

Democratizing Cyber Security

The Need for Customer-Centric Signaling in the Software Market

Submission to the Commission on Cyber Security for the 44th President

October 7, 2008

David Rice

Director, The Monterey Group

Author, "Geekonomics: The Real Cost of Insecure Software"

1.0 Introduction

Poorly written, insecure software is no longer a technology issue; it is a public policy issue. The market does not provide significant or compelling incentives for developing secure software, thus current cyber security spending largely deals with the effects of insecure software. In essence, software manufacturers practice unrestrained vulnerability dumping onto downstream market participants. As such, cyber defenders are too busy mopping the floor to turn off the faucet. This situation must end.

This paper argues that reducing the daily flow of new software vulnerabilities into the global stream of commerce is best accomplished through clear, observable, reliable signals made available to consumers in the form of software assurance labels. Democratize software security and make it available for everyone. Buyers should not be required to become computer security experts or be burdened with complex configuration mandates in order to enjoy rudimentary cyber security. Adversaries exploit software vulnerabilities to nefarious ends. Reduce the supply of vulnerabilities and the adversaries' advantage dissipates considerably.

While a labeling regime will not address all concerns related to cyber security, it is a promising avenue with a successful history in a wide variety of industries.

2.0 Make Intangibles Visible

All markets are plagued to a degree by information asymmetry; that is, sellers often know more about a given product than buyers. Where this information imbalance exists, it is troublesome for buyers to receive trustworthy, objective information from a seller regarding a given product as sellers are biased in the transaction. For intangible aspects of a product, such as quality or safety, this information imbalance is more profound.

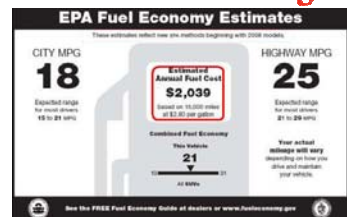
Vehicle safety, food safety, energy efficiency and fuel efficiency are all examples of intangibles in the market place. Intangibles cannot be readily observed before purchase. Software security – the ability of software to withstand foreseeable malicious events – is no different.

Without visible cues regarding the degree to which an intangible is provided by a manufacturer, market participants are substantially disadvantaged. Consumers cannot accurately price – and manufacturers have no incentive to supply on any significant scale – the relevant intangible. Worse, consumers are unable to reliably distinguish between manufacturers desiring to provide more of an intangible from manufacturers that choose to avoid the additional production costs. At best, manufactures focused on intangibles are relegated to high-priced, niche markets. At worst, they are driven from the market entirely.

To correct information asymmetry an external stimulus is needed. The labels at right are examples of intangibles-made-visible through government oversight. In these markets, for



www.nhtsa.gov



one reason or another, manufacturers undersupplied safety, efficiency, and so on. Labels corrected the supply deficiency to a reasonable extent by allowing consumers to discriminate between high-intangible and low-intangible products.

In essence, labels democratize an intangible: consumers need not be experts in vehicular safety, fuel efficiency, or food safety. This is important. Private consumption represents seventy percent of U.S. GDP and nearly sixty percent of EU GDP. In free market economies, private consumption dwarfs government spending. As such, consumers have considerable influence over the supply of a given intangible, but only if it is made visible through clear, observable, reliable signals.

To date, the software industry has no labeling regime in widespread use. Buyers and users of software have little more to go on than vague, un-provable assertions by software manufacturers regarding software quality and security. As a result, software resiliency, security, and quality remain undersupplied and inconsistently distributed at great cost to economic and national security. That some software manufacturers might be “good at security” is laudable, but is simply not enough given all that is now at stake.

3.0 Recommendation: Make Security Visible to the Market

For software security to be part of the market competition, it must be made visible to buyers and sellers alike. While the software industry has no labeling regime in wide spread use, software assurance labels are currently under development by private corporations. One example is Veracode, a software testing company. Currently, Veracode produces a software security rating (seen at right) similar in function to labels such as Underwriters Laboratories or Moodys.

While nascent, this advancement in software security rating as well as others provided by Coverity, Fortify Software, and Ounce Laboratories should be promoted, matured and eventually pursued on a larger, more public scale.



The benefits of a labeling regime are compelling:

- **Creates positive externalities.** Those who may be less concerned with the given supply of an intangible benefit from the demand of others. For instance, while some automobile drivers may not be immediately concerned with the safety of their vehicle, nearly ninety percent of cars in the U.S. are four- or five-star rated. This is due to enough concerned drivers about safety to influence auto manufacturers such that those who did not consider safety in purchasing decision benefited nonetheless. In the case of software, those not immediately concerned with secure software will benefit from those that do.
- **Promotes a “race-to-the-top.”** Complementary to the previous bullet, when buyers can see and therefore measure an intangible, manufacturers respond accordingly. Auto manufacturers are now competing on providing the safest most fuel efficient cars to date. Contrast this to the gas-guzzling, unsafe cars of the 1950s and 60s when labeling was non-existent. In the case of software, when software assurance is made visible, demand for high-quality, secure software will increase as will the supply.
- **Promotes innovation.** Manufacturers can efficiently respond to consumer demand by innovating on new, more effective, and less expensive means by which to supply the intangible. For instance, Honda, as well as other auto manufacturers, has created similar technologies that vary the number of engine cylinders in use while driving. This innovation greatly improves overall fuel efficiency. In the case of software, software manufacturers are free to innovate on the best, most efficient manner to create software that can withstand foreseeable malicious activities.
- **Efficient information sharing.** Labels represent a very simple, but efficient means of transferring information to a wide range of intellects.
- **Clarifies liabilities.** Provides a basis to define the scope and extent of sellers and buyers responsibilities and under what conditions liability might apply.

Some might rightly question the institutional competence of an administrative agency to handle the complex technical questions involved in proposing technology-based regulations for secure software. This is understandable, but entirely indefensible. While no regulatory regime is perfect, it need not be perfect to be relevant as previous labeling regimes have established. The complexity of software is no doubt a considerable hurdle in this endeavor, but in the end, cyber security is not about fighting complexity per se, but incentivizing manufacturers to reduce production of well-known and detectable software vulnerabilities.

4.0 Conclusion

The next President of the United States should take ownership of the critical issue of software assurance and thus cyber security. "We cannot expect the Congress and the Federal Government to stand idly by if the toll of disaster continues to go unchecked." These words, spoken by President Harry S. Truman in 1946 started the wheels in motion to make safety on U.S. roads a reality. President Truman was a champion, a leader, and an example of how the 44th President should approach cyber security for the Information Superhighway. President Truman's words and actions, along with his predecessors President Eisenhower and President Johnson finally debunked the "old truths" of highway safety:

- that safety was only a State responsibility.
- that drivers could be convinced or taught to drive more safely.
- that the automobile industry was capable of setting its own rules and standards for safety.

The ever increasing rate of fatalities and injuries on highways provided plenty of evidence to debunk these old truths. So too, does the ever increasing rate of cyber crime, cyber espionage, and cyber attacks on the Internet debunk the "old truths" of cyber security:

- that security is only a network owner's responsibility.
- that computer users can be convinced or taught to configure their systems securely.
- that the software industry is capable of setting its own rules and standards for secure software.

The next President should champion the security of the cyber infrastructure in the same manner as his predecessors championed highway safety; to ensure that the cyber infrastructure of our lives and our livelihoods is suitable to its task; that it can withstand foreseeable malicious activities, and that accountability is balanced among market participants. A software assurance labeling regime, similar to the NHTSA labeling regime, is a wonderful place to start.