

Recruitment industry gets "100% fail rate" on IT security

---

07 October 2008 5:50pm

<http://www.shortlist.net.au>

The recruitment industry is at risk of losing clients and candidates, breaching privacy laws and damaging the overall reputation of the profession as a result of widespread unsafe IT practices, yet many companies are still in denial, according to an online security expert.

Freelance IT consultant Thomas Shaw, who also recently launched [Recruitment Directory](#), last month started an independent audit on a range of recruitment websites, after becoming concerned at the growing number of reports of poor IT security within the industry.

Shaw told *Shortlist* that over the past two weeks he and his team had examined 20 recruitment agency and job board sites, and had found security gaps in each one.

He stressed that in order to avoid breaching any laws, his team never accessed any of the insecure information - they only went far enough to confirm that it was possible.

Shaw added that his team didn't employ specialised "hacking" programs to find these security gaps, and the techniques they used were available to anyone.

"Most of the data we've found has been through Google searches - looking at pages that have been indexed, following the indexes back to the website, and then manipulating the URL to investigate."

Some of the sensitive information which could be accessed included:

- Lists of current clients, roles being recruited and commission rates, on two recruitment agency websites;
- Open "test" sites for both recruitment companies and job boards;
- Unprotected online files with viewable candidate resumes;
- A job board credit card payment system which could be manipulated to process transactions or provide refunds to existing customers;
- A URL which could be manipulated to login as a candidate or client without having their username or password;
- A job board back-up database, with the usernames, passwords and email addresses of all users.

Shaw said he was shocked at the lack of online security among some of the industry's major brands.

"A 100% failure rate is not good enough... Some of those items could affect their share price, their customer relations.

"For instance, the agency with the data leak - it actually said the client, the email contact, and the job details. If another recruitment agency gets hold of that, it's gold."

## **Companies unwilling to acknowledge the issue**

When he contacted the affected companies, Shaw said, the common response was to deny there was a problem.

He said maintaining strong IT security was time-consuming and costly, and it was naturally tempting to take a reactive rather than proactive approach.

Agencies and job boards needed to conduct monthly security checks on their websites, and require users to change their passwords regularly, he said. Prevention was expensive, but it was much cheaper than fixing problems after the fact.

"For instance the job board where we found all the usernames and passwords, that would cost \$15,000 plus.

"They'd have to rewrite their whole program and do another test, and contractors aren't cheap for that stuff. They can charge anything from \$500 per day."

Nonetheless, companies which failed to protect their clients and candidates from online security breaches could face legal action, Shaw said.

He noted that Principle 4 of the legally binding National Privacy Principles (part of the Privacy Act), required an organisation to: "take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure".

This was echoed in the RCSA's own code of conduct, he said, which called for members to "take reasonable steps to maintain the confidentiality and privacy of candidate, client and member information".

"I wouldn't be surprised if the RCSA or ITCRA calls for an industry-wide campaign, because it's about ethical standards.

"We need to ensure that our client data is safe and our websites are safe to protect the industry."

