Securing school WiFi : take the corporate approach

Schools moving to install wireless networks need to approach their IT security in the same way as corporates do, says Networks Unlimited, distributor of Fortinet.

Schools around South Africa are increasingly looking to technology to enrich learning and make school administration more efficient. Those with ample resources already have in place their own IT systems, IT administrators and strategies to incorporate mobile technologies into the classroom. But, as is the case within any organisation, security has to be of paramount importance within school networks, says Anton Jacobsz, Managing Director of Networks Unlimited.

The risks within a school wireless network are essentially the same as those within any corporate network, says Jacobsz, although some of the potential victims – the children – are significantly more vulnerable. In an unsecured school environment, attackers might seek out sensitive personal or financial information, just as they might in a corporate environment. Users within the school network might try to access privileged information or visit unauthorised sites, as users within a corporate environment might do.

The key difference between school and corporate networks is parents' concerns that access can lead to targeting or exploitation of their children, cyber bullying or access to inappropriate material online. Jacobsz says these issues are taken seriously by schools with mature IT policies in place, and are generally covered in policies governed by the schools. "It needs to be treated like a work environment, where every user is governed by certain restrictions. A school might block all access to certain types of content, or might opt to allow access to certain sites by certain people or at certain times. Strict usage policies should also be implemented with respect to email content, privacy and backup." However, as with the work environment, users can get around these restrictions by bypassing the network and using a 3G card, he points out.

Overall, the approach to mitigating risk within school IT systems is the same as best practice approaches in any organisation, says Jacobz. "Security must be addressed from the ground up, addressing network security, wired and wireless access,

identification and authentication, device and user policies and management. Schools need to control how users are authenticated on the network, what different classes of user – for example, pupils, teachers and guests – may access. The environment must be continually managed, it must be protected by an effective firewall and the IT administrator must stay on top of the changing threat landscape."

In addition, as schools start depending on IT to underpin their daily activities, the security systems in place cannot degrade overall system performance, says Jacobsz. "In many top schools, pupils now get their assignments and post their homework from home, using the school network – you cannot afford to have the site going down," he says.

As schools increasingly move to incorporate connected, mobile devices into the classroom, the security and performance of their networks will increasingly become a competitive differentiator for schools. And with the safety and wellbeing of their pupils at stake, their IT security systems have to deliver multi-layered, advanced protection.