Computer security in schools

Paul Ducklin

Getting computer security right in a school is much trickier than doing so in a business. How much money can you spend? How much time can you devote to the problem? Should you have a regime in which you enforce or merely guide? How do you win the cooperation of parents, principals and students? How do you keep control of students' computers over the holidays? How do you balance freedom and responsibility? What effect will the government's purchase of a laptop for every school student have?

Whether you regard it as an inspired and necessary drive to bring Australian schools to the vanguard of world education, or a wayward and ill-conceived electoral promise, Australia's own "one laptop per child" program is making K12 computer security even harder. I have met school IT administrators who admit that they are considering turning down the government's largesse on account of the hidden costs of safely deploying and managing all the new laptops which they qualify to receive.

In some ways, acquiring a fleet of laptops is a little like acquiring a fleet of cars – merely the start of your expenditure and management headaches. Registration, insurance, badging, garaging, maintenance, running costs, conditions of use, speeding and parking tickets – these are just some of the concomitant responsibilities and hassles of a vehicle fleet. So too with laptops, with the added challenge that the rules of the road – if you will pardon the extended automotive analogy – change frequently and sometimes dramatically as new technologies (and crazes) sweep the internet.

Some schools, and even some education ministries, are seeking refuge in so-called *cloud computing*, or *software as a service* (SaaS), at least for parts of their network infrastructure such as web and email. Cloud email, for example, relies on the idea that you outsource the ownership and operation of your school's email to a third party – to Microsoft, perhaps, or to your ISP, or to Google. This third party takes care of sending, receiving and filtering all your email, so that you don't need to run your own email infrastructure. Similar arrangements can be made for access to the web, for calendaring applications, for discussion forums, for school administration software, and more.

Cloud computing can simplify your IT operations, because external companies – who typically enjoy great economies of scale by sharing their service infrastructure across tens, thousands or even millions of customers – take care of the day-to-day running of various parts of your network. But there are risks, too, since you must trust your cloud computing companies *absolutely*, especially from a security and availability perspective. Outages in service are no longer within your own ability to fix. Data leakages are no longer within your remit to control. Security policies are no longer necessarily yours to decide and to enforce. You may even lose legal jurisdiction over your students' data if you partner with companies which operate outside Australia – companies which may, paradoxically, seem more attractive by virtue of their increased operational redundancy.

Whether to do IT security yourself or to outsource it is a tricky decision, and needs careful consideration. One thing, however, is clear: you cannot outsource or "cloudify" all aspects of computer security. The school laptops currently being bankrolled by the Australian government are not stripped-down thin clients, or single-function mainframe terminals, and with good reason. They are fully-fledged computers which are, quite by design, both flexible and powerful, and which can be used creatively and usefully both on-line and off-line. Technologically, then, some form of endpoint-hosted security software will *always* be required.

This means that endpoint security vendors will therefore remain an important – probably the most important – source of computer security tools. If you can only afford the time and money to deploy computer security technology in one part of your network, the endpoint simply *must* be that part. The threat of data loss and malware incursion via USB devices plugged into laptops is surely, on its own, proof that PC-based security and control software is usefully here to stay.

Another reason why computer security cannot entirely be outsourced and centralised is cultural. Modern internet usage is heavily oriented towards on-line social activities, in which friendships (and, increasingly frequently, relationships and businesses) are forged and built online. Social networking sites make it easy for internet users to share information about themselves – not just with friends in their own school, suburb or town, but almost anywhere in the world. The problem, of course, is how much to share, and with whom.

Circumspect behaviour in the social networking era is hard to enforce with technology alone. As I mentioned above, the

internet's rules of the road are continuously changing, so internet safety and security must be continuously taught, and continuously learned. In particular, the combination of search engines and social networking sites represents a massive risk, since almost everything you share on line is subsequently searchable by anyone. Today's schoolchildren are the first to live in an era in which even the most inconsequential things they say and do on-line may end up indexed and archived for ever.

This is causing many schools to rethink their attitude to online security. Prevention and enforcement are still important – for example, there are many well-known websites which are unarguably inappropriate for children to access while at school. If the school can unambiguously block access to such sites, it should do so. But most schools now recognise that prevention alone is not a solution, since children need to be kept safe not only from explicitly malicious, illegal or dangerous sites on-line, but also from apparently innocent behaviour on legitimate sites – especially social networking sites – which puts them at risk from predators, bullies and cybercriminals.

Australia's own "one laptop per child" program is making K12 computer security even harder

Schools can no longer be expected to create closed networks in which everything not blocked for students is assumed safe. Instead, school IT staff should be permitted – by principals, parents and administrators – to adopt security practices which encourage an open network in which limits are defined by policy. Security technology then becomes a tool to help to manage, but not itself to define, those limits. This leads to an environment in which good behaviour is both permitted and encouraged; in which limits are known and understood; in which mistakes are possible but pedagogically discouraged; and in which egregiously bad behaviour can be nevertheless be detected, remediated and punished.

In conclusion, here are three talking points for taking computer security to the next level:

- You can't outsource all your computer security into the cloud. Endpoint security is still important, so look for a vendor who can offer (and support) a broad security umbrella under a single, simple licence.
- Don't be afraid to consider security technologies which you have previously dismissed as too hard, or not specific enough. Personal firewalls and Network Access Control (NAC) are often considered poor cousins to anti-virus, since they aim to change and moderate risky behaviour, not simply to block known-bad activities.
- Vigorously encourage parents to support the school's computer security policy at home. Get them to ask not what the school's network can do to protect their children, but what their children can do to protect the school's network!

Paul Ducklin is Head of Technology, Asia Pacific, Sophos
email duck@sophos.com.au
www.sophos.com/