How much does cybercrime cost?

18 June 2012

Keyboard. Credit: Jeroen Bennink on flickr

(Phys.org) -- The first systematic study of the cost of cybercrime recommends that society should spend less on antivirus software and more on policing the internet.

The cost of protecting ourselves against cybercrime can far exceed the cost of the threat itself. This is the conclusion of a recent report 'Measuring the cost of cybercrime' by an international team of scientists led by the University of Cambridge.

On the basis of the findings - which provide the first systematic estimate of the direct costs, indirect costs and defence costs of different types of cybercrime for the UK and the world - the authors conclude that we should spend less in anticipation of cybercrime and more on catching the perpetrators.

"Advances in information technology are moving many social and economic interactions, such as fraud or forgery, from the physical worlds to cyberspace," said lead author Ross Anderson, Professor of Security Engineering at the University of Cambridge's Computer Laboratory. "As countries scramble to invest in security to minimise cyber-risks, governments want to know how large that investment should be and where the money should be spent."

However, many of the existing sources of data have either under- or over-inflated estimates of the scale of this risk explain the researchers. For instance, a report released in February 2011 by the BAE subsidiary Detica in partnership with the Cabinet Office's Office of Cybersecurity and Information Assurance suggested that the overall cost to the UK economy from cyber-crime is £27 billion annually, a figure that many industry experts have questioned as being too high and lacking in methodology.

In the new study, the initial impetus for which was a request by the UK Ministry of Defence, the team of researchers has specifically avoided giving a single figure for the cost of cybercrime because the total depends critically on what is counted. They suggest that fraud within the welfare and tax systems - increasingly performed in the 'cyber' world - cost each citizen a few hundred pounds a year on average. Fraud associated with payment cards and online banking costs just a few tens of pounds a year; however, the fear of fraud by businesses and consumers is leading some to avoid online transactions, imposing an indirect cost on the economy that is several times higher.

By contrast, true 'cybercrime' - the new scams that completely depend on the internet - are only costing citizens an average of a few tens of pence per year directly. However the indirect costs, such as the money spent on anti-virus software, can be a hundred times that.

The report finds that each year the UK spends US$1 billion on efforts to protect against or clean-up after a threat, including $170 million on antivirus. By contrast, just $15 million is spent on law enforcement.

Overall, the study concludes that cybercriminals - often only a small number of gangs - are pulling in a few tens of pounds from every citizen per year, but the indirect costs to those citizens, either in protective measures such as antivirus or in cleaning up infected PCs, is at least ten times as much.

The Cambridge scientists, working with colleagues in Germany, the Netherlands, the USA and UK, considered all the main types of cybercrime - online payment and banking fraud, fake antivirus, patent-infringing pharmaceuticals, 'stranded traveller' scams, and botnets (whereby vast numbers of computers are taken over by a 'botnet-herder' who then rents them out to others to commit crimes).

For each crime, the researchers not only collected the best figures for direct and indirect costs, but also for the cost of defending against it, as co-author Dr Richard Clayton, expert in the econometrics of cybercrime in Cambridge's Computer Laboratory, explained: "Take credit card fraud. Direct loss is clearly the monetary loss suffered by the victim. However, the victim might then lose trust in online banking and make fewer electronic transactions, pushing up the indirect costs for the bank because it now needs to maintain cheque clearing facilities, and this cost is passed on to society. Meanwhile, defence costs are incurred through recuperation efforts and the increased security services purchased by the victim. The cost to society is the sum of all of these."

Acknowledging that the study provides a static view of what is a highly changeable category of crime, the researchers nevertheless believe that their data provides "a proper start on the problem", one which they will continue to update as increasingly accurate data comes available. Clayton added: "The study provides a first attempt to pull all available data together. Previous studies have made rough assumptions and not fully explained the methodology they used."

The straightforward conclusion to draw from their study, say the researchers, is that we should spend less on defence and more on policing, as Anderson explained: "Some police forces believe the problem is too large to tackle. In fact, a small number of gangs lie behind many incidents and locking them up would be far more effective than telling the public to fit an anti-phishing toolbar or purchase antivirus software. Cybercrooks impose disproportionate costs on society and we have to become more efficient at fighting cybercrime."

The report will be presented on June 25th at the Workshop on the Economics of Information Security in Berlin, Germany.

Provided by University of Cambridge