope. So government interventions designed to achieve goals in some geographic region (where that government has jurisdiction) must also accommodate the diversity in goals and enforcement mechanisms found in other regions.

Flawed Analogies Lead to Flawed Interventions

Long before there were computers, liability lawsuits served to incentivize the delivery of products and services that would perform as expected. Insurance was available to limit the insured's costs of (certain) harms, where the formulation and promulgation of standards facilitated decisions by insurers about eligibility for coverage. Finally, people and institutions were discouraged from malicious acts because their bad behavior would likely be detected and punished—deterrence.

Computers and software comprise a class of products and services, attackers are people and institutions. So it is tempting to expect that liability, insurance, and deterrence would suffice to incentivize investments to improve cybersecurity.

Liability. Rulings about liability for an artifact or service involve comparisons of observed performance with some understood basis for acceptable behaviors. That comparison is not possible today for software security, since software rarely comes with full specifications of what it should and should not do. Software developers and service providers shun providing detailed system specifications because specifications are expensive to create and could become an impediment to making changes to support deployment in new settings and to support new functionality. Having a single list that characterizes acceptable behavior for broad classes of systems (for example, operating systems or mail clients) also turns out to be problematic. First, by its nature, such a list could not rule out attacks to compromise a property that is specific only to some element in the class. Second, to the extent that such a list rules out repurposing functionality (and thereby blocks certain attacks), the list would limit opportunities for innovations (which often are implemented by repurposing functionality).

Secure systems tend to be less convenient to use because enforcement mechanisms often intrude on usability.

Insurance. Insurance depends for pricing on the use of data about past incidents and payouts to predict future payouts. But there is no reason to believe that past attacks and compromises to computing systems are a good predictor of future attacks or compromises. I would hope successive versions of a given software component will be more robust, but that is not guaranteed. For example, new system versions often are developed to add features, and a version that adds features might well have more vulnerabilities than its predecessor. Moreover, software deployed in a large network is running in an environment that is likely to be changing. These changes—which might not be under the control of the developer, the user, the agent issuing insurance, or even any given national government—might facilitate attacks, and that further complicates the use of historical data for predicting future payouts.

Companies that offer insurance can benefit from requiring compliance with industrywide standards since the domain of eligible artifacts is now narrowed, which simplifies predictions about possible adverse incidents and payouts. Good security standards also will reduce the likelihood of adverse incidents. However, any security standard would be equivalent to a list of approved components or allowed classes of behavior. Such a list only can rule out certain attacks and it can limit opportunities for innovation, so security standards are unlikely to be popular with software producers.

Deterrence. Finally, deterrence is considerably less effective in cyberspace than in the physical world. Deterrence depends on being able to attribute acts to individuals or institutions and then punish the offenders.

- Attribution of attacks delivered over a network is difficult, because packets are relayed through multiple intermediaries and, therefore, purported sources can be spoofed or rewritten along the way. Attribution thus requires time-consuming analysis of information beyond what might be available from network traffic.
- Punishment can be problematic because attackers can work outside the jurisdiction of the government where their target is located. To limit or monitor all traffic that is destined to the hosts within some government's jurisdiction can interfere with societal values such as openness and access to information. Such monitoring also is infeasible, given today's network architecture.

Making Progress

The time is ripe to be having discussions about investment and government interventions in support of cybersecurity. How much should we invest? And how should we resolve trade-offs that arise between security and (other) societal values? It will have to be national dialogue. Whether or not computer scientists lead, they need to be involved. And just as there is unlikely to be a single magic-bullet technology for making systems secure, there is unlikely to be a magic-bullet intervention to foster the needed investments. C

Reference

1. Vardi, M. Cyber insecurity and cyber libertarianism. *Commun. ACM 60*, 5 (May 2017), 5.

Fred B. Schneider (fbs@cs.cornell.edu) Fred B. Schneider is Samuel B. Eckert Professor of Computer Science and chair of the at Cornell University computer science department, Cornell University, USA.

The impetus for this Viewpoint was a series of discussions with *Communications* Senior Editor Moshe Vardi during the two years preceding his May 2017 *Communications* Editor's Letter. Susan Landau, Lyn Millett, and Deirdre Mulligan read an earlier version of this Viewpoint and provided helpful and timely feedback. I am also grateful to the two reviewers for their comments, which resulted in this Viewpoint having a better-defined focus.

The author's work has been supported in part by AFOSR grant F9550-16-0250 and NSF grant 1642120. The views and conclusions contained in this Viewpoint are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of these organizations or the U.S. government.