Opinion **New Technology Policy Forum**

Eli Noam: An 'arms race' no one can stop

Eli Noam SEPTEMBER 25 2005

James Boyle: Trusted or Treacherous?

Thomas Hazlett: Another race markets can win

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.

.....

James Boyle: Trusted or Treacherous?

© Financial Times

Both parents and economists have to remind us sometimes that it is possible to have too much of a good thing. Eli Noam tells us this rule applies to computer security, and I wholeheartedly agree. Let me add two pieces to the puzzle; the costs of software monoculture and the potential anti-competitive effects of "trusted computing."

In crops, ecologists tell us, a monoculture is extremely vulnerable. If we are all growing one kind of genetically engineered rice, then a blight or pest that affects it can suddenly strike at our entire harvest. Multiple plant varieties may be slightly less efficient to farm, but they give natural protection against the spread of a single devastating epidemic. Is the same true of computer operating systems? A number of computer scientists, most prominently Dan Geer, have argued that it is. In a world where 90% of desktop computers run Windows, worms, viruses and trojans can spread rapidly, jumping from machine to machine.

Virus writers naturally target Windows. ("Why do you rob banks?" Willie Sutton was asked. "Because that's where the money is.") But the effects of their efforts are so huge because of the global multiplier effect – so many machines have the same vulnerability, and each sends out more copies of the intruder. The very speed of the spread can often overwhelm attempts to control it. Free and open source software and even the Apple operating system are comparatively free of threats – a competitive advantage. But is it enough of a competitive advantage to challenge the well known network effects and lock in of a dominant operating system? Only time will tell.

The story is complicated by a second issue – the promotion of "trusted computing" which claims to be the way to solve computer security issues. Microsoft has been a big supporter of the concept. What is trusted computing? Well getting people to agree on its real meaning, effects and agenda is about as easy as getting such agreement on abortion.

In effect, trusted computing would allow a computer to match the programs running on it against an approved image of those programmes, perhaps by communicating with a remote entity over the internet, and prevent any unauthorised action. In the most expansive vision, your computer would effectively always be locked down to a certain set of programmes and operations, no interlopers, or forbidden actions – such as infection by a virus, illicit copying or the circumvention of digital rights management would be permitted.

Sounds great, no? But of course, what trusted computing means is greater control. The genius of the PC is that it is a general purpose machine. It will do anything you program it to do. If you do not like the software you have been supplied – say Microsoft Word – you can open those Word documents in another program such as Open Office, and perhaps do things to them that Word does not allow you to do.

That protean openness is what has fuelled the surge in computer innovation, but it also is one of the keys to the vulnerability of Windows. Trusted computing would take control back into the hands of those who approved the list of programmes, and the list of approved tasks. It could certainly have some good effects – making computers more secure, stopping some illicit copying.

But many, and I am among them, fear that it would also be a huge threat to competition and interoperability – particularly to free and open source software which is designed to be tinkered with by users, something that is anathema to the trusted computing ideal of centralised control and validation.

So to Eli Noam's list of worries about "too much security" let me add another one. It would be truly ironic if the security vulnerabilities originally caused by an operating system monoculture led us to turn to a solution that produced an even more monopolistic software industry.

The biggest trojan horse out there might be trusted computing.

.....

Thomas Hazlett: Another race markets can win

© FTcom

Prof. Noam's takes the flip side of the cyber terrorism scare story, and we collapse in a heap: we're chilled (by evil threats) if we don't protect our networks, and chilled (by foolish restraints on system functionality) if we do.

It is good for the two-sided nature of the problem to be laid out; surely, the sensational publicity is squarely on the risks. Costs of avoiding risks are important, too.

But are firms or individuals really over-investing in network security? The costs of the arms race are felt by the customers who pay them. And a brisk competition between MacAfee, Norton, PC-illin and a host of other software solutions makes the "over-hype" fear – well – hype. The truth is, no one knows the optimal level of security, but computer users who face very real maliciousness are purchasing protection in a competitive market.

This sounds a lot like an arms race that –like the last great super-power arms race – markets will win.

.....