

### LATEST NEWS

National Health IT Board calls for greater funding

Datacom chief dies suddenly

Kordia puts the brakes on Wi-Fi plan

Telcos try for mobile copyright loophole

InternetNZ chooses Fellows and Councillors

Damian Swaffield joins Oxygen

### SUBSCRIBE



Computerworld is New Zealand's only specialised information systems fortnightly. Subscribe now for \$97.50 (24 issues) and save more than 37% off the cover price!



### SIGN UP

Get the latest news from Computerworld delivered via email. Sign up now

## Experts cast doubts on Chinese hacking scare

Attacks may appear to come from developing nations, but attacks are only coming from an IP address, with no real idea what is behind that IP, says security expert

BY ROB O'NEILL AND STEPHEN BELL | AUCKLAND | MONDAY, 24 SEPTEMBER, 2007

EMAIL PRINT

Security experts are voicing their doubts about suggestions that [China tried to hack](#) New Zealand government IT systems, saying it is technically very difficult to identify the point of origin of such attacks.

Peter Benson, chief executive of Auckland-based consultancy Security-assessment.com, says he is not convinced, and is more concerned about attacks against the New Zealand economy than the government.

Benson says attacks may appear to come from developing nations, but this could be because technology is being deployed there at a great rate, with security being installed as an afterthought.

"We have seen this in previous years, with attacks coming from Korea and other countries, and it appears [to be] directly related to the notion that the bad guys from anywhere are using the 'easy ingress' (developing nations) points from which to stage attacks," he told *Computerworld* last week.

"Whether these attacks are actually being driven by foreign governments would need a lot more proof for me to be convinced at this stage. Otherwise, as far as I am concerned, the attack is only coming from an IP address, with no real idea what is either behind that IP, or whether that IP is just a staging point."

New Zealand's Security Intelligence Service director, Warren Tucker, in a rare media conference earlier this month, [alleged that attacks from overseas, apparently from China](#), had succeeded in penetrating NZ government agency systems and copying information.

China has denied the claims, which echo similar allegations coming out of the United States and from other governments.

Benson says there has been a lot of fear, uncertainty and doubt over information warfare over the years. He says you can take nothing at face value on the internet.

"I have seen hackers go through six or seven servers, across multiple countries, to get to their destination. So who is hacking who? How reliable is the information as to the actual source attack?" he asks.

"These days, there are so many anonymising servers, and [there is] the ability to spoof or encrypt traffic from the real source, that tracking down the actual source of attacks is both problematic and sometimes impossible."

He adds that identifying whether an attack is state-sponsored or otherwise adds further complexity to the problem.

Symantec's security research leader, Vincent Weafer, doubts there is a specific rise in hacking attacks on the government.

Rather, attackers "go after any organisation active online" and, in recent years, this has included a growing number of government agencies.

The biggest drawback to such a penetration is that many companies can't identify what's been stolen, as their protection is dedicated to detecting and preventing intrusion, rather than the illicit export of data, says Weafer.

There is evidence that a growing number of attacks are now targeted at specific installations that have potentially lucrative information to harvest, rather than making a broad sweep of the internet looking for vulnerable sites, as most hackers used to do, he says. But there is no persuasive evidence that government sites are being targeted in particular, much less that any such attacks are coming from overseas governments.

This view is echoed by Benson.

"I am more interested and worried about attacks against our economy, infrastructure-level attacks, or attacks against intellectual property (industrial espionage), than attacks against the New Zealand Government," he says.

"The vast majority of attacks that we see are not related to foreign governments, but are commercially driven."

*Computerworld* called Security Intelligence Service director Warren Tucker for comment, but was referred to the Government Communications Security Bureau. GCSB did not respond by press-time.

**SUSTAINABLE 60**  
2010 AWARDS

**THE SUSTAINABLE 60 AWARDS**  
Do you have a sustainable business?

**SOPHOS**

GET YOUR FREE COPY OF THE **SOPHOS THREATSAURUS**

DOWNLOAD NOW

### MOST POPULAR

READ COMMENTED EMAILED SHARED

- Kordia abandons trans-Tasman cable plan
- Gen-i completes latest restructure
- iPhone 4 launched delayed
- ITCRA clarifies questions raised by online comments
- iFiasco
- Finalists selected for major Customs project

### POPULAR EVENTS

- Sustainable 60 Awards**  
Entries open now. Click here for more details
- Unlimited Investment Challenge 2010**  
Entries open now. Click here for more details
- Sustainable 60 Workshops**  
Dates confirmed. Click here for more details

### SPONSORED LINKS

- COMPUTERWORLD** Local and International news Enterprise ICT must know info Subscribe today
- PCWORLD \$599!** NZ's most trusted tech advice Free NZ Delivery Subscribe today

- NZ Business Intelligence**  
Affordable Business Intelligence. For the right advice talk to us! [www.Indigo.co.nz](http://www.Indigo.co.nz)
- 16c+GST/minute**  
To call any NZ mobile on Telecom's BusinessTime + mobile plan. [www.telecombusinesshub.co.nz/16c](http://www.telecombusinesshub.co.nz/16c)
- Qlikview Consultant**  
Experienced Qlikview consultant Available now! [www.infoclarity.com.au](http://www.infoclarity.com.au)
- Desktop Central**  
Management & inventory tools for LAN & WAN computers [www.manageengine.co.nz](http://www.manageengine.co.nz)

Ads by Google

SHARE THIS STORY WITH:

EMAIL PRINT