'Evil' network hacker sent to prison for two-and-a-half years

Blog Post from Paul Ducklin, Sophos

An Australian hacker from the New South Wales country town of Orange has beensent to prisonfor two-and-a-half years.The offender, David Cecil, who went under the handle 'Evil', wasarrestedjust under a year ago following a six-month police investigation.

His victim wasPlatform Networks, a Sydney-based company now owned by the ASX-listedEftel Group.
Platform describes itself as offeringwholesale aggregated telecommunications, and was apparently the first service provider signed to Australia's much vaunted National Broadband Network (NBN) as part of the initial trials on the Aussie mainland.
Much was made of the link between Platform and the NBN inheadlinesat the time of hisarrest.

But, as El Reg's ever-reliable Richard Chirgwinpointed out, the attack took place before Platform started offering NBN services at all, so the risk from this hack to the NBN as a whole was non-existent.

(According to Platform's' website, commercial connectivity to the NBN still isn't available, so even today the company is taking only "expressions of interest" from prospective customers.)

Cecil pleaded guilty and received some leniency from the court as a result. He'll be elegible for parole in 12 months.
At the time of his arrest, the Australian Federal Police offered thefollowing adviceto businesses:
Provide employee awareness and education programs.Monitor content going into and out of networks.Implement acceptable use policies for wireless technology, information technology and mobile devices.Complete background checks on staff.Conductmandatory reportingof misuse and abuse of computer equipment.Complete a set of written standard operating procedures for technology.Manage account and password policies.Note especially the fifth point (my emphasis): if you don't record and report misdeeds, you're sweeping potential criminal behaviour under the carpet.
That makes things needlessly tough on law enforcement, and on those whose information might have been compromised.