# Revealing More than You Intended:
# Job Listings and Security

**by M. E. Kabay, PhD, CISSP**
**Security Leader**
**INFOSEC Group**
**AtomicTangerine, Inc.**

There are many thousands of companies and government agencies that advertise job openings on their Web sites. To get a sense of the number of references to jobs, try a simple request for "jobs" on the Google search engine -- it reported over 18M links; "computer security jobs" produced over 926K links.

Could your own organization's security be threatened by excessive detail in your own job listings on the Web? According to Jay Krasnow* perhaps your Web site is providing a bit too much information for your own good.

His literature search found many reports on competitive intelligence (CI) – which he correctly identified as reaching back several thousand years -- and some on CI from job listings, some on CI from the Web, but little on CI from Web-based job listings. He collected about 300 job listings available during a one-week period on the Web sites of three unnamed companies with Department of Defense contracts. His textual analysis used 14 criteria for evaluating the disclosure of sensitive information; the top three criteria that occurred widely in the sample were

- disclosure of a security-clearance or US-citizenship requirement;
- requirement for a technical degree; and
- identification of the corporate team or division completing the particular project for which additional employees are required.

The author recommended that

- organizations raise manager awareness of the security implications of job listings;
- have departmental managers review ads for postings in their sectors; and
- not include the specific name or the department of the prospective employer.

I think it is appropriate for security and network managers to examine the job listings on your own Web sites to see if there's perhaps a bit too much information being given to anyone who wants it. Is it necessary, to take but one example, to specify the precise network operating system and its revision in the advertisement itself? Do you need to specify the number of nodes, the types of processors, the network protocols, the kinds of routers and the types of gateways in your network?

Yes, the information provides a basis for refining the stream of candidates. Yes, security

through obscurity cannot compensate for bad technical security or even for poor security awareness, training and education.
On the other hand, this amount of detail makes it easy for criminals to engage in social engineering by sounding as if they are already insiders when they call vulnerable staff to winkle out interesting bits of information such as account passwords.   For example, seeing how an organization defines its e-mail addresses (such as "first_initial CONCATENATE last_name"@org_name.domain") makes it easy to guess at logon IDs, which is a step towards getting the password by claiming to have forgotten it.

For the same reason -- making social engineering more difficult -- a second category of information that might prudently be kept for later stages in the job interview funnel is the names, titles, phone numbers and faxes for high-ranking managers in the company who will be involved in interviews and candidate selection.   In addition, the amount of detail in the "About Us" section of the corporate Web site should fruitfully be reviewed for its security implications.

* Krasnow, J. D. (2000).   The competitive intelligence and national security threat from Website job listings.    _Proceedings of the 23rd NISSC_:433

Jay D. Krasnow   reported on the master’s thesis he wrote in the Communications, Culture and Technology Program at Georgetown University concerning competitive intelligence (CI) from job listings on the Web.   He presented his work in the student-paper session at the 23rd National Information Systems Security Conference (NISSC) organized by the National Institute of Standards and Technology (NIST) and the National Computer Security Center (NCSC) of the National Security Agency (NSA),   Mr Krasnow won an award for Best Student Paper for his presentation.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>.   He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience.   For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

Copyright © 2001 M. E. Kabay.   All rights reserved.

Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.