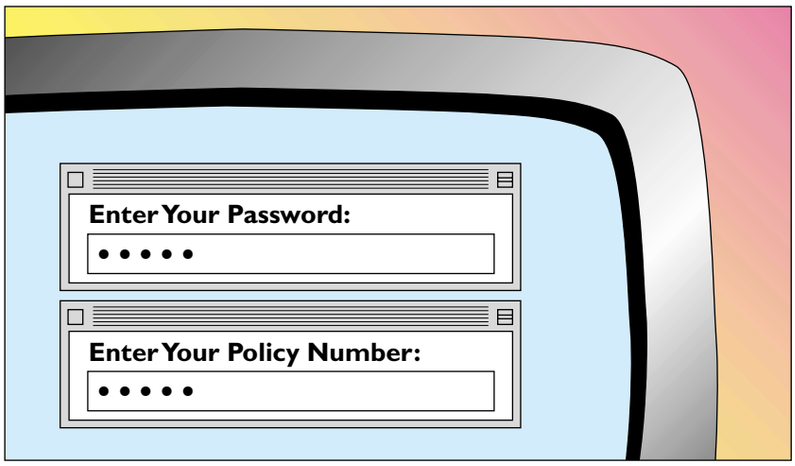
Insurance and the Computer Industry

BRUCE SCHNEIER

In the future, the computer security industry will be run by the insurance industry. I don't mean insurance companies will start selling firewalls, but rather the kind of firewall you use—along with the kind of authentication scheme you use, the kind of operating system you use, and the kind of network monitoring scheme you use—will be strongly influenced by the constraints of insurance.



SANDY WONG

Consider security and safety in the real world. Businesses don't install alarms in their warehouses because it makes them safer; they do it because they get a break in their insurance rates. Hotels and office buildings don't install sprinkler systems because they're concerned about the welfare of their tenants, but because building codes and insurance policies demand it. These are all risk management decisions, and the risk-taker of last resort is the insurance industry.

This is sometimes difficult for computer science professionals to understand because they are so used to technologies solving their problems. In the real world, businesses get security through insurance. They take the risk they are not willing to accept themselves, package it up, and pay someone else to take it. If a warehouse is insured properly, the owner really doesn't care if it burns down. If the owner does care, he or she is underinsured. If a network is insured properly, the owner won't care whether it is hacked or not.

Imagine the future: Every business has network security insurance, just as every business has insurance against fire, theft, and any other reasonable threat. To do otherwise would be to behave recklessly as an executive and be open to lawsuits. Details of network security become check boxes when it comes time to calculate the premium. Do you have a firewall? Which brand? Your rate may be one price if you have one brand, and a different price if you have another brand. Do you have a managed security monitoring service? If you do, your rate is lower.

This process changes everything. What will happen when the CFO looks at his premium and realizes it would go down 50% if the company got rid of all insecure Windows operating systems and replaced them with a secure ver-

sion of Linux? The choice of which operating system to use will no longer be 100% technical. Microsoft, and other companies with shoddy security, will lose sales because companies will refuse to pay the insurance premiums. In this world, how secure a product is becomes a real, measurable, feature that companies are willing to pay for, because it saves them money in the long run.

Other systems will be affected, too. Online merchants and brick-and-mortar merchants will have different insurance premiums, because the risks are different. Businesses can add authentication mechanisms—public-key certificates, biometrics, smart cards—and either save or lose money depending on their effectiveness. Computer security "snake-oil" peddlers, making outlandish claims and selling ridiculous products, will find no buyers as long as the insurance industry doesn't recognize their value. In fact, the whole point of buying a security product or hiring a security service will not be based on threat avoidance, it will be based on risk management.

And it will be about time. For decades, we have tried to solve computer security problems with technologies. Engineers and scientists have built more and better products, and the guiding paradigm has been "avoid the threat." The insurance industry knows the real trick is to manage the risk.

The distinction is important. When you think "threat avoidance," you can either succeed or fail. When you think "risk management," you have many more options. And most of those options don't involve technology.

You can accept the risk as a cost of doing business. Most e-tailers accept the risk of someone eavesdropping on credit card transactions. Sure, they'll use encryption if the customer requests it. But if the customer doesn't, they'll take the order anyway. Keeping the customer buying is worth the risk of eavesdropping.

And you can mitigate the risk. Basically, you have two ways to do this. You can mitigate the risk technologically—with firewalls, virtual private networks, encryption, and all sorts of other security technologies. You can mitigate the risk procedurally, using acceptable-use policies and network monitoring services. And finally, you can transfer the risk. This is where the insurance industry comes in.

Of course, a smart company is going to do some of each. The company will accept some amount of risk, mitigate some more risk with various technologies and procedures, and insure the rest of it. Sounds a lot like fire prevention, or shoplifting, or any of the dozens of other risks that affect all businesses. Computer security is no different.

And sooner or later, it won't be. Sooner or later, the insurance industry will sell everyone anti-hacking policies. It will be unthinkable not to have them. And then we'll start seeing good security rewarded in the marketplace. C

Bruce Schneier is CTO of Counterpane Internet Security, Minneapolis, MN; www.counterpane.com.

Destiny is no matter of chance. It is a matter of choice, it is not a thing to be waited for, it is a thing to be achieved.

—William Jennings Bryan, U.S. political leader