

Basic

Advanced

Topics

Publications

My Research
0 marked items

Interface language:

English

Databases selected: Multiple databases...

Document View<< [Back to Results](#)< [Previous](#) Document 19 of 94 [Next](#) >

Print

Email

 Mark Document[Publisher Information](#)**FT.com site : An 'arms race' no one can stop****Eli M. Noam**, [FT.com](#). London: [Sep 25, 2005](#). pg. 1>> [Jump to full text](#) >> Translate document from: >> [More Like This](#) - Find similar documents**Other available formats:** [Citation](#)

Author(s): [Eli M. Noam](#)
 Publication title: [FT.com](#). London: [Sep 25, 2005](#). pg. 1
 Source type: Periodical
 ProQuest document ID: 902461571
 Text Word Count: 740
 Document URL: <http://proquest.umi.com/pqdweb?did=902461571&sid=5&Fmt=3&clientId=15403&RQT=309&VName=PQD>

Full Text (740 words)*(Copyright Financial Times Ltd. 2005. All rights reserved.)*

Periodic attacks against computers by vandals, terrorists, and allegedly by governments such as that of China, have raised cyber- security to the top of the computer community's agenda.

Computer experts warn. National security officials sound alarm. Banks clamor. The press writes sensational stories. And the public seems fascinated by the exotically named and poorly understood threats. Everybody, it seems, agrees that cyber security needs to be beefed up.

Today indeed there may be a deficit of computer security. But it seems inevitable that tomorrow we will have too much of it. How can there be too much security? Security tends to prevent bad things from happening. But it also prevents some good things from emerging.

Some cyber-security makes private and societal sense, of course. Backup file systems, decentralisation, firewalls, password, all of these are reasonable measures. But since they do not stop determined intruders, the tendency is for increased security measures.

How much should a company spend for its computer security? Total security is neither achievable nor affordable. Instead, a company would engage in some form of cost-benefit analysis, in which it compares the cost of harm avoidance with the benefit of such reduced harm.

But in the real world, the data for such calculation is systematically skewed in the direction of exaggerated harm and understated cost of prevention. Take the cost of harm.

After each virus attack, we keep reading about huge losses, and there are indeed costs of damaged hardware, lost data, and time of computer trouble-shooters. But the biggest component of damage is supposed to be the lost business activity. That number tends to be set far too high. If an airline reservation system is down by three hours it doesn't really lose three hours worth of business. Most transactions will be simply postponed, not dropped. Even where they are shifted to a competitor, the net social loss is much lower than the loss to the affected company.

The second problem is the cost of security measures. Usually, these numbers are being under-estimated. They do not take into account the hassle factor of inconveniencing people. If a computer user must constantly provide passwords and answer queries, the time lost, frustration added, and additional support personnel must all be factored in. Similarly, complex security measures deters customers from engaging in e-commerce.

The third problem is what kind of reduced risk will be produced by added security efforts. The magnitude of this effect will be over-hyped by the vendors of computer security software and devices. But the fact is that computer hackers only seem to be stimulated by higher security walls and learn to climb them. Hence, early security successes will not last.

In consequence, an organization that will follow such flimsy numbers will over-invest in cyber security. This investment will be promoted internally by information systems managers who do not wish to be embarrassed when attackers strike, as they inevitably will from time to time. And since no company will want to be publicly caught with a lower cyber security than its competitors, the over-investment by some will be contagious across an industry.

Today, this tendency to over-investment in security will often be offset by a company ignoring the harm that its own cyber vulnerability causes to others who are connected to its computers, such as its customers or suppliers. But several pending law suits might establish liability by the firm for the damage incurred by others, and this will create still further incentives to greater spending.

On top of all this, government adds its own pressure to raise cyber security. It is a cheap way to raise anti-terrorism protection, since most of the cost is shifted to the private sector.

And hence, cyber-security will creep upwards to ever-more protective levels. Those breaking in will not sit still, either. And therefore, the end result is likely to be a scenario in which few computers are safer than in the past, but everybody will be a lot more uncomfortable. It's an arms race that nobody can stop.

Over-protection, as any child educator will tell, is rarely good for development. Electronic technology and applications are just at their beginning, in their young adolescence. Many new technologies wait in the wings. Grid computing, IP everywhere, sensor networks, machine-to-machine communications, semantic networks, and many more. They will enable new and exciting applications.

Over-protecting ourselves from abuse today will cost us tomorrow dearly in the unborn or delayed generations of innovation.

More Like This - Find similar documents