



## TenStep Supplemental Paper

---

8 July 2005

### Hack the Hacker

#### *Can Counterattacks Backfire?*

Hack attacks and malicious break-ins to corporate computer systems have been on the rise. This prompted the FBI to conduct a survey in order to estimate computer security breaches. The survey drew responses from 538 security experts in various U.S. corporations and government agencies. Sixty-four percent suffered financial losses due to security breaches, and 186 respondents report a total loss of almost USD 378 million. Thirty-eight percent of respondents detected denial of service attacks, compared to 27 percent last year.

However, a follow-up survey conducted by security expert, Schwartau, revealed that about one third of surveyed companies in the US now plan to develop strike-back capabilities for possible hack attacks. Corresponding responses came from England and Australia as well.

But the disadvantages in striking back are not limited to legality. Hackers use several computers along the way to their target. This makes it more difficult for companies to directly attack the originating culprit. The victim could end up being an innocent bystander whose computer was simply used by a hacker. A sophisticated hacker can also make it look like the attack was made by, for example, a company's competitor.

Some security experts believe that striking back would only invite further attacks. Since hackers are familiar with each other, you could end up attracting unwanted attention as well. An ex-hacker confirmed these concerns, "If my machine crashed and I've been hacking . . . I would not give up then. If hackers gave up so easily there wouldn't be any hackers." He claims that it's the challenge that keeps hackers motivated to keep going.

One type of intrusion-detection equipment is called 'honeypot'. The machine set up to look like a network. It runs false information, such as databases, to lure hackers to spend time 'inside' the machine. The longer a hacker is inside, the easier it is for the system administrator to determine the hacker's identity or IP address. Then, the system administrator can launch a counterattack.

Despite this, some victims prefer less drastic action, such as hiring a company to gather evidence and prepare a case for the police. But catching hackers is just one of the first steps in a long process of bringing them to justice. Not only do police lack the resources, many laws still haven't caught up with Internet crime. So, despite all efforts, hacker vigilante methods are not likely to go away any time soon.