

Securing Laptops

Thefts of laptop computers from schools and colleges appear to be on the increase.

According to the 2006 Computer Crime and Security Survey, 58% of reported electronic attacks and computer crime involved laptop theft¹.

Portable electronic equipment is and has historically been a common target for thieves. As laptop computers have become more and more compact, their appeal to thieves seems to have grown and they are now among the most common items of portable electronic equipment stolen.

Whilst we can only surmise as to the motivations behind thefts such as these, our booming economy has left many on the economic fringes, forcing some to commit crime to simply survive. But of course we must also accept that there are those, for whom there is no excuse, opportunists willing to exploit gaps in security to make some quick cash.

Whatever the motivation, laptop thefts leave both the school and the student feeling exposed and vulnerable. Valuable information such as essays, exam preparation and personal details are likely to be contained within each unit, meaning the theft of laptops constitutes not only a physical breach of security, but a potential breach of privacy.

Whilst it is almost impossible to stop offenders from offending, there are some basic risk management tactics that schools and colleges can implement to reduce the potential of laptop thefts occurring on their property.

Taking a risk management approach to reducing laptop theft

As with any other risk, the prevention of laptop theft or any theft for that matter should begin with an assessment of your current security risks. Once you have an understanding of how vulnerable your laptops are to theft, you can begin assessing the likelihood and potential consequences of theft occurring.

An example of property risks that may lead to laptop theft might include:

E.g. Laptop theft risks

Hazard	Risk	Risk Ranking
Laptops left in the open	Thieves may target laptops	Medium
Laptops unsecured in cradle	Easy access for thieves	Medium

Risk Controls

- Devise and implement a policy and procedure on laptop use and secure storage
- Identify and determine the specific theft vulnerabilities of your site
- Avoid using laptop bags when carrying laptops outside as these can entice potential thieves. A padded briefcase is an alternative option
- Password encrypt laptops and consider installing tracking software
- Avoid storing security passwords with or near laptops
- Consider encrypting confidential files
- Attach laptops to desks via a security cable
- Ensure laptop cradles are stored in a lockable storeroom or cabinet, out of plain sight and in an alarmed room
- Secure laptops after-hours in cradles and lock cradles in place with chains of a sufficient tensile strength
- Digitally engrave your laptops and record serial numbers
- When purchasing new laptops, ensure empty boxes are placed within bins and bins are locked securely

¹2006 Computer Crime and Security Survey www.auscert.org.au/images/ACCSS2006.pdf

- Ensure building works or other processes that may interfere with the security of laptops have been considered within your risk assessment and controls are implemented
- Inform staff of laptop and general security measures and make them aware of their responsibilities to secure the premises after hours
- Ensure all doors and windows are locked before departing for the evening and enable your alarm system.

Monitoring & Review

Monitor and review risk controls at regular intervals to ascertain effectiveness and amend controls if deemed inadequate.

Relevant standards and regulations

AS/NZS ISO 31000:2009 Risk Management Principles and Guidelines

HB 266:2010 Guide for managing risk in not-for-profit organisations

For further information and assistance on securing laptops or to obtain a copy of our securing laptops checklist please contact the Risk Management department on 1 300 660 827.

To discuss your insurance options in relation to asset protection, including laptops please contact your Account Executive on 1 800 011 028.

**For assistance with risk management please call
the Risk Management Helpdesk on**

1 300 660 827
www.ccinsurances.com.au

Disclaimer: This Fact Sheet is provided to Catholic Church Insurances Limited clients for informational purposes only and should not be used or considered as a comprehensive coverage of the topic discussed. As this information is of a general nature you should consider obtaining professional advice to ensure that your own circumstances are properly considered.

CCI 03/11