



Early last month, the Washington-based Centre for Strategic and International Studies published a report revealing that cybercrime is estimated to cost the global economy \$445 (£259) billion every year. The report also indicated that losses will continue to grow unless better technology and stronger defences are developed in order to counter it; something which, if you simply Google 'cybercrime,' becomes all too apparent.

Over the past 30 days, a number of stories exemplifying the profitability and proliferation of these offences have been circulated. Take, for example, the kingpin who, via the aptly named 'dark net,' offered a high-performance sports car, worth in excess of several hundred thousand pounds, to the hacker that made him the most money.

In an interview with British newspaper the Independent on Sunday, Troels Oerting, the head of the European Cybercrime Centre, described a video that had been shot in a car show room, had high-production values and featured both scantily-clad models and an individual gesturing towards a Ferrari stating: "those who make the most money can get this car"

It may sound like a scene from a Hollywood blockbuster but, thanks to the dark net – where users and their actions are not easily traceable – such brazen and obviously illegal behaviour is made possible.

A further example of just how profitable cybercrime – in particular that facilitated by the existence of the dark net – can be comes from Silk Road; a site which, prior to it having been shut down by US authorities in October of last year, was used to sell a variety of controlled items and substances – such as firearms and narcotics – around the world. It is estimated that that its owners made over £800 million pounds over a two year period by simply taking a percentage of the value of all exchanges that took place through their site. To put that in context, if the owners' fees stood at 10 per cent of sales, that would mean that as much as £8 billion worth of sales passed through Silk Road over this period.

Private consumers are threatened also, as shown by last month's article on the growth of Ransomware and reports of the hackers who, by exploiting vulnerabilities in Network Attached Storage produced by Taiwanese manufacturer Synology, were able to illegally appropriate almost £300,000.

This is of great concern to Oerting who has claimed that, unless more sophisticated defences and legislations are developed and deployed soon, cybercrime could bring about a "two-tier society" within which the affluent are able to afford the tools required to protect themselves whilst those that are unable to afford such defences are exploited by cyber criminals and also suffer fines from financial institutions that are "no longer able to cover their losses."

Make no mistake, cybercrime is on the rise and those that do not have appropriate electronic security in place are vulnerable to it.