

## Job Interviews - a tool for espionage

### Security Issue:

Employees interviewing with outside firms are enticed and often pressured into disclosing sensitive, confidential and in some cases possibly classified information. Sometimes disclosure of even high level information about projects becomes the basis of derivative intelligence.

### Tactic:

An organization identifies a technical resource that is on a project or may have information about a project, product or program of interest. The organization, cloaked in anonymity through the use of a front person (recruiter) or organization posing as a recruiting firm, establishes contact with the targeted source for information.

"I have the perfect job for you and the salary is over \$250,000 with great benefits. It seems to fit with the work you are currently doing." This was the line used by one such recruiter on a Science and Technology Advisor to a major defense R&D center.

### Advisory

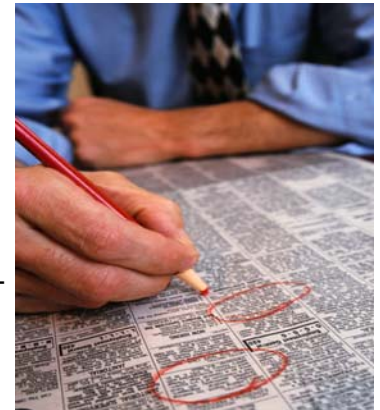
The war on information assets now has a new tool and one that is hard to detect and guard against. The new tool is recruiting. Using false job postings and targeting specific individuals for bogus job interviews have become a tool for spying. The potential target is wooed by the position, salary, benefits or other enticements and, in the interviewing process, becomes comfortable and less guarded when discussing the details of the work they are doing. Answering seemingly harmless questions about strategies, plans, programs, practices, people or even technologies can lead to derivative intelligence. Derivative Intelligence (DI) is synthesized out of the lower level data, facts, timelines and events that may be disclosed during a job interview or on a professional's resume. Defense Security Services did not list this method in their latest Technology Collection Trends 2005 report.

**For more information contact *Spy-Ops* about our security training programs covering this and many more areas.**

Two events that occurred in November 2007, one at the Oak Ridge National Labs and the second at the online job board ClearanceJobs.com could indicate just this type of espionage. The ORNL attack is believed to originate in China and the attack on ClearanceJobs in Russia, two countries well known for computer espionage activities. We may never know the extent of damage caused by these events nor what sensitive technology programs may have been compromised if any. What we do know is that in the past two years there have been over 650 data breaches reported and possibly hundreds unreported.

Human Resources and Security Departments should immediately inform employees to be on the lookout for these activities and report any aggressive information gathering attempts immediately.

With new threats looming in 2008, business, government and the security industry need a wake-up call. While most incidents show our technology vulnerabilities, people remain the weakest link in the security chain. In a study conducted by the Technolytics Institute, the training of employees on security and counter-solicitation is virtually non-existent. Education, training and regular security reminders and advisories are critical to strengthen this weakest of links.



### Quote:

Currently, highly skilled workers with active security clearances are a very hot commodity and in great demand. As such, "Employers and HR professionals must educate their employees about these practices and create a work environment that is so pleasing, employees will not even think of interviewing elsewhere."

Cheryl Veirheilig  
HR Professional

### Statistics:

Clearancejobs.com boasts about 3,000 job postings per month and about 85,000 resumes for cleared job seekers.

Clearedjobs.net posts just under 60,000 openings annually.

### Spy-Ops

4017 Washington Road  
Mail Stop #348  
McMurray, PA 15317  
P 888-650-0800  
F 412-291-1193  
I www.spy-ops.com