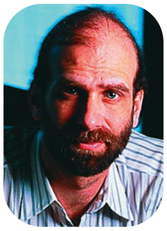
Security and Compliance

It's been said that all business-to-business sales are motivated by either fear or greed. Traditionally, security products and services have been a fear sell: fear of burglars, murderers, kidnappers, and, more recently, hackers. Despite the computer security industry's repeated attempts to position itself as a greed sell—"better managing your risks will make your company more profitable"—fear remains the primary motivator.



Bruce Schneier
Counterpane Internet Security

The problem is that many security risks are not borne by the organization making the purchasing decision. The adverse effects of privacy loss are borne more by those whose privacy is breached. In economics, this is known as an *externality*, an effect of an organizational decision that doesn't affect the organization.

This is the proper backdrop for understanding the recent spate of privacy laws such as the Sarbanes-Oxley Act of 2002, the California Database Protection Act of 2001, the Gramm-Leach-Bliley Act, and the Health Insurance Portability and Accountability Act. Their goal is to bring those externalities into the decision process by adding an additional motivator: fear of lawsuit, criminal penalties, or being out of compliance.

Creation of laws such as these generally follows three steps:

1. Media headlines about data security penetration fuel public outcry and calls for regulation.
2. Regulators mandate policy and technology solutions using stopgaps that are typically vague and untested.
3. Industry develops a response, including policies, processes, and solutions they can live with economically that regulators and the courts negotiated.

The entire process is motivated by fear and, in turn, uses fear to deal with the externality. In step 1, the public realizes that, although organizations do have some fear of attack, it has more to lose from these penetrations than the organizations do. But there are additional vulnerabilities—externalities—that affect the public.

In step 2, regulators attempt to bring those externalities into the organization. By passing laws and mandating compliance, they introduce additional fear to the organizations and motivate them to implement additional security measures.

Each of these laws imposes strict requirements on enterprises to establish or identify, document, test, and monitor "internal control" processes. Because information technology supports most, if not all, of these processes, these laws significantly impact companies' security decisions.

The four acts I mentioned earlier specify varying requirements, but all share these mandates for organizations:

- *Security policies*. Well-defined policies for data privacy and protection that discourage the government from imposing its own standards—which companies find the least desirable of all situations.
- *Security processes*. Demonstrable policy that uses technology in a predictable manner to protect data.
- *Robust audit trail*. A clear evidentiary chain that, in the event of a security breach, justifies what events need not be reported to regulators.
- *Preventive measures*. Encryption, digital signing, and real-time attack detection serve to preempt attacks on data.

Like most legislative actions, the laws are vague and imperfect. Some provisions are simply too expensive or onerous to implement, others are just poorly worded. The end result is step 3: negotiation between the organizations the laws affect and the regulators entrusted with enforcing the laws.

The result? Improvement. More important than the specific list of countermeasures is a process of continual security improvement. Organizations pay more attention to data security. They treat security more as a process than a product.

As a security professional, I applaud these kinds of regulations. Just as I advocate software liability as a way to bring the externalities of insecure software into software manufacturers' decision-making process, I see these data-privacy laws as a way to force organizations to take personal data-security protection more seriously. □

__Bruce Schneier__ is one of the world's foremost security experts and Counterpane Internet Security's chief technology officer. His new book, Beyond Fear, *was published in September 2003. Contact him at www.schneier.com.*