

Cyber-security: How sea-worthy is our digital ship...?

Michael Foley, Director, Voco Limited

How severe can the impact of the Conficker worm be on a single city council that has (apparently) not implemented basic security solutions?

Pretty severe according to a recently released report entitled "Service interruption resulting from ICT disruption in February 2009" which details the financial costs of a Conficker incident affecting Manchester City Council's network - £1.5 million in clean up costs and lost revenue from the downtime.

Recently American Open Source movement founder Bruce Perens reported on his blog that on April 9 unidentified attackers had climbed down four manholes serving the Northern California city of Morgan Hill and cut eight fibre-optic cables in what appeared to have been an organised attack on the electronic infrastructure of that city.

The city and parts of three counties lost 911 service (the equivalent of our '111'), cellular and landline telephone communications, DSL internet and private networks, central station fire and burglar alarms, ATMs, and monitoring of critical utilities. In addition, resources that should not have failed, like the local hospital's internal computer network, proved to be dependent on external resources, leaving the hospital with a "paper system" for the day.

Business was disrupted in a 100-mile radius around the community. With ATMs and EFT systems down 'cash was king' for the day. Services employees dependent on communication were sent home and the many businesses providing just-in-time operations to agriculture could not communicate.

As Mr Perens reports it these implications, though startling, went almost unreported.

Why should we be interested in the misfortunes of our English and American cousins? Why am I writing about this in TR?

In New Zealand security of our ICT systems and infrastructures, what we call "cyber-security", is still a subject shrouded in something like the veil of mysticism that covered the industry as a whole in its earlier years. Whilst there is undeniably a community of skilled and knowledgeable practitioners, it is not apparent that the reality of the threat has registered on the psyche of mainstream business and enterprise, either public or private sector.

In a national context, our failure to address cyber-security has in part been grounded in a lack of awareness of the threat. To my laymans eye, this is due to a regime that is light on disclosure requirements, let alone legislation. The truth is that our institutions and industry are suffering losses; they just go largely unreported.

New Zealand must invest properly in the cyber defense of its critical infrastructure and key industries. Relying, as we currently do, on Australia's Computer Emergency Response Team (CERT) exposes our economy unacceptably as we move into the digital world. This

was been proved again earlier this year when Conficker hit our financial, educational and health sectors hard (again, largely unreported).

Previous attempts to create a semi-commercial/university sponsored CERT in New Zealand have allowed politicians to avoid investing in this most fundamental of capabilities in the digital space.

Why does government need to get involved? Fundamentally, cyber-security is a matter of national security. Our economy is exposed to a considerably greater digital threat than any that one can reasonably contemplate presenting in the military arena.

And if that is not enough, the commercial sensitivity that surrounds the levels of disclosure required to adequately manage the risk means that the management agency must sit independent from commercial/competitive considerations. Ensuring the active engagement of all market participants will demand that it sits at a pan-economy level.

And at the individual organization/enterprise level it is networks, or more specifically the way we design them, that effectively defines our security perimeter. Security controls within applications generally involve a trade-off with functionality and this, coupled with the inevitable diversity of most organisations' application portfolios, means that security must be addressed primarily at the network layer.

How aware are today's CIOs of security – the nature of the threat, the implications for their organisations, the means available to mitigate risk, and the actual means deployed within their organizations ICT infrastructure and operations?

I held CIO positions back in the pre-1990s and I know that I'd have to put my hand up and say I was NOT particularly well versed in the intricacies of what my security spooks (systems programmers in those days) got up to. I may have been able to get away with it given that New Zealand's first Internet connection was only plugged in by John Houliker in 1989. The CIOs and policy-makers who look after the engine rooms of our economy don't have that luxury.

Can we all put hand-on-heart and say that the security of our organisations, and our economy is under control?