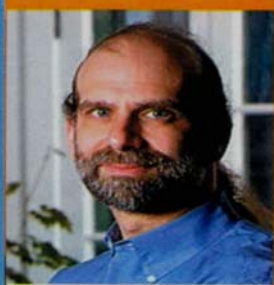


**VIEW**  
**SECURITY**



**BRUCE SCHNEIER**  
CTO, BT COUNTERPANE

# Paying The Cost Of Insecure Software

Having a liability clause is one good way to make sure that software vendors fix the security glitches in their products

**I**NFORMATION INSECURITY is costing us billions. We pay for it—year after year—when we buy security products and services. But all the money we spend isn't fixing the problem, which is insecure software. Typically, such software is badly designed and inadequately tested, comprising of poorly implemented features and security vulnerabilities.

Rather than paying to improve the security of the underlying software by fixing the bug permanently, we pay to deal with the problem on an ad-hoc basis. Vendors are the only ones who can fix this problem for good. However, they will not do so unless it works out to their best financial interests.

Today, the cost of insecure software is borne not by the vendors who produce them but by people not directly involved with its development. In economics, such a situation is known as an externality. Vendors are in no way adversely affected by bad security or low-quality software. Worse, the marketplace often rewards low quality. It rewards additional features and timely releases, even if these are done at the expense of quality.

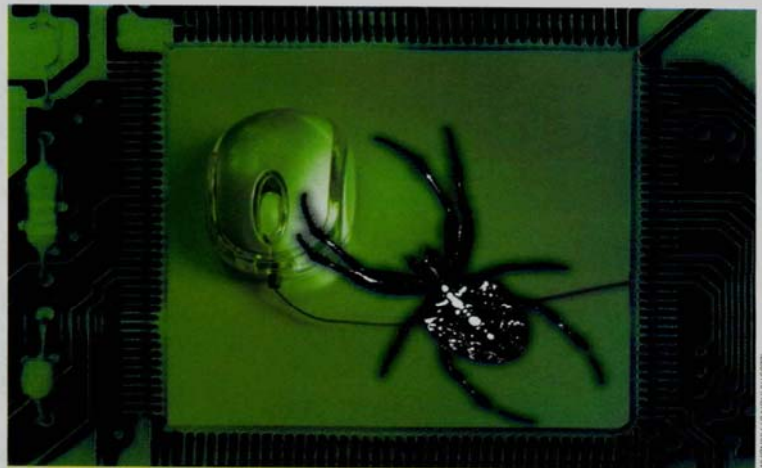
### Demanding Accountability

There's still hope, though. One way to make software vendors pay for quality is through adherence to the liability law. Raising the risk of liability raises the cost of doing it wrongly and, therefore, increases the amount of fund a CEO would be willing to spend on it. Security is risk management; liability fiddles with the risk equation. So, the risk equation needs to be tweaked so that the CEO cares about actually fixing the problem. And the best way to do it is by putting pressure on his balance sheet. Clearly, this isn't all or nothing. There are many parties involved in a typical software attack. There's the company that sells the software with the vulnerability, the person who wrote the attack tool, the attacker himself, who used the tool to break into a network and the owner of the network, who was entrusted with defending that network.

The entire burden of the liability should not fall on the shoulders of the software vendor, just as it shouldn't fall

on the attacker or the network owner alone. Yet, all the cost falls on the network owner. That, has to stop. We will always pay for security. If software vendors have liability costs, they will pass those on to us. It might not be cheaper than what we are paying today. But if we have to pay, we might as well pay to fix the problem. Forcing the software vendor to pay to fix the problem and then pass those costs on to us means that the problem might actually get fixed.

Liability changes everything. Currently, there is no rea-



**The marketplace rewards low quality. It even lauds additional features and timely releases**

son for a software company not to offer feature after feature. Liability forces software companies to think twice before changing something. Liability forces companies to protect the data they're entrusted with. Liability means that those in the best position to fix the problem are actually responsible for the problem. Information security isn't a technological problem. It's a problem related to economics. The way to improve information technology is to fix the economic angle. Do that, and everything else will fall in place. ■