Insecurity through Obscurity

Marc Donner
Associate Editor in Chief

Settling on a design for a system of any sort involves finding a workable compromise among functionality, feasibility, and finance. Does it do enough of what the sponsor wants? Can it be implemented using understood and practical techniques? Is the projected cost reasonable when set against the anticipated revenue or savings?

In the case of security projects, functionality is generally stated in terms of immunity or resistance to attacks that seek to exploit known vulnerabilities. The first step in deciding whether to fund a security project is to assess whether its benefits outweigh the costs. This is easy to state but hard to achieve.

What *are* the benefits? Some set of exploits will be thwarted. But how likely would they be to occur if we did nothing? And how likely will they be to occur if we implement the proposed remedy? What is the cost incurred per incident to repair the damage if we do nothing? Armed with the answers to these often unanswerable questions, we can get some sort of quantitative handle on the benefits of implementation in dollars-and-cents terms.

What are the costs? Specification, design, implementation, deployment, and operation of the solution represent the most visible costs. What about the efficiency penalty that stems from the increased operational complexity the solution imposes? This represents an opportunity cost in production that you might have achieved if you hadn't implemented the solution.

In the current world of security practice, it's far too common, when faced with vast unknowns about benefits, to fall back on one of two strategies: either spend extravagantly to protect against all possible threats or ignore threats too expensive to fix. Protection against all possible threats is an appropriate goal when securing nuclear weapons or similar assets for which failure is unacceptable, but for most other situations, a more pragmatic approach is indicated.

Unfortunately, as an industry, we're afflicted with a near complete lack of quantitative information about risks. Most of the entities that experience attacks and deal with the resultant losses are commercial enterprises concerned with maintaining their reputation for care and caution. This leads them to the observation that disclosing factual data can assist their attackers and provoke anxiety in their clients. The lack of data-sharing arrangements has resulted in a near-complete absence of incident documentation standards; as such, even if organizations want to compare notes, they face a painful exercise in converting apples to oranges.

If our commercial entities have failed, is there a role for foundations or governments to act? Can we parse the problem into smaller pieces, solve them separately, and make progress that way? Other fields, notably medicine and public health, have addressed this issue more successfully than we have. What can we learn from their experiences? Doctors almost everywhere in the world are required to report the incidence of certain diseases and have been for many years. California's SB 1386, which requires disclosure of computer security breaches, is a fascinating first step, but it's just that—a first step. Has anyone looked closely at the public health incidence reporting standards and attempted to map them to the computer security domain? The US Federal Communications Commission (FCC) implemented telephone outage reporting requirements in 1991 after serious incidents and in 2004 increased their scope to include all the communications platforms it regulates. What did it learn from those efforts, and how can we apply them to our field?

The US Census Bureau, because it's required to share much of the data that it gathers, has developed a relatively mature practice in anonymizing data. What can we learn from the Census Bureau that we can apply to security incident data sharing? Who is working on this? Is there adequate funding?

These are all encouraging steps, but they're long in coming and limited in scope. Figuring out how to gather and share data might not be as glamorous as cracking a tough cipher or thwarting an exploit, but it does have great leverage. □

The views expressed herein are solely the views of the author and do not express the views of his employer. —Ed.