The Measure of Information Security is Dollars

Bob Blakley
blakley@us.ibm.com

1. Obituary

The traditional approach to information security has failed. It failed for good technical reasons and good business reasons. A new approach is required. The information security community does not currently have a viable technical alternative to the failed model. Therefore, this paper suggests that we start with an alternative business model, and allow technical approaches to evolve within the framework of that model.

The technical foundations of the traditional security model are secrecy (without which authentication does not work), policy (without which resource access restrictions do not work), and system integrity (without which the policy and authentication mechanisms do not work).

2. Autopsy (Technical)

These technical foundations are fatally flawed, because they are fundamentally at odds with the nature of the systems we are trying to protect. To be specific, the systems we are trying to protect are constructed by composing numbers of general-purpose stored-program computers.

One of the core findings of computer security research over the last 20 years has been that many useful, real-world security properties do not compose. Not surprisingly, the attempt to build large-scale, policy-based secure systems by composition has been a dismal failure.

The attempt to build even a single high-integrity component, however, has been an even more spectacular failure. Most security solutions deployed today are attempts to protect systems against viruses, trojan horses, and malicious mobile code – in other words, to assure or repair system integrity. What system integrity means is, effectively, that a system behaves exactly as if it were a special-purpose device – it has no unexpected behavior, and all its expected behavior conforms to the desired specification. Our real systems are general-purpose systems (which means that their behavior cannot conform to a single consistent specification, which means that by definition they have unexpected behavior), and they are stored-program computers, which means that legal operations can cause large unexpected changes in system behavior. General-purpose stored-program computers are inherently insecure by the definitions of the traditional model.

3. Autopsy (Business)

Our customers have suspected this for a long time. This is an important reason they've been reluctant to buy security solutions. To put the matter plainly, we have failed to describe a problem which is meaningful to business customers, and we have failed to describe how good or bad our solutions are in meaningful business terms.

It's fairly easy to find out how many people die from smoking cigarettes in the United States each year. It's impossible to find out how many hours of computer downtime result from computer virus outbreaks in a year.

It's fairly easy to find out how much physical money is stolen from banks in the United States each year. It's impossible to find out how much money is stolen from banks through electronic attacks.

It's easy to find out how likely you are to be injured in a head-on accident in a particular kind of vehicle in the United States. It's impossible to find out how likely your server is to be taken offline by a virus attack.

It's easy to find out how long a gun safe will resist the attentions of a thief armed with an acetylene torch. It's impossible to find out how long your server will resist the attentions of a thief armed with hacking tools publicly available on the Internet.

A core problem of the information security industry is that, as an industry, we do not even have a unit which measures product effectiveness. We are selling something which is intangible and unquantifiable; we are basically selling fashion rather than function.

To put this problem in economic terms, we operate in a market with severely restricted transparency. Customers do not have good information about product quality. They have no basis on which to compare products. Because information about losses and vulnerabilities is very poor, they do not even have good information about their own requirements.

4. Prescription

The solution to both problems (technical and business) is the same: monetize information security.

What would it mean to monetize information security?

- Quantify and publish loss information in dollar terms
- Quantify and publish product effectiveness information (differential dollar losses with and without a product in otherwise comparable configurations)
- Sell insurance (including discounts for use of effective products)
- Sell "security securities" (availability futures?)

How would monetizing security solve business problems?

- Most importantly, making information-related losses public information would create the necessary conditions for the formation of an economically efficient information security market. These conditions do not exist today.
- An economically efficient information security market would move risk around in an effective fashion. It would also allocate capital to effective security solutions, and stop rewarding ineffective solutions.
- Publishing dollar loss information would create clear cost-justification for use of (effective) security solutions.
- Insurance would create “actual security” in the sense that it would protect business against loss (unless the business in question sells insurance!)
- Insurance discounts would create additional cost-justification for use of (effective) security solutions.
- Insured losses would create incentives for improvement of information security practices and technologies. Furthermore, loss information would provide a unit (dollars) by which the effectiveness of practices and technologies could be measured.
- “Security securities” would provide an information risk management tool which does not depend on technology.

How would monetizing security solve technical problems?

- Accountability (specifically financial liability) is a traditional security property, and it does compose.
- The financial and legal system is already set up to deal with issues of financial liability. It is not yet set up to deal with problems of loss and liability arising from technology but not quantified in dollar terms (hence the emergence of all sorts of strange legislation recently). If security problems can be made into financial and legal problems, the financial and legal systems can stop imposing artificial and counterproductive constraints on the way technology is designed and built.
- As noted above, insuring information security losses, and making information about product effectiveness public, will create incentives for technology improvement and a metric which can be used to measure improvement.

How could information security be monetized?

A variety of mechanisms come to mind. The most straightforward is radical: information technology providers could simply begin to accept financial liability (perhaps limited, initially) for losses due to failures in the security of their systems.

At first blush this may sound to a technology CFO like sheer insanity. But perhaps not. If it became popular, a lot of information about information security losses would quickly become available. A lot of information about losses is precisely the prerequisite for the formation of an insurance market. Once a viable insurance market formed, the risk of assuming limited financial liability for losses could be substantially reduced. A lot of information about losses is also precisely the requirement for planning an effective mitigation strategy for information security losses. Given a large body of information about attacks, and a financial incentive to do something about them, there's a good chance the technology industry could make progress on improving solutions.

Finally, information about both losses and product effectiveness is the prerequisite for the formation of a viable information security solution market. Today, the market for security is a "market for lemons" [Akerlof] in the sense that the value of security solutions is impaired by customers' inability to distinguish between effective and ineffective offerings. Better information about losses would make the market for security products more transparent in the long run, but even before the emergence of a credible body of loss information, the act of accepting liability for losses could be a powerful economic signal of a vendor's belief in the effectiveness of its security solutions.