It's Not About Security Products

The United States, much like the rest of the world, creates laws and regulations to protect its citizens from dangers ranging from tainted food to hazardous children's toys. While these domains are regulated by governments for the safety of its citizens, another consumer product, computer software, is very loosely regulated, if at all. The United States has the Consumer Product Safety Commission to evaluate the safety of consumers products, Underwriter’s Laboratory to certify products for safety, and the FDA to regulate the food industry (among others), however, no such organization exists to oversee the safety of an arguably more important product: computer software. The lack of regulation from an oversight body is alarming because there are no set standards for what is considered acceptable computer software. While there are laws which allow the government to prosecute individuals who spread malicious software, there is very little that can be done to those who negligibly create release insecure software.

Computer software products are one of the only products sold in the United States that have no safety regulations. Other industries recognize, address, and deal with safety issues in an organized way as seen by the swift recall of toys by Mattel after the Consumer Product Safety Commission determined the toys contained lead. However, in computer technology, problems caused by safety issues can both lie dormant and can be much more disastrous: they have the potential to affect more people with more immediacy than any other type of commercially available products. If major structural security problems were found in Microsoft’s Internet Explorer or a critical piece of the Windows operating system, it would be virtually impossible to find a hospital or a government agency that would escape unaffected from such an event. Additionally, Microsoft is under no obligation to notify the public to the existence of such a flaw, and commonly, they do not. This threat becomes more significant when one realizes that most users of computer technology do not understand the intricacies of how such software works. Software that has been patched looks the same as software that has not. This information asymmetry puts the consumer at a great disadvantage in even determining whether they are at risk and suggests that government regulation may be necessary to level the playing field.
Looking at regulation in the consumer health care industry, in response to a batch of contaminated vaccines that killed 13 children, Congress passed the Biologics Control Act in 1902 which laid the groundwork for what would later become the Food and Drug Administration (FDA) in 1906. Since then, the FDA’s authority has expanded to cover the safety of food, dietary supplements, drugs, blood products, and so on. Testing done by the FDA minimizes such events and uncovers safety issues before products reach the market. If safety issues are uncovered after a product is in the hands of consumers, the FDA has shown itself to be highly competent in using its authority to stop production and importation of unsafe products as well as issue recalls. This can be seen in the recent counterfeit Colgate toothpaste recall earlier this summer.

Regulation of the health care industry began in the early 1900's after thousands of years of medicine and snake oils. The clearly defined processes which their industry follows to deal with safety events are the result of decades of development and refinements. When we look at the technology industry, it is still in its infancy and is poorly understood in comparison. Yet, we rely on it as much if not more. Aspects of information technology have worked their way into our banking services, health care, airline travel, public utilities, our home office, and so on. Even when considered alone, the technology industry makes billions of dollars headlined by such stars as Google, Facebook, Microsoft, and Apple. However, as our use of information technology has increased, so has our exposure to security problems in the underlying technology. We saw these problems reach a peak in the summer of 2003 when a number of high profile worms affected Microsoft products (SQL Slammer, Blaster, Welchia, Sobig, Sober) and one was even potentially the cause of the North-East blackout in August of that year. This fact makes the development of such processes for the technology industry all the more pressing as the potential for disaster is enormous and highly likely.

Yet, public response to such catastrophic events has been low and industry-wide actions taken to prevent their recurrence have been ineffective, non-existent, or quickly forgotten about. It seems that in the minds of the public, security issues have become so commonplace that they are accepted as a fact of life. Home users are targeted again and again for "user education" and are told to buy anti-virus software, firewall software, anti-spyware software and so on however, even with all these layers of protection, they are still vulnerable due to the inherently faulty code on the systems that the security products are trying to protect. No amount of security products can make up for poorly written software permeating all aspects of your computing environment.
The constant patching and updating users must endure is a testament to the shoddy products that are released to the market in the first place.

Although there has been little push to regulate computer software, certain agencies and firms have begun to realize the importance of finding and fixing flaws in widely used software in a way one might call a public service and instead of selling you another product. Recently, the Department of Homeland Security in an attempt to protect users of information technology against security problems, hired Coverity, a private software company that develops code scanning tools, to identify flaws in open source applications critical to the functioning of the Internet and alert their developers before attackers have a chance to find those flaws themselves and exploit them. This project has been exceedingly well received both by developers and by users of the applications and has resulted in the discovery and remediation of thousands of potential flaws among dozens of critical software projects. Actions like those taken by the DHS have resulted in a greatly improved software ecosystem in a way that another security product could never have provided.

The proactive approach taken by the Department of Homeland Security in its partnership with Coverity is an excellent example of a method that should be implemented for the entire computer industry and its reach expanded. While various security vendors have released product after product and update after update, each claiming that they are the end-all for your security needs, DHS has provided an invaluable service to all users of technology in improving the structural integrity of software programs we all use and rely upon. Regulation does not have to take the form of the FDA, which requires that all drugs be tested and approved for use prior to reaching the market. Rather, a publicly-funded organization which tests and certifies the structure and code security of software as they reach the market and is involved in releasing proactive security measures back into the industry would be highly beneficial in fixing flaws before they become real problems. Such a certification authority, as Underwriter's Laboratory does for many products and the National Highway Traffic Safety Administration does for cars, would help level the information asymmetry currently present when consumers are attempting to make informed decisions about the software products they buy.

In today’s computer industry, consumers are bombarded with products which fix faults in another product. This leads to inefficiencies, increased costs, and confusion for the consumer. Other industries, such as the food industry or the financial industry have become regulated over
time to fix such inefficiencies (particularly problems of inadequate information) and to protect the safety of the consumer. Given the explosive pace of the current software market, time to market times are getting smaller while software is getting more complex. The aggressive and competitive nature of the software market reduces the testing time for flaws, integrity, and reliability and without a consumer who is able to differentiate, poorer quality products flood the market and the consumer is the victim. Much like the consumer who needs a vaccine, but understands very little about the nature and reasoning behind it is protected by the Food and Drug Administration, the average software consumer knows little about what is going on inside their computer. This situation must be helped by a public organization so that our computing experience is safe, reliable, and dependable. Government participation in aid of software development is a necessary evolutionary step to alleviate the security problems which our products face today.