Nonsecurity Considerations in Security Decisions

Security decisions are generally made for nonsecurity reasons. For security professionals and technologists, this can be a hard lesson. We like to think that security is vitally important. But anyone who has tried to convince the sales VP to give up her department's BlackBerries, or the CFO to stop sharing his password with his secretary knows security is often viewed as a minor consideration in a larger decision. This issue's articles on managing organizational security make this point clear.

Bruce Schneier
BT Counterpane

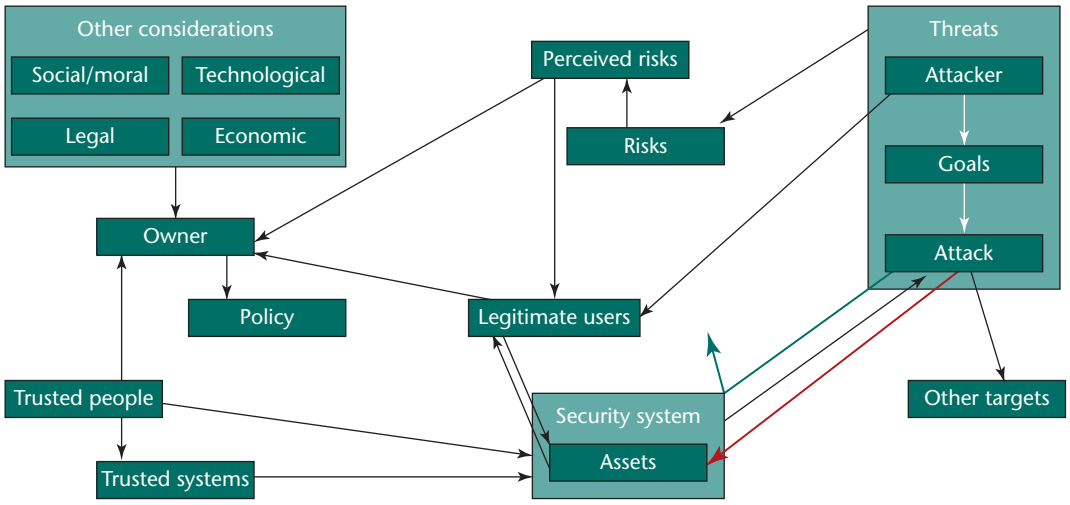
Below is a diagram of a security decision. At its core are assets, which a security system protects. Security can fail in two ways: either attackers can successfully bypass it, or it can mistakenly block legitimate users. There are, of course, more users than attackers, so the second kind of failure is often more important. There's also a feedback mechanism with respect to security countermeasures: both users and attackers learn about the security and its failings. Sometimes they learn how to bypass security, and sometimes they learn not to bother with the asset at all.

Threats are complicated: attackers have certain goals, and they implement specific attacks to achieve them. Attackers can be legitimate users of the asset as well (imagine a terrorist who needs to travel by air, but eventually wants to blow up a plane). And a perfectly reasonable outcome of defense is attack diversion: the attacker goes after someone else's asset instead.

Asset owners control the security system, but not directly. They implement security through some sort of policy—either formal or informal—that some combination of trusted people and trusted systems carry out. Owners are affected by risks ... but really, only by perceived risks. They're also affected by a host of other considerations, including those legitimate users mentioned previously, and the trusted people needed to implement the security policy.

Looking over the diagram, it's obvious that the effectiveness of security is only a minor consideration in an asset owner's security decision. And that's how it should be. ▢

***Bruce Schneier** is chief technical officer of BT Counterpane. His most recent book is* Beyond Fear: Thinking Sensibly about Security in an Uncertain World. *Subscribe to his email newsletter, Crypto-Gram, at www.schneier.com.*



b figure caption here. sdfksdfljsdflkjsdf