FINANCIAL TIMES All times are London time

ft.com/energysource

Shell's directory leak shouldn't be taken lightly

February 12, 2010 1:12pm by Kate Mackenzie

Shell must have been a little shocked to hear a database of its entire staff directory - all 170,000 employees - had been emailed to environmental and human rights groups.

But it's not clear, as Ed Crooks writes on ft.com, exactly who leaked it; although it claims to be a group of 116 employees, who are apparently concerned about Nigeria:

> *The e-mail sets out a four-stage strategy for raising awareness of allegations about Shell's practices in Nigeria, including campaigns to target the media and institutional investors.*

> *It also advocates "having people from NGOs [non-governmental organisations] becoming full-time (undercover) employees of corporations (in western countries)" to campaign for change in corporate practices.*

Meanwhile John Donovan at royaldutchshellplc.com is irked, because he says Shell asked him not to make the directory public for security and personal reasons (he agreed); but the company subsequently told the press, including the FT, that the database leak was not a security risk. We don't necessarily agree with Donovan's accusation that the Shell staff in question were deliberately misleading anyone. Indeed the directory doesn't contain personal home contact details, so opinions probably varied. But to say there are *no* security implications from such a leak isn't quite correct.

Because leaked staff directories are not as safe as handing out business cards. The reason is: social engineering. Not some kind of Orwellian concept; it's a well-known method for computer hackers to get into an organisation's network. Dumpster diving and dressing as a contract repairman are a couple of the more entertaining types of social engineering, but just knowing someone's job title and phone number can create an easy guise for, say: impersonating a senior manager, calling the internal IT helpdesk, and demanding a password. Most companies have security proceeds to guard against it; but there are plenty of tales of hackers getting a crucial piece of information with just a name, job title, and a persuasive phone manner.

This from a white paper at the SANS Institute, a long-established security firm, on social engineering:

> *Unfortunately, social engineers thrive on easily attainable information such as phone numbers. Social engineers planning to pose as an internal employee will first need to identify someone to masquerade as. Corporate directories are often easy to come by, and not viewed by internal employees as containing sensitive information. Many individuals may think that sharing names, positions and phone numbers is harmless.*

Of course as the paper goes on to say, names, job titles and phone numbers can be found out a number of ways, such as calling switchboard or front desk staff - and some organisations publish part of all of their staff directory online (though most security experts frown on this). But the office contact details for 170,000 employees would no doubt be a prize for hackers.

Shell staff might want to take care with their phone conversations, in case the directory has fallen into a hacker's hands.

Related links:

February 12, 2010 1:12pm in Corporate news, Oil, Politics | Comment

---

You need to be signed in to comment. Please sign in or open a free account with FT.com now.

Comments
No comments yet

RSS feed